1ª COMISSÃO PERMANENTE

PARECER N.º 1/VI/2020

Assunto: Proposta de lei intitulada «*Alteração à Lei n.º 11/2009 – Lei de combate à criminalidade informática*».

I - Introdução

1. O Governo da Região Administrativa Especial de Macau, doravante designada RAEM, apresentou, em 23 de Julho de 2019, a proposta de lei intitulada «Alteração à Lei n.º 11/2019 – Lei de combate à criminalidade informática», a qual foi admitida pelo Presidente da Assembleia Legislativa, no dia 26 de Julho, através do Despacho n.º 1016/VI/2019.

2. Na reunião plenária da Assembleia Legislativa realizada no dia 17 de Outubro de 2019 foi a referida proposta de lei discutida e votada na generalidade, tendo sido aprovada por unanimidade. Nessa mesma data, foi distribuída à 1.ª Comissão Permanente para efeitos da sua apreciação na especialidade e emissão de parecer, até ao dia 17 de Dezembro de 2019, nos termos do Despacho do

Presidente da Assembleia Legislativa n.º 1371/VI/2019, prazo que foi prorrogado, devido a vicissitudes várias, até 9 de Abril de 2020.

3. A Comissão reuniu-se, nos dias 29 de Outubro de 2019 e 22 de Janeiro, 27 e 28 de Fevereiro de 2020 e 8 de Abril, a fim de proceder à análise da proposta de lei, tendo contado com a presença de representantes do Governo em três dessas reuniões. Foi ainda realizada uma reunião de trabalho entre a assessoria da Assembleia Legislativa e a assessoria do Governo com vista ao aperfeiçoamento técnico da proposta de lei.

4. Dado a proposta de lei incluir alterações a uma norma de natureza processual, a Comissão considerou conveniente a audição da Associação dos Advogados de Macau, face ao disposto no artigo 30.º n.º 3 do Decreto-Lei n.º 42/95/M, de 21 de Agosto, e uma vez que aquando da elaboração da Lei a alterar foi pedido que essa Associação se pronunciasse[1]. Para tal, em 1 de Novembro de 2019 foi enviado um ofício àquela Associação, ao qual a mesma respondeu através de um Parecer enviado em 15 de Novembro[2].

5. Na sequência da discussão havida na Comissão e das sugestões aí apresentadas, o proponente acabou por proceder a alterações à versão original da proposta de lei que foi aprovada na generalidade e, em consequência, a 7 de Abril, apresentou uma versão final, sobre a qual esta Comissão elaborou o presente parecer, tendo em conta o disposto no artigo 119.º do Regimento da Assembleia Legislativa.

[1] Conforme consta da página 2 do Parecer n.º 3/III/2009 da 3.ª Comissão Permanente, acessível em https://www.al.gov.mo/uploads/lei/leis/2009/11-2009/parecer.pdf.
[2] Cf. Parecer em Anexo.

II – A iniciativa

Nos termos da Nota Justificativa, *«a presente proposta de lei visa quatro objectivos bem determinados:*

• A criação de um tipo penal, que preveja a criminalização da prática de utilizar dispositivos e programas informáticos e aparelhos próprios, do tipo "sting ray", para operar uma estação simulada (ilegal ou não autorizada) de telecomunicações móveis;

• A garantia de uma melhor harmonia com a Lei n.º 13/2019 (Lei da cibersegurança), recentemente aprovada, de forma a conferir maior protecção penal aos sistemas informáticos utilizados pelos operadores de infra-estruturas críticas, como tal definidos na referida Lei da cibersegurança, bem como pelas instituições do Governo Popular Central estabelecidas em Macau, definidas no Regulamento Administrativo n.º 22/2000 (Garantias das instituições do Governo Popular Central estabelecidas em Macau para a prossecução das suas atribuições e respectivas isenções), ou seja, os actuais Gabinete de Ligação do Governo Popular Central na Região Administrativa Especial de Macau, Comissariado do Ministério dos Negócios Estrangeiros na Região Administrativa Especial de Macau e Guarnição em Macau do Exército de Libertação do Povo Chinês;

• A clarificação legislativa no sentido de permitir a extracção, para efeitos de prova no processo penal, de cópia de dados informáticos que possam encontrar-se fora da RAEM, desde que tais dados sejam legalmente acessíveis ou obteníveis a partir do sistema informático situado na RAEM;

• A autonomização de uma espécie particular, agravada, de crimes de violação de segredo profissional».

Quanto ao primeiro objectivo, o proponente refere que *«nos últimos anos, tem aumentado substancialmente a ocorrência de práticas ilegais de simulação de estações de telecomunicações móveis com recurso a dispositivos e programas informáticos e a aparelhos próprios, do tipo "sting ray"»*, que *«estas "estações" operam induzindo os aparelhos de telemóvel a identificá-las como sendo uma estação de telecomunicações legítima (...) e são operadas geralmente junto de locais de grande concentração ou passagem de pessoas, tais como as zonas dos postos fronteiriços, com o objectivo de enviar ardilosamente mensagens para os telemóveis dos cidadãos que passam, devassando a sua privacidade e importunando-as com divulgação ou publicidade de actividades ilegais (prostituição, empréstimo ilícito para jogo, propostas com características de burlas, etc.)»* causando *«grande perturbação não apenas aos residentes daquela zona, como também a cidadãos e turistas que entram e saem de Macau, propiciando a ocorrência de crimes e danos para os cidadãos, o que afecta gravemente o funcionamento do estado de direito e a imagem turística da RAEM.»*

Diz ainda que *«estas condutas de simulação de estação de telecomunicações são difíceis de combater, porque são realizadas à distância, de forma não pessoal, e porque são usados instrumentos (computadores pessoais, programas informáticos e aparelhos do tipo "sting ray") de pequena dimensão, fáceis de dissimular, e instalados em fracções habitacionais, o que torna substancialmente mais difícil a investigação e a recolha de provas.»*

Quanto ao segundo objectivo, refere o proponente que *«a ampliação da protecção penal é prosseguida mediante duas formas:*

- *Por um lado, alterando o actual artigo 12.º da Lei n.º 11/2009 para que fiquem abrangidos pela agravação não só os crimes informáticos*

cometidos contra entidades públicas, mas também os cometidos contra operadores privados de infra-estruturas críticas e contra as instituições do Governo Popular Central estabelecidas em Macau definidas no Regulamento Administrativo n.º 22/2000;

- *Por outro lado, alterando as normas actuais que respeitam ao direito de queixa; a solução é a de introduzir um novo artigo (artigo 12.º-A) que regule o direito de queixa, revogando as disposições dispersas sobre esse tema como constam na lei actual (n.º 3 do artigo 4.º, n.º 3 do artigo 5.º, n.º 5 do artigo 7.º e n.º 4 do artigo 11.º da Lei n.º 11/2009)*

Da nova disciplina legal, resultará que os crimes informáticos cuja pena deva ser agravada, por terem tido por alvo os operadores de infra-estruturas críticas e as outras entidades relevantes referidas, serão sempre qualificados como crimes públicos, não dependendo de queixa para se iniciar e prosseguir o correspondente procedimento penal».

Quanto ao terceiro objectivo, relacionado com a alteração da alínea 6) do n.º 1 do artigo 16.º da Lei n.º 11/2009, esclarece o proponente que «*a prática internacional que se vem consolidando é o de que uma autoridade judiciária da jurisdição A pode aceder a dados informáticos armazenados num sistema localizado materialmente na jurisdição B e obter uma cópia dos mesmos sem violar a soberania desta jurisdição B, desde que esse acesso (transfronteiriço) se reporte a dados publicamente acessíveis ou tenha o consentimento da pessoa legalmente autorizada (sendo que este consentimento deve ser especialmente acautelado, nos casos de menoridade ou de anomalia psíquica do visado, por exemplo).*

Assim, na proposta de lei sugere-se uma redacção que elimine a expressão "situado na RAEM", constante da lei actual, permitindo que seja a autoridade judiciária a avaliar, em cada caso concreto, se existem condições de legitimidade para recolher cópia de dados informáticos armazenados noutras jurisdições. A eliminação daquela expressão fará com que a legislação da RAEM passe a ter solução semelhante à preconizada:

- *no n.º 5 do artigo 15.º da Lei do Cibercrime, de Portugal; e*
- *no artigo 588 sexies, da Lei de Instrução Criminal (Ley de Enjuiciamiento Criminal), da Espanha.*

Naturalmente, a autoridade judiciária da RAEM continuará a precisar de recorrer aos mecanismos da cooperação judiciária internacional:

- *quando não estejam reunidos os requisitos acima referidos (dados publicamente acessíveis ou consentimento da pessoa legalmente autorizada); ou*
- *quando, em vez de se tratar do simples acesso e obtenção de cópia de dados armazenados, se tratar de outras diligências tais como apreensões físicas de suportes digitais, de intercepções de dados em tempo real e de acesso a dados de tráfego*».

Quanto ao quarto e último objectivo, o proponente esclarece que «*quando está em causa a revelação de vulnerabilidades críticas de segurança de sistemas informáticos, o interesse a proteger passa a ter uma dimensão de grande relevância pública, que vai além dos interesses privados dos donos dos sistemas informáticos em causa, porque os sistemas informáticos interagem através das redes e, nessa medida, uma vulnerabilidade de um sistema pode repercutir-se negativamente sobre todo o conjunto dos sistemas, afectando também*

negativamente toda a sociedade.

Assim, a proposta de lei contém um aditamento (artigo 9.º-B) que sugere a punição de forma agravada (com pena de prisão até 3 anos ou pena de multa) de quem, no exercício das suas funções ou por causa delas, tomar conhecimento de vulnerabilidade crítica de segurança, ainda que temporária, de sistema, dispositivo ou programa informático e, com qualquer intenção ilegítima, revelar esse facto a outrem, de forma adequada a criar perigo da prática de crime informático».

III. Apreciação

A. Na generalidade

1. A Lei n.º 11/2009, que ora se pretende alterar, prevê a criminalização de determinados delitos informáticos e normas processuais penais que visam facilitar a investigação desse tipo de delitos e de crimes cometidos por meio de sistemas informáticos, além de estabelecer um regime especial de recolha e conservação de prova em suporte electrónico da prática de quaisquer crimes.

2. A criminalidade informática tem vindo a registar um enorme incremento por todo o mundo e emerge cada vez mais rapidamente, com variáveis mais e mais sofisticadas no seu *modus operandi,* exigindo medidas mais eficazes de investigação e de prevenção e um reforço do quadro punitivo relativamente a novas condutas criminosas que, nestes últimos 10 anos, têm vindo a surgir um pouco por todo o mundo e, também, na RAEM.

