REGIÃO ADMINISTRATIVA ESPECIAL DE MACAU

Lei n.º /2019

(Proposta de lei)

Lei da cibersegurança

A Assembleia Legislativa decreta, nos termos da alínea 1) do artigo n.º 71 da Lei Básica da Região Administrativa Especial de Macau, para valer como lei, o seguinte:

CAPÍTULO I
Disposições gerais

Artigo 1.º
Objecto e finalidade

A presente lei estabelece e regula o sistema de cibersegurança da Região Administrativa Especial de Macau, doravante designada por RAEM, visando a protecção das redes, sistemas e dados informáticos dos operadores de infra-estruturas críticas.

Artigo 2.º
Definições

1. Para efeitos da presente lei, entende-se por:
   1) «Cibersegurança», a actividade permanente e plurissectorial desenvolvida pela RAEM com o objectivo de assegurar o normal funcionamento das redes e sistemas informáticos utilizados pelos operadores de infra-estruturas críticas e a integridade, confidencialidade e disponibilidade dos dados informáticos, prevenindo, em especial, que tais redes, sistemas e dados sejam comprometidos por actos não autorizados;

2.ª versão enviada à AL

2) «Redes informáticas»:
   (1) Os dispositivos e ou sistemas informáticos interligados;
   (2) As redes de comunicações electrónicas, através das quais se processa a interligação de dispositivos e sistemas, designadamente as redes de telecomunicações referidas na Lei n.º 14/2001 (Lei de Bases das Telecomunicações); e
   (3) Os dados informáticos armazenados, tratados, trocados ou transmitidos no âmbito dos dispositivos, sistemas e redes referidos nas subalíneas anteriores, tendo em vista o seu funcionamento, utilização, protecção e manutenção;
3) «Infra-estruturas críticas», os patrimónios, redes e sistemas informáticos relevantes para o normal funcionamento da sociedade, e cuja perturbação, destruição, revelação de dados, suspensão de funcionamento ou diminuição significativa da eficiência é susceptível de causar prejuízos graves para o bem-estar, segurança ou ordem públicas ou outro interesse público especialmente relevante;
4) «Operadores de infra-estruturas críticas», as entidades, públicas ou privadas, que operam infra-estruturas críticas e que prestam serviços ligados às mesmas;
5) «Acto não autorizado», o acesso, obtenção, utilização, disponibilização, intercepção, dano ou outro tipo de interferência nas redes, sistemas e dados informáticos não consentidos pelos seus proprietários ou demais titulares de direitos sobre eles;
6) «Incidente de cibersegurança», qualquer situação que configure um acto não autorizado e, em geral, qualquer evento com um efeito real adverso na segurança das redes, sistemas e dados informáticos;
7) «Operadores de redes», as entidades habilitadas a explorar redes públicas de telecomunicações fixas ou móveis e a prestar serviços de acesso à *internet*.

2. Para efeitos do disposto na presente lei, as expressões «sistema informático» e «dados informáticos» são entendidas nos termos das respectivas definições constantes da Lei n.º 11/2009 (Lei de combate à criminalidade informática).

Artigo 3.º

Actividade de cibersegurança

1. A actividade de cibersegurança é prosseguida mediante:
   1) A definição de orientações, objectivos e estratégias com vista à prossecução das finalidades da cibersegurança;
   2) A emissão de normas técnicas vinculativas para os operadores de infra-estruturas críticas;
   3) O cumprimento dos deveres previstos na presente lei e nas normas técnicas;
   4) A execução de medidas de cibersegurança excepcionais que visem dar resposta a incidentes de cibersegurança, em especial quando ocorram ou estejam eminentes incidentes graves;
   5) A monitorização dos dados informáticos transmitidos entre as redes dos operadores de infra-estruturas críticas e a *internet*, com a finalidade de prevenir, detectar e combater incidentes de cibersegurança;
   6) A fiscalização do cumprimento dos deveres e medidas de cibersegurança e a instauração dos correspondentes procedimentos sancionatórios.

2. As normas técnicas visam definir processos e mecanismos de segurança das redes, sistemas e dados informáticos e são emitidas pelas entidades referidas no capítulo II através de circulares, dirigidas à generalidade dos operadores de infra-estruturas críticas ou de instruções, dirigidas a categorias específicas de operadores de infra-estruturas críticas.

