1.ª COMISSÃO PERMANENTE

Parecer n.º 3/VI/2019

Assunto: Análise na especialidade da proposta de lei n.º 20/2018/VI, intitulada «*Lei da cibersegurança*».

I – Introdução

O Governo da Região Administrativa Especial de Macau apresentou, em 12 de Setembro de 2018, a proposta de lei intitulada «Lei da cibersegurança», a qual foi admitida, nos termos regimentais, pelo Despacho do Presidente da Assembleia Legislativa n.º 1265/VI/2018.

A proposta de lei foi apresentada, discutida e votada na generalidade em reunião plenária realizada no dia 18 de Outubro de 2018, tendo sido aprovada por maioria, com vinte e sete votos a favor e três votos contra.

Na mesma data, a proposta de lei foi distribuída a esta Comissão para efeitos de apreciação na especialidade e emissão de parecer até ao dia 18 de Janeiro de 2019, nos termos do Despacho do Presidente da Assembleia Legislativa n.º 1344/VI/2018. No entanto, devido ao facto de estarem a ser analisadas na especialidade outras iniciativas legislativas, a Comissão necessitou de solicitar a prorrogação do prazo concedido pelo Presidente da Assembleia Legislativa para a apreciação na especialidade e apresentação do respectivo

parecer, solicitação que foi gentilmente acolhida.

Para prestar apoio à Comissão na análise na especialidade foram destacados os membros da Equipa de Trabalho "C" da Assessoria, nos termos da Comunicação n.º 30/VI/2018.

A Comissão procedeu à análise da proposta de lei num total de nove reuniões, realizadas nos dias 9 de Novembro de 2018, 7, 9, 11 e 25 de Janeiro, 1 de Fevereiro, 8 de Abril e 7 e 22 de Maio de 2019, tendo contado com a presença de representantes do Governo em sete dessas reuniões. A par das reuniões da Comissão, foram realizadas duas reuniões de trabalho entre as assessorias da Assembleia Legislativa e do Governo com vista ao aperfeiçoamento técnico da proposta de lei, as quais tiveram lugar nos dias 4 e 6 de Março de 2019.

Em 20 de Maio de 2019, o Governo apresentou à Assembleia Legislativa a versão final da proposta de lei, a qual reflecte, em parte, as opiniões expressas no seio da Comissão e a análise técnico-jurídica efectuada pela assessoria da Assembleia Legislativa. Ao longo do presente Parecer, as referências aos artigos são feitas com base na versão final da proposta de lei, excepto quando seja conveniente fazer referência à versão inicial, como tal devidamente identificada.

II – Apresentação

Segundo a Nota Justificativa que acompanha a 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. (...)

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, (...) 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».

O Governo da RAEM levou a cabo uma consulta pública sobre a presente iniciativa legislativa, a qual decorreu entre 11 de Dezembro de 2017 e 24 de Janeiro de 2018, tendo o respectivo Relatório Final sido divulgado em 6 de Setembro de 2018 (disponível em https://www.gss.gov.mo/media/Relatorio_P.pdf). De acordo com este documento, «o público, na generalidade, concorda com o estabelecimento do sistema de protecção da cibersegurança em Macau e algumas pessoas consideram que, com o desenvolvimento de Macau como "cidade inteligente" e a popularização dos pagamentos electrónicos, a criação do sistema de protecção da cibersegurança poderá ajudar Macau a prevenir os ataques cibernéticos que possam causar impactos negativos no funcionamento da sociedade; assim, o público concorda que o Governo proceda, o mais rápido possível, ao aperfeiçoamento das respectivas leis para proteger a população, especialmente para resolver o problema da devassa fácil das informações pessoais. (...) Mais de 87% das opiniões, quer dos sectores, quer do público, consideram que é necessário e urgente estabelecer um sistema de protecção da cibersegurança, apontando que a cibersegurança e configura como pressuposto e garantia da segurança pública e pessoal, pelo que a RAEM se obriga a criar um bom sistema de gestão preventivo, mediante acto legislativo, no intuito de assegurar o normal funcionamento dos sistemas da rede e proteger a confidencialidade e a integridade dos dados da rede».

III – Análise genérica

As tecnologias da informação, em particular a *internet*, são instrumentos fundamentais para o desenvolvimento económico e social e o bem-estar da sociedade. O seu uso no quotidiano da população aumenta, de forma exponencial, as potencialidades da difusão da informação, da comunicação entre pessoas ou do comércio à distância. Contudo, a sua proeminência na sociedade hodierna representa um risco agravado de dependência tecnológica, o qual tem necessariamente reflexos a nível da segurança individual e colectiva. As tecnologias da informação estão presentes, muitas vezes de forma imperceptível para a generalidade da população, na garantia do funcionamento normal e eficaz das infra-estruturas que suportam a vida em sociedade: no funcionamento das redes eléctrica, de água ou de transportes, na prestação de cuidados de saúde, no abastecimento alimentar ou na actividade bancária ou financeira. Estes são meros exemplos de sectores altamente dependentes da operacionalidade de redes e sistemas informáticos, os quais necessitam de ser protegidos contra o risco de actos, intencionais ou não, que afectem ou reduzam a sua operacionalidade.

1. Conceito de cibersegurança

O conceito de segurança[1] abrange, hoje em dia, a segurança informática ou cibernética, isto é, a cibersegurança. Esta, genericamente considerada como a capacidade de controlar o acesso a sistemas informáticos interligados e à informação neles contida,[2] visa proteger a

[1] «*Condição relativa de protecção na qual se é capaz de neutralizar ameaças discerníveis contra a existência de alguém ou de alguma coisa*», Marco Cepik, «Segurança Nacional e Segurança Humana: Problemas conceituais e consequências políticas», in *Security and Defense Studies Review*, Vol. 1, Washington, 2001, p. 2, citado no Parecer n.º 4/II/2002, da 2.ª Comissão Permanente da II Legislatura da Assembleia Legislativa, relativo à *Lei de Bases da Segurança Interna da Região Administrativa Especial de Macau* (Lei n.º 9/2002).

[2] Jennifer L. Bayuk *et al.*, *Cyber Security Policy Guidebook*, Wiley & Sons, New Jersey, 2012, p. 1.

vivência da sociedade que opera para além das dimensões humana e física, às quais corresponde a protecção de pessoas e bens. De facto, «no mundo globalizado de hoje, em que se procura o acesso a grandes quantidades de informação em tempo útil, o ciberespaço constitui uma dimensão crítica do funcionamento normal da sociedade moderna, da sua segurança, da sua economia, dos seus negócios, etc. A necessidade de acesso e troca permanente de informação tem inerentemente associada critérios de segurança, uma vez que esta informação deve ser protegida contra acessos ou modificações não autorizados».[3] A cibersegurança visa proteger o valor intrínseco das redes e sistemas informáticos e dos dados que neles estão contidos ou que neles circulam,[4] o qual vai além de um mero valor económico, tendo igualmente relevância ao nível do exercício de direitos fundamentais, como por exemplo o direito à privacidade. Essa protecção depende, em primeiro lugar, da arquitectura da rede, *i.e.* da forma como as redes e sistemas informáticos são concebidos e desenhados, e do grau de vulnerabilidade que comportam. Mas depende também de um conjunto de medidas legislativas adequadas (tanto de natureza penal como administrativa), de instrumentos de defesa tecnológica (nomeadamente, sistemas de encriptação, *firewalls*, mecanismos de autenticação e anti-intrusão, aplicações anti-vírus e instrumentos que impeçam a negação de serviço[5]), da existência de uma cultura organizacional, tanto das empresas como dos governos, conducente à salvaguarda do bom funcionamento das redes e sistemas informáticos e dos dados informáticos neles contidos. Depende, ainda, da

[3] Fernando Freire e Paulo Viegas Nunes, «Estratégia da Informação e Segurança no Ciberespaço», in *IDN Cadernos*, n.º 12, 2013, p. 10.

[4] Quanto à definição de cibersegurança adoptada pela Organização Internacional de Normalização *vd.* 皮勇 (Pi Yong), *Research on Cyber-Security Law*, Research Centre for Criminal Law of Wuhan University, People's Public Security University of China, Pequim, 2008, p. 341.

[5] Exemplificação constante do artigo 2.º, n.º 1, alínea 1), da versão inicial da proposta de lei. Sobre a natureza e modo de funcionamento dos diferentes meios de defesa tecnológica, *vd.* James Graham, Richard Howard e Ryan Olson (eds.), *Cyber Security Essentials,* CRC Press, Boca Raton, 2011, pp. 1-69.

consciência ou sensibilidade pessoal sobre a importância da segurança informática.[6]

O valor estratégico do ciberespaço potencia ataques destinados a comprometer o normal funcionamento da sociedade ou a retirar benefícios económicos ilícitos da informação nele partilhada. A resposta do poder público a estes ataques informáticos, consubstanciados no acesso ou modificação não autorizados à informação constante das redes e sistemas informáticos, passa amiúde pela criminalização de tais actos não autorizados, tal como aconteceu na RAEM com a aprovação da Lei de combate à criminalidade informática (Lei n.º 11/2009). Contudo, independentemente do seu enquadramento penal, o risco de ataques informáticos requer a existência de mecanismos que, na prática, evitem a sua ocorrência ou, não sendo tal possível, que possibilitem a sua detecção atempada e uma resposta rápida, de natureza técnica, para a sua neutralização e redução do seu impacto negativo.[7] O sistema de cibersegurança que a presente iniciativa legislativa vem estabelecer visa, precisamente, criar o enquadramento institucional adequado para que tal resposta seja possível e eficaz. A sua criação assenta no conceito legal de cibersegurança: nos termos da alínea 1) do n.º 1 do artigo 2.º, a cibersegurança é entendida como uma «*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*».

[6] Por exemplo, no momento de escolher uma palavra-chave segura. *Vd.* Jennifer L. Bayuk *et al.*, *ob. cit.*, pp. 7-13.

[7] *Vd.* Nathan Alexander Sales, «Regulating Cyber-Security», in *Northwestern University Law Review*, Vol. 107, 2013, pp. 1546-1552.

2. *Sistema de cibersegurança da RAEM: características e enquadramento institucional*

O sistema de cibersegurança da RAEM assenta em três características fundamentais: *i)* a identificação dos sectores-chave para o normal funcionamento da sociedade e cuja protecção urge garantir; *ii)* o estabelecimento de instrumentos legais de cooperação institucional entre entidades públicas e privadas no âmbito da cibersegurança; e *iii)* o seu carácter eminentemente preventivo e técnico.

2.1. Em primeiro lugar, importa realçar o facto de o sistema ora criado visar, tão-só, a protecção das redes e sistemas informáticos considerados essenciais para o normal funcionamento da sociedade. Assume particular relevo, portanto, o conceito de *infra-estruturas críticas*, ou seja, «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» [artigo 2.°, n.° 1, alínea 3)]. Tal como referido na Nota Justificativa que acompanha a proposta de lei, «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». Daqui resulta uma delimitação negativa do âmbito de aplicação da futura lei: os mecanismos de protecção decorrentes da presente iniciativa apenas beneficiam as redes e sistemas informáticos das entidades, públicas ou privadas, que operam infra-estruturas críticas – *e só estas*. De igual forma, os deveres ora consagrados apenas incumbem aos operadores dessas infra-estruturas críticas – *e só a estes*.

A identificação dos sectores essenciais para o normal funcionamento da sociedade abrange toda a Administração Pública, assim como os sectores listados no n.º 3 do artigo 4.º da proposta de lei. Desta forma, a Lei da cibersegurança não é uma lei que se destina à generalidade da população e a todas as redes e sistemas informáticos da RAEM, mas tão-só àquelas consideradas como infra-estruturas críticas e aos seus operadores. Tal como referido no Relatório Final da consulta pública, «a "Lei da Cibersegurança", de acordo com a intenção legislativa subjacente, visa constituir, sempre tendo em conta a "salvaguarda da segurança da população e respeito da privacidade pessoal", um sistema de gestão eficaz e destinado às infra-estruturas críticas, para prevenir e reduzir um eventual impacto na sociedade de Macau resultante de ataques cibernéticos» (p. 15).