3. Ciente dessa realidade e da necessidade de adaptação do regime legal existente à Lei da cibersegurança, recentemente aprovada pela Assembleia Legislativa, a Comissão acolheu de forma muito positiva a presente proposta de alteração, volvidos que estão mais de 10 anos sobre a vigência da Lei actual, não deixando, contudo, de colocar e discutir com o proponente algumas das alterações propostas, visando alcançar a sua compreensão em termos de tutela penal e o aperfeiçoamento técnico-jurídico de algumas das suas normas.

4. A discussão no seio da Comissão incidiu, essencialmente, sobre os seguintes aspectos:

a) O âmbito do alargamento da agravação das penas, previsto na alteração ao artigo 12.º, relativamente aos crimes previstos na Lei n.º 11/2009;

b) O âmbito e forma de execução da medida especial prevista na alínea 6) do artigo 16.º da mesma Lei;

c) O bem jurídico protegido pelos novos tipos de crime aditados nos artigos 9.º-A e 9.º-B, a sua definição legal e o seu âmbito de aplicação.

5. Quanto à alteração proposta para o artigo 12.º que prevê, agora, a agravação das penas para os crimes previstos na Lei n.º 11/2009, sempre que os mesmos tiverem por objecto dados ou sistemas informáticos utilizados no âmbito da respectiva actividade, pelos operadores de infra-estruturas críticas previstos na Lei da cibersegurança ou por instituições do Governo Popular Central estabelecidas em Macau, a Comissão quis saber se pretende abranger-se apenas os operadores públicos de infra-estruturas críticas, que correspondem, no fundo, às entidades e órgãos públicos antes previstos no artigo 12.º, ou, também, as entidades de direito privado que são operadores privados de infra-estruturas

críticas, nos termos do artigo 4.º, n.º 3 da Lei n.º13/2019 e a razão de ser dessa alteração.

6. Pelo propoente foi esclarecido que «*ficarão abrangidos nessa expressão tanto os operadores públicos de infra-estruturas críticas como os operadores privados de infra-estruturas críticas. Por via desta agravação das penas, pretende-se conferir maior protecção penal aos operadores de infra-esfruturas críticas. Ora, para esse efeito, o que interessa não é a natureza pública ou privada dos operadores: é a sua relevância crítica para o normal funcionamento e bem-estar da Sociedade*».

7. A Comissão realçou que, no parecer da 3.ª Comissão Permanente da AL, elaborado aquando da apreciação da Lei n.º 11/2009 na especialidade[3], se considerou que «*o n.º 1 do artigo 12.º consagra a agravação das penas dos crimes informáticos, previstas nos artigos 4.º a 11.º em função dos dados ou sistemas informáticos envolvidos na conduta criminosa serem titulados por entidades públicas da RAEM. Pretende-se, com esta agravação, dispensar uma maior protecção à utilização da informática pelas autoridades oficiais locais, pretendendo-se «reforçar a protecção da confidencialidade e a integridade de sistemas informáticos ou dados informáticos»* e que, ao prever-se agora essa agravação quando estejam envolvidos na conduta criminosa dados ou sistemas informáticos utilizados no âmbito da respectiva actividade pelos operadores de infra-estruturas criticas, públicos e privados, amplia-se muito o número de casos em que vai haver lugar à agravação da pena, já que aqueles passam a ser em

[3] Página 41 do Parecer n.º 3/III/2009, acessível em https://www.al.gov.mo/uploads/lei/leis/2009/11-2009/parecer.pdf.

número muito mais elevado do que as entidades que antes determinavam a agravação[4].

8. Por isso a Comissão questionou o proponente se, sendo a agravação da pena uma opção de política criminal determinada por razões especiais de prevenção e tendo em conta a definição que é dada no artigo 2.º, alínea 3) da Lei n.º 13/2019 sobre infra-estruturas críticas, não deveria colocar-se antes a tónica da agravação na protecção directa das infra-estruturas críticas em vez de a mesma ser feita em função dos seus operadores pois o que interessa é conferir maior protecção penal às redes e sistemas informáticos que integram as infra-estruturas críticas, cujos ataques poderão ter maior impacto e prejudicar directamente a segurança e ordem públicas e o bem-estar da população em geral e, portanto, punir de forma mais grave os crimes cometidos contra essas infra-estruturas críticas.

9. O proponente referiu que o âmbito da agravação não será assim tão amplo, posto que na RAEM há milhares de empresas e só apenas uma pequena percentagem dessas empresas são operadores privados de infra-estruturas críticas e que ao se estabelecer a agravação em função da qualidade da vítima e, portanto, em função da qualidade de operador de infra-estruturas críticas, seja ele público ou privado, se está a proteger de forma eficaz as infra-estruturas críticas que são operadas por aqueles, o que foi considerado adequado pela Comissão.

---

[4] Além dos operadores públicos de infra-estruturas críticas previstos no artigo 4.º, n.º2 da Lei n.º 13/2019 refere-se no Parecer n.º 3/VI/2019 da 1ª Comissão desta Assembleia, página 10, acessível em https://www.al.gov.mo/uploads/attachment/2019-05/366705ceb9fc59eab8.pdf que «*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)*».

10. Quanto à alteração da alínea 6) do artigo 16.º da Lei n.º 11/2009, a discussão tida no seio da Comissão visou, em primeiro lugar, obter esclarecimentos do proponente sobre as exigências legais e procedimentais que permitem a realização de uma busca ou acesso inicial a um determinado sistema informático e, em segundo lugar, esclarecer o modo como é feita a extensão dessa busca e o âmbito dessa extensão, quer quanto ao tipo de dados a que se pode aceder, quer quanto ao procedimento legal para aceder, sobretudo quando os dados se encontrem num sistema informático identificado fora da RAEM ou em que se desconheça a sua localização geográfica.

11. Essa discussão permitiu clarificar que, na pesquisa ou acesso inicial de dados informáticos armazenados num determinado sistema informático, há sempre que ter em conta o disposto no Código de Processo Penal quanto às buscas e apreensões, por força do disposto no artigo 14.º da Lei n.º 11/2009 e que a extensão de busca prevista nesta alínea 6), pressupondo sempre a apreensão de um dispositivo na busca inicial, exige que o novo sistema informático a procurar ou a parte diferenciada do sistema inicial que foi pesquisado sejam acessíveis a partir do sistema inicial, isto é, a partir do dispositivo apreendido. A extensão de busca tem de ser autorizada ou ordenada pela autoridade judiciária competente nos termos do n.º 1 do artigo 16.º da mesma lei, mas pode ser executada pelos órgãos de polícia criminal (designadamente pela Polícia Judiciária, a quem, nos termos da alínea 10) do n.º 1 do artigo 7.º da Lei n.º 5/2006, está atribuída a competência exclusiva para realizar a investigação dos crimes relacionados com a informática) sem prévia autorização da autoridade judiciária competente, nos casos previstos no n.º 2 do mesmo artigo. Neste caso a realização da extensão da busca tem de ser imediatamente comunicada à autoridade judiciária competente, sob pena de

nulidade, e por ela apreciada, em ordem à sua validação, no prazo máximo de 72 horas – n.º 3 do artigo 16.º que, à semelhança do corpo do n.º 1 e do n.º 2, do mesmo artigo, não sofreu qualquer alteração. Esta intervenção dos órgãos de polícia criminal, que é excepcional, só se justifica em caso de urgência ou perigo na demora que possam representar grave perigo para bens jurídicos de valor relevante e é em tudo semelhante ao regime constante no próprio Código de Processo Penal para as revistas e buscas (artigo 159.º, n.º 4) e para as apreensões (artigo 163.º, n.º 4).

Os dados informáticos a que é possível aceder nesta extensão de busca, são dados de conteúdo e não dados de tráfego, cujo acesso e recolha continuam a ser feitos, tal como até aqui, nos termos da alínea 2) do n.º 1 do artigo 16.º da Lei n.º 11/2009.

12. A Comissão realça que as exigências legais previstas nesta alínea 6) para a obtenção deste tipo de prova são as mesmas desde a entrada em vigor da Lei n.º 11/2009 e não foram questionadas ao longo destes anos da sua vigência e que o acesso a estes dados, nos termos acima referidos, não afasta, nem substitui, o disposto no Código de Processo Penal, que, sendo supletivo, continua a ser o diploma legal de referência a ter em conta quanto aos meios de obtenção de prova e quanto às garantias nele previstas para tutelar segredos legalmente protegidos.

13. Já quanto ao procedimento para aceder a dados informáticos situados num outro sistema informático ou numa parte diferenciada do sistema inicial quando esses dados estejam localizados fora da RAEM, num território identificado ou na chamada "nuvem", que é no fundo o objectivo da proposta de lei ao retirar a expressão "situado na RAEM" da alínea 6) do n.º 1 do artigo 16.º da Lei n.º

11/2009, a Comissão teve a oportunidade de confirmar junto do proponente que a intenção legislativa da proposta de lei foi a de estabelecer um regime legal coincidente com o artigo 32.º da Convenção do Cibercrime (Convenção de Budapeste), por forma a permitir o acesso e recolha de prova digital transfronteiriça, desde que reunidos os pressupostos legais. Tais pressupostos são aqueles que já antes constavam desta alínea, isto é, tem de haver razões para crer que os dados procurados se encontram armazenados nesse sistema ou numa parte do mesmo e esses dados têm de ser legalmente acessíveis ou obteníveis a partir do sistema inicial, o que segundo o proponente «*implica que as Autoridades da RAEM podem aceder a dados informáticos acessíveis ao público (fonte aberta), ou não acessíveis ao público, desde que obtido o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar tais dados através de tal sistema informático, ou seja, em regra, a própria pessoa titular dos dados.* Foi ainda reiterada a ideia, pelo proponente, de que, quando os dados estiverem situados numa outra concreta jurisdição, caberá à autoridade judiciária avaliar se quer ou não utilizar os mecanismos de cooperação judiciária internacional ou inter-regional disponíveis na RAEM.

14. A Comissão sabe que o cibercrime não é hoje uma questão secundária, mas antes uma das principais preocupações dos Governos, da Sociedade e dos indivíduos e que há hoje em todo o mundo milhares de ataques por dia contra os sistemas informáticos, sendo por isso cada vez mais importante o acesso rápido à prova electrónica, tendo em conta a natureza transnacional e volátil desse tipo de prova.

