As principais dificuldades na investigação do crime informático e o conteúdo das alterações na “Lei de combate à criminalidade informática”

A Lei de combate à criminalidade informática oferece uma garantia jurídica fundamental para o combate eficaz ao crime informático. Contudo, desde a sua entrada em vigor, em Agosto de 2009, até à actualidade, tem-se registado um grande desenvolvimento na sociedade e a nível tecnológico, que para além dos novos estilos e modos de vida, fomentou ainda mudanças no modus-operandi da criminalidade informática, que dificultam a capacidade de resposta de acordo com a legislação em vigor. Para fazer face às novas formas e modelos de crime informático, é necessário efectuar, atempadamente, a revisão sobre as situações não contempladas na lei, de modo a colmatar as lacunas e preencher o vazio legislativo, garantindo assim, a eficácia do regime e a capacidade de resposta para os desafios trazidos pelos novos tipos de criminalidade informática.

A Secretaria para a Segurança e a PJ fizeram um balanço das experiências práticas obtidas ao longo dos últimos dez anos no âmbito da execução da lei, assim como das tendências da criminalidade informática e cibernética nos últimos anos e, após a análise extensa e o estudo aprofundado com base nas realidades e dificuldades vivenciadas na RAEM, propõe-se a introdução das seguintes alterações:

（1）Tipificar as estações emissoras simuladas como um crime autónomo;

（2）Reforçar a protecção penal dos sistemas informáticos utilizados pelos operadores de infra-estruturas críticas e por outras entidades relevantes;

（3）Extrair, nos termos da lei, cópia dos dados informáticos que se encontram fora da RAEM para efeitos de prova no processo penal;

（4）Proceder-se à autonomização criminal das condutas de violação de

segredo profissional e de revelação ilegítima da vulnerabilidade crítica de segurança.

A alteração referida no ponto (3) tem merecido especial atenção, uma vez que implica questões jurídicas e técnicas mais complexas. Deste modo, convém fazer aqui uma abordagem mais detalhada, apresentando os seguintes esclarecimentos:

I. As dificuldades enfrentadas durante a recolha de provas digitais em meios que disponibilizam serviços de nuvem fora de Macau

Com o desenvolvimento rápido e a generalização da internet, da comunicação transfronteiriça e da tecnologia da computação em nuvem, os dados informáticos atravessam as fronteiras geográficas e o seu armazenamento em diferentes jurisdições é um facto comum. Nos últimos anos, durante as investigações, especialmente no que diz respeito à criminalidade informática, notamos que muitos criminosos não fazem o armazenamento dos dados digitais ligados aos casos investigados apenas em Macau, mas também nas plataformas que prestam serviços de nuvem, o que tem vindo a trazer, tanto a nível tecnológico como jurídico, grandes desafios ao trabalho de investigação e de recolha de provas.

Actualmente, no âmbito da obtenção de provas digitais armazenadas nas plataformas de serviços de nuvem que se encontram fora da RAEM, podemos apenas recorrer ao processo convencional, ou seja, a cooperação judiciária em matéria penal, desencadeada com estrutura

bilateral ou multilateral. Porém, este processo é complexo e moroso, muitas vezes os pedidos não são respondidos em tempo oportuno e alguns deles até nem chegam a ser respondidos, havendo assim a possibilidade de as provas digitais relevantes serem destruídas ou perdidas, suspendendo ou impedindo que a investigação seja concluída com eficácia.

Na era da internet, a cooperação judiciária já não é a melhor solução. Um outro motivo essencial é que este meio só é aplicável em situações em que haja uma identificação clara do prestador de serviços em nuvem e do local onde estão armazenados os dados. Sendo que, em termos técnicos, existem serviços de internet que são anónimos ou dissimulados intencionalmente, tais como: a *deep web*, *dark web*, *websites* fictícios e *websites* para jogos ilegais, em que muitas vezes os prestadores de serviços desses *websites* e a localização dos dados armazenados não são identificáveis e o acesso e rastreio são impossíveis através de formas regulares a utilização desses métodos para ocultar a identificação real e praticar crime tem dificultado significativamente a investigação e a obtenção das provas digitais.

