NOTA JUSTIFICATIVA

Lei da cibersegurança

(Proposta de lei)

I. Necessidade para a elaboração da presente proposta de lei

Com o desenvolvimento rápido e a vulgarização do uso da *internet* e das tecnologias de comunicação, a Região Administrativa Especial de Macau, doravante designada por RAEM, tais como outros países e regiões, tem vindo a desenvolver-se no sentido duma cidade inteligente. A "Indústria 4.0" levou Macau a entrar na era da inteligência artificial e *Big Data*, onde a informatização está estreitamente ligada às actividades de todas as áreas da sociedade e à vida quotidiana das diversas camadas de cidadãos. Assim, os computadores, as redes informáticas e a *internet* tornaram-se instrumentos imprescindíveis para os diversos sectores e para a vida quotidiana da população em geral.

Com efeito, a informatização e a inteligência artificial têm trazido muitas vantagens e facilidades às pessoas, empresas e organizações, mas, precisamente por causa dessa extraordinária importância e perante as ameaças de cibersegurança a nível mundial, bem como os sérios desafios decorrentes de invasões e ataques cibernéticos, com os quais se têm defrontado os sectores público e privado nas suas redes e segurança informática, torna-se imprescindível instituir mecanismos adequados de protecção, de forma a assegurar que as redes informáticas essenciais funcionem, de forma pacífica e ininterrupta, e a garantir a confidencialidade e integridade dos dados informáticos.

O Governo da RAEM sublinhou, no Relatório das Linhas de Acção Governativa para o Ano Financeiro de 2016, no âmbito da segurança que *"como existem lacunas nas tecnologias e há uma escassa consciência de prevenção, os problemas relacionados com os sistemas informáticos estão cada vez mais evidentes, a segurança da internet e das informações na área pública ou privada enfrentam agora desafios enormes. As variações na tipologia do crime cibernético e os acidentes de segurança cibernética surgem a níveis sem precedentes, especialmente no que diz respeito a escala, gravidade e complexidade"*.

Assim, a presente proposta de lei visa institucionalizar, na área jurídica, os aludidos mecanismos de protecção, definindo claramente deveres e responsabilidades, em matéria de cibersegurança, no intuito de salvaguardar os interesses públicos especialmente relevantes, tais como a segurança ou ordem pública e a estabilidade social, bem como a garantia dos interesses dos residentes de Macau, através de intensificação da segurança cibernética das infra-estruturas críticas operadas pelos organismos públicos e privados. No decurso do processo da consulta pública da proposta de lei, as opiniões dos sectores das actividades relacionadas e do público reconhecem em geral a necessidade da legislação da matéria em causa. Para assegurar os direitos legítimos dos residentes de Macau, é sempre observado pelo Governo da RAEM o previsto da Lei da Protecção de Dados Pessoais no processo da elaboração da Lei da Cibersegurança, sendo que se manterá fazer revisão necessária quanto à eficácia da lei após a sua entrada em vigor.

O objecto da protecção directa da presente proposta de lei são as redes e sistemas informáticos dos serviços públicos e das entidades privadas que operam actividades críticas, incluindo as actividades taxativamente elencadas no artigo 4.º da presente proposta de lei (âmbito subjectivo de aplicação), tais como as actividades nos domínios dos transportes, telecomunicações, banca e seguros, cuidados de saúde e fornecimento de água e electricidade. Assim sendo, é dada a esses serviços públicos e entidades privadas a designação dos operadores das infra-estruturas críticas.

A opção por estes sectores e entidades justifica-se porque os eventuais ataques às respectivas redes e sistemas informáticos poderão ter maior impacto, prejudicando directamente a segurança e ordem públicas, e o bem-estar da população em geral e causando inevitavelmente graves consequências à comunidade.

II. Conteúdo da proposta de lei

1. Ordem e estrutura da proposta de lei

A presente proposta de lei é composta por cinco capítulos: disposições gerais, disposições institucionais, deveres de cibersegurança, regime sancionatório e disposições transitórias e finais.

