O uso da inteligência artificial dificulta a prevenção de burlas. Mantenha a calma e proceda a verificações antes de agir para não cair em armadilhas

Desde que surgiu o primeiro caso de burla com recurso à Inteligência Artificial (IA) em Abril deste ano, que a Polícia Judiciária (PJ) já recebeu mais um caso. A partir de 2023, as autoridades policiais passaram a divulgar, de forma contínua, o modus operandi das burlas com recurso à IA, pelo que o público tem algum conhecimento e precaução. Não houve prejuízos patrimoniais nesses dois casos. Contudo, atendendo ao crescente número de casos de burlas e outros crimes com recurso à IA em todas as partes do mundo, este artigo explica o modus operandi usado frequentemente na burla com IA, para que o público possa entender abrangentemente os golpes e identificá-los oportunamente, para evitar prejuízos.

A IA é uma tecnologia que simula o modo de pensar humano através de sistemas informáticos, que se otimiza progressivamente com a auto-aprendizagem e, no final, produz resultados em função das necessidades dos utilizadores. Por proporcionar várias conveniências, actualmente, a IA tem sido amplamente utilizada na vida quotidiana. Em paralelo, os grupos criminosos também têm recorrido constantemente à tecnologia da IA para a prática de crimes ou para a sua preparação, fazendo com que, desta forma, se aumentem significativamente os efeitos enganosos e a complexidade dos truques das burlas. Por conseguinte, a taxa de sucesso aumenta consideravelmente, o que constitui uma maior ameaça para o público.

O modus operandi mais comum das burlas com recurso à IA

No âmbito do cometimento de crimes, o mais comum é o uso da tecnologia Deepfake da IA para a prática de burlas, com a qual “trocam-se o rosto e a voz” para criar vídeos ou fazer videochamadas em tempo real. Os dois casos investigados pela PJ são desse tipo. Os burlões retiraram de vídeos de entrevistas o rosto e voz de celebridades de Macau e, com recurso à tecnologia Deepfake, criaram vídeos com figuras personificando essas celebridades a fazerem promoções de investimentos. Como complemento do esquema fraudulento, foram criados sites de phishing onde se acedia a jornais locais falsificados, na tentativa de induzir o público a fazer investimentos falsos, para ganhar ilicitamente quantias avultadas.

Da mesma forma, os burlões podem utilizar a tecnologia Deepfake para se fazerem passar por qualquer pessoa, tal como fingir serem um familiar ou amigo para fazer videochamadas à vítima, alegando estar a padecer de uma doença aguda, de ter sofrido um acidente ou invocando outros motivos urgentes para pedir “ajuda de emergência”. Podem ainda fazer-se passar por um chefe para ligar ao seu subordinado e solicitar transferências para fins comerciais. Na Região Administrativa Especial de Hong Kong, ocorreram dois casos de burla com recurso à IA que envolveram mais de cem milhões de dólares de Hong Kong. Estes dois crimes foram cometidos através da simulação de um superior hierárquico. Num dos casos, na videoconferência convocada o burlão chegou a representar, ao mesmo tempo, vários papéis, levando a vítima a acreditar no que lhe foi dito, e conforme a ordem do “tal superior”, transferiu 200 milhões de dólares de Hong Kong. Como se pode ver, não é apenas o público em geral, mas também as empresas multinacionais,

assim como as pequenas e médias empresas, que podem ser alvos de burlas praticadas com recurso à IA.

Uso da tecnologia da IA em todo o processo da prática do crime

Além de ser utilizada para o cometimento directo de burlas, a tecnologia da IA já penetrou na sequência de actos criminosos: na fase preparatória, a IA pode concluir automaticamente a recolha e análise de informações de rede, seleccionar potenciais vítimas e dados críticos, assim como gerar voz e conteúdo de texto necessários para serem usados em esquemas fraudulentos; na fase de execução, os chatbots da IA conseguem simular “atendimento ao cliente” ou “amante” para manter o contacto diário com a vítima, construindo assim gradualmente a confiança; em termos de suporte técnico, a IA consegue procurar automaticamente vulnerabilidades do sistema para lançar ataques cibernéticos ou criar rapidamente sites de phishing.