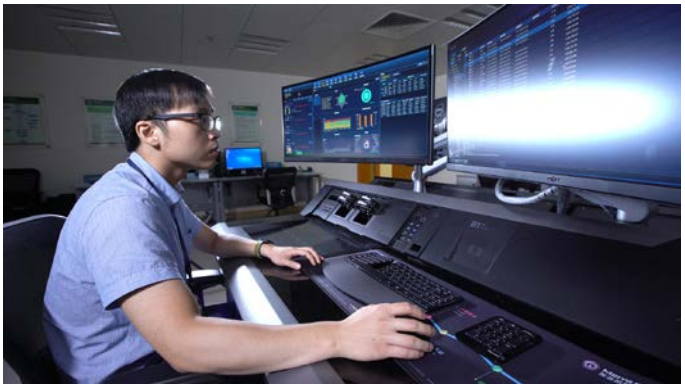
II. Novos modelos de resposta adoptados pelos diversos países para a recolha de provas digitais a nível transfronteiriço

Para superar estas dificuldades, muitos países e regiões, tais como os EUA, a União Europeia (designadamente em Portugal), a China e Singapura, atentos ao desenvolvimento das tecnologias da internet e as características dos serviços de computação em nuvem, definiram novas medidas para a recolha de provas digitais na internet através da produção legislativa. Uma das medidas mais representativas é a “recolha de provas online” que é geralmente adoptada e reconhecida por muitos países. Esta medida consiste tanto na obtenção online, de acordo com a lei, de informações de dados acessíveis ao público, como na recolha online do conteúdo dos dados através de equipamentos electrónicos, relacionados com o crime, legalmente aprendidos, e directamente conectados aos serviços de internet .

III. Extracção, nos termos da lei, da cópia de dados informáticos que se encontram fora da RAEM para efeitos de prova no processo penal

Para se adaptar às características da era cibernética e satisfazer as necessidades do trabalho de execução da lei de Macau, sugere-se nesta proposta de lei que seja eliminada a expressão de limitação geográfica "situado na RAEM", constante da alínea 6) do n.° 1 do artigo 16.° da Lei de combate à criminalidade informática e que seja adoptado o novo modelo de "recolha de provas online". Isso não irá alterar o actual procedimento penal em Macau, visto que continua a ser exigida à polícia a prévia autorização das autoridades judiciais, ou seja, a apreensão de equipamentos electrónicos mediante procedimentos legais depende do despacho de autorização ou ordem do magistrado, emitido consoante as circunstâncias concretas do caso e nos termos da lei. Só assim é que poderá ser feita a recolha online de cópias dos dados nos serviços de internet directamente conectados aos equipamentos para efeitos de prova no processo penal, quer os dados electrónicos tenham sido armazenados

em Macau quer no exterior. Ao mesmo tempo, aos dados digitais da *deep web*e da*dark web*, cujos prestadores de serviços em nuvem e os locais de armazenamento não são identificáveis, também pode ser aplicada a medida de “recolha de provas online”, no sentido de ultrapassar as actuais dificuldades encontradas na investigação e na recolha deste tipo de provas.



IV. Conclusão

À medida que o modus operandi com recurso aos computadores e às redes evolui, os respectivos regimes jurídicos penais também devem ser actualizados e aperfeiçoados. A presente revisão à Lei de combate à criminalidade informática permitirá que as autoridades judiciais e os órgãos policiais tenham um suporte legal mais completo e específico, de modo a garantir o desenvolvimento eficaz do trabalho de investigação e de recolha de provas, a melhorar a eficácia da prevenção e combate à criminalidade informática, a manter a cibersegurança e proteger os direitos e interesses legítimos do público em geral, bem como salvaguardar a estabilidade da sociedade a longo prazo.