O artigo 4.º da proposta de lei prevê a existência de dois tipos de operadores de infra-estruturas críticas: operadores públicos e operadores privados. Em princípio, todas as entidades públicas são consideradas como operadores públicos de infra-estruturas críticas e as redes, sistemas e dados informáticos por si utilizados são alvo de protecção (artigo 4.º, n.º 2). Contudo, excluem-se desta classificação e do âmbito de aplicação da futura lei os «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» [artigo 5.º, n.º 1, alínea 1)]. Por seu turno, os operadores privados de infra-estruturas críticas são, de acordo com o previsto no n.º 3 do artigo 4.º, de três tipos:

i. As sociedades comerciais de capitais exclusivamente públicos;

ii. As pessoas colectivas de utilidade pública administrativa cuja actividade se cinja à área científica e tecnológica;

iii. As entidades de direito privado que, a título de concessão de exploração, de prestação

de serviços à Administração ou de licenciamento, alvará ou título de idêntica natureza, exerçam actividade nos sectores de:

- Abastecimento de água;
- Actividade bancária, financeira e seguradora;
- Prestação de cuidados de saúde em hospitais;
- Tratamento de águas residuais e recolha e tratamento de resíduos;
- Abastecimento público grossista de combustíveis e de produtos alimentares sujeitos a controlos sanitários e fitossanitários;
- Abate de animais em matadouros legais;
- Fornecimento e distribuição de electricidade e gás natural;
- Prestação de serviço público de transporte marítimo, terrestre e aéreo regular;
- Exploração de portos, terminais marítimos, aeroportos e heliportos;
- Radiodifusão televisiva e sonora (excepto se a actividade se cingir à difusão de conteúdos de entretenimento[8]);
- Exploração de jogos de fortuna e azar em casino;
- Exploração de redes públicas de telecomunicações fixas ou móveis;
- Prestação de serviços de acesso à *internet*.

O Governo informou a Comissão que estão preliminarmente identificados 117 operadores privados de infra-estruturas críticas, espalhados pelos diferentes sectores, com especial destaque para o sector da actividade bancária, financeira e seguradora (64 entidades). Esta lista, sujeita a actualização constante, foi trazida ao conhecimento da Comissão e será divulgada, após a aprovação da presente proposta de lei, através da regulamentação complementar, nos termos da alínea 2) do artigo 27.º.

[8] Exclusão prevista no artigo 5.º, n.º 1, alínea 2).

2.2. Em segundo lugar, o sistema de cibersegurança é caracterizado pelo facto de conjugar o natural papel de liderança reservado à RAEM, enquanto entidade que visa salvaguardar o interesse colectivo, com o envolvimento de diversas entidades públicas e privadas na prossecução das finalidades subjacentes à presente iniciativa legislativa e ao sistema ora criado. Faz-se, assim, apelo à cooperação institucional entre os órgãos que compõem o sistema de cibersegurança e os operadores, públicos e privados, de infra-estruturas críticas. São estes que têm o dever de cumprir os diversos deveres previstos na proposta de lei, em particular o dever de alertar as entidades vocacionadas para gerir a resposta a incidentes de cibersegurança. Há, portanto, uma partilha de responsabilidades ao nível da cibersegurança entre as entidades públicas de gestão do respectivo sistema criadas ao abrigo desta lei (nomeadamente a Comissão para a Cibersegurança[9] e o Centro de Alerta e Resposta a Incidentes de Cibersegurança), as entidades públicas que passam a assumir novas competências ao nível da supervisão no âmbito da cibersegurança e os operadores de infra-estruturas críticas. Tal partilha pressupõe um esforço colectivo e cooperativo entre diversos sectores da sociedade, com o objectivo de protegê-la dos efeitos nefastos decorrentes de incidentes de cibersegurança.

A nível institucional, o sistema divide-se em diversos níveis e prevê a existência de diferentes intervenientes:

i. A ***Comissão para a Cibersegurança***, a qual é o órgão de topo, de natureza essencialmente política, ao qual compete a definição de orientações e objectivos de carácter geral e estratégico com vista à prossecução das finalidades da cibersegurança (artigo 7.º, n.º 1). Este órgão é presidido pelo Chefe do Executivo.

[9] A Comissão para a Cibersegurança era designada na versão inicial da proposta de lei como Comissão Permanente para a Cibersegurança.

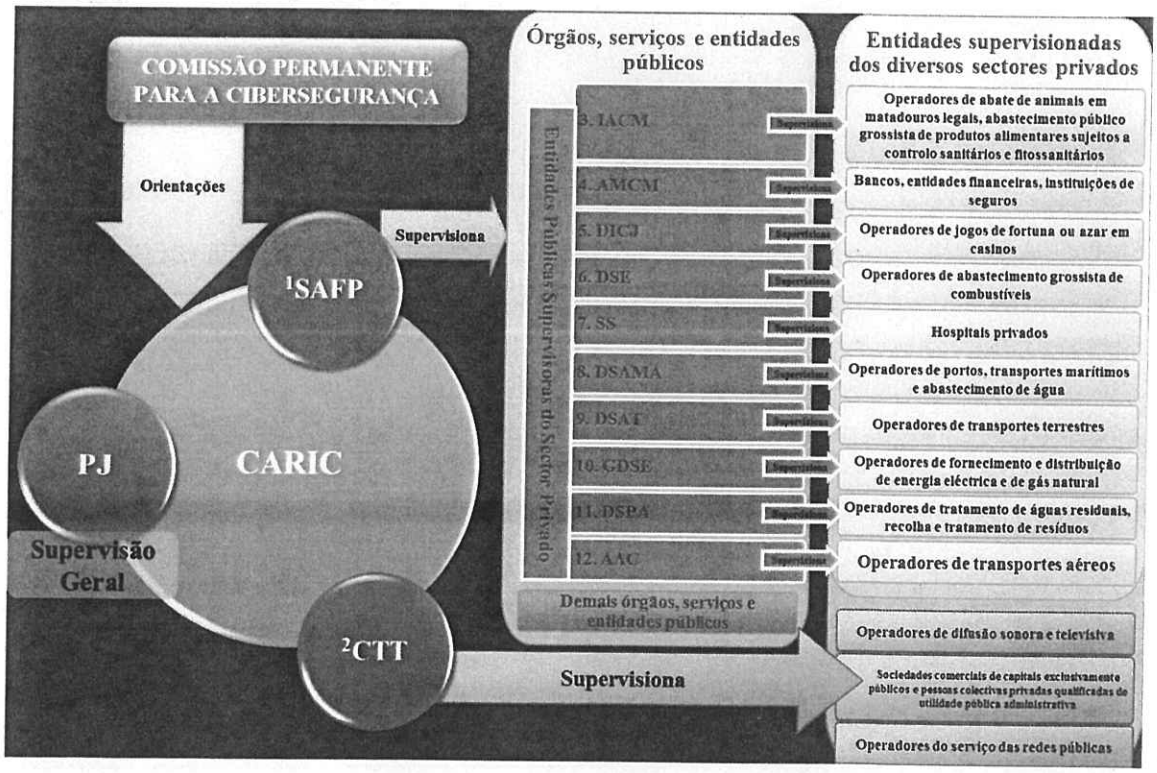
ii. O ***Centro de Alerta e Resposta a Incidentes de Cibersegurança*** (CARIC), o qual é uma estrutura de natureza técnica especializada (não é, portanto, um órgão administrativo inserido na estrutura da Administração Pública) especialmente vocacionada para gerir e executar medidas de resposta aos incidentes de cibersegurança. O CARIC está pensado como uma entidade de gestão da resposta a incidentes de cibersegurança. Assim, cabe-lhe, em especial, centralizar a recepção de informações sobre incidentes de cibersegurança; definir as medidas excepcionais para dar resposta a incidentes de cibersegurança, em especial quando ocorram ou estejam eminentes incidentes graves; coordenar a resposta das diversas entidades intervenientes, de modo a evitar ou mitigar os efeitos dos incidentes de cibersegurança; 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*; e emitir alertas sobre incidentes de cibersegurança. A sua vocação técnica leva a que seja a entidade capaz de disponibilizar assistência especializada quando outros intervenientes no sistema dela necessitem. O CARIC é coordenado pela Polícia Judiciária.

iii. As ***entidades de supervisão de cibersegurança***, as quais são 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. Prevê-se que os SAPF façam a supervisão dos demais operadores públicos de infra-estruturas críticas e que os operadores privados sejam «supervisionados por 11 serviços públicos relacionados com as áreas de actividade envolvidas ou a natureza desses operadores».[10]

[10] Relatório final da consulta pública, ponto 4.3, p. 26.

iv. Os ***operadores de infra-estruturas críticas***, aos quais incumbe o cumprimento dos deveres previstos no Capítulo III da (proposta de) lei e que são as entidades que, em primeira linha, têm a incumbência de se protegerem de eventuais incidentes de cibersegurança, detectá-los e neutralizá-los, ainda que, para tal, possam socorrer-se do auxílio do CARIC e das respectivas entidades de supervisão. Os operadores de infra-estruturas críticas não integram, em rigor, a estrutura orgânica do sistema de cibersegurança da RAEM (note-se que não constam do artigo 6.º), mas são elementos fundamentais do funcionamento desse sistema.

Enquadramento institucional do sistema de cibersegurança da RAEM



Fonte: *Governo da RAEM – Relatório Final da Consulta Pública (2018)*

A Comissão esforçou-se por clarificar a relação institucional entre as diferentes entidades que integram o sistema de cibersegurança. Pretendeu-se reforçar a estrutura piramidal do sistema e o papel cimeiro que cabe à Comissão para a Cibersegurança nesse sistema. Assim, na versão final da proposta de lei foi previsto que a Comissão para a Cibersegurança tem competência para «supervisionar a actividade desenvolvida no âmbito da presente lei pelas demais entidades que integram o sistema de cibersegurança» [artigo 7.º, n.º1, alínea 2)] e que ao CARIC compete «disponibilizar apoio técnico às entidades de supervisão, a pedido destas, no exercício das suas competências» [artigo 8.º, n.º1, alínea 7)].

Por outro lado, a Comissão ponderou a opção legislativa de atribuir o poder de supervisão a onze entidades diferentes, tanto mais que o poder em causa implica competências regulatória (artigo 3.º, n.º 2) e sancionatória (artigo 21.º). A preocupação manifestada no seio da Comissão foi que o grande número de entidades de supervisão pudesse levar a situações de aplicação desigual da lei, a uma falta de harmonia aquando da emissão das normas técnicas e até uma atitude de desresponsabilização pela aplicação da futura Lei da cibersegurança. Foi sugerido que estas situações poderiam ser evitadas caso existisse uma entidade centralizadora das funções de supervisão, que adoptasse critérios uniformes a nível regulatório e sancionatório. O proponente, pelo contrário, considerou ser mais adequado proceder à supervisão através dos serviços especializados dos respectivos domínios por causa da especificidade de cada tipo das infra-estruturas críticas, em vez de o ser de forma centralizada através de uma única entidade de supervisão. Por outro lado, defendeu que as competências de coordenação política atribuídas à Comissão para a Cibersegurança e as competências de cooperação técnica atribuídas ao CARIC são bastantes para assegurar a necessária padronização na execução da lei.

2.3. A terceira característica que urge realçar relaciona-se com o tipo de intervenção levada a cabo ao abrigo do sistema ora estabelecido. Tal intervenção é de natureza essencialmente técnica, de carácter preventivo e independente do desvalor jurídico que se atribua aos actos que visa prevenir.

A protecção das redes, sistemas e dados informáticos dos operadores de infra-estruturas críticas é feita através de soluções técnicas adoptadas pelos próprios operadores. São estes que têm o dever de criar as necessárias condições técnicas, humanas, organizacionais e processuais para prevenir, detectar e neutralizar eventuais incidentes de cibersegurança, ainda que possam contar com o apoio e coordenação das entidades públicas que integram o sistema. Esta resposta técnica é, portanto, independente do tratamento que o ordenamento jurídico dá aos actos não autorizados que constituem um incidente de cibersegurança. Se tais actos constituem ou não ilícitos penais é algo que não tem resposta na presente iniciativa legislativa, mas antes noutras leis vigentes no ordenamento jurídico local, nomeadamente na Lei de combate à criminalidade informática (Lei n.º 11/2009). Desta forma, a presente iniciativa legislativa vem completar o edifício jurídico da RAEM ao nível da prevenção de ataques informáticos, conjugando a prevenção técnica, que sairá reforçada com o sistema de cibersegurança ora estabelecido, com a prevenção, geral e especial, associada ao direito penal e à lista de crimes informáticos constante da Lei n.º 11/2009. De acordo com as explicações prestadas à Comissão pelo proponente, «a proposta de lei cria um sistema de gestão administrativa que visa assegurar a cibersegurança da RAEM, definindo os deveres e as responsabilidades dos operadores das infra-estruturas críticas. A "Lei da cibersegurança" é um diploma que visa a 'protecção', 'prevenção' e 'gestão'; quanto aos ilícitos criminais que envolvem as áreas de *internet*, informações e computadores, mantêm-se regulados na "Lei de combate à criminalidade informática". A "Lei da cibersegurança" tem como objecto as medidas preventivas (a tomar *a anteriori*, portanto) que visam a gestão preventiva da cibersegurança das infra-estruturas críticas (...). A "Lei de Combate à

Criminalidade Informática" é uma lei penal relativa aos crimes informáticos e cibernéticos, ou seja, as diligências de investigação criminal são efectuadas após a prática dos crimes».

