# Nota justificativa

# Alteração à Lei n.º 11/2009 – Lei de combate à criminalidade informática

*(Proposta de lei)*

## 1. Objectivos

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.

Complementarmente, dado que a Lei n.º 13/2019 procedeu ao aditamento de um novo capítulo (capítulo III-A, compreendendo os artigos 16.º-A e 16.º-B) à Lei n.º 11/2009, e atendendo às novas alterações agora propostas, sugere-se que a Lei de combate à criminalidade informática seja republicada, para melhor segurança jurídica e mais fácil conhecimento pelos cidadãos.

**2. Criminalização das "estações" ilegais simuladas**

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"*.

Estas "estações" operam induzindo os aparelhos de telemóvel a identificá-las como sendo uma estação de telecomunicações legítima e que, portanto, se devem conectar a elas. De facto, os aparelhos de telemóvel conectam-se a tais estações porque, tecnicamente, não conseguem certificar-se se elas são legítimas ou não, e porque estão construídos para optimizar a comunicação e, portanto, a procurar ligar-se, de forma automática, à estação mais próxima, por, em regra, ser a que tem o sinal mais forte.

As "estações" ilegais 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.)*.

Estas práticas causam 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.

Perante esta situação, a Polícia Judiciária tem procurado combater constantemente os crimes ligados a estas práticas de simulação de estações de telecomunicações móveis. Desde Novembro de 2014 até meados de Agosto de 2017, a Polícia Judiciária efectuou um total de 17 operações de combate a este tipo de estações, tendo esmagado 86 estações deste tipo e apresentado 66 pessoas envolvidas ao Ministério Público.

No entanto, 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.

Acresce que a maior parte dos suspeitos de crimes associados às estações emissoras simuladas *(ou seja, crimes que são praticados utilizando as estações emissoras simuladas como um instrumento desses crimes)* é residente do Interior da China; assim, quando os crimes são puníveis com penas de prisão até 3 anos, é impossível, de acordo com as normas jurídicas vigentes em Macau, aplicar a medida de prisão preventiva. Por isso, a maioria das pessoas envolvidas é expulsa da RAEM, procedendo-se, depois, à aplicação da medida de interdição de entrada.

Aliás, quanto aos indivíduos que operam as estações emissoras simuladas, eles podem invocar o alheamento dos crimes (burlas, propostas de jogo ilícito, etc.), argumentando que se limitavam a operar a estação não autorizada e que esse facto, só por si, não constitui crime, à luz da lei de Macau, mas tão-somente uma infracção administrativa, punível com multa de 120 000 a 1 000 000 patacas e encerramento imediato das instalações, de acordo com o artigo 26.º do Regulamento Administrativo n.º 7/2002 (Operação de redes públicas de telecomunicações e prestação de serviços de telecomunicações de uso público móveis terrestres).

Conclui-se, assim, que o quadro legal descrito não propicia o combate a este tipo de práticas ilegais, que são tão lucrativas para os criminosos e tão nocivas para os cidadãos e para a imagem da RAEM.

Aliás, as tentativas de reprimir penalmente estas condutas com base no artigo 8.º da Lei n.º 11/2009 também não têm tido sucesso, pois os órgãos judiciais entendem que os criminosos não interferem com o normal funcionamento das emissões dos operadores de rede legais.

Por isso, a proposta de lei prevê o aditamento de um novo artigo à Lei n.º 11/2009 (artigo 9.º-A), pelo qual se tipifica como crime de perigo (independentemente de qualquer resultado concreto danoso), punível com pena de prisão até 3 anos, a prática de utilizar dispositivos e programas informáticos associados a aparelhos emissores com o objectivo de simular uma estação de serviços de telecomunicações de uso público móveis terrestres.

Em determinadas circunstâncias que são susceptíveis de maior censurabilidade e maior gravidade objectiva da conduta, pela sua danosidade social, a moldura penal deverá ser de 1 a 5 anos, admitindo, em abstracto, a medida de prisão preventiva. Essas circunstâncias de maior censurabilidade são as três seguintes: se o agente tiver intenção lucrativa com a estação simulada; se ele utilizar a "estação" para transmitir qualquer publicidade proibida por lei e/ou para disseminar, divulgar ou qualquer forma de incitar à prática, adesão ou consumo de pornografia, prostituição ou actividades de jogo ilícito; ou se a "estação" for instalada para preparar, facilitar ou executar um outro crime.

