Melhor prevenir do que remediar com IA pública

jornaleconomico.sapo.pt/noticias/melhor-prevenir-do-que-remediar-com-ia-publica

Bruno Castro, CEO da VisionWare, especialista em Segurança da Informação, Cibersegurança e Investigação Forense

A recente revelação de que o diretor responsável da CISA (Cybersecurity and Infrastructure Security Agency), a principal agência de cibersegurança dos Estados Unidos, introduziu documentos internos marcados como "*for official use only*" numa versão pública do ChatGPT veio expor uma contradição central do momento digital que vivemos: nunca falámos tanto de risco, resiliência e governação tecnológica, e nunca estivemos tão despreparados para lidar, na prática, com as implicações reais do uso quotidiano destas ferramentas.

Este é um sintoma claro de algo mais profundo, nomeadamente, a banalização do uso de sistemas de IA pública em contextos onde a noção de fronteira, confidencialidade e controlo, deveria ser absoluta. O facto de a informação não ser classificada serve apenas para suavizar a narrativa, não para a tornar aceitável. Informação "*for official use only*" existe precisamente porque a sua exposição pode ter consequências. Caso contrário, seria pública por definição.

Plataformas públicas de IA generativa estão a ser tratadas como se fossem extensões naturais do desktop institucional, quando na realidade são sistemas externos, opacos, fora do perímetro de segurança e regidos por lógicas comerciais que nada têm a ver com interesse público ou com soberania digital.

A defesa habitual de que "não há evidência de que os dados tenham sido acedidos ou explorados" é, no mínimo intelectualmente preguiçosa. Segurança não se mede somente por danos visíveis, começa exatamente por superfícies de ataque criadas. O simples facto de a informação ter saído do ambiente governamental já constitui por si só, uma falha. Esperar pela prova do prejuízo para reconhecer o erro é a mesma lógica que, durante décadas, normalizou incidentes de segurança até ao momento em que se tornaram crises.

Veja-se o caso da DeepSeek (solução de chat com IA), que no início de 2025, viu uma base de dados sua exposta, com conversas de utilizadores e credenciais sensíveis acessíveis na internet, demonstrando quão frágeis podem ser as promessas implícitas de segurança feitas por fornecedores de tecnologia de ponta.

O mais inquietante é que este comportamento ocorre precisamente nas instituições que deveriam saber melhor, e prevenir. Se a agência responsável por proteger infraestruturas críticas e definir boas práticas de cibersegurança trata uma IA pública como um espaço aceitável para trabalhar informação sensível, que mensagem fica para o resto da administração pública? Que regras são opcionais? Que a conveniência justifica o risco?

Este não é um debate sobre proibir a IA ou travar a inovação, de todo. É antes um debate sobre maturidade digital e sobre reconhecer que a adoção apressada de ferramentas poderosas, sem enquadramento claro, cria riscos sistémicos silenciosos. Hoje são

documentos “apenas” sensíveis. Amanhã poderão ser dados pessoais, informação estratégica ou decisões automatizadas baseadas em contextos que nunca deveriam ter saído de sistemas fechados.

A verdade desconfortável é esta: a maior ameaça da IA generativa não é a tecnologia em si, mas a ilusão de controlo que ela cria. A ideia de que sabemos o suficiente para a usar com segurança, quando na prática estamos apenas a improvisar políticas à medida dos incidentes. Não posso deixar de olhar para estes episódios com preocupação acrescida. Não porque sejam excecionais, mas justamente porque revelam quão facilmente até profissionais experientes subestimam os riscos diários associados ao uso de tecnologias que se tornaram banais no nosso dia a dia. A distância entre a perceção de risco e a realidade operacional continua a ser demasiado grande.

Na parte que nos toca, na nossa organização, temos insistido de forma consistente na formação e capacitação das equipas para o uso responsável de ferramentas digitais e de IA generativa. Esse mesmo esforço estende-se também aos nossos clientes. Ao longo dos últimos anos, temos promovido várias ações de sensibilização, workshops e iniciativas de consciencialização precisamente sobre estes temas: onde termina a conveniência e onde começa o risco, o que distingue um ambiente controlado de uma plataforma pública, e porque é que nem toda a inovação é compatível com todos os contextos. A experiência demonstra-nos que a maioria dos incidentes não resulta de intenções maliciosas, mas sim, de decisões mal-enquadradas.

A governação da IA não pode ser implementada apenas depois do incidente, nem delegada exclusivamente aos fornecedores de tecnologia. O caso da CISA é um alerta claro de que não podemos construir dependência antes de construir governação. Por isso, para os colegas americanos, em Portugal dizemos “*better to prevent than to remediate*”.