3. *Salvaguarda dos direitos fundamentais*

A Comissão ponderou a relação desta iniciativa legislativa com o exercício e gozo de determinados direitos fundamentais da população de Macau. Isto porquanto a proposta de Lei da cibersegurança tem suscitado dúvidas em alguns sectores da sociedade quanto ao seu impacto ao nível da liberdade de expressão e o sigilo das comunicações, entre outros. O Relatório final da consulta pública deu notícia da existência da «preocupação de que o Governo possa aproveitar (...) a 'Lei da cibersegurança" para legalizar a vigilância cibernética, a qual poderá prejudicar os direitos dos cidadãos, nomeadamente a liberdade de expressão e o sigilo das comunicações».[11] A preocupação identificada aquando da consulta pública foi igualmente manifestada no decurso da análise da proposta de lei na Assembleia Legislativa, tanto na generalidade como na especialidade. Ela manifestou-se em duas vertentes: ao nível da possibilidade de monitorização de dados informáticos; e ao nível das competências da Polícia Judiciária.

3.1. A liberdade e o sigilo das telecomunicações são protegidos pelo artigo 32.º da Lei Básica, nos termos do qual «nenhuma autoridade pública ou indivíduo poderá violar a liberdade e o sigilo dos meios de comunicação dos residentes, sejam quais forem os motivos, excepto nos casos de inspecção dos meios de comunicação pelas autoridades competentes, de acordo com as disposições da lei, e por necessidade de segurança pública ou de investigação em processo criminal». De igual forma, a liberdade de expressão e a privacidade estão

[11] Relatório final da consulta pública, ponto 1, p. 15.

salvaguardadas na mesma Lei. Nestes termos, o sistema de cibersegurança da RAEM e as medidas adoptadas no seu âmbito têm *necessariamente* de respeitar as garantias dos direitos fundamentais constantes da Lei Básica. Não é demais relembrar que, tal como estatuído no parágrafo 2.º do artigo 11.º da Lei Básica, «nenhuma lei, decreto-lei, regulamento administrativo ou acto normativo da Região Administrativa Especial de Macau pode contrariar esta Lei».

O proponente teve oportunidade de reiterar a intenção legislativa subjacente à proposta de lei nesta matéria. Em primeiro lugar, afirmando o respeito pela privacidade pessoal enquanto princípio fundamental do ordenamento jurídico, em geral, e da futura Lei de cibersegurança, em particular. Em segundo lugar, esclarecendo que «a "Lei da cibersegurança" tem como objecto as medidas (...) que visam a gestão preventiva da cibersegurança das infra-estruturas críticas, sendo que as mesmas não [interferirão] nem prejudicarão os direitos fundamentais dos residentes, nomeadamente a liberdade de expressão, a privacidade pessoal e a liberdade de imprensa». O proponente teve ainda a oportunidade de esclarecer que, «quanto à questão da existência ou não violação da privacidade dos cidadãos, (...) o pessoal do CARIC e das entidades de supervisão não pode obter quaisquer dados pessoais directamente ou mediante o recurso à técnica de recuperação dos datagramas, informações relativas aos sectores ou conteúdo das comunicações, sob pena de o pessoal responsável pela supervisão assumir as responsabilidades penais e responsabilidades decorrentes da infracção administrativa previstas na Lei n.º 8/2005 (Lei da Protecção de Dados Pessoais), Lei n.º 11/2009 (Lei de combate à criminalidade informática) e Código Penal, bem como as responsabilidades disciplinares previstas no ETAPM. Quando reunidos os pressupostos, poderão assumir responsabilidade civil, em conformidade com o estabelecido no Código Civil».

A preocupação com a salvaguarda dos direitos, liberdades e garantias fundamentais da população foi particularmente evidente aquando da análise das normas que prevêem a possibilidade de ser feita 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 [artigo 3.º, n.º 1, alínea 5)]. Esta monitorização, que é feita em tempo real pela Polícia Judiciária,[12] incide exclusivamente sobre a linguagem máquina ou binária, procedendo à análise do volume e as características do tráfego entre as redes dos operadores de infra-estruturas críticas e a *internet* [artigo 8.º, n.º 1, alínea 5), e n.º 3].

A monitorização ora permitida fica limitada aos dados de tráfego, excluindo o acesso ao conteúdo das comunicações. Tal como afirmado pelo Secretário para a Segurança aquando da apresentação da proposta de lei na reunião plenária do dia 18 de Outubro de 2018, «no futuro, aquando da execução da lei, os serviços responsáveis apenas poderão avaliar, nos termos legais, a dimensão do fluxo dos dados informáticos e os diferentes tipos de riscos de segurança produzidos por ataques à rede, por forma a emitir alertas e instruções para garantir a segurança da rede, não exercendo, nem podendo exercer, actividade de fiscalização sobre os conteúdos na rede, pelo que, de modo nenhum, poderão constituir restrição, privação ou até prejuízo para a liberdade de expressão da população. Na realidade, no pressuposto da cibersegurança, a liberdade de comunicação e a privacidade dos cidadãos tornar-se-ão mais eficazmente protegidas pela lei e, a não ser que seja autorizado pelo órgão judicial, os serviços estão impedidos de interferir em qualquer conteúdo na rede, não podendo fazer a descodificação dos conteúdos nos dados que nela fluem».

[12] A monitorização dos dados informáticos transmitidos entre as redes dos operadores de infra-estruturas críticas e a *internet* é uma competência atribuída ao CARIC, a qual é exercida, em concreto, pela Polícia Judiciária (artigo 8.º, n.º 3).

A Comissão ponderou e acolheu as explicações, de facto e de direito, dadas pelo proponente para justificar que a futura Lei da cibersegurança não terá um impacto negativo nos direitos, liberdades e garantias fundamentais da população, em particular na liberdade de expressão e no sigilo das comunicações. Reconhece-se que o acesso aos dados de tráfego pode, em abstracto, levar à detecção de padrões de conduta e à construção do perfil do utilizador, ainda que isso não aconteça na prática,[13] e que tais dados devem estar protegidos pelas garantias legais da inviolabilidade das comunicações.[14] Razão pela qual, a Comissão considerou importante que a redacção do articulado reflectisse, de forma inequívoca, a intenção legislativa e consagrasse as garantias necessárias para dissipar eventuais dúvidas quanto ao respeito devido aos direitos fundamentais. Assim, a Comissão diligenciou no sentido de ser expressamente prevista no articulado a proibição de recolha ou descodificação dos dados informáticos sujeitos a monitorização, i.e., a proibição de acesso ao conteúdo das comunicações[15] (artigo 8.º, n.º 2, *in fine*). Este aditamento representa uma garantia adicional de que a Lei da cibersegurança não será um instrumento de controlo do conteúdo das comunicações e da liberdade de expressão no ciberespaço.

A Comissão reitera a importância da conjugação do reforço da cibersegurança, enquanto garantia do bem-estar, segurança e ordem públicas, com a salvaguarda dos direitos fundamentais. Crê-se, à semelhança do afirmado pelo proponente em diversas ocasiões, que

---

[13] O Governo afirmou à Comissão que «sobre esta matéria, é importante realçar que a inspecção do fluxo de dados de informações e as características dos datagramas é feita de uma forma corrente, não se conservando nenhum dado, nem se efectuando qualquer registo de informação envolvendo conteúdos com informações ou comunicações de dados pessoais e sectoriais. Por esta razão, é praticamente impossível ao pessoal do [CARIC] e das entidades supervisoras obter, directamente ou através da técnica de recuperação de datagramas, os dados pessoais, as informações sectoriais ou o conteúdo de comunicação».

[14] *Vd.* António Manuel Abrantes, «O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações», *Revista do Ministério Público*, n.º 156, 2018, pp. 162-163.

[15] A monitorização dos dados informáticos fará um exame de segurança dos datagramas que passam em tempo real, tais como o fluxo de dados, o destino, as características dos datagramas, visando identificar anomalias ou sinais de ataques invasivos, não sendo a monitorização efectuada sobre os conteúdos dos dados.

o ordenamento jurídico da RAEM tem os mecanismos administrativos, civis e penais adequados para reagir contra eventuais aplicações abusivas da Lei da cibersegurança, que atentem contra os direitos, liberdades e garantias dos cidadãos. Em resposta a perguntas da Comissão, o proponente esclareceu que «os mecanismos para fazer efectivar esses diferentes tipos de responsabilidade estão abertos aos cidadãos, seja por via da normal impugnação administrativa, seja através de queixa ao Ministério Público e/ou ao CCAC, ou através de acções judiciais próprias *(por exemplo, acção para reconhecimento de direitos ou interesses legalmente protegidos, acção para determinação da prática de actos administrativos legalmente devidos, acção para efectivação de responsabilidade civil extracontratual)*».

3.2. De acordo com a proposta de lei, a Polícia Judiciária (PJ) integra e coordena o CARIC; efectua a monitorização dos dados informáticos transmitidos entre as redes dos operadores de infra-estruturas críticas e a *internet*; e emite parecer sobre a idoneidade dos candidatos a exercer as funções de principal responsável pela cibersegurança, bem como do respectivo substituto.

A Comissão ponderou as funções atribuídas à PJ no âmbito do sistema de cibersegurança. Em particular, ponderou a preponderância deste órgão de polícia criminal, o qual tem como atribuições a prevenção e a investigação criminal, bem como a coadjuvação das autoridades judiciárias,[16] no contexto de um diploma legal que, segundo reconhecido pelo próprio proponente, «regula especificadamente a gestão administrativa da segurança da rede, uma lei com objectivos de protecção, prevenção e gestão, que regula de forma administrativa as condições que as infra-estruturas críticas devem preencher para enfrentar as questões relativas à cibersegurança». A Comissão questionou o proponente sobre as razões de política legislativa subjacentes ao papel da PJ no sistema de cibersegurança, e se o mesmo

[16] *Vd.* artigo 2.º, n.º 1, da Lei n.º 5/2006 (Polícia Judiciária).

poderia alterar inintencionalmente a natureza administrativa do sistema, dando-lhe um cunho mais policial.

O Governo esclareceu que a sua opção teve como referência os sistemas de cibersegurança de diferentes jurisdições e que, em muitos deles, é atribuída a órgãos policiais a competência de monitorizar a segurança da rede para além dos devidos trabalhos policiais, como como acontece com as polícias da China continental e de Hong Kong. Em Macau, «a PJ, enquanto entidade principal que aplica a Lei de combate à criminalidade informática, tem acompanhado a situação da segurança da rede local e durante as investigações e acções de combate aos casos associados à segurança da rede ocorridos em Macau tem acumulado uma grande experiência». Ademais, a PJ tem a capacidade técnica necessária para monitorizar a segurança da rede, tendo vindo a formar pessoal qualificado e experiente nos domínios da segurança da rede e da informática forense. Neste âmbito, a PJ, «ao longo dos anos, tem enviado funcionários para participar em seminários, acções de formação e troca de experiências relativas à cibersegurança, realizadas em diferentes jurisdições vizinhas. Nesse enquadramento, foi-se criando uma rede de partilha e de experiências e de adequada quantidade de pessoal qualificado e com capacidade, que são indispensáveis no âmbito da segurança da rede, acreditando-se que esses aspectos são extremamente importantes para a questão de como fazer, com eficácia e com recurso a meios técnicos, a prevenção e detecção precoce de eventuais problemas gerais relacionados com a segurança da rede de Macau. No que diz respeito à resposta atempada, perante os constantes incidentes de ataque à segurança da rede ocorridos, nos últimos anos, em toda a parte do mundo, uma vez que esses ataques foram realizados de forma transfronteiriça e complexa e eram bem dissimulados e sendo as provas fáceis de se alterar e de se perder, é necessário que haja uma estreita ligação entre as fases inicial, média e final dos incidentes; desde a detecção dos sinais do ataque até à investigação criminal, a intervenção deve ter uma ligação estreita, para que a resposta e o rastreamento sejam eficazes quando houver ataque à segurança da rede, sendo nesse aspecto

que se demonstra plenamente a relação de complementação entre a Lei da cibersegurança e a Lei de combate à criminalidade informática». Por estas razões, o proponente disse acreditar que as funções atribuídas à PJ, nomeadamente para executar a monitorização dos dados informáticos pelo CARIC, irão produzir efeitos positivos na criação e funcionamento do sistema de cibersegurança local.