2. Disposições gerais

O primeiro capítulo desta proposta de lei define (como o objecto da presente proposta de lei) a criação do sistema de enquadramento da cibersegurança. Assim sendo, definem-se claramente várias expressões relevantes, tais como rede informática, infra-estruturas críticas, actos não autorizados, incidentes de cibersegurança, entre outros, assim como se esclarece em que consiste a actividade de cibersegurança (artigo 3.º) e o âmbito subjectivo de aplicação (artigo 4.º) da presente proposta de lei. O âmbito subjectivo é delimitado negativamente, no artigo 5.º, em relação a determinadas entidades cuja inclusão não se justifica.

O sistema de cibersegurança é um sistema de natureza administrativa, de carácter predominantemente preventivo das ameaças às redes informáticas.

A presente proposta de lei não regula as próprias medidas concretas de cibersegurança, em si, (por exemplo, "*firewalls*", autenticações, controlos de acesso, assinaturas digitais, sistemas de detecção de intrusões, sistemas de encriptação, etc.), pois estas têm natureza muito mutável e revestem-se de grande tecnicidade. Trata-se da matéria que deve ser objecto de disposições de natureza puramente regulamentar, e que são instituídas através das instruções e circulares das entidades supervisoras (vide a alínea 2) do artigo 3.º). Nesta medida, o regime proposto tem semelhança com o modelo de supervisão e regulação técnica seguido no Regime Jurídico do Sistema Financeiro.

3. Disposições institucionais

O capítulo II da presente proposta de lei define a estrutura (ou organização) de todo o sistema de cibersegurança que inclui duas categorias de entidades:

- Entidades de carácter geral: a Comissão Permanente para a Cibersegurança, doravante designada por Comissão Permanente, o órgão de topo, ao qual compete, essencialmente, a definição de orientações e objectivos de carácter geral e estratégico com vista à prossecução das finalidades da cibersegurança; e o Centro de Alerta e Resposta a Incidentes de Cibersegurança, doravante designado por CARIC, especialmente vocacionado para gerir e implementar medidas de resposta a emergências;

- Entidades de carácter sectorial: as entidades públicas que exercem a supervisão, de forma permanente e rotineira, do cumprimento dos deveres de cibersegurança por parte dos operadores de infra-estruturas críticas que incluem os serviços, órgãos e entidades públicos, nos sectores das suas actividades.

A presente proposta de lei especifica as atribuições mais importantes das aludidas entidades. Propõe-se que sejam definidas, em regulamento administrativo complementar, as matérias relacionadas com as suas competências e funcionamento.

4. Deveres de cibersegurança

No capítulo III da presente proposta de lei, são definidos os deveres que os operadores de infra-estruturas críticas devem cumprir, para que seja conseguido um nível adequado de cibersegurança.

Para obter melhor clareza de exposição, os deveres são especificados, consoante a sua natureza, em quatro artigos:

- Deveres de carácter orgânico;
- Deveres de carácter procedimental, preventivo e reactivo;
- Deveres de auto-avaliação e relato;
- Deveres de colaboração.

O padrão dos deveres de cibersegurança dos operadores privados de infra-estruturas críticas é definido nos artigos 10.º a 13.º. No artigo 14.º, fixam-se os deveres dos operadores públicos de infra-estruturas críticas, tendo em conta a sua natureza específica.

Este capítulo contém o cerne da presente proposta de lei. Os operadores de infra-estruturas críticas implementam, de forma efectiva, padronizada e monitorizada, os deveres de cibersegurança, com vista a garantir que são atingidas as seguintes finalidades essenciais do novo regime jurídico: assegurar a operacionalidade, integridade e disponibilidade das redes e dos sistemas informáticos utilizados pelos referidos operadores, bem como a confidencialidade dos dados informáticos, para

evitar que tais redes, sistemas e dados sejam prejudicados ou por qualquer forma afectados por actos não autorizados.

A criação do cargo de "principal responsável de cibersegurança" visa introduzir um mecanismo de maior responsabilização individual dentro das organizações. A proposta estabelece exigências de idoneidade e de experiência profissional para estas pessoas e faz algumas imposições que pretendem garantir que essa pessoa está efectivamente disponível na RAEM para colaborar com as autoridades, especialmente em casos de emergência.