15. A Comissão louvou, por isso, a preocupação do Governo de conformar a Lei da RAEM com a legislação internacional, designadamente com a Convenção do Conselho da Europa sobre o cibercrime (Convenção de Budapeste) mas realçou que a alteração agora introduzida à alínea 6) do artigo 16.º da Lei n.º 11/2009 não estabelece, de forma expressa, os limites previstos naquela Convenção para o acesso transfronteiriço de uma Parte, sem a autorização de outra Parte, aos dados informáticos armazenados, no território de outra parte os quais são, de acordo com o seu artigo 32.º: a) que tais dados informáticos armazenados sejam acessíveis ao público (fonte aberta), independentemente da sua localização geográfica; b) que a Parte obtenha o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar-lhe tais dados através de tal sistema informático e que, fora dessas situações, a Convenção de Budapeste apenas prevê que a pesquisa e acesso sejam feitos através do auxilio mútuo (cooperação internacional).

16. A Comissão tem presente que a cooperação judiciária em matéria penal, sendo de difícil execução no contexto da computação em nuvem, tem se revelado um procedimento complexo, dispendioso e pouco eficiente, o que tem levado vários Estados a adoptarem, para além da Convenção de Budapeste, soluções unilaterais similares à que agora se pretende estabelecer na RAEM com esta alteração e que essas soluções têm vindo a ser discutidas, desde há vários anos, no âmbito do Comité da Convenção do Conselho da Europa sobre Cibercrime (T-CY), mais concretamente no seio do CEG (Cloud Evidence Group), que no seu relatório final de 16 de Setembro de 2016, sugeriu um protocolo adicional à Convenção de Budapeste por forma a permitir, uma mais efectiva assistência legal mútua, facilitar a directa cooperação com os fornecedores de serviços noutras jurisdições, estabelecer condições e garantias relativamente às práticas existentes

de acesso transfronteiriço a dados e estabelecer requisitos quanto à protecção dos dados[5].

17. Da discussão desenvolvida a esse propósito, a Comissão acabou por concluir que aqueles limites estabelecidos pela Convenção de Budapeste no seu artigo 32.º, acabam por estar presentes, ainda que de forma não expressa, nos pressupostos legais que são exigíveis para a extensão de busca prevista na alínea 6) do artigo 16.º, na medida em que os dados a aceder têm de ser legalmente acessíveis ou obteníveis a partir do sistema inicial, o que, pressupondo a apreensão de um dispositivo, significa que os dados informáticos a aceder pelas autoridades da RAEM têm de ser acessíveis ao público (fonte aberta) ou desde que obtido o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar tais dados através do sistema informático daquele dispositivo, que é, por regra, a própria pessoa titular dos dados.

18. A Comissão considerou por isso, face ao acima exposto, não sugerir qualquer alteração à redacção proposta para a nova alínea 6) do número 1 do artigo 16.º da lei n.º 11/2009.

19. Quanto ao novo tipo de crime aditado no artigo 9.º-A, com a designação de "Utilização de dispositivo informático para simular estação de serviços de telecomunicações móveis", a Comissão reconhece a necessidade na definição deste novo tipo legal de crime no âmbito da criminalidade informática, por ser cada vez mais frequente, principalmente junto aos postos fronteiriços, o

---

5 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e

surgimento de estações de comunicações móveis simuladas que, com recurso a dispositivos informáticos, se conectam com os telemóveis das pessoas que entram no território e dessa forma divulgam e incentivam à prática de actividades associadas à prostituição, pornografia e jogo ilícito, acabando por propiciar a ocorrência de criminalidade associada a tais actividades, que afecta o funcionamento do estado de direito e a imagem turística da RAEM.

20. A conduta desvaliosa que aqui é relevante e que importa punir é a de simular estação de serviços de telecomunicações móveis para, segundo refere o proponente, "*atrair a conexão dos telemóveis das pessoas e passar-lhes mensagens contendo propostas que se revestem de ilicitudes várias, utilizando para tanto dispositivos e programas informáticos associados a outros instrumentos ou aparelhagem*" e por isso a Comissão concorda que no n.º 1 se puna apenas o perigo da mera simulação de uma estação de serviços de telecomunicações móveis através da utilização de um programa e dispositivo informático associados a outros instrumentos ou aparelhagem e no número 3, como um crime agravado, se prevejam determinadas circunstâncias qualificativas que traduzem um maior desvalor da acção, a exigirem uma maior censurabilidade e, portanto, uma pena mais grave que permite a possibilidade de ser aplicada a prisão preventiva, pois esta pode ser uma medida cautelar dissuasora deste tipo de criminalidade.

21. Quanto ao novo tipo de crime previsto no artigo 9.º-B, designado de "Exposição ilegítima de vulnerabilidade grave de segurança informática", a Comissão reconhece, tal como o proponente, a necessidade de proteger a segurança dos sistemas informáticos, em geral, por forma a não expor as suas

vulnerabilidades críticas pois, na medida em que os sistemas informáticos interagem através das redes, há que proteger, os interesses da sociedade e dos indivíduos que são postos em causa pela prática dos crimes informáticos previstos na lei, que a divulgação dessas vulnerabilidades críticas pode potenciar.

22. A Comissão quis saber se se pretende criar uma espécie de segredo profissional e qual o âmbito de abrangência quanto ao agente que pode praticar este crime, isto é, se apenas está em causa o funcionário público ou aquele que exerce funções em organismos ou instituições públicas, ou se pretende abranger-se outros funcionários, como por exemplo os funcionários bancários.

23. O proponente esclareceu que não se pretende criar uma espécie de crime de violação de segredo profissional, mas antes um crime de "*violação de sigilo de função*" na medida em que o acesso a informação privilegiada constante dos relatórios de cibersegurança referidos na alínea 2) do artigo 12.º e no n.º 2 do artigo 14.º, ambos da Lei n.º 13/2019, pode chegar ao conhecimento de pessoas em relação às quais não se pode dizer, inquestionavelmente, que exercem uma profissão e que, por isso, "*pretende-se abranger todas as pessoas que, no exercício da função (profissional, institucional/política, meramente consultiva) que exercem, e por causa dela, tomaram conhecimento de uma vulnerabilidade crítica de um determinado sistema informático*" e a revelem a outrem de tal forma que, assim, criem perigo da prática de crime informático. "*O objectivo é pois o de abranger qualquer profissão (incluindo funcionários bancários, obviamente) ou outra função, incluindo funções políticas*".

24. A Comissão, ciente da necessidade de ter sistemas informáticos seguros e do impacto que uma falha crítica desses sistemas pode ter na segurança das

pessoas, dos Serviços Públicos e das Instituições, manifestou a sua concordância com o âmbito do conceito de agente que pode praticar este crime e que está vinculado a esse sigilo decorrente da função que exerce ou por causa dela.

25. Quanto ao artigo 12.º-A, designado por "Queixa", cujo aditamento tem como consequência a revogação prevista no artigo 3.º da proposta de lei, relativamente ao n.º 3 do artigo 4.º, n.º 3 do artigo 5.º, n.º 5 do artigo 7.º e nº 4 do artigo 11.º da Lei n.º 11/2009, a Comissão constatou que estamos apenas perante uma alteração da técnica legislativa que foi usada aquando da elaboração daquela Lei (em que o legislador optou por prever, expressamente, em relação a cada um dos crimes previstos naqueles artigos, quando o mesmo depende de queixa), concentrando-se agora num só artigo todos os casos em que o procedimento penal pelos crimes previstos naquela Lei fica dependente de queixa.

26. Uma vez que a exigência quanto à necessidade de queixa se reporta a vários preceitos dentro da mesma lei e por se tratar de uma técnica legislativa que também é usada em casos semelhantes no Código Penal, por exemplo, nos crimes contra a liberdade e autodeterminação sexuais (artigo 172.º) e nos crimes contra a honra (artigo 182.º), a Comissão considerou ser adequado proceder a tal revogação e aditar o artigo 12.º-A, por forma a prever num só artigo todos os casos em que o procedimento criminal depende de queixa e evitar a repetição do mesmo conteúdo em cada um dos artigos em causa.

27. Quanto ao artigo 5º, que prevê a data da entrada em vigor da lei, foi discutida a fixação de uma nova data em virtude de a data inicialmente proposta se mostrar ultrapassada, tendo a Comissão sugerido a forma inicial de estabelecer

uma data concreta por assim haver mais certeza quanto à data de produção dos efeitos da lei e ser mais adequado ao melhor conhecimento pela população.

28. O parecer da Associação dos Advogados de Macau aborda não só as alterações da proposta de lei em causa, mas, também, a Lei de combate à criminalidade informática no seu todo. A Comissão considera, tal como o proponente, que esta parte do parecer deve ser ponderada com atenção numa futura revisão global da Lei.

B. Na especialidade

29. 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.

30. Artigo 1.º (**Alteração à Lei n.º 11/2009**)

Este artigo introduz alterações aos artigos 12.º e 16.º da Lei n.º 11/2009.

31. Quanto ao artigo 12.º, respeitante à «agravação das penas», o n.º 1 passa agora a consagrar a agravação das penas dos crimes informáticos, previstas nos artigos 4.º a 11.º, nos termos já antes previstos, isto é, de um terço nos seus limites mínimo e máximo, sempre que tais crimes tiverem por objecto dados ou sistemas informáticos utilizados no âmbito da respectiva actividade por duas entidades diversas:

a) Operadores de infra-estruturas críticas, previstos na Lei n.º 13/2019 (Lei da cibersegurança);

b) Instituições do Governo Popular Central estabelecidas em Macau definidas no artigo 1.º do Regulamento Administrativo n.º 22/2000 (Garantias das instituições do Governo Popular Central estabelecidas em Macau para a prossecução das suas atribuições e respectivas isenções).

32. Pretende-se, desta forma, conferir uma maior protecção penal aos sistemas informáticos utilizados pelos operadores de infra-estruturas críticas, como tal definidos na Lei da cibersegurança, independentemente da natureza pública ou privada dos operadores, uma vez que os ataques às infra-estruturas críticas, dada a sua relevância para o normal funcionamento da sociedade, poderão ter maior impacto e prejudicar directamente a segurança e ordem públicas e o bem-estar da população em geral e conferir, também, uma maior protecção na prossecução das atribuições das instituições do Governo Popular Central existentes na Região, que são o Gabinete de Ligação do Governo Popular Central na Região Administrativa Especial de Macau, o Comissariado do Ministério dos Negócios Estrangeiros na Região Administrativa Especial de Macau e a Guarnição em Macau do Exército de Libertação do Povo Chinês.