A Comissão foi sensível ao argumento da capacidade técnica que a PJ já possui no domínio da segurança informática, adquirida ao abrigo da execução da Lei n.º 11/2009. Por outro lado, a concentração na PJ da função de monitorização permite que o número de pessoas e entidades envolvidas nesta actividade seja limitado, o que contribui para diminuir os riscos inerentes a eventuais e indesejadas violações da privacidade dos dados pessoais. Acolheu-se, portanto, a opção legislativa subjacente à proposta de lei. Contudo, a Comissão considerou não se justificar que a PJ fosse chamada a dar parecer sobre a experiência profissional do principal responsável pela cibersegurança dos operadores de infra-estruturas críticas e do respectivo substituto, tal como decorria da alínea 2) do n.º 1 do artigo 10.º da versão inicial da proposta de lei. Considerou-se que a experiência profissional não carece de parecer obrigatório, ainda que não vinculativo, e que não compete a um órgão policial fazer a avaliação da competência técnica de profissionais que os operadores de infra-estruturas críticas pretendem contratar. Assim, na versão final, o parecer da PJ foi limitado à questão da idoneidade e de eventuais impedimentos das pessoas que se pretende designar como principal responsável pela cibersegurança e respectivo substituto (artigo 10.º, n.º 6). Este parecer é, nos termos do n.º 2 do artigo 91.º do Código do Procedimento Administrativo, *obrigatório* e *não vinculativo*. Ou seja, o parecer tem de ser pedido (tal como previsto no n.º 6 do artigo 10.º), mas as suas conclusões não têm de ser seguidas por quem o pede. Caso os operadores não peçam o parecer da PJ, incorrem em infracção administrativa, nos termos do n.º 1 do artigo 15.º.

4. Deveres de cibersegurança

A elevação dos padrões de cibersegurança na RAEM pressupõe que os operadores de infra-estruturas críticas adoptem um conjunto de medidas de protecção contra eventuais ataques informáticos. A adopção dessas medidas é feita em nome do interesse pessoal da entidade em causa, muitas vezes de natureza económica, em que as suas redes e sistemas informáticos funcionem adequadamente e que os respectivos dados informáticos sejam protegidos. Neste sentido, o Relatório final da consulta pública deu conta da existência de opiniões segundo as quais a responsabilidade da garantia da cibersegurança pertence aos próprios operadores de infra-estruturas críticas, devendo o poder público abster-se de intervir na gestão destas entidades, muitas das quais de cariz empresarial. Contudo, a relevância social das infra-estruturas em causa – que, recorde-se, correspondem aos sectores nucleares da sociedade – conduz a que exista, a par do interesse individual referido, um interesse colectivo em que todos os operadores de infra-estruturas críticas tenham mecanismos eficazes de protecção das suas redes, sistemas e dados informáticos. Isto porque a vulnerabilidade de um desses operadores pode ter impacto negativo noutros operadores e, consequentemente, na sociedade em geral. Assim, a proposta de lei vem introduzir um conjunto de deveres de cibersegurança que os operadores de infra-estruturas críticas, públicos e privados, ficam obrigados a cumprir a partir da sua entrada em vigor. Estes deveres visam generalizar uma cultura de cibersegurança, criando os instrumentos legais e institucionais para que haja uma uniformização de padrões de segurança, uma coordenação na resposta a incidentes de cibersegurança, assim como uma maior acessibilidade às soluções técnicas para prevenir e combater tais incidentes.

De acordo com a Nota Justificativa que acompanha a proposta de lei, o capítulo III, relativo aos deveres de cibersegurança, «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 proposta de lei prevê para os operadores privados de infra-estruturas críticas um conjunto de deveres de carácter orgânico (artigo 10.º); de carácter procedimental, preventivo e reactivo (artigo 11.º); de auto-avaliação e relato (artigo 12.º); e de colaboração (artigo 13.º). Os deveres dos operadores públicos estão consagrados no artigo 14.º.

4.1. Os deveres de cibersegurança têm aplicação ao nível da organização interna dos operadores privados de cibersegurança. De acordo com o disposto no artigo 10.º, aqueles têm de criar unidades próprias para tratar das questões da cibersegurança e dotá-las com os recursos humanos, financeiros, materiais e patrimoniais adequados ao seu funcionamento. Ao nível dos recursos humanos, é de realçar o dever de nomeação de uma pessoa com experiência profissional específica como principal responsável pela cibersegurança de cada operador privado, bem como do respectivo substituto. Estas pessoas devem ter residência habitual na RAEM e estar sempre contactáveis pelo CARIC para, em caso de necessidade, poderem activar as medidas internas de protecção face a um ataque informático eminente ou que já esteja em curso.[17]

[17] Segundo a Nota Justificativa, «a criação do cargo de "principal responsável [pela] 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».

Para além de se exigir que o principal responsável pela cibersegurança e respectivo substituto tenham a experiência profissional adequada ao cargo, a proposta de lei exige que eles tenham a idoneidade para o exercício das funções. A natureza sensível da cibersegurança, tanto ao nível da importância dos sectores nos quais se encontram as infra-estruturas críticas, como ao nível da protecção dos dados pessoais, justificam que se exija que as pessoas responsáveis por esta área sejam moralmente íntegras. O n.º 2 do artigo 10.º determina que «na apreciação da idoneidade, devem ser ponderados quaisquer factos que, pela sua gravidade, frequência ou outras circunstâncias atendíveis, suscitem dúvidas sérias quanto à garantia da cibersegurança». Este é um juízo de valor sobre a correcção moral dos candidatos levado a cabo pelos operadores privados no momento da selecção das pessoas para o exercício das funções em causa, bem como pela PJ aquando da emissão do respectivo parecer. Três situações existem, contudo, que implicam *necessariamente* a falta de idoneidade:

i. A condenação por crimes previstos na Lei relativa à defesa da segurança do Estado (Lei n.º 2/2009);

ii. A condenação por 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;

iii. A condenação por qualquer outro crime punível com pena de prisão superior a 5 anos.

Nestes casos, a lei presume – de forma inilidível – que a natureza dos crimes pelos quais o agente foi condenado, ou a gravidade da moldura penal abstracta associada a tais crimes, são demonstrativos da falta da correcção moral necessária para o exercício de funções com tamanha relevância. Razão pela qual, quem tenha sido condenado por estes crimes não pode ser nomeado como principal responsável pela cibersegurança ou respectivo substituto (artigo

10.º, n.º 3). Este regime de impedimentos foi clarificado aquando da apreciação na especialidade da proposta de lei, tendo sido reforçada a natureza absoluta do impedimento derivado da condenação pelos crimes previstos no n.º 3 do artigo 10.º. Contudo, uma vez que as penas não podem ter como efeito necessário a perda de direitos profissionais (artigo 60.º, n.º 1, do Código Penal), sentiu-se a necessidade de delimitar temporalmente tal impedimento legal, criando-se um regime especial de reabilitação de direito ligeiramente diferente do disposto no artigo 24.º do Decreto-Lei n.º 27/96/M, de 3 de Junho. Assim, o n.º 4 do artigo 10.º passou a prever que os períodos de impedimento são de:

i. 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, caso a condenação tenha sido pena de prisão igual ou inferior a 5 anos;

ii. 10 anos a contar da cessação do cumprimento da pena, ou das respectivas prorrogações, caso a condenação tenha sido pena de prisão efectiva superior a 5 anos.

A Comissão manifestou preocupação com uma eventual escassez de profissionais locais na área da cibersegurança. O cumprimento dos deveres de carácter orgânico, nomeadamente o dever de dotar as unidades de gestão de cibersegurança com os meios humanos adequados e o dever de nomear o principal responsável pela cibersegurança e o respectivo substituto, pode ser dificultado pela insuficiência de pessoas para desempenar tais funções de natureza técnica e altamente especializada. O Governo mostrou sensibilidade para a questão, tendo afirmado ter vindo a reforçar a formação de quadros nesta área, nomeadamente na PJ e através do intercâmbio e cooperação com serviços homólogos da China continental. É intenção do Governo aprofundar a sua estratégia de formação, não descartando a possibilidade de contratação no exterior de profissionais capazes de suprir a insuficiência de recursos humanos locais, tanto para o sector público, como para o sector privado.

4.2. Os deveres de carácter procedimental, preventivo e reactivo (artigo 11.º) visam dotar os operadores privados de infra-estruturas críticas de um regime de gestão da cibersegurança e respectivos procedimentos operacionais internos. Este regime deve prever a forma como as medidas internas de protecção, definidas através de normas técnicas, são aplicadas *na prática*, para que seja efectuada a monitorização, alerta e resposta aos incidentes de cibersegurança. O artigo 11.º prevê, ainda, deveres de comunicação da ocorrência de incidentes ao CARIC e às entidades de supervisão, sem prejuízo de o operador dever, de imediato, iniciar as acções de resposta a incidentes graves. A nível preventivo, os operadores devem controlar o estado de funcionamento das suas redes informáticas, nomeadamente através de testes e de actualização de *software*, a fim de assegurar a sua inviolabilidade e a manutenção dos adequados padrões de segurança.

4.3. Segundo a Nota Justificativa, «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». A avaliação da segurança e dos riscos existentes nas redes e sistemas informáticos dos operadores privados pode ser efectuada pelos próprios ou ser confiada a entidades terceiras que, a título comercial, procedam a tal avaliação.

4.4. O dever de colaboração previsto no artigo 13.º «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 (...). 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».[18]

A Comissão questionou o proponente sobre o âmbito da colaboração exigida aos operadores privados, nomeadamente no que diz respeito ao acesso do CARIC e das entidades de supervisão às instalações e equipamentos dos operadores. Deu-se nota de uma preocupação relativa ao potencial impacto de tal acesso na privacidade pessoal, no sigilo das comunicações, profissional ou comercial, bem como na liberdade de imprensa, uma vez que os operadores de radiodifusão televisiva e sonora estão abrangidos pelo âmbito subjectivo de aplicação da Lei da cibersegurança [artigo 4.º, n.ºs 1 e 3, alínea 1), subalínea (10)].

O Governo esclareceu que tal acesso só pode ser solicitado por representantes daquelas entidades devidamente credenciados e que se destina à verificação do cumprimento dos deveres de carácter procedimental, preventivo e reactivo. Isto é, os representantes do CARIC e das entidades de supervisão podem solicitar o referido acesso para fiscalizar se o operador está a adoptar as medidas internas de protecção, monitorização, alerta e resposta a incidentes de cibersegurança. Esta possibilidade é particularmente relevante, segundo a explicação dada à Comissão, quando o CARIC actua no âmbito da execução de medidas de cibersegurança excepcionais, nos termos do previsto na alínea 2) do n.º 1 do artigo 8.º, a fim de evitar ou mitigar os efeitos dos incidentes de cibersegurança, em particular os incidentes graves. Nestes casos, os elementos do CARIC devem poder aceder às instalações e equipamentos dos operadores para se assegurar que as medidas técnicas estão a ser efectiva e correctamente aplicadas.

[18] Nota Justificativa.

O proponente garantiu à Comissão que o poder de acesso às instalações e equipamentos é apenas para efeitos da fiscalização dos deveres previstos no artigo 11.º, não podendo ser usado para efeitos de verificação do cumprimento de outros deveres ou de outros aspectos da actividade dos operadores. A fiscalização do cumprimento dos demais deveres é feita pelas entidades de supervisão através da solicitação de informações aos operadores, as quais podem ter de ser comprovadas documentalmente.

4.5. Operadores públicos estão igualmente sujeitos aos deveres de cibersegurança. Os deveres consagrados no artigo 14.º são semelhantes aos deveres previstos para os operadores privados, ainda que a lei lhes introduza algumas especificidades decorrentes da natureza pública das entidades em causa. No geral, os deveres de cibersegurança aplicam-se em igualdade para os operadores públicos e privados: a alínea 3) do n.º 1 deste artigo, manda aplicar aos operadores públicos, por remissão, os deveres previstos nos artigos 11.º a 13.º para os operadores privados. Aqueles devem cumpri-los e fazê-los cumprir «internamente e no âmbito dos serviços, órgãos ou entidades públicos cuja cibersegurança constitua sua responsabilidade» [artigo 14.º, n.º 1, alínea 3)].

4.6. Uma última nota para referir a possibilidade legal de os operadores de infra-estruturas críticas delegarem a responsabilidade de execução das medidas de cibersegurança em terceiros, contratados para o efeito.

Relativamente aos operadores privados de infra-estruturas críticas, a alínea 1) do artigo 12.º permite que a avaliação da segurança e dos riscos existentes nas redes e sistemas informáticos dos operadores privados seja feita através de entidades especializadas; e a alínea 1) do artigo 16.º prevê, em geral, que a cibersegurança dos operadores privados possa ser assegurada por terceiros. Quando tal aconteça, os operadores privados não ficam isentos da responsabilidade infraccional prevista na lei. Ou seja, 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).