Os deveres técnico-operacionais de cibersegurança a que alude o artigo 11.º da presente proposta de lei ("*firewalls*", autenticações, controlos de acesso, assinaturas digitais, sistemas de detecção de intrusões, sistemas de encriptação, etc.) tratam de matérias de natureza muito mutável e de grande tecnicidade, pelo que estas serão reguladas por acto normativo.

Os deveres de auto-avaliação e relato a que se refere o artigo 12.º têm em vista dois objectivos: obrigar os operadores de infra-estruturas críticas a proceder, periodicamente, à auto-avaliação e, simultaneamente, dotar as autoridades públicas do conhecimento real e concreto necessário para propor ajustamentos e melhorias nos regimes legal e regulamentar, a fim de melhorar os níveis de cibersegurança na RAEM.

Finalmente, o dever de colaboração afigura-se imprescindível para garantir uma adequada e eficaz intervenção em caso de emergência de ataque cibernético. A entrada dos representantes do CARIC nas infra-estruturas críticas dos operadores está prevista apenas para efeitos de verificação do cumprimento dos deveres relativos a mecanismos de defesa, como por exemplo "*firewalls*", autenticações, controlos de acesso, assinaturas digitais, sistemas de detecção de intrusões e sistemas de encriptação. Esta intervenção pode ser fundamental em caso de ataque cibernético, visando evitar a contaminação por vírus das redes e dos sistemas informáticos dos operadores por motivo da disseminação de ameaças de cibersegurança.

A fim de flexibilizar o funcionamento do sistema de cibersegurança, é admitido

que os operadores de infra-estruturas críticas "deleguem" a implementação e garantia da sua cibersegurança em terceiros, com excepção dos seguintes casos:

- No caso dos operadores públicos, a "delegação" num prestador privado de serviços de cibersegurança só é permitida mediante autorização prévia do Chefe do Executivo e não isenta a entidade pública em causa de "fiscalizar" e monitorizar atentamente o desempenho desse prestador privado e de actuar em sua substituição em caso de necessidade e de o responsabilizar por eventuais erros ou omissões (alínea 3) do n.º 1 do artigo 14.º da proposta de lei);
- No caso dos operadores privados, ressalva-se que essa "delegação não os isenta da responsabilidade infraccional administrativa". Assim, eles poderão ser sancionados mesmo que o incumprimento dos deveres de cibersegurança seja imputável ao prestador privado de serviços de cibersegurança; eventualmente, tais operadores poderão, posteriormente, procurar responsabilizar civilmente os prestadores privados (n.º 3 do artigo 15.º da proposta de lei).

5. Regime administrativo sancionatório

O capítulo IV da presente proposta de lei respeita às disposições sancionatórias.

A violação dos deveres de cibersegurança é sancionada com multas que, para os casos mais graves, pode variar entre 150 000 e 5 000 000 patacas, e para os casos considerados menos graves, entre 50 000 e 150 000 patacas.

Todavia, prevê-se que, em casos especiais (quando a situação não consubstancie um perigo substancial para a cibersegurança e não se trate de uma situação de reincidência), a entidade de supervisão pode advertir o infractor para sanar a irregularidade dentro dum prazo fixado.

Ao invés, pelas infracções que se mostrem de maior gravidade, poderão ser aplicadas, isolada ou cumulativamente, as seguintes sanções acessórias:

- Privação do direito de participar em concursos públicos que tenham por objecto a aquisição de bens ou serviços por serviços, órgãos e entidades públicos;

- Privação do direito a subsídios ou benefícios concedidos por serviços, órgãos e entidades públicos.

Dado que algumas condutas infractoras podem constituir simultaneamente violação de outras normas (por exemplo, da Lei da Protecção de Dados Pessoais), prevê-se, na presente proposta de lei, uma norma própria para regular esse assunto. Além disso, também se prevêem especificamente as questões da reincidência, competência instrutória e sancionatória,

Não obstante, o capítulo não é muito extenso. Para essa simplicidade teve-se em conta as características dos destinatários deste regime legal, que são, basicamente, empresas estáveis, de média / grande dimensão.