33. Quanto ao artigo 16.º (Medidas especiais), altera-se a alínea 6) do número 1 por forma a que, no âmbito de uma investigação criminal, as autoridades judiciárias da RAEM possam, através da extensão de uma busca inicial a um determinado sistema informático, aceder a dados contidos em sistemas informáticos localizados no exterior da RAEM ou não localizados especificamente

em lado nenhum (por circularem na chamada nuvem), ou que estejam numa parte diferenciada do sistema informático que é alvo da diligência inicial.

34. Os pressupostos para essa extensão de busca são os já anteriormente previstos na lei – fundadas razões para crer que os dados informáticos procurados são relevantes para uma investigação criminal e se encontram armazenados num outro sistema ou numa parte diferenciada do sistema inicial e que os mesmos são legalmente acessíveis ou obteníveis a partir do sistema inicial - o que, pressupondo a apreensão de um dispositivo, significa que os dados informáticos a aceder pelas autoridades competentes através desta extensão de busca têm de ser acessíveis ao público (fonte aberta) ou desde que obtido o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar tais dados através do sistema informático daquele dispositivo, que é, por regra, a própria pessoa titular dos dados. Fora desses casos deverá ser colocada a questão à autoridade judiciária, que avalia se quer utilizar os mecanismos de cooperação judiciária internacional ou inter-regional em vigor.

35. A Comissão espera que, no futuro, a aplicação do disposto nesta alínea 6) se faça de acordo com tal interpretação e que no acesso a tais dados transfronteiriços os órgãos de polícia criminal recorram, preferencialmente, aos mecanismos de cooperação internacional ou inter-regional, sempre que esteja claramente identificado o território onde estão armazenados os dados a aceder, por forma a evitar conflitos de territorialidade ou de jurisdição.

36. Além disso, a Comissão espera que na execução do procedimento para aceder a tais dados os órgãos de polícia criminal tenham em consideração as regras de protecção dos dados e as normas estabelecidas no Código de Processo

Penal quanto à proteção dos vários segredos nele previstos[6], por forma a proteger os direitos individuais.

37. Artigo 2.º (**Aditamento à Lei nº 11/2009**)

Através deste artigo são aditados três novos artigos à Lei n.º 11/2009, dois deles prevendo dois novos tipos de crime no âmbito da criminalidade informática, que passam a ser os artigos 9.º-A e 9.º-B, e um outro, que passa a ser o artigo 12.º-A, respeitante ao regime do procedimento criminal quanto aos crimes previstos no n.º 1 do artigo 4.º, no artigo 5.º, nos nºs 1 e 2 do artigo 7.º e nos n.ºs 1 e 2 do artigo 11.º daquela Lei.

38. No artigo 9.º-A passa a estar previsto o crime de «Utilização de dispositivo informático para simular estação de serviços de telecomunicações móveis», em que o bem jurídico protegido é a segurança e fiabilidade dos serviços e meios de telecomunicações móveis. Trata-se de um crime doloso, que não pode ser praticado por negligência.

39. Como já referimos em sede de análise na generalidade, no n.º 1 pune-se apenas, como crime de perigo abstracto, a simulação de uma estação de serviços de telecomunicações móveis através da utilização de um programa e dispositivo informático associados a outros instrumentos ou aparelhagem, enquanto que no número 3, como um crime agravado, estão previstas determinadas circunstâncias qualificativas agravantes que traduzem um maior desvalor da acção, a exigirem uma maior censurabilidade em termos de pena.

[6] Como são os segredos profissional, de funcionário e da Região Administrativa Especial de Macau previstos nos artigos 122.º, 123.º e 124.º do Código de Processo Penal.

40. Por sugestão da Comissão este número passou a ter três alíneas, em vez das duas alíneas que constavam da proposta inicial, sendo as duas primeiras alíneas apenas um desdobramento da alínea 1) original, por estarem em causa circunstâncias qualificativas agravantes respeitantes a uma diferente intenção do agente, e a alínea 3), que antes correspondia à alínea 2), que tem a ver com características da própria conduta objectiva e o seu maior desvalor em termos de resultado.

41. Na versão inicial da proposta de lei estava prevista nesta alínea, que correspondia à alínea 2), a circunstância de "*a conduta se traduzir na transmissão de qualquer publicidade proibida por lei e/ou na disseminação, divulgação ou qualquer forma de incitação de outrem à prática, adesão ou consumo de pornografia, prostituição ou ilícito penal ou administrativo previsto no regime do jogo ilícito*".

A Comissão salientou não ver necessidade em distinguir a actividade de disseminação da actividade de divulgação de prostituição, consumo de pornografia e de jogo ilícito, por se tratar de termos com o mesmo significado e questionou o proponente sobre a necessidade de autonomizar, em termos de tutela penal, o incitamento à prática de cada uma daquelas actividades, do incitamento à adesão dessas mesmas actividades na medida em que se pode considerar a adesão como inerente à prática ou consumo de cada uma dessas actividades - quem as pratica ou consome é porque a elas aderiu.

42. A Comissão realçou ainda que essa modalidade de conduta - adesão -não está prevista noutros crimes mais graves do Código Penal, como por exemplo, no crime de associação criminosa (artigo 288.º) ou no crime de incitamento à

alteração violenta do sistema estabelecido (artigo 298.º), nem mesmo nos crimes previstos na Lei n.º 3/2006 (Prevenção e repressão dos crimes de terrorismo).

43. Na versão final da proposta de lei o proponente acabou por reformular esta alínea e dar-lhe uma nova redacção eliminando não só a actividade de "disseminação", mas, também, a conduta de "adesão", o que teve a concordância da Comissão.

Salienta-se que, na versão final em chinês substituiu-se a expressão "賣淫" por "性交易". Ambas têm o sentido da palavra "prostituição" que se mantém, por isso, inalterada na versão portuguesa.

44. No artigo 9.º-B com a designação de "Exposição ilegítima de vulnerabilidade grave de segurança informática", prevê-se uma espécie de crime de violação de sigilo de função, quando essa violação seja adequada a criar perigo da prática de algum dos crimes informáticos previstos na Lei. Pretende-se, assim, proteger a segurança dos sistemas informáticos por forma a não expor as suas vulnerabilidades críticas, ou graves e, indirectamente, na medida em que os sistemas informáticos interagem através das redes, proteger os interesses da sociedade e dos indivíduos que podem ser postos em causa pela prática dos crimes informáticos que a divulgação dessas vulnerabilidades críticas pode potenciar. O agente deste crime tem de ser alguém que, no exercício da sua função, seja ela profissional, institucional, política ou meramente consultiva, ou por causa dela, tome conhecimento de uma vulnerabilidade grave de um determinado sistema informático e a divulgue.

45. A versão original que foi apresentada referia "vulnerabilidade crítica de segurança" e correspondia apenas ao que agora consta do número um da versão final sob apreciação.

A Comissão considerou que a lei seria mais clara e determinada se dela constasse o que se deve entender por vulnerabilidade crítica de segurança para efeitos da incriminação da conduta prevista neste novo tipo de crime, por forma a que as pessoas em geral possam saber, em termos objectivos, qual o conteúdo da informação que o agente está obrigado a não divulgar.

46. Por isso a Comissão sugeriu que a definição do tipo legal de crime passasse para o n.º 1 e que fosse acrescentado o n.º 2 em que se estabelece o que se entende por vulnerabilidade crítica de segurança para efeitos do disposto no n.º 1, tal como acontece com a formulação de outros tipos legais de crime previstos no Código Penal de Macau como, por exemplo, no crime de tortura e outros tratamentos cruéis, degradantes ou desumanos (artigo 234.º), no crime de captura ou desvio de aeronave, navio ou comboio (artigo 275.º) ou no crime de participação em motim armado (artigo 292.º). O que foi aceite pelo proponente, que, além disso, decidiu substituir a expressão "vulnerabilidade crítica" por "vulnerabilidade grave", que tem o mesmo significado.

47. Ainda quanto a este tipo de crime, a Comissão questionou quanto ao uso da expressão "com qualquer intenção ilegítima", por a considerar inadequada para traduzir o elemento respeitante à ilicitude da conduta e ser de conteúdo indeterminado para transmitir uma específica intenção do agente, que caracteriza o chamado "dolo específico".

48. A Comissão tem presente que, tal como referiu o proponente, essa mesma expressão é usada nos crimes previstos nos artigos 4.º e 5.º da Lei n.º 11/2009 e não tem sido questionada pelos Tribunais na aplicação desta Lei. Porém, nesses tipos legais de crime também é usada a expressão "sem autorização" que confere à conduta prevista em cada um deles a sua natureza ilícita, o que não acontece no crime agora previsto no artigo 9.º-B.

A Comissão realçou que "a ilegitimidade da intenção" acaba por ser um elemento normativo do tipo que remete para uma valoração global sobre a ilicitude da conduta e por isso a expressão "qualquer intenção ilegítima" acaba por traduzir apenas a ilicitude, isto é, o reforço da ideia de que a conduta é contrária à lei.

49. A Comissão, tendo em vista o aperfeiçoamento técnico-jurídico da lei, fez várias sugestões alternativas ao uso daquela expressão, a última das quais foi a de que se usasse antes a expressão "sem consentimento", à semelhança do disposto no Código Penal para os crimes de violação de segredo (artigo 189.º) e de aproveitamento indevido de segredo (artigo 190.º), o que não foi, contudo, aceite pelo proponente.

50. A Comissão acabou por acolher a opção do proponente mas considera, que o uso, sem mais, da expressão "com qualquer intenção ilegítima", que consta do número um deste artigo apenas confere à conduta a sua natureza ilegítima ou ilícita e não significa que se exige uma intenção específica do agente ou um dolo específico. O crime basta-se, pois, ao nível do elemento subjectivo ou dolo com o dolo genérico, em qualquer das suas modalidades. Para haver crime basta que o agente, de forma ilegítima, revele a outrem uma vulnerabilidade grave de segurança da qual tomou conhecimento no exercício das suas funções ou por causa

delas, de forma adequada a criar perigo da prática de um dos crimes previstos na lei.

51. No artigo 12.º-A, estabelece-se que, "salvo quando haja lugar à agravação da pena prevista no artigo 12.º, o procedimento criminal pelos crimes previstos no n.º 1 do artigo 4.º, artigo 5.º, nºs 1 e 2 do artigo 7.º e nºs 1 e 2 do artigo 11.º depende de queixa", isto é, tais crimes têm a natureza semi-pública. Fica, assim, concentrado num só artigo o que antes estava disperso por vários artigos quanto ao procedimento criminal dos crimes em causa.