Relativamente aos operadores públicos de infra-estruturas críticas, a alínea 4) do n.º 1 do artigo 14.º prevê a existência de contratos de prestação de serviços de cibersegurança celebrados entre os operadores públicos e entidades privadas, mediante autorização prévia do Chefe do Executivo (artigo 14.º, n.º 3). Neste caso, a existência de um contrato de prestação de serviços não isenta a entidade pública de monitorizar a sua execução, devendo assumir a execução dos mesmos em caso de incumprimento das entidades privadas, sem prejuízo das responsabilidades que lhe vierem a ser imputadas [alíneas 4) e 5) do n.º 1 do artigo 14.º]. A proposta de lei prevê, ainda, que a cibersegurança de um serviço, órgão ou entidade pública seja, nos termos dos respectivos diplomas orgânicos ou de despacho do Chefe do Executivo, responsabilidade de outras entidades públicas. Caso em que o serviço, órgão ou entidade estão excluídos do âmbito de aplicação da Lei da cibersegurança [artigo 5.º, n.º 1, alínea 1)]. Um dos exemplos fornecidos à Comissão é o do Gabinete do Secretário para a Segurança, cuja cibersegurança é assegurada pela Direcção dos Serviços das Forças de Segurança de Macau.[19]

5. *Medidas de segurança complementares*

A proposta de lei vem introduzir regulação ao nível da obrigatoriedade de identificação dos clientes de serviços de telecomunicações e da conservação e fornecimento de registo de tradução de endereços de rede. Estas são «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».[20]

[19] Nos termos da alínea 8) do artigo 2.º do Regulamento Administrativo n.º 9/2002 (Organização e funcionamento da Direcção dos Serviços das Forças de Segurança de Macau).

[20] Nota Justificativa.

5.1. O artigo 25.º vem impor a obrigatoriedade de os operadores de redes de comunicações verificarem e registarem a identidade dos seus clientes no momento da celebração de contratos ou da confirmação da prestação de serviços de acesso à *internet*, serviços de registo de nomes de domínio ou serviços públicos de telecomunicações fixas ou móveis. O artigo 24.º resolve, 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. Através destes dois artigos, o ordenamento local consagra uma política de identificação dos utilizadores de serviços de telecomunicações móveis (*Real-Name System*), o qual visa dissuadir a utilização de módulos de identificação de assinante (cartões SIM) usados em terminais telefónicos móveis para finalidades criminosas.

O Relatório final da consulta pública[21] esclarece que, «de acordo com a situação actual do sector de telecomunicações em Macau, excepto quanto aos cartões pré-pagos, os utentes dos serviços telefónicos fixos e móveis têm de fazer registo com a prestação dos dados de identificação verdadeiros. O "*Real-Name System*" visa impor às pessoas que adquirem cartões pré-pagos que disponibilizem esses dados para efeitos do registo, prevenido que os criminosos utilizem esses cartões não nominais como instrumento para escapar à investigação criminal, de forma a melhor salvaguardar a ordem pública e garantir os direitos e interesses legítimos dos cidadãos em geral. Por conseguinte, a solicitação aos utentes de cartões pré-pagos dos dados é uma exigência básica e, aliás, uma regra comum nos negócios jurídicos. Noutros países, esta regra para proteger o interesse social já foi implementada».

A Comissão acolhe esta medida de política legislativa e considera-a importante para combater a criminalidade informática e a criminalidade praticada através de meios de comunicações. Sem prejuízo de o anonimato proporcionado pelas tecnologias da informação

[21] Página 41.

poder trazer benefícios ao nível da liberdade de expressão,[22] ele pode favorecer a prática de determinados crimes, como burla, extorsão, difamação ou acesso indevido a dados pessoais, entre outros.[23] Assim, importa garantir que a política de identificação ora adoptada é um instrumento de combate à criminalidade sem conduzir a um enfraquecimento da privacidade dos utilizadores, nem a um controlo ilegítimo dos conteúdos. O proponente assegurou que o regime introduzido pelos artigos 24.º e 25.º vem, apenas, alargar aos utilizadores de cartões SIM as regras já vigentes para os utentes de telefone fixo e de telemóvel. O proponente afirmou que «no que diz respeito à venda de cartões pré-pagos por operadores de telecomunicações em colaboração com lojas, as operadoras de telecomunicações e as lojas de venda de cartões pré-pagos devem cumprir a Lei de protecção de dados pessoais sobre a conservação de informações, caso contrário, serão legalmente responsabilizados. O incumprimento das normas legais, nesta matéria, é sancionado, conforme os casos, em termos de infracção administrativa (artigos 30.º a 36.º da Lei n.º 8/2005) ou infracção criminal (artigos 37.º a 42.º da Lei n.º 8/2005), a que podem acrescer certas sanções

[22] *Vd.* Jyh-An Lee e Ching-Yi Liu, «Real-Name Registration Rules and the Fading Digital Anonymity in China», in *Washington International Law Journal*, Vol. 25, No. 1, 2016, pp. 4-10; Song Guangxing e Yang Pingfang, «The Influence of Network Real-name System on the Management of Internet Public Opinion», in *Public Administration in the Time of Regional Change - Proceedings of the Second International Conference on Public Management (ICPM 2013)*, 2013, pp. 47-53.

[23] De acordo com o afirmado pelo Governo à Comissão, «mesmo que não haja uma estatística formal sobre os dados do crime relativo a cartões pré-pagos e cartões SIM do exterior, de acordo com a situação das investigações efectuadas ao longo dos anos e o *modus operandi* utilizado, os cartões pré-pagos, que não necessitam do registo de nome verdadeiro e são bastante baratos, são amplamente usados aquando da prática de crimes como, "estações emissoras simuladas", "burlas telefónicas", "extorsões telefónicas" e "*nude chat*", o que dificulta as investigações. De facto, a PJ descobriu que muitos criminosos compram uma grande quantidade de cartões pré-pagos em Macau e que alguns deles [utilizam] estes cartões pré-pagos para burlar os chineses que vivem no exterior. Esta situação é bastante grave. Para além disso, os criminosos podem fazer com que os códigos telefónicos não representem a origem verdadeira das chamadas através da falsificação dos números telefónicos; por outro lado, segundo as investigações, os números telefónicos do exterior utilizados aquando da prática do crime, na realidade, vêm de cartões pré-pagos de Macau, e vice-versa. Por conseguinte, a implementação do *Real-Name System* em Macau pode produzir efeitos no combate, caso contrário, a Região será mais facilmente usada para praticar crimes».

acessórias, para ambos os casos (artigos 43.º e 44.º da mesma Lei)».

A Comissão questionou, ainda, a forma como esta política vai ser executada, preocupando-se com a maneira como a identificação dos utentes vai ser verificada. O proponente esclareceu que relativamente ao procedimento operacional do *Real-Name System* para cartões telefónicos pré-pagos será de considerar a opção pelo modo da certificação electrónica, que é a forma mais fácil para os utentes.

5.2. A segunda medida de segurança complementar consta do artigo 26.º e respeita à obrigatoriedade de conservação e fornecimentos de registos de tradução de endereços de rede (*network address translation*). Segundo o aditamento à Lei n.º 11/2009 (Lei de combate à criminalidade informática) ora efectuado, os prestadores de serviços de *internet* passam a estar obrigados a conservar, por um ano, os registos de tradução de endereços de rede privada em endereços de rede pública.

Para que a *internet* funcione é preciso que cada aparelho com acesso à rede seja identificado com um código numérico, que permite que os dados possam ser emitidos e recebidos adequadamente e que se possa ter acesso à informação. Na quarta versão do protocolo de *internet* (IPv4), actualmente em uso, os endereços IP são compostos por 32 *bits*, o que faz com que exista um número relativamente pequeno de combinações possíveis para tais endereços.[24] Enquanto esta situação não for colmatada com a generalização do IPv6, o qual introduz endereços IP compostos por 128 *bits*, é necessário limitar o número de endereços que funcionem como pontos de acesso à rede. Assim, permite-se que diversos aparelhos que façam parte de uma rede privada (cada qual com o seu próprio endereço IP privado) partilhem um mesmo endereço IP público quando necessitem de enviar ou receber dados na rede. Para tal, faz-se a tradução de endereços de rede privada em endereços de rede

[24] O IPv4 sustenta aproximadamente 4,29 biliões de endereços IP em todo o mundo

pública através dos *router*. Esta necessidade prática e técnica resultante das limitações do IPv4 faz com que os endereços de rede privada sejam de mais difícil conhecimento quando seja necessário identificar um aparelho, i.e. um endereço IP, específico, nomeadamente no âmbito de uma investigação criminal. A conservação de registos de tradução de endereços de rede destina-se a permitir uma mais fácil identificação do terminal com acesso à *internet* envolvido na prática de um crime informático e, assim, chegar à identificação do agente em causa. Não se destina, portanto, ao conhecimento dos comportamentos praticados por via electrónica ou das páginas visitadas pelos utilizadores.

A consagração da obrigatoriedade de registos de tradução de endereços de rede é feita através de um aditamento à Lei de combate à criminalidade informática. Deste facto resulta uma limitação do âmbito da utilização destes registos: a autoridade judiciária pode ordenar que os prestadores de serviços de *internet* forneçam tais registos, nos termos do artigo 15.º da Lei n.º 11/2009, no âmbito da investigação e nos actos processuais relativos a processos por crimes previstos na referida lei e por crimes cometidos por meio do sistema informático, assim como na recolha de prova em suporte electrónico pela prática de qualquer crime. Ou seja, na investigação de um destes crimes, os órgãos de polícia criminal só podem obter os registos da tradução de endereços de rede após a autorização do juiz, nos termos da lei processual penal.

A Comissão considera justificada a consagração da obrigatoriedade de conservação e fornecimentos de registos de endereços de rede, tendo em vista as necessidades de investigação da criminalidade informática ou cometida por meio de sistema informático, bem como da obtenção e recolha de provas em suporte electrónico. Considera, igualmente, que estão garantidos os mecanismos jurídicos para a salvaguarda da privacidade da população, o que acontece através da aplicação subsidiária do Código de Processo Penal.

IV – Análise na especialidade

Para além da apreciação genérica apresentada no ponto anterior, a análise efectuada na Comissão teve como propósito, nos termos do artigo 119.º do Regimento da Assembleia Legislativa, apreciar a adequação das soluções concretas aos princípios subjacentes à proposta de lei e assegurar a perfeição técnico-jurídica das disposições legais. Das questões analisadas na Comissão e das alterações introduzidas no articulado, cumpre destacar as seguintes:

- **Artigo 1.º - Objecto e finalidade**

Na versão inicial da proposta de lei, o artigo relativo ao objecto estava redigido de uma forma extensa, o que dificultava a sua compreensão, e era repetitivo face a outras normas. Assim, foi feito um esforço no sentido da simplificação da redacção normativa, eliminando-se elementos constantes das definições do artigo 2.º. Por outro lado, clarificou-se a finalidade da lei: a protecção das redes, sistemas e dados informáticos dos operadores de infra-estruturas críticas. Com esta redacção, faz-se uma referência expressa aos bens jurídicos que merecem tutela com a presente lei. No seguimento desta clarificação, considerou-se adequado alterar a epígrafe do artigo, a qual passou a ser "objecto e finalidade" para melhor reflectir o conteúdo do mesmo.

Versão inicial	Versão final
Artigo 1.º **Objecto** A presente lei estabelece o sistema de cibersegurança da Região Administrativa Especial de Macau, doravante designada por RAEM, e regula o seu funcionamento, com o objetivo de salvaguardar os interesses públicos especialmente relevantes, tais como o bem-estar, a segurança ou ordem pública, através de intenficação da segurança cibernética dos operadores de infra-estruturas críticas.	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**

O artigo das definições sofreu várias alterações. Desde logo, procedeu-se a uma reordenação das definições, passando a constar em primeiro lugar a definição de "cibersegurança", enquanto conceito nuclear de toda a proposta de lei.

N.º 1, alínea 1): Eliminou-se a exemplificação dos meios de prevenção,[25] por considerar-se não ser necessária a sua previsão legal. Trata-se de soluções técnicas que estão sujeitas a permanente evolução. Ademais, tais soluções serão previstas nas normas técnicas, emitidas ao abrigo do disposto na alínea 2) do n.º 1 e no n.º 2 do artigo 3.º.

N.º 1, alínea 2): A definição de "redes informáticas" constante da versão inicial suscitou dúvidas quanto à sua precisão técnica. A resolução de tais dúvidas passou pelo recurso a definições utilizadas a nível internacional,[26] o que, crê-se, facilitará a cooperação

[25] «(...) através de instrumentos tecnicamente adequados, tais como sistemas de encriptação, "*firewalls*", mecanismos de autenticação e anti-intrusão, em geral, aplicações anti-vírus e instrumentos que impeçam a negação de serviço (...)»

