Executar, de forma ordenada, as garantias complementares e implementar, nos termos da lei, a salvaguarda da cibersegurança

I. Breve apresentação e valor da "Lei da Cibersegurança"

A Lei n.º 13/2019 "Lei da Cibersegurança" já foi publicada no dia 24 de Junho de 2019, entrando oficialmente em vigor 180 dias após a sua publicação, ou seja, no dia 22 de Dezembro de 2019. A "Lei da Cibersegurança" visa estabelecer e regularizar o sistema da cibersegurança de Macau, tendo por principal objecto a caracterização do sujeito participante da gestão das actividades da cibersegurança, o enquadramento institucional do sistema da cibersegurança, o regime de deveres e sanções administrativas pelo respectivo incumprimento, entre outros.

A "Lei da Cibersegurança" responde à crescente necessidade de segurança das redes informáticas da sociedade de Macau, adapta-se à tendência internacional da legalização do espaço cibernético, preenche o vazio legal da respectiva protecção em Macau, marcando uma nova fase de desenvolvimento da sua governação no que diz respeito ao espaço cibernético. De tudo isto resulta uma significativa e profunda quanto ao reforço da capacidade de protecção da cibersegurança dos operadores das infra-estruturas críticas, um aumento do nível de gestão da cibersegurança, bem como um incremento da eficácia da prevenção e combate dos diversos tipos de riscos inerentes, de forma a proteger a segurança de Macau ou até a segurança do Estado.

II. Actual foco do trabalho da cibersegurança em Macau

Sendo uma lei-quadro, a implementação eficaz da “Lei da Cibersegurança” requer ainda diplomas complementares e trabalhos concretos para garantir a sua implementação, por isso, após a publicação da “Lei da Cibersegurança”, as autoridades estão a avançar activamente nas quatro áreas que a seguir se identificam:

(1) Elaboração das normas para o funcionamento do sistema da cibersegurança

Nos termos da “Lei da Cibersegurança” estipula-se que a gestão do sistema da cibersegurança é composta por três entidades: a Comissão para a Cibersegurança (doravante designada por CPC), o Centro de Alerta e Resposta a Incidentes de Cibersegurança (doravante designado por CARIC) e Entidades de Supervisão de Cibersegurança (doravante designadas por entidades de supervisão). As autoridades já elaboraram o regulamento administrativo complementar sobre a composição concreta, as competências e a forma de funcionamento deste sistema, tendo-o entregue aos departamentos da área da justiça para obter pareceres, procurando implementá-los, dentro do corrente ano, simultaneamente com a entrada em vigor da “Lei da

Cibersegurança". Por outro lado, o Governo da RAEM vai designar, através de actos normativos complementares, uma lista concreta das entidades de supervisão e das entidades dos operadores privados das infra-estruturas críticas supervisionadas, para concretizar a implementação dos poderes, responsabilidades e deveres da gestão da cibersegurança.

(2) Elaboração de normas técnicas complementar da cibersegurança

O "Grupo de trabalho interdepartamental da elaboração de critérios da cibersegurança", formado pelos PJ, SAFP e DSCT, está a elaborar o texto relativo às normas técnicas relevantes, o qual constitui uma base fundamental para futuros operadores que realizem actividades da cibersegurança. A primeira fase das normas técnicas inclui principalmente as seguintes duas partes:

1. "Regulação de padrões de gerenciamento da cibersegurança" , destinada a fornecer aos operadores das infra-estruturas críticas padrões de gerenciamento básicos e requisitos técnicos para a avaliação de protecção de segurança do sistema informático e avaliação de risco, permitindo que os operadores elaborarem um

sistema de gerenciamento da cibersegurança que atenda às suas necessidades operacionais, conjugando esses padrões com a situação real desses operadores, garantindo a segurança das redes de informações e o sistema informático, bem como a dos dados que nelas gerenciam, fazendo com que reforçam as capacidades de prevenção e de resposta da cibersegurança dos operadores.