52. Artigo 3.º **(Revogação)**

Este artigo prevê a revogação de preceitos que estabeleciam um conteúdo semelhante ao que agora consta do novo artigo 12.º-A da Lei n.º 11/2009, quanto ao procedimento criminal relativamente aos crimes nele previstos.

53. Artigo 4.º **(Republicação)**

Determina-se a republicação em anexo da Lei n.º 11/2009, integrando as alterações aprovadas pela presente lei e pela Lei n.º 13/2019. A republicação da versão actualizada daquela Lei permite uma melhor assimilação das alterações nela introduzidas e o seu conhecimento actualizado pelos seus destinatários em geral e, em particular por aqueles a quem compete a sua aplicação.

54. Artigo 5.º **(Entrada em vigor)**

Estabelece-se como data da entrada em vigor da lei o dia 1 de Julho de 2020.

A adopção de uma data fixa é mais clara do que escrever-se que "a lei entra em vigor xx dias após a sua publicação", devido à discrepância de interpretação

desta expressão em português e em chinês, apesar de ser uma redacção muito usada em diplomas locais.

O uso daquela expressão em português tem origem na legislação de Portugal, onde continua a usar-se. O seu sentido é o de o diploma entrar em vigor a partir das zero horas e zero minutos de um determinado dia. Assim, se o diploma entra em vigor 30 dias após a sua publicação significa que o diploma entra em vigor às zero horas e zero minutos do trigésimo dia.

Isto é diferente da interpretação que é dada em chinês em que se exige que tenham decorrido os 30 dias completos para a entrada em vigor do diploma, isto é, o diploma só entra em vigor depois de decorridas as 24 horas do trigésimo dia. Tendo um dia 24 horas, o ponto de início para a entrada em vigor de um diploma é, assim, na versão em português às zero horas e zero minutos de um dia enquanto, na versão em chinês é depois das 24 horas do mesmo dia.

Por isso a forma - data fixa - permite uma maior certeza e clareza quanto ao momento a partir do qual a lei entra em vigor e começa a produzir os seus efeitos, tanto na versão chinesa como na versão portuguesa.

IV. Conclusão

Em conclusão, apreciada e analisada a proposta de lei intitulada "Alteração à Lei n.º 11/2019 – Lei de combate à criminalidade informática", a Comissão emite o seu parecer no sentido de que:

a) A versão final da proposta reúne os requisitos necessários para apreciação e votação na especialidade, pelo Plenário.

b) Na reunião plenária destinada à votação na especialidade, o Governo se faça representar a fim de poderem ser prestados os esclarecimentos necessários.

Macau, 8 de Abril de 2020

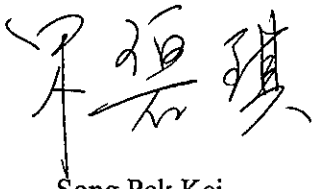
A Comissão,

Ho Ion Sang
(Presidente)

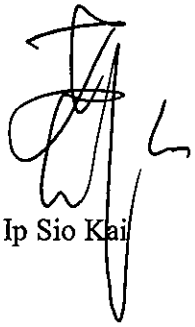
Ma Chi Seng
(Secretário)

Au Kam San

Lei Cheng I

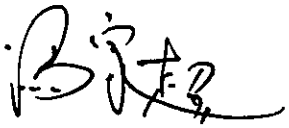


Song Pek Kei

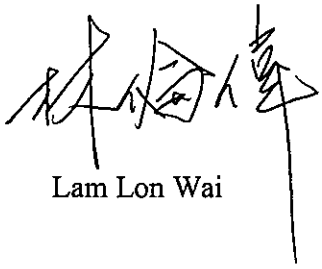


Ip Sio Kai

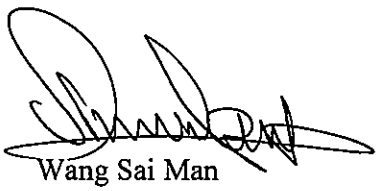
Iau Teng Pio



Fong Ka Chio



Lam Lon Wai



Wang Sai Man

Anexo

Associação dos Advogados de Macau
澳 門 律 師 公 會

Exmo. Senhor
Presidente da 1.ª Comissão Permanente da Assembleia Legislativa
Dr. Ho Ion Sang
Edifício da Assembleia Legislativa,
Praça da Assembleia Legislativa,
Macau

Macau, 15 de Novembro de 2019
N/Ref.: 2136/19

Assunto: Alterações à Lei de combate à criminalidade informática – Lei n.º 11/2009 – Recolha de opiniões e comentários da Associação dos Advogados de Macau

Conforme solicitado através do vosso ofício do dia do 1 do corrente mês, após sujeição da proposta de lei acima identificada à consulta dos advogados, vimos, pelo presente, remeter o Parecer da Associação dos Advogados de Macau, aprovado em reunião da Direcção.

Ficamos à disposição de V. Exa. para o que houver por conveniente.

Com os melhores cumprimentos.

Pel´A Direcção

Álvaro Rodrigues

Av. da Amizade, nº 918. Edificio World Trade Center, 11º, MACAU 澳門友誼大馬路918號,世界貿易中心大廈11樓 Caixa Postal 郵箱：1293 MACAU 澳門
Tel 電話：28728121, 28728122 Fax 傳真：28728127 E-mail 電子郵箱：aam@macau.ctm.net Website 網頁：http://www.aam.org.mo

PARECER

Assunto: Lei n.º 11/2009 – Lei de combate à criminalidade informática – Alterações

Foi solicitado, pela Assembleia Legislativa, que a AAM se pronunciasse sobre a proposta de lei acima referida.

Nos termos do n.º 3 do artigo 30.º do Estatuto do Advogado, aprovado pelo Decreto-Lei n.º 31/91/M, de 6 de Maio[1], a AAM «será obrigatoriamente ouvida sobre propostas ou projectos de diplomas que regulem a organização judiciária, o exercício da advocacia, o processo civil e o processo penal. Não se estabelece o momento ou fase para a auscultação, sendo no entanto usual a consulta à AAM na fase preliminar à entrega de uma proposta de lei na AL. Também ocorre, ocasionalmente, já depois da PL ser submetida à análise da AL.

Chamamos a atenção para o facto de, não obstante ter sido referido no Parecer n.º 3/III/2009 da 3.ª Comissão Permanente da AL, relativo à proposta de lei intitulada «Lei de combate à criminalidade informática», que a Comissão enviou a 6 de Abril de 2009 um ofício à AAM a solicitar opiniões relativas à proposta de lei em causa, dos nossos registos não consta a entrada desse ofício, pelo que não foi possível darmos resposta a essa solicitação.

Nesse sentido, a AAM procedeu à auscultação dos seus associados, tendo recebido opiniões de advogados, as quais que se reflectem no parecer da AAM.

Nestes termos, com base na análise da proposta de lei (1.ª versão), e após a compilação e sistematização das opiniões recebidas, a AAM elaborou o presente parecer, o qual aborda a Lei de combate à criminalidade informática no seu todo e não apenas relativamente à proposta de lei de alterações.

Por razões sistemáticas, apresentamos primeiro uma introdução, seguida de uma análise da Lei n.º 11/2009 na especialidade, incluindo as alterações ora constantes da Proposta de Lei, finalizando por uma conclusão.

[1] Na versão vigente após as alterações e republicação em anexo ao Decreto-Lei n.º 42/95/M, de 21 de Agosto.

Av. da Amizade, nº 918. Edifício World Trade Center, 11º, MACAU 澳門友誼大馬路918號,世界貿易中心大廈11樓 Caixa Postal 郵箱：1293 MACAU 澳門
Tel 電話：28728121, 28728122 Fax 傳真：28728127 E-mail 電子郵箱：aam@macau.ctm.net Website 網頁：http://www.aam.org.mo

I

Introdução

Na *Nota Justificativa* da Proposta de Lei (adiante designada abreviadamente por PL), fundamenta-se a mesma com a necessidade de atingir quatro objectivos bem determinados:

a) A criação de um tipo penal para criminalização de estações simuladas (ilegais e não autorizadas) de telecomunicações móveis;

b) Harmonização com a Lei n.º 13/2019 – Lei da cibersegurança, conferindo maior protecção penal aos sistemas informáticos operados pelas instituições do Governo Popular Central estabelecidas em Macau;

c) Regular a extracção, para efeitos de prova em processo penal, de cópia de dados informáticos que possam encontrar-se fora de Macau, e

d) Autonomização de uma espécie particular, agravada, de crimes de violação de segredo profissional.

Tendo em conta esses objectivos e com base na análise do articulado, constata-se que existem áreas em relação às quais temos sugestões de melhoria de redacção e que iremos indicar ao longo do parecer.

Mencionamos também, em termos de análise na especialidade, quais as normas que julgamos deverem ser repensadas para as conciliar com o ordenamento jurídico existente.

No pressuposto de que a nossa posição se revela mais fácil de entender, em relação a cada norma específica, passamos de seguida à análise na especialidade.

II

Apreciação na especialidade da Lei n.º 11/2009 – Lei de combate à criminalidade informática bem como das alterações constantes da PL

1. Artigo 1.º da PL - Alteração à Lei n.º 11/2009 – Artigo 12.º, n.º 1, alínea 2) – Ordem das alíneas

Tendo em conta que as instituições que se encontram referidas no artigo 1.º do Regulamento Administrativo n.º 22/2000 – Garantias das instituições do Governo Popular Central estabelecidas em Macau para a prossecução das suas atribuições e respectivas isenções – são, como a própria designação do diploma indica, instituições do Governo Popular Central, entidade que se situa hierarquicamente acima dos operadores das infra-estruturas críticas previstos na Lei n.º 13/2019 - Lei da cibersegurança, sugerimos que, em termos de alteração de colocação sistemática, passe a ser a alínea 1).

Por outro lado, julgamos que o âmbito subjectivo de aplicação da lei deve ser delimitado com rigor, dado tal ter reflexos em termos de direitos, liberdades e garantias, considerando que se encontra previsto um agravamento das penas em caso de crimes tendo por objecto dados ou sistemas informáticos utilizados por determinadas entidades.