Como nota final, sublinha-se que o que se pretende com a presente alteração legislativa não é criminalizar a instalação de estações não autorizadas de telecomunicações, protegendo o bem jurídico da integridade e exclusividade do espectro radioeléctrico; o que se quer é criminalizar a utilização insidiosa, mais dissimulada, de dispositivos e programas informáticos, associados a aparelhos emissores, simulando estações de telecomunicações, com o objectivo de proteger a privacidade dos cidadãos e de evitar o uso de tais "estações" simuladas como instrumentos para o cometimento de crimes pelos delinquentes.

**3. Maior protecção penal dos sistemas informáticos utilizados pelos operadores de infra-estruturas críticas e outras entidades relevantes**

À medida que a dependência da *internet* de governos, empresas, instituições e dos cidadãos individuais tende a ser cada vez maior, aumentam progressivamente os ataques aos sistemas informáticos. Em Maio e Junho de 2017, vários países foram atingidos por dois ataques com vírus para extorsão, *"Wannacry"* e *"Petya"*, e em Macau alguns sistemas informáticos também chegaram a ser invadidos.

Apesar de os sistemas informáticos das infra-estruturas locais não terem sido afectados por aqueles dois ataques, verifica-se que estas acções no mundo cibernético têm sido difíceis de prevenir. Se ocorrer um ataque deste género aos referidos sistemas, tal é susceptível de afectar gravemente o normal funcionamento da rede de telecomunicações e outros serviços

essenciais e de paralisar serviços públicos, prejudicando a estabilidade social. Por isso, devemos tomar precauções (como diz um ditado chinês "em tempos prósperos, temos que nos preparar para a adversidade"), tal como, aliás, vários governos vêm fazendo, preocupados com a evolução e tendência desse novo tipo de criminalidade.

Assim, é conveniente que a RAEM aproveite a oportunidade da revisão da lei para efectivar mais amplamente a protecção penal conferida aos sistemas informáticos utilizados pelos operadores de infra-estruturas críticas, independentemente da respectiva natureza pública ou privada, tal como esses operadores estão definidos na Lei n.º 13/2019.

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.

**4. Extracção de cópia de dados informáticos que possam encontrar-se fora da RAEM, para efeitos de prova no processo penal**

A vulgarização dos serviços de computação em nuvem e a deslocalização geográfica da informação para diversas jurisdições têm criado obstáculos jurídicos muito importantes, em termos práticos, à investigação criminal; em certos casos, esses obstáculos podem conduzir ao bloqueio da investigação criminal e, consequentemente, à impunidade.

A Lei n.º 11/2009 dispõe, na alínea 6) do n.º 1 do artigo 16.º que é possível à autoridade judiciária *"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."*

Todavia, parece não fazer muito sentido lógico que a RAEM imponha esta restrição a si própria, unilateralmente, porque 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.

Em certa medida, a solução será também semelhante à da lei belga. O artigo *39bis* do Código de Processo Penal da Bélgica prevê a possibilidade de ser alargada a pesquisa informática a outras jurisdições independentemente da sua localização, desde que, quando se suspeite que a informação não esteja armazenada na Bélgica, a informação não seja eliminada mas apenas copiada e sob condição de o Ministro da Justiça informar o Estado pesquisado, quando este possa ser identificado (o que, ao que parece nunca aconteceu, na prática).

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.

**5. Autonomização de uma espécie de crime de violação de segredo profissional**

O Código Penal já prevê, como regras gerais, a título de crime de perigo, a punição da violação de segredo profissional, com pena de prisão até 1 ano ou com pena de multa até 240 dias (artigo 189.º). Por outro lado, o artigo 190.º também prevê a mesma pena para quem se aproveitar de segredo relativo à actividade comercial, industrial, profissional ou artística alheia, de que tenha tomado conhecimento em razão do seu estado, ofício, emprego, profissão ou arte, e provocar deste modo prejuízo a outra pessoa ou à RAEM (como crime de dano, portanto).

Ora, os artigos referidos estão incluídos num capítulo do Código Penal que expressamente se refere aos interesses da reserva da vida privada (Capítulo VII do Título I do Livro II). Todavia, 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.