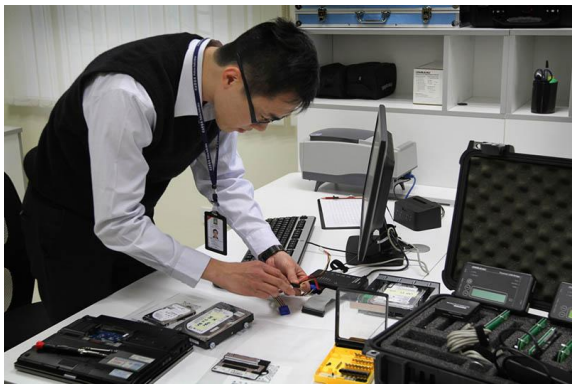
2. "Regulação de alerta, resposta e comunicação a incidentes de cibersegurança" , com o objectivo de criar um mecanismo para emitir informações de alertas e fornecer aos operadores orientações gerais para a resposta dos incidentes de cibersegurança, bem como procedimentos e requisitos para a comunicação de incidentes. Os operadores devem elaborar, segundo a regulação, os seus próprios planos de resposta, bem como os procedimentos de comunicação de incidentes, para que os operadores possam proceder atempada e eficaz acção de resposta aos incidentes de cibersegurança, assim reduzindo os impactos desvantajosos causados nas infra-estruturas críticas.

(3) Regulamentação sobre a implementação do Real-Name System dos cartões telefónicos

O Real-Name System dos cartões telefónicos é outro trabalho de gestão principal da "Lei da Cibersegurança". Este regime é diferente do "regime do nome verdadeiro de redes" aplicado por alguns países ou regiões, sendo o conteúdo concreto do Real-Name System os seguintes: quando se efectuar a compra de cartões telefónicos, o utente tem que facultar às operadoras de telecomunicações os seus reais dados de identificação para efeitos de verificação e registo, sem necessidade, todavia, de usar os seus nomes verdadeiros quando usarem esses

cartões telefónicos para o acesso à internet (tais como para abrir conta no Facebook ou exprimir as suas ideias no fórum). Os dados de identificação são guardados pelas operadoras de telecomunicações e protegidos pela “Lei da Protecção de Dados Pessoais”.

Quanto à implementação do Real-Name System dos cartões telefónicos, nos termos do artigo 24.o da “Lei da Cibersegurança”, foi também concedido às operadoras de telecomunicações um período de transição de 120 dias a contar da data da sua entrada em vigor para que os mesmos efectuem os trabalhos preparativos e adaptações à implementação do mesmo sistema. Entretanto, com vista a dar conveniência aos utentes, as entidades competentes estão a discutir com os operadores de redes no intuito de facilitar a boa implementação do Real-Name System dos cartões telefónicos, planeando também o registo e a verificação dos dados de identificação dos utentes de forma totalmente electrónica.



(4) Promoção de trabalhos de sensibilização e divulgação relativos à cibersegurança

“A Lei da Cibersegurança” vai entrar em vigor no dia 22 de Dezembro do corrente ano. Para além de bom desencadeamento de trabalhos

preparativos, o mais importante é que o Governo, os operadores de infra-estruturas críticas e a população em geral fiquem a conhecer a importância da “Lei da Cibersegurança”, nomeadamente para que todas as partes intervenientes na gestão da cibersegurança conheçam bem o cumprimento dos deveres, reforçando de forma continuada a consciência da cibersegurança de todos os sectores da sociedade para a boa implementação da lei. Por conseguinte, os respectivos serviços estão a aproveitar meios diferentes para desenvolver, de forma activa, as actividades de sensibilização sobre a “Lei da Cibersegurança”, com vista que as respectivas entidades de supervisão e os operadores das infra-estruturas críticas conheçam bem os seus papéis, as suas responsabilidades e relações de cooperação, empenhando-se no desenvolvimento de todos os trabalhos de gestão relativos à cibersegurança, criando em conjunto um ambiente seguro de redes, assegurando o normal funcionamento das infra-estruturas críticas da sociedade e dando contributo para o público.