Note-se que a técnica de enumerar os operadores públicos e privados de infra-estruturas críticas, mas omitindo as instituições do Governo Popular Central estabelecidas em Macau foi também utilizada na Lei n.º 13/2019, designadamente no seu artigo 4.º - Âmbito subjectivo de aplicação. Julgamos que esta não é a melhor técnica legislativa, dado que, em termos de cibersegurança não se mencionam essas instituições, mas já se mencionam em termos de criminalidade informática. Tendo em conta que, na *Nota Justificativa*, se assinala, como um dos objectivos da PL, «a garantia de uma melhor harmonia com a Lei n.º 13/2019 – Lei da cibersegurança, não se entende esta opção legislativa, pelo que sugerimos a sua reponderação.

2. **Artigo 1.º da PL – Alteração à Lei n.º 11/2009 - Artigo 16.º, n.º 1, alínea 6) - «Estender de forma expedita a busca ou o acesso de forma semelhante a uma parte diferenciada do sistema informático alvo da diligência inicial, ou a outro sistema informático, quando tiverem razões para crer que os dados procurados se encontram armazenados nessa parte diferenciada ou nesse outro sistema informático e os mesmos forem legalmente acessíveis ou obteníveis a partir do sistema inicial.»**

A Lei 11/2009 dispõe no seu artigo 16.º, n.º 1, 6) o seguinte:

n.º 1 *"Quando houver fundadas razões para crer que os dados informáticos são relevantes para uma investigação criminal, a autoridade judiciária competente pode, por despacho e devendo, sempre que possível, presidir à diligência, autorizar ou ordenar as seguintes medidas":*

(...)

6)"Estender de forma expedita a busca ou o acesso de forma semelhante a um sistema informático situado na RAEM, quando tiverem razões para crer que os dados procurados se encontram armazenados nesse sistema ou numa parte do mesmo e que são legalmente acessíveis ou obteníveis a partir do sistema inicial"

Relativamente a esta norma, apesar de o proémio do n.º 1 não ser alterado pela PL ora em análise, consideramos que a expressão «sempre que possível» resulta muito ambígua em termos de interpretação da norma, devendo assim ser, em primeiro lugar, devidamente explicada a razão ou razões para a sua inserção no texto da lei e, em segundo lugar, correctamente delimitadas e enumeradas as excepções que se têm em vista, de modo a reduzir o mais possível a ambiguidade que se constata na redacção actual.

Nos termos da PL pretende retirar-se a expressão "na RAEM" do n.º 1 do artigo 16.º, 6) da Lei 11/2009, passando a constar "*Estender de forma expedita a busca ou o acesso de forma semelhante a um sistema informático alvo da diligência inicial, ou a outro sistema informático, quando tiverem razões para crer que os dados procurados se encontram armazenados nesse sistema ou numa parte do mesmo e que são legalmente acessíveis ou obteníveis a partir do sistema inicial*".

Assim, a proposta pretende alargar o âmbito de actuação dos órgãos de polícia criminal para que estes possam aceder a dados que se encontram em outros servidores que se encontram situados fora da Região Administração Especial de Macau, podendo visar-se inclusive a computação em nuvem.

A *Nota Justificativa*[2] refere que "*a autoridade judiciária da RAEM continuará a precisar de recorrer aos mecanismos da cooperação judiciária internacional:*

- *quando não estejam reunidos os requisitos acima referidos (dados publicamente acessíveis ou consentimento da pessoa legalmente autorizada); ou*
- *quando, em vez de se tratar do simples acesso e obtenção de cópia de dados armazenados, se tratar de outras diligências tais como apreensões físicas de suportes digitais, de intercepções de dados em tempo real e de acesso a dados de tráfego.*".

A nota justificativa aponta para razões de ordem prática que têm sido seguidas na ordem jurídica internacional e cita exemplos de normas similares em Portugal, Espanha e Bélgica.

Importa, porém, alertar para o facto de que em Portugal a norma é significativamente diferente da presente no artigo 16.º da Lei 11/2009.

[2] Disponível em: https://www.al.gov.mo/uploads/attachment/2019-07/692345d3ab6588a0ba.pdf

De seguida, apontaremos algumas diferenças de regime de forma a facilitar a compreensão do quadro vigente na RAEM e, bem assim, entender a relevância prática da alteração proposta.

Em primeiro lugar, no artigo 15.º da Lei n.º 109/2009 (*Lei do Cibercrime*, em **Portugal**) consta a norma que permite as buscas/pesquisas informáticas em sistemas informáticos alheios.

O n.º 1 do citado artigo dispõe que: "*Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.*".

Em **Macau**, diferentemente, há já no próprio artigo 16.º da Lei n.º 11/2009 um conjunto mais alargado de medidas a serem aprovadas pela autoridade judiciária competente (sobre a qual impende o dever de presidir a diligência). São elas:

2) Proceder ao acesso e recolha de dados de tráfego relativos a comunicações ou a serviços utilizados pelo suspeito, em tempo real, associados a comunicações específicas transmitidas por meio de um sistema informático, dentro da RAEM;

3) Ordenar a uma pessoa que comunique os dados informáticos específicos, na sua posse ou sob o seu controlo e armazenados num sistema informático ou num suporte de armazenamento de dados informáticos;

4) Ordenar a um prestador de serviços de Internet que comunique os dados de base na sua posse ou sob o seu controlo, relativos aos assinantes de serviços de Internet;

5) Ordenar a um prestador de serviços de Internet que aplique medidas para remover os dados informáticos específicos e ilegais, ou impedir o acesso aos mesmos, de forma expedita; (artigo 16.º, n.º1 da Lei n.º 11/2009)

Outra diferença é a de que na RAEM, "*Os órgãos de polícia criminal podem adoptar as medidas referidas no número anterior, mesmo sem prévia autorização da autoridade judiciária competente, quando tiverem fundadas razões para crer que os dados informáticos relacionados com o crime são susceptíveis de servirem a prova e que, de outra forma, poderiam perder-se ou quando a demora possa representar grave perigo para bens jurídicos de valor relevante.*" artigo 16.º, n.º 2 da Lei n.º 11/2009), ou seja, as autoridades judiciárias podem sem prévia autorização judicial aceder, por exemplo, a um computador, ou smartphone, e observar, copiar e monitorizar esses dados desde que tenham fundadas razões para considerar que os dados informáticos relacionados com o crime são susceptíveis de servirem de prova e cuja obtenção seja urgente.

Ainda assim, ressalva-se que a comunicação da realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação, a efectuar no prazo máximo de 72 horas (n.º 3 do artigo 16.º da Lei n.º 11/2009).

Por exemplo, será o caso em que procede ao acesso e recolha de dados de tráfego relativos a comunicações ou a serviços utilizados pelo suspeito, em tempo real, associados a comunicações específicas transmitidas por meio de um sistema informático, dentro da RAEM, e posteriormente, porque revelada a urgência da perda de dados que podem consubstanciar prova fulcral da prática de um crime, alarga urgentemente ao computador pessoal do visado, porquanto se apercebe que poderá constar nesse sistema informático a informação necessária.

Note-se, neste caso, que há uma autorização para a diligência inicial, e não há autorização para a estendida diligência.

Por sua vez, em **Portugal** o regime estabelece que as pesquisas informáticas só podem ser efectuadas sem prévia aprovação da autoridade judiciária competente quando "a*) a*

mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;" (n.º 3, a) do artigo 15.º da Lei n.º 109/2009), só se excluindo o seu consentimento nos casos de suspeitas de terrorismo, criminalidade violenta ou altamente organizada (alínea 3). Em todo o caso, também será necessário uma validação posterior pela autoridade judiciária competente.

Porém, esta faculdade dos órgãos de polícia criminal em **Portugal** não se estende ao procedimento previsto no artigo 15.º, n.º 5 da *Lei do Cibercrime* portuguesa, norma que terá inspirado o 16.º, n.º1, 6) da Lei n.º 11/2009 de Macau.

Isto é, não podem sem autorização do juiz fazer uso do meio previsto no artigo 15.º, n.º 5 da *Lei do Cibercrime* portuguesa.

Já em **Macau**, os órgãos de polícia criminal podem, sem prévia aprovação da autoridade judiciária competente, fazer uso da busca alargada prevista no artigo 16.º, n.º 1, alínea 6) da Lei n.º 11/2009 de Macau.

E, por seu turno, o citado artigo 16.º não refere o consentimento do visado como requisito para a realização das referidas medidas sem prévia aprovação da autoridade judiciária competente. Isto significa que à partida, em Macau, poderiam ser realizadas diligências sem a prévia aprovação da autoridade judiciária competente e sem a autorização do visado.

Ainda assim, cremos que, para salvaguardar os direitos e garantias dos residentes, deverá ser aplicado o regime de revistas e buscas constante dos artigos 159.º e seguintes do Código de Processo Penal, por remissão do artigo 14.º da Lei n.º 11/2009.

Uma conclusão que se retira é que o regime estabelecido no artigo 15.º da *Lei do Cibercrime* portuguesa é a de que a letra da lei impede, fora nos casos referidos, a

possibilidade de uma monitorização à distância (oculta, ou seja, sem necessidade de os órgãos de polícia criminal estarem no local onde se situa fisicamente o computador) sem autorização de autoridade judiciária competente.

Ademais, a *Lei do Cibercrime* portuguesa refere-se explicitamente a acções encobertas no seu artigo 19.º, remetendo para a Lei n.º 101/2001 portuguesa (Regime jurídico das acções encobertas para fins de prevenção e investigação criminal), mas no seu n.º 2 refere que "*Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações*".

A este respeito, importa mencionar que o regime da intercepção de comunicações se encontra previsto no artigo 18.º da *Lei do Cibercrime portuguesa*, e estabelece que "*a intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público*" (n.º 2 do citado artigo).

E, ainda, "*a intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação*" (n.º 3 do citado artigo).

Há, portanto, na própria lei portuguesa uma clara divisão e regulação das práticas de investigação criminal através dos meios informáticos.

Já em **Macau**, fica a dúvida sobre se o âmbito da intrusão no sistema informático dos particulares previsto na proposta alínea 6) do n.º 1 do artigo 16.º da Lei n.º 11/2009, conforme a PL, significa que o sistema informático é investigado *in loco*, caso em que o visado da investigação tem conhecimento ou, diferentemente, se significa que há

uma monitorização à distância e para lá da aplicação do regime de revistas e buscas, designadamente com o acesso a dados para além da RAEM.

No primeiro caso, em que se trata de órgãos de polícia criminal acederem ao sistema informático *in loco* e observar e recolher dados para prova, compreende-se a opção legislativa no sentido de agilizar a investigação criminal e evitar que provas relevantes de crimes se percam com a demora do procedimento legal.