3. As circulares e instruções são publicadas no *Boletim Oficial da Região Administrativa Especial de Macau* ou, quando a sua natureza reservada o justifique, entregues por protocolo ou expedidas sob registo postal com aviso de recepção.

Artigo 4.º

Âmbito subjectivo de aplicação

1. A presente lei aplica-se aos operadores públicos e privados de infra-estruturas críticas.

2. São operadores públicos de infra-estruturas críticas:
   1) O Gabinete do Chefe do Executivo, os gabinetes dos titulares dos principais cargos, os serviços de apoio à Assembleia Legislativa, o Gabinete do Presidente do Tribunal de Última Instância e o Gabinete do Procurador;
   2) Os serviços públicos da RAEM;
   3) Os Institutos públicos e fundos autónomos, qualquer que seja a modalidade que revistam.

3. São operadores privados de infra-estruturas críticas:
   1) Todas as entidades de direito privado, com sede na RAEM ou no exterior, habilitadas a exercer actividades nos domínios a seguir especificados, seja a título de concessão de exploração, de prestação de serviços à Administração ou de licenciamento, alvará ou título de idêntica natureza:
      (1) Abastecimento de água;
      (2) Actividade bancária, financeira e seguradora;
      (3) Prestação de cuidados de saúde em hospitais;
      (4) Tratamento de águas residuais e recolha e tratamento de resíduos;
      (5) Abastecimento público grossista de combustíveis e de produtos alimentares sujeitos a controlos sanitários e fitossanitários;
      (6) Abate de animais em matadouros legais;
      (7) Fornecimento e distribuição de electricidade e gás natural;
      (8) Prestação de serviço público de transportes marítimos, terrestres e aéreos realizados com regularidade, segundo itinerários, frequência de viagens, horários e preços previamente definidos;
      (9) Exploração de portos, terminais marítimos, aeroportos e heliportos;
      (10) Radiodifusão televisiva e sonora;
      (11) Exploração de jogos de fortuna e azar em casino;
      (12) Exploração de redes públicas de telecomunicações fixas ou móveis e prestação de serviços de acesso à *internet*;

2.ª versão enviada à AL

2) As sociedades comerciais de capitais exclusivamente públicos;
3) As pessoas colectivas privadas qualificadas de utilidade pública administrativa cuja actividade se cinja à área científica e tecnológica.

Artigo 5.º
Exclusões e isenção

1. O disposto na presente lei não se aplica:
1) Aos serviços, órgãos ou entidades públicos da RAEM que não utilizem redes ou sistemas informáticos, ou que apenas utilizem redes e sistemas cuja cibersegurança constitua responsabilidade de outras entidades públicas, nos termos das disposições dos diplomas orgânicos aplicáveis ou de despacho do Chefe do Executivo;
2) Aos operadores de radiodifusão televisiva e sonora, cuja actividade se cinja à difusão de conteúdos de entretenimento.

2. O Chefe do Executivo, a pedido dos interessados e mediante despacho, pode isentar do cumprimento dos deveres de cibersegurança os operadores privados de infra-estruturas críticas que:
1) Não exerçam a actividade para a qual tenham sido licenciados, desde que o diferimento do início ou a suspensão da actividade tenha sido antecipadamente comunicado à entidade licenciadora;
2) Não usem sistemas e redes informáticas na sua actividade;
3) Demonstrem que o bom e regular desempenho da sua actividade não depende da permanente operacionalidade dos sistemas e redes informáticos.

CAPÍTULO II
Disposições institucionais

Artigo 6.º
Enquadramento institucional

Integram o sistema de cibersegurança da RAEM:

1) A Comissão para a Cibersegurança, doravante designada por CPC;
2) O Centro de Alerta e Resposta a Incidentes de Cibersegurança, doravante designado por CARIC;
3) As Entidades de supervisão de cibersegurança, doravante designadas por entidades de supervisão.

