



澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
行政長官辦公室
Gabinete do Chefe do Executivo

Nota Justificativa

Combate à Criminalidade Informática (Proposta de lei)

Com o crescente avanço das tecnologias da informação, verifica-se uma vulgarização da utilização da informática e da Internet, o que levou ao aumento significativo da eficácia do trabalho, das comunicações, da aprendizagem e das diversões na vida quotidiana, e trouxe grandes facilidades e vantagens para a vida das pessoas. Entretanto, a par deste avanço verifica-se o aparecimento gradual de criminosos que utilizam as tecnologias da informação como uma nova plataforma favorável à prática de crimes, o que coloca novos desafios a todos os países e regiões do mundo no âmbito da prevenção e combate à criminalidade informática.

Como é do conhecimento geral, a criminalidade informática assume várias expressões e caracteriza-se pela vulgarização, sofisticação técnica, ocultação, celeridade e por ser de difícil investigação, pelo que os métodos tradicionais de combate à criminalidade informática se revelam insuficientes face ao carácter virtual dos actos praticados na Internet. Para além de praticarem os tipos tradicionais de crimes através da informática, como sejam a burla, o furto, o dano, entre outros, os criminosos aproveitam também as tecnologias da informação para a prática de um novo tipo de criminalidade, nomeadamente a propagação de vírus informáticos, a intercepção ilegítima de dados informáticos, a obstrução de sistema informático, entre outros, fazendo com que a segurança e a funcionalidade na área informática sejam ameaçadas.

Face a diversos actos ilícitos que consistem na utilização abusiva das tecnologias da informação, as medidas legislativas adoptadas, para além de prevenirem a ocorrência de actos criminosos, visam também promover uma cultura de segurança no ciberespaço, protegendo os dados pessoais e a privacidade, a fim de fortalecer a confiança das pessoas para com a sociedade da informação.



澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
行政長官辦公室
Gabinete do Chefe do Executivo

Para o efeito, foi assinada pelo Conselho da Europa, em Budapeste a 23 de Novembro de 2001, a Convenção sobre o Cibercrime, e muitas regiões e países, presentemente, já procederam a acções legislativas quanto à prevenção e combate à criminalidade informática, nomeadamente o Interior da China, Hong Kong, Taiwan, Singapura, Portugal, Alemanha e Estados Unidos.

No ordenamento jurídico da RAEM, apenas no Código Penal estão previstos os crimes de burla informática (artigo 213.º) e de devassa por meio de informática (artigo 187.º). Por exemplo, quanto aos actos de dano provocados em sistemas informáticos, também não existem normas específicas para a sua regulamentação, podendo os mesmos ser punidos apenas como crimes de dano previstos nos artigos 206.º e 207.º. Na legislação avulsa, apesar de existirem algumas normas relativas a esta matéria, como é o caso do artigo 14.º da Lei n.º 8/2002 (Regime do bilhete de identidade de residente da Região Administrativa Especial de Macau), que estabelece os princípios relativos à responsabilidade penal de quem atente contra a segurança do sistema do BIR, as medidas legislativas para o combate à criminalidade informática são insuficientes, pelo que há necessidade de aperfeiçoar as normas em causa, no sentido de estabelecer determinados novos tipos de crimes relativos a actos que prejudiquem a informática ou a Internet, agravando ainda as penas para certos actos, que já são considerados crimes, mas que agora sejam praticados através da Internet, por exemplo, os crimes de instigação pública a um crime, difamação, injúria e devassa da vida privada, previstos no Código Penal, quando os mesmos sejam praticados através da Internet. É de realçar que a população de Macau goza da liberdade de expressão nos termos da lei, sendo um direito fundamental protegido por força da Lei Básica. No que se refere às ideias apresentadas, independentemente de as mesmas serem exprimidas através da Internet, o agente só é punido se violar as normas previstas na lei. Assim, na Proposta de Lei, não se encontram estipulados novos tipos de crimes que envolvam qualquer matéria relacionada com a liberdade de expressão, nem se impõem mais restrições à mesma.