Compete fazer a ressalva de que, nesse caso, tratar-se-á de uma busca, pelo que a presente lei deveria incluir uma remissão para o regime das buscas presente no artigo 159.º e seguintes do Código de Processo Penal, com as devidas adaptações.

É que, pese embora haja uma remissão geral para as regras constantes do Código de Processo Penal (artigo 14.º do Código de Processo Penal), não há uma equiparação da busca ao regime de buscas presente na lei processual, ao contrário do que se faz para as apreensões de correio electrónico (artigo 15.º, n.º 5).

E, efectuada a remissão para esse regime, a título de exemplo menciona-se que *"tratando-se de busca em escritório de advogado ou em consultório médico, ela é, sob pena de nulidade, presidida pessoalmente pelo juiz, o qual avisa previamente o presidente do organismo representativo da respectiva profissão, se um tal organismo existir, para que o mesmo, ou um seu delegado, possa estar presente."* (n.º 3 do artigo 162.º do Código de Processo Penal).

Diferentemente, será o caso em que a busca é feita num computador que entra no sistema informático alheio sem necessidade de os órgãos de polícia criminal se deslocarem ao local onde este fisicamente se encontra.

Essa questão torna-se pertinente também porque outra das diferenças entre a lei portuguesa e a alteração proposta é a de que enquanto em Portugal se denomina o acto de pesquisa e se equipara a mesma às buscas (n.º 5 e 6.º da *Lei do Cibercrime*

portuguesa), em Macau não se determina o que se entende por "*busca ou o acesso de forma semelhante*" nos termos do artigo 6) do n.º 1 do artigo 16.º da Lei n.º 11/2009, nem, como se disse, é feita qualquer equiparação ao regime das buscas do Código de Processo Penal de Macau.

Fica a dúvida se o "*acesso de forma semelhante*" se reporta a uma monitorização oculta e, assim, nos termos do n.º 2 do artigo 16.º da Lei n.º 11/2009, pode ser realizada sem prévia autorização (todavia, sujeita a validação de autoridade judiciária competente no prazo de 72 horas após a diligência).

Ou seja, se quando o artigo 16.º, n.º 1, alínea 6) se refere a buscas "*(...) a outro sistema informático*" e esta é realizada sem autorização prévia (nos termos do n.º 2), pretende significar apenas buscas no local onde se encontra esse meio informático (e.g., o computador do suspeito) ou se poderá significar ainda uma acção encoberta através de meios e dispositivos informáticos (diligências informáticas operadas à distância).

Se, por seu turno, entendermos por um lado que por buscas pretende a lei significar apenas o acesso ao sistema informático no local e que, por outro lado, deverá ser aplicado o regime de revistas e buscas da lei processual nos termos do artigo 14.º da presente lei (como aliás, apontava o Parecer da AL n.º 3/III/2009 em relação à Lei n.º 11/2009[3]), então questiona-se o que pretende referir a lei quando menciona o "*acesso de forma semelhante (...) a outro sistema informático*", sobretudo agora que os dados podem não se encontrar na RAEM.

Em **Macau**, todavia, a presente lei limita-se a fazer uma remissão para o regime geral, pese embora a especialidade das suas normas.

Aqui chegados, resta analisar como a alteração proposta ao artigo 16.º, n.º 1, alínea 6) da Lei n.º 11/2009 permite a obtenção de dados armazenados em computação em

[3] Disponível em: https://www.al.gov.mo/uploads/lei/leis/2009/11-2009/parecer.pdf

nuvem tendo em conta as possibilidades de investigação criminal por meios informáticos com as considerações acima referidas.

Um exemplo prático da aplicação do artigo 16.º n.º 1, alínea 6) como alterado na proposta de lei intitulada "Alteração à Lei n.º 11/2009 – Lei de combate à criminalidade informática" é o seguinte:

"Uma vez iniciada a pesquisa informática no computador do suspeito, percebe-se que existe muito pouca informação com relevo probatório, excepto alguns elementos que indiciam que a informação relevante há-de estar algures na cloud. Consultados os Favoritos do navegador de Internet do computador pesquisado, constata-se que aí se encontra, de facto, o link para um serviço de armazenamento de informação baseado na cloud. Ao seleccionar o link, percebe-se que as credenciais de acesso estão memorizadas e que, por isso, basta clicar na opção sign in para se poder ter acesso à informação pretendida.

O Ministério Público prepara-se para autorizar a extensão da pesquisa à conta do utilizador nessa cloud, ao abrigo do disposto no artigo 15.º, n.º 5, da Lei do Cibercrime, quando se apercebe que o fornecedor de serviços de armazenamento tem a sua sede na Alemanha e todos os seus servidores na Holanda, Bélgica e Irlanda. Pergunta-se: poderá clicar legitimamente na opção sign in para aceder e apreender a informação armazenada noutro Estado? Ou será que essa pesquisa e apreensão se lhe encontra vedada, sob pena de violação da soberania do Estado pesquisado, devendo por isso recorrer-se obrigatoriamente aos mecanismos de cooperação judiciária disponíveis? E se a informação pesquisada estiver, porventura, na Dark Web, sem que seja possível identificar o concreto Estado onde está armazenada? E se estiver armazenada em diferentes Estados em simultâneo, seja replicada, seja fragmentada? A questão não é de resolução fácil"[4].

[4] Exemplo disponível na página 57 do estudo "O DOMÍNIO DO IMATERIAL: PROVA DIGITAL, CIBERCRIME E A TUTELA PENAL DE DIREITOS INTELECTUAIS", disponível em http://www.ccj.mj.pt/ccj/recursos/ebooks/penal/eb_ProvaDigital.pdf

Aqui colocar-se-á a necessidade de esclarecer como efectivamente será feito o controlo da penetração em dados que se encontram para além da RAEM. É que, retirando-se a presença do sistema informático na RAEM como requisito essencial para a realização do artigo 16.º, n.º 1, alínea 6) da Lei n.º 11/2009, então, os órgãos de polícia criminal da RAEM podem efectivamente entrar em dados que se encontram, tecnicamente, alojados no ambiente digital de uma outra jurisdição.

Na prática sucede que, na maioria das vezes, será um esforço incompatível com a celeridade necessária à obtenção de prova perceber onde se encontra sediado o prestador do serviço de computação em nuvem, bem como saber se o mesmo tem servidores nacionais.

Assim, pode na prática não ser respeitado o dever de comunicação a outro Estado para cooperar judiciariamente na obtenção dos dados alojados em território de sua soberania. E, ainda, pode suceder que com esse Estado não haja ainda qualquer tratado de cooperação jurídica e judiciária ou acordo semelhente.

Tem sido entendido que a par de uma discussão académica da necessidade de cooperação judiciária para o acesso a dados que se encontram alojados em diferentes jurisdições, há uma outra realidade prática que com ela contrasta. Com efeito, tem-se como adquirido que as autoridades judiciárias actuam com o entendimento de que a eventual violação de soberania não provoca qualquer dano e, portanto, essa violação é de valor reduzido, e que a celeridade do deterioramento da prova exige que se intervenha no ambiente digital estrangeiro para obter os dados aí armazenados.

O Transborder Group, junto do **Conselho da Europa**, declarou o seguinte: «*As noted by the T-CY previously, given these limitations and in the absence of a clear, efficient and feasible international legal framework, governments increasingly pursue unilateral solutions in practice. It seems to be widespread practice that law enforcement in a specific criminal investigation access data not only on the device of the suspect but also on connected devices such as email or other cloud service*

accounts if the device is open or the access credentials have been obtained lawfully even if they know that they are connecting to a different, known country» [5]

Quanto à primeira hipótese apresentada pela nota justificativa de necessidade de cooperação judiciária, ou seja, "*quando não estejam reunidos os requisitos acima referidos (dados publicamente acessíveis ou consentimento da pessoal legalmente autorizada)*", cumpre dizer que em nenhuma parte da Lei n.º 11/2009 é estabelecida a necessidade do consentimento do visado (ao contrário do regime português, como se disse supra).

Porém, se se atender ao articulado no Parecer da AL n.º 3/III/2009 (em relação à Lei n.º 11/2009), às buscas deve ser aplicado também o regime geral de revistas e buscas do artigo 159.º e seguintes do Código de Processo Penal (nomeadamente, aos pressupostos constantes do n.º 4, alíneas a), b) e c) do artigo 159.º), apesar de não haver uma remissão directa (ao contrário do que é feito para as apreensões de correio electrónico, em que o artigo 15.º da Lei 11/2009 dispõe que o regime constante dos artigos 164.º e 235.º do Código de Processo Penal é aplicável com as necessárias adaptações), então será necessário sempre o consentimento do visado.

Ainda assim, fica também a dúvida em relação a este ponto quando o acesso é feito "*de forma semelhante*" e se trata de dados não situados na RAEM.

Já quanto aos dados estarem disponíveis publicamente, não se coloca qualquer problema pois qualquer pessoa os pode facilmente obter sem qualquer autorização.

Por sua vez, a *Nota Justificativa* menciona que será sempre necessário cooperação judiciária *"quando, em vez de se tratar do simples acesso e obtenção de cópia de dados armazenados, se tratar de outras diligências tais como apreensões físicas de suportes digitais, de intercepções de dados em tempo real e de acesso a dados de*

[5] COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME (T-CY), Criminal Justice Access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Estrasburgo: Conselho da Europa, Setembro de 2016, disponível em https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

tráfego.".

Porém, fica-se sem saber o que se entende por *"simples acesso e obtenção de cópia de dados armazenados"*. Questiona-se: será de considerar como sendo de simples acesso os dados disponíveis em serviços de computação em nuvem? Será só de simples acesso quando aberto o computador do suspeito e verificado que a palavra-passe já se encontra automaticamente inserida, porque previamente gravada, e basta a qualquer pessoa com o computador em mãos fazer um mero *click* para entrar na nuvem?

Julgamos que não será, porém, de simples acesso a observação e cópia de correspondência electrónica (e-mail ou similares) porque aí a lei já estabelece um regime próprio (n.º 6 do artigo 15.º da Lei n.º 11/2009).

Estas são algumas das questões que assumem um maior relevo quando a actividade é realizada sem prévia aprovação pela autoridade judiciária competente, pois ainda que esta rejeite *a posteriori* os motivos indicados pelos órgãos de polícia criminal nos termos do artigo 16.º, n.º 2 da Lei n.º 11/2009, certo é que já foi feita uma pesquisa informática em jurisdição estrangeira de dados pessoais de um residente.