Artigo 7.º

Comissão para a Cibersegurança

A CPC é o órgão presidido pelo Chefe do Executivo, à qual cabe:

1) Assegurar a actividade referida na alínea 1) do n.º 1 do artigo 3.º;
2) Supervisionar a actividade desenvolvida no âmbito da presente lei pelas demais entidades que integram o sistema de cibersegurança;
3) Propor ao Governo a celebração e revisão de acordos, protocolos ou contratos com entidades públicas ou privadas, da RAEM ou do exterior, que se mostrem adequados à elevação dos padrões de cibersegurança na RAEM.

Artigo 8.º

Centro de Alerta e Resposta a Incidentes de Cibersegurança

1. O CARIC é uma estrutura de natureza técnica especializada em matéria de alerta e resposta a incidentes de cibersegurança, coordenado pela Polícia Judiciária, ao qual cabe:

1) Centralizar a recepção de informações sobre incidentes de cibersegurança;
2) Definir as medidas de cibersegurança previstas na alínea 4) do n.º 1 do artigo 3.º e coordenar a resposta das diversas entidades intervenientes, de modo a evitar ou mitigar os efeitos dos incidentes de cibersegurança;
3) Assegurar e promover a cooperação institucional, incluindo com entidades congéneres do exterior;
4) Adoptar uma classificação dos incidentes de cibersegurança por níveis de gravidade e definir os procedimentos de alerta e resposta de acordo com esses níveis;

5) Monitorizar, em tempo real, o tráfego e as características dos dados informáticos transmitidos entre as redes dos operadores de infra-estruturas críticas e a *internet*, nos termos do disposto na alínea 5) do n.º 1 do artigo 3.º;
6) Emitir alertas sobre incidentes de cibersegurança;
7) Disponibilizar apoio técnico às entidades de supervisão, a pedido destas, no exercício das suas competências.

2. A monitorização referida na alínea 5) do número anterior é efectuada pela Polícia Judiciária e incide exclusivamente sobre a linguagem máquina, não podendo os dados informáticos ser recolhidos ou, por qualquer forma, descodificados.

3. O disposto nos números anteriores não prejudica o regime de competências e de autoridade da Polícia Judiciária.

Artigo 9.º

Entidades de supervisão de cibersegurança

1. As entidades de supervisão são serviços e organismos da Administração Pública aos quais compete, no âmbito das suas atribuições:
1) Zelar pelo cumprimento dos deveres previstos na presente lei e nas normas técnicas, sem prejuízo das competências próprias do CARIC nas situações referidas na alínea 4) do n.º 1 do artigo 3.º;
2) Fiscalizar os planos e acções dos operadores de infra-estruturas críticas relativos à respectiva cibersegurança;
3) Exercer a competência sancionatória prevista na presente lei.

2. As competências referidas no número anterior são exercidas:
1) Pela Direcção dos Serviços de Administração e Função Pública, doravante designada pelos SAFP, relativamente aos operadores públicos de infra-estruturas críticas;
2) Pelas entidades públicas designadas por regulamento administrativo, relativamente aos operadores privados de infra-estruturas críticas.

CAPÍTULO III
Deveres de cibersegurança

Artigo 10.º
Deveres de carácter orgânico

1. Constituem deveres dos operadores privados de infra-estruturas críticas, no âmbito da respectiva organização:

1) Criar unidades de gestão de cibersegurança capazes de executar as respectivas medidas internas de protecção;
2) Dotar as unidades de gestão de cibersegurança com os meios humanos, financeiros, materiais e patrimoniais adequados;
3) Designar o principal responsável pela cibersegurança e respectivo substituto, de entre indivíduos com a idoneidade e experiência profissional adequadas e com residência habitual na RAEM;
4) Diligenciar para que o principal responsável pela cibersegurança e o seu substituto estejam permanentemente contactáveis pelo CARIC;
5) Estabelecer mecanismos de reclamação e denúncia relativas à cibersegurança.

2. Na apreciação da idoneidade, devem ser ponderados quaisquer factos que, pela sua gravidade, frequência ou outras circunstâncias atendíveis, indiciem que a pessoa suscita dúvidas sérias quanto à garantia da cibersegurança.