Com o uso da tecnologia da IA, as actividades criminosas tornam-se altamente enganosas, precisas e personalizadas, o que não só reduz os custos do cometimento de crimes, como também aumenta os lucros ilícitos. O que merece maior atenção é que a velocidade do desenvolvimento da IA ultrapassa em muito o progresso do desenvolvimento de ferramentas de controlo e prevenção, prevendo-se que os crimes impulsionados pela IA sejam cometidos sem contacto físico, o que se irá tornar numa das principais tendências no futuro.

Medidas adoptadas pelo Governo e recomendações de prevenção para o público

Para prevenir crimes relacionados com a IA, os governos, as Polícias e as empresas tecnológicas de vários países têm actuado de forma proactiva, nomeadamente através da aprovação de legislação que exige a identificação obrigatória de imagens produzidas pela IA e o desenvolvimento de aplicações móveis com funcionalidades de detecção baseadas na IA. A PJ de Macau introduziu no sistema de cibersegurança a tecnologia de IA para a análise de riscos, tendo o Centro de Coordenação de Combate às Burlas passado a integrar, também, novos equipamentos publicitários interactivos para a demonstração de troca de rosto e de voz através de IA, com o objectivo de promover o conceito de “reforçar o trabalho policial com o uso da tecnologia” e aumentar a capacidade de prevenção e de detecção de crimes relacionados com a IA.

Apesar do constante aperfeiçoamento das medidas tecnológicas de prevenção, os burlões continuam a adaptar os seus métodos em função da evolução da tecnologia. Por isso, o reforço da consciencialização pública contra as burlas permanece como uma estratégia fundamental. Para prevenir eficazmente as burlas com recurso à IA, é necessário: **Gerir rigorosamente os dados pessoais, efectuar múltiplas verificações de identidade, certificar-se várias vezes da veracidade dos factos e manter a calma perante qualquer incidente.** As recomendações concretas são as seguintes:

1. Gerir com prudência todos os dados pessoais, evitar a revelação na rede ou fornecer a desconhecidos dados biométricos como imagens do rosto, impressões digitais e impressões de voz, gerir cuidadosamente as permissões de visualização nas redes sociais,

guardar de forma segura os dados pessoais e financeiros importantes, nomeadamente os dados de identificação e as senhas das contas bancárias, a fim de prevenir o uso indevido para fins ilícitos.

2. Deve manter-se sempre alerta aos conteúdos de vídeos online, especialmente, os que explicitamente referem “recomendações de celebridades” ou “orientações para investimentos”. No contacto através de videochamada ou de mensagens de som, se tiver dúvidas relativas à identidade da outra parte, deve prestar muita atenção aos seus movimentos invulgares (tais como os contornos ou as bordas do corpo), ou pode fazer perguntas cuja resposta apenas é conhecida por si e pela pessoa real, para verificar a respectiva veracidade.
3. Caso lhe seja pedido dinheiro ou que faça transacções de grande valor, ou ainda, que faça transferências bancárias por motivos de emergência, não ceda imediatamente e examine a situação com cuidado, através dos meios de contactos habitualmente utilizados, e confirme pessoalmente com a pessoa em causa, para verificar a respectiva veracidade.
4. Caso suspeite de ter sido vítima de uma burla, deve ligar imediatamente para a linha aberta da PJ para consultas sobre a prevenção de burlas, 8800 7777, ou pela linha de denúncias 993 para pedir intervenção.

Os sons e as imagens podem não ser verdadeiros, por isso, verifique com calma para distinguir o real do falso. Embora os crimes com recurso à IA sejam altamente enganadores e em constante evolução, basta que

o público proteja bem os seus dados pessoais, se mantenha alerta e verifique cuidadosamente a veracidade das situações para que os riscos de ser burlado reduzam significativamente. Em simultâneo, o público deve estar atento às informações antiburla mais recentes, tomar precauções pessoais e transmitir proactivamente essas informações às pessoas que o rodeiam, de modo a construir em conjunto um sistema comunitário antiburla, salvaguardando os bens e a segurança pessoal e da sociedade.