Não se lhe deve qualquer reparo se a mesma seguir o regime de revistas e buscas e outras normas do Código de Processo Penal, mas sim se se tratar de uma diligência que, pelo seu cariz tecnológico, possa não se equiparar a esse regime.

Há que ter ainda em conta que, ao que parece, estas medidas especiais do artigo 16.º, n.º 1, alínea 6) podem ser efectuadas em conjunto com as outras medidas previstas nas restantes alíneas do n.º1.

Finalmente, caberá ainda dizer apenas que a presente proposta de alteração à Lei n.º 11/2009 não faz alterações de fundo no quadro vigente. No entanto, para a presente apreciação da proposta, consideramos que uma análise comparativa ao regime português poderá elucidar e fomentar a reflexão sobre o âmbito das buscas e pesquisas

informáticas na investigação criminal e, bem assim, compreender em que medida as acções ao abrigo da presente alteração se podem verificar na prática tendo em conta o âmbito alargado da investigação criminal por meios informáticos.

3. **Artigo 2.º da PL – Aditamento à Lei n.º 11/2009 – Artigo 9.º - A – Utilização de dispositivo informático para simular estação de serviços de telecomunicações móveis**

Esta norma, sendo nova, leva a que a definição do tipo de crime deva ser clara e inequívoca, pelo que se julgamos ser necessário definir o que se entende por «estação de serviços de telecomunicações móveis».

Com efeito, por exemplo, no artigo 2.º do Regulamento Administrativo n.º 32/2000 - Licenciamento provisório dos serviços de telecomunicações de uso público móveis terrestres – remete-se a definição dos conceitos utilizados nesse regulamento administrativo para o sentido estabelecido pelo União Internacional de Telecomunicações.

Posto isto, se quanto à utilização deste tipo de remissão num diploma a nível de regulamento administrativo já não é a melhor técnica, atendendo ao princípio da unidade de regulamentação de uma mesma realidade jurídica, ainda mais relativamente à redacção ora em análise, nos parece ser da maior importância proceder a essa definição na Lei, dado que dela se extraem cominações penais e não apenas do foro das infracções administrativas.

Sucintamente, sempre se dirá que as estações "ilegais" simuladas se consubstanciam na utilização de dispositivos de telecomunicação que não são autorizados para exercer a actividade de telecomunicações mas que utilizam meios telefónicos, por exemplo, através do envio de mensagens para cometer crimes (nomeadamente, burlas).

O facto de ser uma actividade criminosa que faz uso relativamente original dos meios

de telecomunicação e em relação à qual se têm verificado várias queixas na RAEM, a sua inclusão na lei n.º 11/2009 justifica-se pelo facto de não ser possível a sua punição através dos outros crimes constantes na lei, mas salientamos a necessidade de uma definição clara que sustente a punição.

4. **Artigo 2.º da PL – Aditamento à Lei n.º 11/2009 – Artigo 9.º - A – Utilização de dispositivo informático para simular estação de serviços de telecomunicações móveis, alínea 1) do n.º 3 - «A pena de prisão é de 1 a 5 anos quando ocorra qualquer uma das seguintes situações: 1) O agente tiver intenção lucrativa ou tiver em vista preparar, facilitar ou executar um outro crime.»**

Entendemos que a parte da norma acima sublinhada é de difícil prova e que, estando em causa a putativa intenção de um arguido, da sua aplicação podem decorrer acusações e condenações baseadas apenas em suspeitas de intenções, o que deve ser evitado em normas penais.

5. **Artigo 2.º da PL–Aditamento à Lei n.º 11/2009 – Artigo 9.º- B – Exposição ilegítima de vulnerabilidade crítica de segurança - «Quem, no exercício das suas funções ou por causa delas, tomar conhecimento de vulnerabilidade crítica de segurança, ainda que temporária, de sistema, dispositivo ou programa informático e, com qualquer intenção ilegítima, revelar esse facto a outrem, de forma adequada a criar perigo da prática de crime previsto na presente lei, é punido com pena de prisão até 3 anos ou com pena de multa.»**

Analisando esta norma, tendo em conta a parte acima sublinhada, consideramos que se vai tornar a sua aplicação baseada em suspeitas e intenções.

Note-se ainda que toda a norma se apresenta desprovida de critérios objectivos a não ser a revelação de um facto a um terceiro, podendo levar a acusações e condenações assentes em supostas intenções.

Pode-se considerar que esta norma consubstancia um crime de perigo, não sendo necessário que o crime seja efectivamente praticado.

Pode questionar-se se, tendo em conta que todos os tipos de crime possibilitam a punição da tentativa, como se articula este crime com os restantes em sede de co-

autoria. Poderá o «delator» ser condenado por este crime e pelo crime que vier a ser praticado em cúmulo jurídico, se se provar que foi o autor moral ou instigador?

6. **Artigo 16.º - A - «Conservação e fornecimento de registos de tradução de endereços de rede»**

Este preceito, que foi aditado à Lei n.º 11/2009 pelo artigo 26.º da Lei n.º 13/2019, contém um termo técnico que não aparece definido e que é «registos de tradução de endereços de rede»[6].

Achamos que deve ser incluída no articulado essa definição, de modo a tornar mais clara a letra da lei e evitar dúvidas de interpretação.

7. **Artigo 4.º da PL - Republicação - «...integrando as alterações aprovadas pela presente lei e pela Lei n.º 13/2019 (Lei da cibersegurança)**

Em termos de técnica legislativa, a consolidação num único documento de diversas alterações legislativas ao mesmo diploma é uma boa medida, pelo que concordamos com a republicação da lei.

8. **Artigo 5.º da PL - Entrada em vigor - «22 de Dezembro de 2019»**

Constatamos e concordamos com a fixação da data de 22 de Dezembro para fazer coincidir a entrada em vigor da PL ora em análise com a entrada em vigor da Lei n.º 13/2009 – Lei da Cibersegurança.

[6] Julgamos que o legislador se quer referir ao que em língua inglesa se denomina por «network address translation». Consiste este conceito no que também se denomina por *masquerading*, e que se traduz numa técnica que consiste me reescrever, utilizando-se uma tabela *hash*, os endereços IP de origem de um pacote que passam por um *router* ou *firewall* de maneira a que um computador de uma rede interna tenha acesso ao exterior ou à *World Wide Web*.

III

Conclusões

Na sequência do exposto acima, e para além do que expusemos em relação a diversas normas, apresentamos as seguintes conclusões:

a) Necessidade de coordenação internacional

Da leitura do articulado actual da Lei n.º 11/2009 bem como das alterações previstas em sede da PL, não existe nenhum capítulo ou mesmo norma que trate especificamente da cooperação internacional.

Tal contrasta, por exemplo, com a Lei do cibercrime portuguesa, que lhe consagra um capítulo inteiro com sete artigos.

Deve também ser tido em conta o disposto no Artigo 6.º do Código de Processo Penal (Aplicação da lei processual penal no espaço): «A lei processual penal é aplicável em toda a Região Administrativa Especial de Macau e fora dela nos limites definidos pelas convenções internacionais aplicáveis na Região Administrativa Especial de Macau e pelos acordos no domínio da cooperação judiciária.»

A Macau não se aplica a Convenção sobre o Cibercrime, assinada em Budapeste a 23 de Novembro de 2001, por estados membros do Conselho da Europa e outros estados signatários. Nos termos da Parte III, ponto 16, do documento denominado Minuta do Relatório Explicativo relativo à Convenção sobre o Cibercrime, a Convenção tem por objecto principal:

- A harmonização dos elementos relativos a infracções no contexto do direito penal substantivo de âmbito nacional e das disposições conexas na área da cirbercriminalidade,
- A definição, ao abrigo do código de processo penal interno, dos poderes necessários para investigar e intentar acções penais relativamente a tais infracções, assim como a outras infracções cometidas por meio de um sistema informático ou às provas com

elas relacionadas e existentes sob a forma electrónica,
- A implantação de um regime rápido e eficaz de cooperação internacional.

Assim, só com uma adequada consideração da necessidade de cooperação internacional é que a lei contra a criminalidade informática poderá, em nossa opinião, ter êxito.
Neste sentido, entendemos que, para que a cooperação internacional seja efectiva e, tendo em conta que a Convenção de Budapeste foi assinada por estados que fazem parte do Conselho da Europa e não só, o Governo da RAEM deveria diligenciar no sentido de adoptar as suas soluções em termos de direito interno, adaptando-as nos casos em que tal se revele necessário.

b) A **alteração ao n.º1, alínea 6) do artigo 16.º** não é de fundo, inovando apenas na possibilidade de os órgãos de polícia criminal poderem estender a busca a dados armazenados na computação em nuvem, dados que se encontram para além da jurisdição da RAEM. Não é uma prática nova, nem incomum.

No entanto, sem prejuízo do acima dito, não se quer deixar de salientar que a proposta de lei intitulada "Alteração à Lei n.º 11/2009 – Lei de combate à criminalidade informática" não é explícita quanto ao modo como as medidas especiais previstas no artigo 16.º serão efectuadas no ambiente digital transfronteiriço, não obstante se crer que se deverá sempre conjugar com o regime de prova previsto no Código de Processo Penal.

c) **Julgamos que se deve ponderar uma reformulação mais profunda da Lei n.º 11/2009**, tendo em conta que a realidade e evolução tecnológica implica nesta área uma muito maior atenção do legislador ao que se passa em termos de direito comparado quanto à evolução legislativa necessária de modo a manter um diploma, neste domínio, actualizado e eficiente, pelo que se deve equacionar o acolhimento de soluções de outras jurisdições.

d) Por outro lado, com a **harmonização desejável** - relativamente a esta matéria – da legislação de Macau com a aplicada noutras jurisdições de modo a evitar a possível exploração de lacunas pelo cada vez mais sofisticado crime internacional, sugerimos que a Convenção sobre o cibercrime seja considerada como o padrão legislativo a atingir, com as adaptações necessárias a Macau.

Neste sentido, achamos que o Governo da RAEM deve envidar esforços no sentido de adoptar o conjunto de soluções constantes da Convenção de Budapeste, obviamente com as adaptações que se revelem necessárias.

É este, com as limitações de tempo impostas, o nosso parecer que apresentamos à consideração da 1.ª Comissão da Assembleia Legislativa.

Aprovado em reunião da Direcção da AAM

de 14 de Novembro de 2019