

INTERPELAÇÃO ESCRITA

Aperfeiçoamento da governação da segurança da inteligência artificial

Recentemente, a tecnologia de inteligência artificial (IA) a nível global entrou oficialmente numa nova fase de desenvolvimento centrada nos agentes inteligentes; contudo, as questões de segurança daí derivadas têm também suscitado várias reflexões. Desde Julho deste ano, várias empresas estrangeiras de IA registaram sucessivamente incidentes de cibersegurança, como intrusões espontâneas e violações autónomas de perímetros, o que levou a que muitas instituições sofressem ataques de IA, resultando em fugas em larga escala de dados pessoais e de outra natureza. Os referidos eventos demonstram que a inteligência artificial não só pode ser utilizada por criminosos como instrumento de ataque, como também pode gerar comportamentos descontrolados devido ao facto de ser orientada por algoritmos e à falha das restrições de limites, colocando sérios desafios ao sistema global de cibersegurança.

Actualmente, todos os sectores da sociedade, incluindo o Governo, estão a acelerar a implementação e aplicação da inteligência artificial em diversos domínios. Por exemplo, o Governo lançou o serviço de atendimento inteligente “Assistente GovInfo”, promovendo a modernização dos serviços públicos inteligentes, e os trabalhos de capacitação por IA nos sectores do turismo cultural, das convenções e exposições e das pequenas e médias empresas continuam a avançar. Com a expansão contínua dos cenários de aplicação da inteligência artificial, os novos riscos de cibersegurança associados à IA aplicada em infra-estruturas críticas, serviços à população e dados do público da RAEM têm igualmente aumentado. Importa salientar que, por enquanto, Macau ainda não estabeleceu normas específicas de cibersegurança dedicadas à inteligência artificial, dependendo a respectiva regulamentação principalmente da Lei da

Cibersegurança, da Lei da Protecção de Dados Pessoais, bem como de orientações emanadas por organismos responsáveis pela protecção de dados de outros países ou regiões. Perante os novos desafios representados pelos ataques autónomos de agentes de IA, pelos riscos na cadeia de abastecimento de modelos de código aberto e pelo desvio algorítmico, é necessário acompanhar atempadamente estas questões, nomeadamente, no que concerne a legislação e à falta de orientações aplicáveis, lacunas em matéria de normas técnicas ou imprecisão quanto aos limites de responsabilidade.

Cumprir referir que, com vista a reforçar os trabalhos de governação da segurança da inteligência artificial e a concretizar uma regulamentação precisa e uma prevenção eficaz, o Estado publicou em Setembro deste ano o “Quadro Geral de Governação da Segurança da Inteligência Artificial 3.0”. Este quadro geral, acompanhando de perto a tendência de desenvolvimento da tecnologia de agentes inteligentes, estabelece requisitos centrais relativos ao controlo do comportamento dos agentes, à segurança do ecossistema de código aberto, aos mecanismos de resposta a emergências e à governação hierarquizada e classificada, fornecendo assim orientações rígidas e uma referência importante para o aperfeiçoamento do respectivo sistema de governação em Macau.

Assim sendo, interpelo sobre o seguinte:

1. Tendo em conta que já ocorreram a nível internacional incidentes em que agentes de IA executam autonomamente ciberataques em grande escala, será que os diversos serviços públicos já elaboraram alguns planos especiais e mecanismos de resposta para fazer face a novos riscos como acções autónomas, operações abusivas e descontrolo comportamental por parte de agentes de IA, de modo a melhor gerir e prevenir potenciais riscos de segurança?

2. Considerando que o “Quadro Geral de Governação da Segurança da Inteligência Artificial 3.0”, recentemente publicado pelo Estado em Setembro, define com maior clareza os requisitos de governação do risco de segurança face

ao aumento significativo das capacidades de automatização, escala e inteligência dos ciberataques potenciados por inteligência artificial, vão as autoridades, tomando como referência o referido Quadro Geral, ponderar a actualização atempada das respectivas leis, regulamentos e orientações, a fim de garantir melhor o funcionamento normal e ordenado dos serviços governamentais, dos serviços prestados à população e das infra-estruturas?

3. Segundo se sabe, a Direcção dos Serviços da Protecção de Dados Pessoais da RAEM participa no Laboratório Conjunto para o Desenvolvimento Seguro da Inteligência Artificial Generativa da Grande Baía Guangdong-Hong Kong-Macau, iniciativa liderada conjuntamente pelo Gabinete de Ciberespaço do Comité Provincial de Guangdong e pelo Centro Nacional de Resposta a Emergências Cibernéticas – Subcentro de Guangdong, sob a orientação do Centro Nacional de Resposta a Emergências Cibernéticas do Estado. Como é que as autoridades vão usar os resultados e as experiências avançadas do referido laboratório conjunto, promovendo a articulação das normas de segurança da IA de Macau com as normas nacionais, para fazer face à rápida evolução dos meios de ataque impulsionados pela IA?

16 de Outubro de 2026

A Deputada à Assembleia Legislativa da RAEM,

Wong Kit Cheng