[26] Nomeadamente, a definição de "rede e sistema de informação" constante da alínea a) do artigo 4.º da Directiva (EU) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de Julho de 2016.

internacional na área da cibersegurança, desenvolvida ao abrigo da alínea 3) do n.º 1 do artigo 7.º.

N.º 1, alínea 3): Na definição de "infra-estruturas críticas", a expressão «perda de função» constante da versão inicial foi substituída por «suspensão de funcionamento ou diminuição significativa da eficiência» para indicar que pode existir prejuízo para a sociedade quando as redes e sistemas, não estando totalmente inutilizados, apenas se encontrem diminuídos na sua capacidade de processamento, o que afecta a eficácia dos serviços prestados. Nesta alínea foi, ainda, eliminada a expressão «independentemente da natureza pública ou privada dos respectivos operadores», por a mesma constar da definição de "operadores de infra-estruturas críticas", evitando-se uma repetição desnecessária.

N.º 1, alínea 5): A redacção da definição de "acto não autorizado" foi revista no sentido de fazer a ligação com os actos que constituem crimes informáticos, previstos e punidos pela Lei n.º 11/2009. Tal ligação resulta da utilização dos conceitos de «acesso, obtenção, utilização, disponibilização, intercepção, dano ou outro tipo de interferência».

N.º 1, alínea 6): Na definição de "incidente de cibersegurança" foi eliminada a referência a «tentativa de acto», por forma a excluir do âmbito do conceito situações de menor gravidade que, sendo tentativas de intercepções de tráfego ou de propagação de programas maliciosos, não causam danos substanciais às redes e sistemas informáticos. A expressão «efeito real adverso», inspirada na legislação europeia, permite restringir o âmbito do conceito definido, excluindo-se actos que apenas causem danos diminutos à segurança das redes e sistemas informáticos.

N.º 2: A alínea 2) do artigo 2.º da versão inicial definia "sistema informático" e "dados informáticos" por remissão para as definições constantes na Lei de combate à criminalidade informática. Uma vez que, de um ponto de vista técnico, esta remissão não corresponde a definições em sentido próprio, optou-se por dar-lhe um tratamento diferenciado. Assim, o

artigo das definições foi separado em dois números, passando a constar do n.º 2 a remissão para as definições de "sistema informático" e "dados informáticos" constantes da Lei n.º 11/2009. Esta remissão tem a desvantagem de levar o aplicador da lei a utilizar dois instrumentos legais para obter as definições legais dos conceitos em causa. Contudo, apresenta as vantagens de evitar uma duplicação normativa e de garantir que os conceitos usados em ambas as leis têm o mesmo conteúdo. Assim, caso seja necessário, no futuro, alterar estas definições, tal alteração é feita somente na Lei n.º 11/2009, não sendo necessário alterar a Lei da cibersegurança.

Versão inicial	Versão final
Artigo 2.º **Definições** Para efeitos da presente lei, entende-se por: 1) «Redes informáticas», o dispositivo ou dispositivos que integram um sistema informático, as redes que suportam a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, trocados ou transmitidos por tais dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção; 2) «Sistema informático» e «dados informáticos», os sistemas e dados previstos na Lei n.º 11/2009 (Lei de Combate à Criminalidade Informática); 3) «Cibersegurança», a actividade permanente e plurisectorial desenvolvida pela RAEM com o objectivo de preservar a operacionalidade, integridade e disponibilidade das redes e dos sistemas informáticos utilizados pelos operadores de infra-estruturas críticas, bem como a confidencialidade dos dados	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) «Redes informáticas»: (1) Os dispositivos ou sistemas informáticos interligados; (2) As redes de comunicações electrónicas, através das quais se processa a interligação de dispositivos e sistemas informáticos, designadamente as redes de telecomunicações referidas na Lei n.º

informáticos, e de prevenir através de instrumentos tecnicamente adequados, tais como sistemas de encriptação, "*firewalls*", mecanismos de autenticação e anti-intrusão, em geral, aplicações anti-vírus e instrumentos que impeçam a negação de serviço, que tais redes, sistemas e dados sejam prejudicados ou por qualquer forma afectados por actos não autorizados; 4) «Infra-estruturas críticas», patrimónios, redes e sistemas, que se consideram relevantes para o interesse da sociedade e para o seu funcionamento normal, independentemente da natureza pública ou privada dos respectivos operadores, e cujo dano, revelação dos dados ou perda da função é susceptível de causar prejuízos graves para o bem-estar, a segurança ou ordem públicas ou para outro interesse público especialmente relevante; 5) «Operadores das infra-estruturas críticas», entidades, públicas ou privadas, que operam infra-estruturas críticas e que prestam serviços ligados às mesmas; 6) «Acto não autorizado», qualquer tipo de comportamento que se consubstancie no acesso ou interferência não consentidos nem permitidos pelos proprietários das redes ou dos sistemas informáticos ou por titulares do direito dessas redes ou sistemas; 7) «Incidente de cibersegurança», qualquer situação que configure um acto ou uma tentativa de acto não autorizado; 8) «Operadores de redes», as entidades habilitadas a explorar redes públicas de telecomunicações fixas ou móveis e a prestar serviços de acesso à *internet*.	14/2001 (Lei de Bases das Telecomunicações); (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**

A redacção deste artigo foi alterada no sentido de fazer menção expressa à emissão de normas técnicas enquanto parte integrante da actividade de cibersegurança. Assim, a nova alínea 2) do n.º 1 faz referência à «emissão de normas técnicas vinculativas para os operadores de infra-estruturas críticas». Esta forma de regulação técnica visa «definir processos e mecanismos de segurança das redes, sistemas e dados informáticos» (n.º 2, 1.ª parte) e, segundo o proponente, irão concretizar os padrões ISO/IEC 27000 da Organização Internacional de Normalização e da Comissão Electrotécnica Internacional. As normas técnicas assumem a forma de *circulares*, quando têm como destinatários a generalidade dos operadores de infra-estruturas críticas, e de *instruções*, quando dirigidas a categorias específicas de operadores (n.º 2, 2.ª parte). Por regra, as normas técnicas são publicadas no Boletim Oficial da RAEM, excepto quando tenham natureza reservada, caso em que são entregues aos destinatários directamente ou por via postal (n.º 3). A competência para a emissão destas normas é conferida a qualquer entidade que integra o sistema de cibersegurança da RAEM, designadamente a Comissão para a Cibersegurança, o CARIC e as (onze) entidades de supervisão. Parte do regime relativo às normas técnicas constava da alínea 2) do n.º 1 do artigo 11.º da versão inicial.

Na alínea 5) do n.º 1 foi incluída parte das normas relativas à monitorização dos dados informáticos. Considerou-se que a delimitação material deste poder devia ser efectuada aquando da sua primeira previsão legal, dado o seu carácter geral. Assim, a expressão relativa

à finalidade da monitorização («com a finalidade de prevenir, detectar e combater incidentes de cibersegurança») foi transposta da alínea 3) do n.º 2 do artigo 8.º da versão inicial para a actual alínea 5) do n.º 1 do artigo 3.º, tendo-se feito uso do conceito de «incidentes de cibersegurança» e abdicado de utilizar a expressão «ataques e invasões cibernéticos» para evitar a introdução de nova terminologia legal.

Versão inicial	Versão final
Artigo 3.º **Actividade de cibersegurança** A actividade de cibersegurança é prosseguida mediante: 1) A definição de orientações, objectivos de ordem geral e de estratégias com vista à prossecução das finalidades da cibersegurança; 2) A implementação, pelos operadores de infra-estruturas críticas, dos deveres e medidas de cibersegurança de rotina definidos na presente lei e nas instruções ou circulares emitidas pelas entidades de supervisão; 3) A implementação de deveres e de medidas de cibersegurança excepcionais, que visem a resposta a incidentes de cibersegurança, em especial nos casos de incidentes graves; 4) A monitorização dos dados relativos à cibersegurança dos operadores de infra-estruturas críticas; 5) A fiscalização do efectivo cumprimento dos deveres e medidas de cibersegurança e a instauração dos correspondentes procedimentos sancionatórios.	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 obtenção de adequados padrões de 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 informáticas 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**

N.º 1: A redacção do n.º 1 visa, de uma forma clara e sucinta, identificar os dois tipos de sujeitos desta lei: os operadores públicos e os operadores privados de infra-estruturas críticas. Por outro lado, clarifica-se que a norma diz respeito ao âmbito de aplicação da lei («a presente lei aplica-se aos...») e não, tal como decorria da versão inicial, à sujeição aos deveres de cibersegurança («estão sujeitos aos deveres de cibersegurança»).

N.º 2: A versão inicial previa que «todos os serviços, órgãos e entidades públicos da RAEM» são considerados operadores públicos de infra-estruturas críticas, fornecendo exemplos adicionais de entidades públicas incluídas na regra geral. Esta redacção suscitou dúvidas, tendo sido alterada sem que o seu âmbito sofresse modificação. Assim, mantendo-se o princípio geral segundo o qual todas as entidades públicas são consideradas como operadores públicos de infra-estruturas críticas, a sua enumeração, por grupos, consta tão-só das alíneas do n.º 2. Tal princípio geral está reflectido, em particular, na forma abrangente como está redigida a alínea 2) do n.º 2: «os serviços públicos da RAEM».

Na alínea 1) foi eliminada a referência aos gabinetes do Comissariado Contra a Corrupção e do Comissariado da Auditoria por já estarem ambos abrangidos pelo conceito de titulares dos principais cargos, nos termos da Lei Básica e do Regulamento Administrativo n.º 24/2010 (Estatuto dos titulares dos principais cargos da Região Administrativa Especial de Macau). Por outro lado, foi eliminada a referência aos serviços de apoio administrativo dos gabinetes dos titulares dos principais cargos por não existir, nos termos do Regulamento Administrativo n.º 14/1999 (Estatuto do Gabinete do Chefe do Executivo e dos Secretários), uma separação formal entre tais gabinetes e os respectivos serviços de apoio administrativo.

N.º 3, alínea 3): A proposta de lei considera as pessoas colectivas de utilidade pública administrativa como operadores privados de infra-estruturas críticas. Na versão inicial, esta norma estava consagrada na subalínea (3) da alínea 2) do artigo 4.º. Contudo, a intenção legislativa era – e continua a ser – que nem todas as pessoas colectivas de utilidade pública administrativa estejam sujeitas à aplicação da lei, mas apenas aquelas cuja actividade seja relevante para efeitos de cibersegurança. Esta opção legislativa tinha expressão, na versão inicial, através de uma norma de exclusão: a alínea 3) do n.º 1 do artigo 5.º excluía do âmbito de aplicação da lei «as pessoas colectivas privadas qualificadas de utilidade pública administrativa nos termos legais, cujas finalidades se relacionam com as actividades filantrópicas, assistenciais, educativas, culturais e/ou recreativas». Esta delimitação negativa do âmbito de aplicação da lei suscitou dúvidas aquando da análise na especialidade. Em primeiro lugar, por a expressão «cujas finalidades se relacionam...» consagrar um critério diferente do critério da "prossecução dos fins" consagrado no n.º 1 do artigo 3.º da Lei n.º 11/96/M, de 12 de Agosto (Declaração de utilidade pública administrativa), o que resulta num critério ambíguo, uma vez que as pessoas colectivas podem ter finalidades relacionadas com mais do que uma das actividades indicadas; em segundo lugar, por a terminologia utilizada na descrição das finalidades não ser inteiramente coincidente com a da Lei n.º

11/96/M, de 12 de Agosto, o que levantava a questão de saber se se pretendia consagrar categorias diferentes das previstas no referido diploma legal; por fim, por ser do conhecimento da Comissão que o proponente pretende que a Lei da cibersegurança seja aplicada, de momento, apenas a duas pessoas colectivas de utilidade pública administrativa que prosseguem fins de investigação científica e tecnológica. Assim, por forma evitar dúvidas sobre o âmbito de aplicação da futura lei optou-se por fazer uma delimitação positiva, determinando-se que apenas as pessoas colectivas de utilidade pública administrativa cuja actividade se cinja à área científica e tecnológica caiem no âmbito subjectivo de aplicação da Lei da cibersegurança.

Procedeu-se, ainda, à uniformização terminológica entre a proposta de lei e outros diplomas legais, nomeadamente a Lei n.º 11/96/M, de 12 de Agosto. Assim, o conceito legal «pessoa colectiva de utilidade pública administrativa» substituiu a expressão «pessoas colectivas privadas qualificadas de utilidade pública administrativa nos termos legais».