3. Sem prejuízo do disposto no número anterior, os operadores estão impedidos de designar como principal responsável pela cibersegurança e respectivo substituto, pelos períodos referidos no número seguinte, quem tiver sido condenado, por sentença transitada em julgado, por:

1) Crimes previstos na Lei n.º 2/2009 (Lei relativa à defesa da segurança do Estado);
2) Crimes informáticos ou de falsificação de notação técnica, danificação ou subtracção de notação técnica, devassa por meio de informática, aproveitamento indevido de segredo, violação de segredo de correspondência ou telecomunicações ou violação de segredo profissional;
3) Qualquer outro crime punível com pena de prisão superior a 5 anos.

4. Os períodos de impedimento são de:

1) 5 anos a contar do termo do período de suspensão de execução da pena ou da cessação do cumprimento da pena, ou das respectivas prorrogações, se a condenação foi em pena de prisão igual ou inferior a 5 anos;
2) 10 anos a contar da cessação do cumprimento da pena, ou das respectivas prorrogações, se a condenação foi em pena de prisão efectiva superior a 5 anos.

5. As sentenças proferidas por tribunal do exterior são relevantes para efeitos das alíneas 2) e 3) do nº 3, contanto que, no caso da alínea 3), a conduta em causa também constitua crime nos termos da legislação da RAEM.

6. Os operadores devem solicitar parecer à Polícia Judiciária sobre a idoneidade e eventuais impedimentos relativos às pessoas que pretendam designar como principal responsável pela cibersegurança e o seu substituto.

Artigo 11.º

Deveres de carácter procedimental, preventivo e reactivo

Constituem deveres dos operadores privados de infra-estruturas críticas, em matéria de procedimentos e de prevenção e resposta a incidentes de cibersegurança:

1) Estabelecer um regime de gestão da cibersegurança e respectivos procedimentos operacionais internos;
2) Adoptar, conforme o regime de gestão da cibersegurança e as normas técnicas aplicáveis, medidas internas de protecção, monitorização, alerta e resposta a incidentes de cibersegurança;
3) Informar o CARIC da ocorrência de incidentes de cibersegurança e dar conhecimento do facto à respectiva entidade de supervisão, bem como iniciar, de imediato, as acções de resposta a incidentes graves;
4) Monitorizar e registar o estado de funcionamento da rede.

Artigo 12.º

Deveres de auto-avaliação e relato

Constituem deveres dos operadores privados de infra-estruturas críticas, em matéria de auto-avaliação e relato:

1) Proceder, por si próprios ou através de entidades especializadas, à avaliação da segurança e dos riscos existentes nas suas redes e sistemas;
2) Submeter anualmente à respectiva entidade de supervisão um relatório de cibersegurança, mencionando, designadamente, os eventuais incidentes registados, os resultados da avaliação referida na alínea anterior e as medidas de melhoramento tomadas.

Artigo 13.º

Dever de colaboração

Constituem deveres dos operadores privados de infra-estruturas críticas, bem como dos respectivos administradores, gerentes ou mandatários, em matéria de colaboração com o CARIC e as entidades de supervisão:

1) Permitir a entrada nas suas instalações dos representantes daqueles serviços, facultar-lhes o acesso às suas redes e prestar-lhes as informações que estes solicitem, na medida necessária à verificação do cumprimento dos deveres referidos no artigo 11.º;
2) Prestar o apoio e a colaboração necessários para garantir a boa gestão da cibersegurança.

Artigo 14.º

Deveres dos operadores públicos de infra-estruturas críticas

1. Constituem deveres dos operadores públicos de infra-estruturas críticas:
   1) Designar um responsável pela cibersegurança, de entre o pessoal de direcção e chefia;
   2) Diligenciar pela obtenção dos meios humanos, financeiros, materiais e patrimoniais adequados para o bom funcionamento do respectivo regime de gestão de cibersegurança;

3) Cumprir e fazer cumprir os deveres previstos nos artigos 11.º a 13.º, internamente e no âmbito dos serviços, órgãos ou entidades públicos cuja cibersegurança constitua sua responsabilidade;
4) Monitorizar a execução do contrato de prestação de serviços de cibersegurança celebrado com entidades privadas;
5) Assumir a execução dos serviços de cibersegurança contratados com entidades privadas, em caso de incumprimento por estas do respectivo contrato e sem prejuízo da responsabilidade que lhe vierem a ser imputadas.

