Proteção de Dados na Era da Inteligência Artificial

digitalinside.pt/protecao-de-dados-na-era-da-inteligencia-artificial

Bruno Castro

No dia 28 de janeiro assinalou-se o Dia Europeu da Proteção de Dados, uma data que visa reforçar a importância da Privacidade e Proteção dos Dados pessoais. Este é um tema particularmente relevante e sensível perante a ascensão das plataformas de Inteligência Artificial (IA) Generativa, como modelos de texto, imagem e código que vieram revolucionar a forma como nos relacionamos e também como trabalhamos ao utilizarem os dados para treinar os seus modelos.

Cada vez mais indivíduos e empresas utilizam plataformas de IA para facilitar o seu trabalho diário, no entanto, seja por desconhecimento ou descuido, muitas vezes acabam por partilhar informações sensíveis e comprometedoras em ferramentas de IA para a criação de textos, análises ou relatórios. Algo que é sobretudo perigoso em ambientes corporativos, onde informações estratégicas, financeiras e até segredos industriais/propriedade intelectual podem ser expostos a sistemas cuja segurança e privacidade nem sempre são garantidas. Esses dados podem ser armazenados nos servidores das empresas que operam essas ferramentas e expor as empresas a riscos de violação de dados, e por inerência, à sua eventual exposição, espionagem industrial e violações de privacidade. No atual cenário, no qual ciberataques são cada vez mais sofisticados, confiar informações críticas a plataformas cujas práticas de segurança nem sempre são transparentes, torna-se, uma aposta arriscada. É importante também recordar que, em termos de roubo de propriedade intelectual e informação sensível, as ferramentas de IA e os servidores nos quais os dados dos sistemas de IA são armazenados podem igualmente ser atacados. Por exemplo, ainda há dias, o assistente de IA da startup chinesa DeepSeek foi vítima de ciberataque após a aplicação ter ganho popularidade repentina como líder dos downloads na AppStore nos Estados Unidos, e superar o ChatGPT.

Além disso, mesmo que essas plataformas aleguem anonimizar os dados, há sempre o risco de que informações sensíveis sejam utilizadas para treinar modelos futuros, perpetuando a exposição de dados, sem o conhecimento ou consentimento dos utilizadores. No contexto de dados pessoais, o perigo é ainda maior e a única certeza, é a incerteza. Informações como identidades, endereços, preferências ou mesmo padrões comportamentais podem ser identificados, analisados e explorados, violando direitos fundamentais, facto que levanta sérias questões éticas sobre o uso de dados pessoais para fins comerciais e algoritmos que podem perpetuar preconceitos ou discriminações.

Este é um tópico que merece particular atenção por qualquer empresa que considere integrar plataformas externas de IA Generativa no seio dos seus processos internos. Ao mesmo tempo, as próprias empresas que desenvolvem essas tecnologias também têm

um papel importante a desempenhar ao adotarem políticas de proteção de dados que garantam que o treino da IA seja feito somente com base em materiais licenciados ou de domínio público.

Na sua essência, a IA aprende ao assimilar e recombinar as ideias humanas existentes online. De acordo com o Relatório do Índice de IA de 2024 da Universidade de Stanford, quase 66% dos modelos de IA lançados no ano passado eram de código aberto, e modelos de linguagem como o ChatGPT dependem fortemente de dados disponíveis na web e chips avançados para treino dos seus modelos. No caso da DeepSeek, a startup chinesa precisou de uma quantidade muito menor de chips para treinar, comparativamente com os seus concorrentes ocidentais, contudo demonstra capacidades equivalentes às dos líderes norte-americanos do setor. Ou seja, com um investimento muitíssimo reduzido, esta startup chinesa conseguiu alcançar um desempenho comparável ao das principais empresas deste setor e já está a bater recordes em popularidade. A ascensão da DeepSeek é mais um exemplo que intensifica preocupações de proteção de dados, já que plataformas de IA têm acesso a vastas quantidades de dados pessoais e podem influenciar significativamente a disseminação dessas informações. Esta situação é comparável às preocupações anteriormente levantadas em relação ao TikTok, outra aplicação chinesa que enfrentou escrutínio nos Estados Unidos devido ao potencial acesso do governo chinês aos dados dos utilizadores.

Em suma, embora as plataformas de IA generativa representem um marco no avanço tecnológico, é crucial que o seu desenvolvimento e uso sejam equilibrados com a garantia de proteção da propriedade intelectual e a segurança dos dados. O desafio é encontrar um equilíbrio que permita à IA prosperar em inovação sem comprometer os direitos e a segurança dos utilizadores.

Bruno Castro é Fundador & CEO da VisionWare. Especialista em Cibersegurança e Investigação Forense.