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