2. Os operadores públicos de infra-estruturas críticas que não integrem o CARIC apresentam, anualmente, aos SAFP um relatório de avaliação da segurança e dos riscos existentes nas suas redes e sistemas.

3. A celebração do contrato de prestação de serviços de cibersegurança previsto na alínea 4) do n.º 1 depende de autorização prévia do Chefe do Executivo.

CAPÍTULO IV
Regime sancionatório

Artigo 15.º
Infracções administrativas

1. Sem prejuízo de outra responsabilidade que ao caso couber, a violação, por acção ou omissão, dos deveres previstos nos artigos 10.º a 13.º, é sancionada com multa de 150 000 a 5 000 000 patacas, salvo o disposto no número seguinte.

2. A violação, por acção ou omissão, dos deveres previstos na alínea 4) do n.º 1 do artigo 10.º, na alínea 2) do artigo 12.º, na alínea 2) do artigo 13.º e nas normas técnicas é sancionada com multa de 50 000 a 150 000 patacas.

Artigo 16.º

Responsabilidade por infracções administrativas

A imputação de responsabilidade pelas infracções administrativas previstas no artigo anterior aos operadores de infra-estruturas críticas:

1) Aplica-se às situações em que a cibersegurança é assegurada por terceiros;
2) Não depende da identificação do agente de cuja acção ou omissão resultou a prática da infracção administrativa;
3) Não depende da relação entre o agente, sendo este identificável, e o operador ou o prestador de serviços de cibersegurança por este contratado.

Artigo 17.º

Sanções acessórias

1. Pelas infracções ao disposto nas alíneas 1) a 3) do n.º 1 do artigo 10.º, na alínea 1) do artigo 11.º, na alínea 1) do artigo 12.º e na alínea 1) do artigo 13.º, podem ser aplicadas, isolada ou cumulativamente, as seguintes sanções acessórias:

1) Privação do direito de participar em ajustes directos, consultas restritas ou concursos públicos que tenham por objecto a aquisição de bens ou serviços por serviços, órgãos e entidades públicos;
2) Privação do direito a subsídios ou benefícios concedidos por serviços, órgãos e entidades públicos.

2. As sanções acessórias referidas no número anterior têm a duração máxima de dois anos, contada a partir da data em que a correspondente decisão se tenha tornado inimpugnável.

Artigo 18.º

Advertência

1. Caso se verifique uma irregularidade no cumprimento dos deveres de cibersegurança, a entidade de supervisão pode fixar um prazo para a sua sanação, quando:

1) A irregularidade seja sanável e dela não tenha resultado um perigo significativo para a cibersegurança;
2) Não haja reincidência.

2. Sendo a irregularidade sanada no prazo fixado, a entidade de supervisão pode decidir-se por uma simples advertência ao infractor.

3. A falta de sanação da irregularidade no prazo fixado determina o prosseguimento do procedimento para aplicação das sanções que couberem à infracção.

Artigo 19.º
Reincidência

1. Para efeitos da presente lei, considera-se reincidência a prática de infracção administrativa prevista no artigo 15.º no prazo de um ano após a decisão sancionatória administrativa se ter tornado inimpugnável e desde que entre a prática da infracção administrativa e a da anterior não tenham decorrido mais de cinco anos.

2. Em caso de reincidência, o valor mínimo da multa é elevado de um quarto e o valor máximo permanece inalterado.

Artigo 20.º
Cumulação de infracções administrativas

1. Quando a conduta constitua simultaneamente infracção administrativa aos deveres de cibersegurança e aos previstos noutra legislação, o infractor é punido de acordo com a legislação que estabeleça multa de limite máximo mais elevado.

2. O disposto no número anterior não prejudica a aplicação, isolada ou cumulativamente:

1) Das sanções acessórias previstas para as diversas infracções administrativas;

2) De normas que prevejam a revogação ou suspensão de licenças ou títulos equivalentes ou outras medidas de natureza não sancionatória.

Artigo 21.º

Competência sancionatória

1. Compete às entidades referidas no artigo 9.º, relativamente aos operadores privados de infra-estruturas críticas sujeitos à sua supervisão, instaurar os procedimentos pelas infracções administrativas previstas na presente lei e instruir os respectivos processos.