Versão inicial	Versão final
Artigo 4.º **Âmbito subjectivo de aplicação** Estão sujeitos aos deveres de cibersegurança: 1) Os operadores públicos de infra-estruturas críticas, compreendendo todos os serviços, órgãos e entidades públicos da RAEM, incluindo: (1) O Gabinete do Chefe do Executivo, os gabinetes dos titulares dos principais cargos do Governo e os respectivos serviços de apoio administrativo, os serviços de apoio à Assembleia Legislativa, o Gabinete do Presidente do Tribunal de Última Instância, o Gabinete do Procurador, o Gabinete do Comissariado Contra a Corrupção e o Gabinete do Comissariado da Auditoria; (2) Institutos públicos e fundos autónomos, qualquer que seja a modalidade que estes revistam; (3) Demais serviços e organismos públicos que, embora desprovidos de personalidade jurídica, possuam autonomia patrimonial e financeira; 2) Os operadores privados de infra-estruturas críticas, compreendendo: (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: (i) Abastecimento de água; (ii) Actividades bancária,	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) As entidades de direito privado, com sede na RAEM ou no exterior, habilitadas a exercer actividades nos domínios a seguir especificados, 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

financeira e seguradora; (iii) Prestação de cuidados de saúde em hospitais; (iv) Tratamento de águas residuais, recolha e tratamento de resíduos; (v) Abastecimento público grossista em geral de combustíveis e de produtos alimentares sujeitos a controlos sanitários e fitossanitários; (vi) Abate de animais em matadouros legais; (vii) Fornecimento e distribuição de electricidade e gás natural; (viii)Prestação de serviço público de transportes marítimos, terrestres e aéreos realizados com regularidade, segundo itinerários, frequência de viagens, horários e preços previamente definidos; (ix) Exploração de portos, terminais marítimos, aeroportos e heliportos; (x) Difusão televisiva e sonora; (xi) Exploração de jogos de fortuna e azar em casino; (xii) Exploração de redes públicas de telecomunicações fixas ou móveis e prestação de serviços de acesso à *internet*; (2) As sociedades comerciais de capitais exclusivamente públicos; (3) As pessoas colectivas privadas qualificadas de utilidade pública administrativa nos temos legais.	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) As sociedades comerciais de capitais exclusivamente públicos; 3) As pessoas colectivas de utilidade pública administrativa cuja actividade se cinja à área científica e tecnológica.

- **Artigo 7.º - Comissão para a Cibersegurança**

A Comissão debateu com o proponente o papel reservado à Comissão para a Cibersegurança e a forma como o mesmo estava reflectivo no articulado da proposta de lei. Desse debate resultaram diversas alterações ao artigo 7.º.

Os deputados consideraram que a designação «Comissão Permanente para a Cibersegurança», constante da versão inicial, podia diminuir o papel deste órgão e a sua inserção na estrutura administrativa da RAEM. Os órgãos administrativos são, por regra, permanentes, não sendo necessário que esta característica conste da sua designação. Por esta razão, a denominação da Comissão foi alterada, passando a chamar-se Comissão para a Cibersegurança.

A redacção do proémio do n.º 1 sofreu alterações. Na versão inicial afirmava-se que a Comissão é um «órgão decisório do Governo». A afirmação desta natureza decisória, por oposição a uma natureza consultiva, afigurava-se incongruente com a competência para propor ao Governo a celebração de acordos, protocolos ou contratos, prevista na alínea 3) do n.º 1. Passou a prever-se que a Comissão para a Cibersegurança é presidida pelo Chefe do Executivo.

Os deputados sugeriram a inclusão da competência prevista na alínea 2) do n.º 1 para esclarecer a relação entre a Comissão para a Cibersegurança e as demais entidades que integram o sistema criado pela presente iniciativa legislativa.

Versão inicial	Versão final
Artigo 7.º **Comissão Permanente para a Cibersegurança** A Comissão Permanente é o órgão decisório do Governo, ao qual cabe: 1) Assegurar a actividade referida na alínea 1) do artigo 3.º; 2) 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 obtenção de padrões mais elevados de cibersegurança na RAEM.	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**

O artigo 8.º foi alterado no sentido de clarificar a natureza jurídica do CARIC. O proponente esclareceu que a intenção legislativa é que este não seja um órgão administrativo, mas antes uma equipa de resposta rápida de natureza técnica composta por diversos serviços públicos. Esta intenção foi reflectida no proémio do n.º 1, no qual se determina que «o CARIC é uma estrutura de natureza técnica especializada em matéria de alerta e resposta a incidentes de cibersegurança».

O n.º 2 passou a regular a competência para efectuar a monitorização referida na alínea 5) do n.º 1, a qual é atribuída à PJ, e proclama os limites a que tal monitorização está sujeita. As razões para a inclusão de tais limites já foram apresentadas na análise genérica do presente Parecer.

Versão inicial	Versão final
Artigo 8.º **Centro de Alerta e Resposta a Incidentes de Cibersegurança** 1. O CARIC integra as entidades públicas com competências técnicas específicas em matéria de cibersegurança e é coordenado pela Polícia Judiciária. 2. Sem prejuízo do regime de competências e da autoridade da Polícia Judiciária, o CARIC tem as seguintes atribuições: 1) Assegurar a actividade referida na alínea 3) do artigo 3.º, centralizando, para o efeito, a recepção dos alertas sobre incidentes de cibersegurança e coordenando a cooperação e acções adequadas entre as diversas entidades intervenientes, bem como cooperando com as entidades congéneres do exterior, de modo a evitar ou mitigar os efeitos dos incidentes de cibersegurança; 2) Definir e divulgar junto de todos os intervenientes no sistema de cibersegurança os níveis de gravidade dos incidentes de cibersegurança, as instruções e o procedimento das acções de alerta e resposta a incidentes, nos termos das orientações elaboradas pela Comissão Permanente; 3) Monitorizar, através da Polícia Judiciária, em tempo real, o tráfego e as características dos dados informáticos transmitidos sob a forma de linguagem máquina, entre as redes dos operadores de infra-estruturas críticas e a internet, com a finalidade de prevenir, detectar e combater os ataques e invasões cibernéticos;	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 informáticas 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

4) Emitir, quando necessário, alertas sobre incidentes de cibersegurança.	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**

O artigo relativo às entidades de supervisão era, na versão inicial, algo lacunar no que dizia respeito às suas competências. Assim, foi feito um esforço de densificação normativa, reunindo neste artigo diversas competências que se encontravam dispersas no articulado. A nível formal, a listagem das competências permite que todos os artigos relativos às entidades que integram o sistema de cibersegurança tenham uma estrutura idêntica.

Relativamente à natureza das entidades de supervisão, passou a prever-se que elas são «serviços e organismos da Administração Pública» que, já existindo, passam a desempenhar novas funções no âmbito desta lei.

Versão inicial	Versão final
Artigo 9.º **Entidades de supervisão de cibersegurança** 1. As entidades de supervisão de cibersegurança são as entidades públicas que prosseguem as atribuições de supervisão em matéria de cibersegurança, perante os operadores de infra-estruturas críticas.	Artigo 9.º **Entidades de supervisão de cibersegurança** 1. As entidades de supervisão são serviços ou 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

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

- **Artigo 10.º - Deveres de carácter orgânico**

Para além do anteriormente referido quanto aos deveres de carácter orgânico (ponto 4.1 da análise genérica), importa mencionar a alteração do entendimento quanto ao substituto do principal responsável pela cibersegurança. A versão inicial consagrava o dever de o principal responsável pela cibersegurança, em caso de ausência ou impedimento, «assegurar a sua substituição por outro interlocutor que seja habilitado e conhecedor dos sistemas e contactável pelo CARIC, devendo o mesmo interlocutor aguardar a respectiva colocação na RAEM». Tratava-se de um dever imposto ao próprio principal responsável, quando, em rigor, o artigo se destina a consagrar os deveres dos operadores privados. A norma presumia que a substituição em causa tinha carácter ocasional e breve e, como tal, o substituto não estava sujeito aos requisitos de idoneidade aplicáveis ao principal responsável pela cibersegurança. Esta solução foi ponderada, tendo-se concluído que as razões que justificam o escrutínio para o desempenho destas funções são aplicáveis a quem as exerce, independentemente de o

serem a título principal ou em regime de substituição. Assim, a versão final da proposta de lei passou a exigir a nomeação, em simultâneo, de duas pessoas – o principal responsável pela cibersegurança e o seu substituto – aplicando-lhes as mesmas regras e requisitos, nomeadamente ao nível da residência habitual na RAEM, idoneidade, experiência profissional e disponibilidade permanente.

Versão inicial	Versão final
Artigo 10.º **Deveres de carácter orgânico** 1. Constituem deveres dos operadores privados de infra-estruturas críticas, no âmbito da respectiva organização: 1) Dotar a estrutura operacional das unidades de gestão da cibersegurança e designar os respectivos responsáveis para implementar, com recurso aos meios humanos, financeiros, materiais e patrimoniais, as medidas internas de protecção da cibersegurança; 2) Verificar a idoneidade e a experiência profissional do principal responsável pela cibersegurança dos operadores de infra-estruturas críticas, solicitando obrigatoriamente, para esse efeito, parecer à Polícia Judiciária; 3) Estabelecer mecanismos e meios de reclamações e denúncias relativas à cibersegurança. 2. Para efeitos do disposto na alínea 2) do número anterior, considera-se não possuir idoneidade para o exercício das funções do principal responsável pela cibersegurança, quem for condenado por tribunais da RAEM ou do exterior, por sentença transitada em julgado, por qualquer dos seguintes crimes: 1) Por crimes previstos na Lei n.º	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 os indivíduos com idoneidade e experiência profissional adequadas e com residência habitual na RAEM; 4) Diligenciar para que o principal responsável pela cibersegurança e respectivo 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

2/2009 (Lei relativa à defesa da segurança do Estado); 2) Por crimes informático 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) Por qualquer outro crime punível com pena de prisão superior a cinco anos. 3. No caso previsto na alínea 3) do número anterior, as sentenças proferidas por tribunal do exterior da RAEM apenas produzem os efeitos estatuídos nas alíneas 2) e 3) do número anterior, quando os respectivos actos constituam também crimes nos termos da legislação da RAEM. 4. O principal responsável pela cibersegurança deve ter residência habitual na RAEM para estar contactável, a qualquer momento, pelo CARIC, devendo, em caso de ausência ou impedimento, assegurar a sua substituição por outro interlocutor que seja habilitado e conhecedor dos sistemas e contactável pelo CARIC, devendo o mesmo interlocutor aguardar a respectiva colocação na RAEM.	sua gravidade, frequência ou outras circunstâncias atendíveis, suscitem dúvidas sérias quanto à garantia da cibersegurança. 3. Sem prejuízo do disposto no número anterior, os operadores privados de infra-estruturas críticas 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 caso a condenação tenha sido pena de prisão igual ou inferior a 5 anos; 2) 10 anos a contar da cessação do cumprimento da pena, ou das respectivas prorrogações caso a condenação tenha sido 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 n.º 3, contanto que, no caso da alínea 3), a conduta em causa

	também constitua crime nos termos da legislação da RAEM. 6. Os operadores privados de infra-estruturas críticas devem solicitar parecer à Polícia Judiciária sobre a idoneidade e eventuais impedimentos relativos às pessoas que pretendam designar como principal responsável pela cibersegurança e respectivo substituto.

- **Artigo 17.º - Sanções acessórias**

A alínea 1) do n.º 1 previa a sanção acessória de privação do direito de participar em concursos públicos. A Comissão considerou que os motivos que justificam essa sanção são igualmente válidos para interditar a participação em ajustes directos e consultas restritas, tal como previsto na alínea b) do n.º 1 do artigo 10.º da Lei n.º 6/96/M, de 15 de Julho (Regime jurídico das infracções contra a saúde pública e contra a economia). Assim, o âmbito da sanção acessória foi alargado, passando a incluir a participação em ajustes directos e consultas restritas que tenham por objecto a aquisição de bens ou serviços por serviços, órgãos e entidades públicos.