A presente Proposta de Lei foi elaborada com base na Convenção sobre o Cibercrime do Conselho da Europa, bem como nas legislações relacionadas das regiões e países acima referidos, tendo como conteúdo principal o seguinte:



澳門特別行政區政府
Governo da Região Administrativa Especial de Macau

行政長官辦公室
Gabinete do Chefe do Executivo

1. Em termos formais, optou-se pela elaboração de uma lei especial em alternativa à inserção destes novos tipos de crime no Código Penal, pelo facto de, por um lado, o Código Penal não punir as pessoas colectivas, não correspondendo às exigências das normas dos instrumentos de direito internacional relativas à efectivação da responsabilidade penal das pessoas colectivas que pratiquem crimes informáticos, e por outro lado, garantir a estabilidade do Código Penal, e fazer com que as normas sobre o combate à criminalidade informática possam corresponder às necessidades de desenvolvimento da sociedade, no sentido de prevenir situações complexas em que o Código Penal ficaria sujeito a sucessivas alterações resultantes dos problemas originados pelo desenvolvimento acelerado das tecnologias da informação.

2. Quanto ao conteúdo material penal:

- (1) Tipificaram-se novos tipos de actos criminosos. Foram tipificados como crimes os actos ilícitos de obtenção ou utilização ilegítima de dados informáticos, acesso ilegítimo a sistema informático, interceptação ilegítima de dados informáticos, dano a dados informáticos, obstrução de sistema informático, dispositivos ou dados informáticos destinados à prática de crimes e falsidade informática.
- (2) Previu-se a responsabilidade penal das pessoas colectivas que praticam aqueles crimes. No ordenamento jurídico da RAEM, tem sido prevista, face a determinados crimes, a efectivação da responsabilidade penal em relação às pessoas colectivas, tal como acontece na Lei n.º 4/2002 (Relativa ao cumprimento de certos actos de direito internacional), na Lei n.º 2/2006 (Prevenção e repressão do crime de branqueamento de capitais), na Lei n.º 3/2006 (Prevenção e repressão dos crimes de terrorismo) e na Lei n.º 6/2008 (Combate ao crime de tráfico de pessoas), que estipulam a responsabilidade penal das pessoas colectivas, sendo estas normas excepcionais em relação às regras gerais da responsabilidade das pessoas singulares previstas no artigo 10.º do Código Penal. Além disso, a responsabilidade penal das pessoas colectivas prevista na Proposta de Lei corresponde também às exigências das normas dos instrumentos de direito internacional relativas à efectivação



澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
行政長官辦公室
Gabinete do Chefe do Executivo

da responsabilidade penal das pessoas colectivas que pratiquem crimes informáticos.

- (3) Previu-se a agravação da pena: para proteger a confidencialidade e a integridade de sistemas informáticos ou dados informáticos dos órgãos executivo, legislativo ou judicial ou de outras entidades públicas, estipulando ainda a Proposta de Lei a agravação de um terço da respectiva pena nos casos em que os actos criminosos envolvam sistemas informáticos ou dados informáticos dos órgãos e outras entidades públicas acima referidos; além disso, para melhor prevenção e combate a qualquer crime praticado através da Internet como meio amplo de transmissão, a Proposta de Lei prevê também a agravação de um terço da respectiva pena.

3. Relativamente às disposições processuais penais, foram atribuídos às autoridades competentes meios de investigação mais eficazes para o combate à criminalidade informática, incluindo:

- (1) Previsão expressa da admissibilidade como prova do sistema informático, do suporte de armazenamento de dados informáticos e dos dados ou programas informáticos.
- (2) Previsão de várias medidas necessárias e urgentes que podem ser adoptadas pelos órgãos de polícia criminal mesmo antes de receberem ordem da autoridade judiciária competente para procederem a investigações, quando os órgãos de polícia criminal tiverem razões para crer que os dados informáticos são relevantes para uma investigação criminal. Estas medidas incluem: a conservação expedita dos dados informáticos, o acesso a dados de tráfego (não incluindo dados relativos ao conteúdo), o impedimento do acesso a dados informáticos específicos e ilegais, entre outras. No entanto, a adopção destas medidas está sujeita ao controlo da autoridade judiciária competente, devendo os órgãos de polícia criminal, comunicar imediatamente as diligências realizadas à autoridade judiciária competente, que a apreciará em ordem à sua validação, sob pena de nulidade.