2. Compete ao responsável máximo da entidade de supervisão determinar a instauração do procedimento sancionatório, designar instrutor e aplicar as sanções.

Artigo 22.º

Cumprimento do dever omitido

Sempre que a infracção resulte da omissão de um dever, a aplicação da sanção e o pagamento da multa não dispensam o infractor do seu cumprimento, se este ainda for possível.

Artigo 23.º

Responsabilidade dos trabalhadores dos operadores públicos de infra-estruturas críticas

1. Sem prejuízo de outra responsabilidade que ao caso couber, os trabalhadores dos operadores públicos de infra-estruturas críticas são disciplinarmente responsáveis pelas infracções aos deveres previstos nos artigos 11.º a 14.º.

2. As infracções disciplinares por violação dos deveres de carácter procedimental, preventivo e reactivo são puníveis com as penas de aposentação compulsiva ou demissão ou com pena de suspensão.

CAPÍTULO V
Disposições transitórias e finais

Artigo 24.º
Módulos de identificação de assinante

1. No prazo de 120 dias a contar da data de entrada em vigor da presente lei, os operadores de redes devem diligenciar no sentido de registar a identidade dos utilizadores de todos os módulos de identificação de assinante vendidos antes daquela data, sem prévia identificação, na modalidade de pré-pagos.

2. Os operadores de rede devem suspender o serviço relativamente aos módulos cujos utilizadores não forneçam os seus dados de identificação até ao termo do prazo referido no número anterior, sem prejuízo da posterior reactivação dos mesmos a partir da data em que os dados de identificação sejam fornecidos.

3. O incumprimento dos deveres previstos nos números anteriores constitui infracção administrativa, sancionada com multa de 50 000 a 150 000 patacas.

4. Compete à Direcção dos Serviços de Correios e Telecomunicações instaurar os procedimentos sancionatórios pela infracção referida no número anterior, designar instrutor e aplicar as sanções.

Artigo 25.º
Identificação de clientes

1. Os operadores de redes devem verificar e registar a identidade dos clientes no momento da celebração de contratos ou da confirmação da prestação de serviços para acesso à *internet*, registo de nomes de domínio ou serviços públicos de telecomunicações fixas ou móveis.

2. O incumprimento do dever previsto no número anterior constitui infracção administrativa, sancionada com multa de 50 000 a 150 000 patacas.

3. É correspondentemente aplicável o disposto no n.º 4 do artigo anterior.

Artigo 26.º

Aditamento à Lei n.º 11/2009

É aditado à Lei n.º 11/2009 o capítulo III-A, denominado "Infracção administrativa", constituído pelos artigos 16.º-A e 16.º-B, com a seguinte redacção:

«Artigo 16.º-A

Conservação e fornecimento de registos de tradução de endereços de rede

1. Os prestadores de serviços de *internet* estão obrigados a conservar, por um ano, os registos de tradução de endereços de rede privada em endereços de rede pública.

2. O incumprimento do dever previsto no número anterior constitui infracção administrativa, sancionada com multa de 50 000 a 150 000 patacas.

3. A autoridade judiciária competente pode, quando necessário, ordenar o fornecimento dos registos referidos no n.º 1, observando-se, para o efeito, o disposto nos n.os 1 a 4 do artigo 15.º.

Artigo 16.º-B

Competência

Compete à Direcção dos Serviços de Correios e Telecomunicações instaurar os procedimentos sancionatórios pela infracção administrativa prevista no n.º 2 do artigo anterior, designar instrutor e aplicar as sanções.»

Artigo 27.º

Regulamentação complementar

O Chefe do Executivo aprova os regulamentos administrativos complementares ou os despachos regulamentares externos que se mostrem necessários à execução da presente lei, nomeadamente em matéria de:

1) Composição, competências e modo de funcionamento da CPC e do CARIC;
2) Designação das entidades de supervisão e dos operadores privados de infra-estruturas críticas abrangidos pelo respectivo poder de supervisão.

Artigo 28.º

Entrada em vigor

A presente lei entra em vigor 180 dias após a sua publicação.

Aprovada em de de 2019.

O Presidente da Assembleia Legislativa, _____

Ho Iat Seng

Assinada em de de 2019.

Publique-se.

O Chefe do Executivo, _____

Chui Sai On