Versão inicial	Versão final
Artigo 16.º **Sanções acessórias** 1. Pelas infracções ao disposto nas alíneas 1) e 2) do n.º 1 do artigo 10.º, no n.º 1 do artigo 11.º, na alínea 1) do artigo 12.º e na alínea 1) do artigo 13.º, podem ser aplicadas aos operadores privados de infra-estruturas críticas, isolada ou cumulativamente, as seguintes sanções acessórias: 1) Privação do direito de participar em concursos públicos que tenham por objecto a aquisição de bens ou serviços	Artigo 17.º **Sanções acessórias** 1. Pela infracção 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, contados a partir da data do início da execução das mesmas.	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**

O regime sancionatório previsto no Capítulo IV inclui a figura da advertência. Com ela pretende-se dar uma oportunidade de correcção de irregularidades no cumprimento de deveres sem que sejam aplicadas as sanções, principais e acessórias, por infracção administrativa. É, portanto, uma fase preliminar que pode levar à extinção do procedimento infraccional. A advertência tem na sua génese um juízo de desvalor jurídico em relação à conduta do agente, a qual, no entanto, tem um reduzido grau de ilicitude. Trata-se, assim, de meras irregularidades no cumprimento dos deveres de cibersegurança e não de incumprimento total e absoluto; de irregularidades que podem ser corrigidas; e de irregularidades que não tiveram efeitos particularmente gravosos, i.e. das quais não resultou um perigo significativo para a cibersegurança. O reduzido grau de ilicitude resulta, igualmente, do facto de o agente não ser reincidente. Reunidos estes requisitos, é fixado um prazo para o agente sanar a irregularidade, podendo o procedimento ser encerrado ou ser emitida uma simples advertência ao infractor, caso a entidade de supervisão entenda que a irregularidade, mesmo que já esteja corrigida, não deve passar sem repreensão. O n.º 2 do artigo 18.º determina que «sendo a irregularidade sanada no prazo fixado, a entidade de supervisão pode decidir-se por uma simples advertência ao infractor». Se a irregularidade não for sanada no prazo fixado para o efeito, o procedimento por infracção administrativa segue

os seus termos normais, com vista à aplicação das respectivas sanções (n.º 3). A figura da advertência constante da proposta de lei foi inspirada em soluções semelhantes vigentes no ordenamento jurídico local, nomeadamente no artigo 130.º do Regime Jurídico do Sistema Financeiro, aprovado pelo Decreto-Lei n.º 32/93/M, de 5 de Julho.

A versão inicial foi alterada no sentido de clarificar os pressupostos de aplicação da advertência. Considerou-se que a mesma não podia ser aplicada por mera «suspeita de incumprimento dos deveres», mas apenas quando exista uma situação de efectivo incumprimento que, pela sua natureza, possa ser considerado uma mera irregularidade. Por outro lado, na versão inicial a advertência correspondia ao acto de fixação do prazo para a correcção da situação («a entidade de supervisão pode adverti-lo para sanar a irregularidade dentro dum prazo fixado»). Esta solução foi equacionada, tendo-se considerado ser mais curial que a advertência corresponda à fase final do procedimento, na qual se emite uma admoestação para que a situação detectada e já corrigida não torne a ocorrer.

Versão inicial	Versão final
Artigo 17.º **Advertência** 1. Caso se verifique a suspeita do incumprimento dos deveres previstos nos artigos 10.º a 13.º pelo operador privado de infra-estrutura crítica, a entidade de supervisão pode adverti-lo para sanar a irregularidade dentro dum prazo fixado, salvo se: 1) A situação consubstanciar um perigo substancial para a cibersegurança; 2) O operador visado tiver sido punido por infracção administrativa de idêntica natureza há menos de um ano. 2. Na falta da sanação da irregularidade	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.

pelo operador privado no prazo referido no número anterior, a entidade de supervisão instrui o processo sancionatório relativamente à respectiva infracção.	3. A falta de sanação da irregularidade no prazo fixado determina o prosseguimento do procedimento para aplicação das sanções que couberem à infracção.

- **Artigo 24.º - Módulos de identificação de assinante**

Os prazos previstos para a adopção do *Real-Name System* foram alargados de 60 para 120 dias, dando mais tempo aos operadores de redes para o cumprimento da obrigação prevista no artigo 24.º. Este alargamento permite, igualmente, que todo o processo de pedido e fornecimento dos dados de identificação fique concluído dentro desse prazo.

O n.º 2 prevê a suspensão do serviço em caso de não fornecimento dos dados. Passou, ainda, a contemplar a situação de reactivação do serviço logo que os dados sejam fornecidos e o cartão ainda esteja válido. Caso contrário, a suspensão corresponderia a um tipo de sanção, prejudicial para o consumidor, quando a intenção é que seja um mero indutor da cooperação do utente no fornecimento dos dados de identificação.

A versão inicial consagrava as sanções para a infracção ao dever de identificação através de remissão para o «diploma legal que estabelece o regime de acesso e exercício da actividade de prestação de serviços de *internet*, com a multa de montante mais elevado fixado nesse diploma». Considerou-se que esta solução não garantia a necessária certeza e segurança jurídicas e que podia conflituar com o princípio da integralidade da lei, consagrado no n.º 2 do artigo 4.º da Lei n.º 13/2009 (Regime jurídico de enquadramento das fontes normativas internas), uma vez que não estava suficientemente identificado o diploma legal aplicável, nem a sanção para a infracção em causa. Por esta razão, na versão final foi prevista, de forma expressa, a moldura sancionatória aplicável: multa de 50 000 a 150 000 patacas. Foi, igualmente, consagrada a respectiva competência sancionatória, a qual foi

atribuída à Direcção dos Serviços de Correios e Telecomunicações. Iguais soluções foram adoptadas no artigo 25.º (identificação de clientes).

Versão inicial	Versão final
Artigo 23.º **Módulos de identificação de assinante adquiridos antes da entrada em vigor da presente lei** 1. No prazo de 60 dias após a entrada em vigor da presente lei, os operadores de redes devem diligenciar no sentido de obter e registar a identidade dos utilizadores de módulos de identificação de assinante, doravante designados por cartões SIM, não sujeitos à prévia identificação e adquiridos na modalidade de pré-pagos, antes da entrada em vigor da presente lei. 2. Os adquirentes ou utilizadores dos cartões SIM devem fornecer a sua identidade no prazo de 60 dias após solicitada pelos operadores de redes. 3. A partir da data do termo do prazo referido no número anterior, os operadores de rede devem desactivar os cartões SIM, caso os respectivos utilizadores não cumpram o dever de identificação, sem prejuízo da suspensão de serviços que ocorra por virtude do termo da validade dos próprios cartões. 4. O incumprimento pelos operadores de redes dos deveres previstos nos n.^{os} 1 e 3 constitui infracção administrativa, punível nos termos do diploma legal que estabelece o regime de acesso e exercício da actividade de prestação de serviços de *internet*, com a multa de montante mais elevado fixado nesse diploma.	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 de identificação de assinante 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 administrativa prevista no número anterior, designar instrutor e aplicar as sanções.

- **Artigo 26.º - Aditamento à Lei n.º 11/2009**

A consagração da obrigatoriedade de conservação e fornecimentos de registos de tradução de endereços de rede é feita através de um aditamento à Lei de combate à criminalidade informática. A solução constante da versão inicial fazia o aditamento do artigo 15.º-A no Capítulo III da Lei n.º 11/2009, relativo a disposições processuais penais. Contudo, o conteúdo do artigo aditado não só não diz respeito a matérias processuais, como consagra uma infracção administrativa pelo incumprimento do dever nele consagrado. A sua inserção sistemática prejudicava a coerência interna da referida lei. Razão pelo qual, a versão final passou a prever que o aditamento fosse feito num capítulo próprio – o Capítulo III-A, denominado "Infracção administrativa" – também ele ora aditado. Foi, ainda, prevista a competência sancionatória, constante do novo artigo 16.º-B.

Versão inicial	Versão final
Artigo 25.º **Aditamento à Lei n.º 11/2009** É aditado à Lei n.º 11/2009 o artigo 15.º-A, com a seguinte redacção: «Artigo 15.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, punível nos termos do diploma legal que estabelece o regime de acesso e	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

exercício da actividade de prestação de serviços de *internet*, com a multa de montante mais elevado fixado nesse diploma. 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 anterior.»	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 26.º da versão inicial – Direito subsidiário aplicável**

O artigo que previa a aplicação subsidiária de vários diplomas legais foi eliminado por entender-se ser o mesmo desnecessário. A aplicação subsidiária do Código de Procedimento Administrativo resulta do seu artigo 2.º. Ademais, a previsão do n.º 2 do artigo 26.º repetia a norma constante do n.º 3 do artigo 3.º do Decreto-Lei n.º 52/99/M, de 4 de Outubro (Regime geral das infracções administrativas e respectivo procedimento).

Versão inicial	Versão final
Artigo 26.º **Direito subsidiário aplicável** 1. Aos actos administrativos previstos na presente lei são subsidiariamente aplicáveis o Código de Procedimento Administrativo e o Código de Processo Administrativo Contencioso. 2. Às infracções administrativas previstas na presente lei são aplicáveis, subsidiária e sucessivamente, as disposições constantes do Decreto-Lei n.º 52/99/M, de 4 de Outubro (Regime geral das infracções administrativas e respectivo procedimento) e, com as necessárias adaptações, as disposições do Código do Procedimento Administrativo e os princípios gerais do direito e do processo penal.	

- **Artigo 27.º – Regulamentação complementar**

Em sede de regulamentação complementar, a versão inicial previa apenas a designação das entidades de supervisão. Esta previsão foi alargada à designação dos operadores privados de infra-estruturas críticas abrangidos pelo poder de supervisão de cada uma dessas entidades. Pretendeu-se que a relação existente entre o supervisor e os operadores privados fosse estabelecida com maior precisão.

A redacção do artigo foi simplificada, eliminando-se a referência aos diplomas legais que o Chefe do Executivo deve ter em consideração aquando da elaboração dos diplomas complementares.

Versão inicial	Versão final
Artigo 27.º **Regulamentação complementar** A regulamentação complementar necessária à execução da presente lei, nomeadamente no que diz respeito às seguintes matérias, é aprovada pelo Chefe do Executivo mediante regulamento administrativo ou despacho regulamentar externo: 1) Definição da composição, competências e modo de funcionamento da Comissão Permanente e do CARIC; 2) Indicação das entidades de supervisão referidas na alínea 2) do n.º 2 do artigo 9.º, tendo em conta a natureza ou o âmbito de actividades responsáveis pelas entidades referidas na alínea 2) do artigo 4.º e as orientações previstas na Lei n.º 2/1999 (Lei de Bases da Orgânica do Governo) e no Regulamento Administrativo n.º 6/1999 (Organização, competências e funcionamento dos serviços e entidades públicos).	Artigo 27.º **Regulamentação complementar** O Chefe do Executivo aprova, por regulamento administrativo complementar ou despacho regulamentar externo, as normas complementares que se mostrem necessárias à execução da presente lei, nomeadamente em matéria de: 1) Composição, competências e modo de funcionamento da Comissão para a Cibersegurança 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 versão inicial previa a entrada em vigor da lei 180 dias após a sua publicação, salvo quanto ao dever de conservação dos registos de tradução de endereços das redes internas privadas dos utentes em endereços públicos IP da *internet*. O n.º 2 do artigo 28.º determinava que os operadores de redes teriam de cumprir esse dever em data diferente, que se pretendia que fosse posterior, para que lhes fosse possível fazer os preparativos necessários a esse cumprimento.

No decurso da análise na especialidade da proposta de lei, o Governo informou a

Comissão que considerava já não se justificar uma diferenciação entre a entrada em vigor da lei e a produção de efeitos do artigo 25.º porquanto a *vacatio legis* de 180 dias é suficiente para que os operadores reúnam as condições necessárias para o integral cumprimento de todos os deveres legais ora consagrados.

Versão inicial	Versão final
Artigo 28.º **Entrada em vigor e produção de efeitos** 1. A presente lei entra em vigor 180 dias após a sua publicação. 2. O disposto no artigo 25.º produz efeitos a partir de de de 201 .	Artigo 28.º **Entrada em vigor** A presente lei entra em vigor 180 dias após a sua publicação.

- **Ajustamentos técnico-jurídicos**

Para além dos aspectos abordados nos pontos anteriores, a Comissão efectuou melhorias de redacção e sistematização de várias normas visando o seu aperfeiçoamento técnico-jurídico, sem reflexos no conteúdo substancial das mesmas.

V – Conclusão

Em conclusão, apreciada e analisada a proposta de lei, a Comissão:

a) É de parecer que a versão final da proposta de lei reúne os requisitos necessários para apreciação e votação, na especialidade, pelo Plenário;

b) Sugere que, na reunião plenária destinada à votação na especialidade da presente proposta de lei, o Governo se faça representar, a fim de poderem ser prestados os esclarecimentos necessários.

Macau, 22 de Maio de 2019.

A Comissão,

Ho Ion Sang

(Presidente)

Ma Chi Seng

Ma Chi Seng

(Secretário)

Kou Hoi In

Au Kam San

Lei Cheng I

Song Pek Kei

Ip Sio Kai

Iau Teng Pio

Fong Ka Chio

Lam Lon Wai