Relativamente aos operadores públicos das infra-estruturas críticas, os seus responsáveis, quando não cumprirem os respectivos deveres, com dolo ou por negligência, irão assumir responsabilidades disciplinares e poderão, ainda, ser punidos com a pena de demissão em casos graves.

6. Disposições transitórias e finais

No último capítulo da presente proposta de lei, são abordadas substantivamente duas questões que, não respeitando directamente à cibersegurança, têm forte conexão com ela, pois também têm em vista a melhoria da protecção das redes informáticas e dos seus utilizadores, em geral.

A primeira questão respeita ao "*Real-Name System*": os operadores ao celebrarem contratos com seus utentes e ao confirmarem a prestação de serviços de acesso à *internet*, serviços de registo de nomes de domínio, serviços públicos de telecomunicações fixas ou móveis, aos utentes, devem solicitar os dados de identificação verdadeiros. Este regime segue um modelo que está implementado internacionalmente, constituindo um mecanismo dissuasor da utilização de módulos de identificação de assinante, doravante designados por cartões SIM, usados em terminais telefónicos móveis para finalidades criminosas.

No artigo 23.º, é resolvida, a título transitório, a situação de cartões SIM não sujeitos à prévia identificação e adquiridos na modalidade de pré-pagos, antes da entrada em vigor da lei.

A segunda questão respeita à "conservação e fornecimentos de registos de tradução de endereços de rede privada em endereços de rede pública (*network address translation*): ao disponibilizarem aos utentes serviço de acesso à *internet*, os operadores de redes devem conservar, por um ano, os registos das traduções (conversões) entre os endereços das redes internas privadas dos utentes e os endereços públicos IP da *internet*. Dado que esta é uma questão de conservação de dados para efeitos de eventual investigação criminal, ela é inserida, harmoniosamente, na Lei n.º 11/2009 (Lei de combate à criminalidade informática), mediante o aditamento de um artigo a essa lei; o acesso a esses dados pelas autoridades policiais segue, assim, o regime de controlo pelos órgãos judiciais, não se suscitando, por isso, problemas de protecção da privacidade.

Para além das duas questões referidas, prevêem-se, no último capítulo, as disposições usuais em matéria de direito subsidiário aplicável, regulamentação complementar e entrada em vigor.

Quanto ao direito subsidiário aplicável, a formulação do artigo 26.º está feita de modo a conseguir a simplicidade da presente proposta de lei.

Assim, pela remissão para o Decreto-Lei n.º 52/99/M, de 4 de Outubro (Regime geral das infracções administrativas e respectivo procedimento), torna-se desnecessário prever na proposta de lei as questões, como por exemplo, o destino das multas e o prazo para o respectivo pagamento.

Por outro lado, pela remissão para os princípios gerais do direito e do processo penal, torna-se desnecessária, por exemplo, a previsão, na proposta de lei, de disposições sobre graduação das sanções (são aplicáveis, com as adaptações necessárias, os princípios contidos no artigo 65.º do Código Penal).

Quanto à regulamentação complementar, a presente proposta de lei prevê, genericamente, que compete ao Chefe do Executivo emitir as normas complementares

necessárias à boa execução da Lei da cibersegurança. Todavia, especifica expressamente:

- A regulamentação da composição, competências e modo de funcionamento da Comissão Permanente e do CARIC;
- A designação das entidades públicas que ficam encarregues da supervisão dos operadores privados de infra-estruturas críticas, apontando a lógica que deve presidir à designação de tais entidades de supervisão, por remissão para a Lei n.º 2/1999 (Lei de Bases da Orgânica do Governo) e o Regulamento Administrativo n.º 6/1999 (Organização, competências e funcionamento dos serviços e entidades públicos).

No que respeita à entrada em vigor, prevê-se que ocorra 180 dias após a publicação da presente proposta de lei, salvo quanto ao específico dever de conservação, por um ano, dos registos de tradução de endereços das redes internas privadas dos utentes em endereços públicos IP da *internet* (os operadores de redes só terão de passar a cumprir esses deveres em data posterior, a definir, para lhes permitir implementar os preparativos práticos necessários a esse cumprimento).