REGIÃO ADMINISTRATIVA ESPECIAL DE MACAU

Lei n.º 11/2009

Lei de combate à criminalidade informática

A Assembleia Legislativa decreta, nos termos da alínea 1) do **artigo 71.º da Lei Básica da Região Administrativa Especial de Macau**, para valer como lei, o seguinte:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objecto

A presente lei tem como objecto a tipificação de crimes informáticos e a instituição de um regime de recolha de prova em suporte electrónico.

Artigo 2.º

Definições

Para efeitos da presente lei considera-se:

1) Sistema informático: qualquer dispositivo isolado ou grupo de dispositivos interligados ou relacionados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos;

2) Dados informáticos: qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo um programa apto a fazer um sistema informático executar uma função;

3) Programa informático: instruções capazes, quando inseridas num suporte explorável em sistema informático, de permitir ao sistema informático indicar, executar ou produzir determinada função, tarefa ou resultado;

4) Dados de base relativos aos assinantes de serviços de Internet: informações contidas sob a forma de dados informáticos ou sob qualquer outra forma, detidas por um prestador de serviços de Internet e que digam respeito aos assinantes dos seus serviços, que não sejam dados de tráfego ou dados informáticos relativos ao conteúdo de uma comunicação ou de uma mensagem e que permitam determinar o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a

esse respeito e o período de serviço, a identidade, a morada postal ou domiciliária e o número de telefone do assinante ou qualquer outro número de contacto, os dados respeitantes à facturação e ao pagamento, bem como qualquer outra informação sobre a localização do equipamento de comunicação, disponíveis com base num contrato ou acordo de serviços;

5) Dados de tráfego: todos os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo de serviço subjacente;

6) Emissão electromagnética: sinais ou ondas que são emitidos por componentes electrónicos e fios transportando sinais electrónicos.

CAPÍTULO II

Disposições penais

Artigo 3.º

Direito subsidiário

1. Aos crimes previstos na presente lei são subsidiariamente aplicáveis as normas do **Código Penal**.

2. As penas previstas na presente lei não se aplicam se outras penas mais graves ao caso couberem por força de outra disposição legal.

Artigo 4.º

Acesso ilegítimo a sistema informático

1. Quem, sem autorização e com qualquer intenção ilegítima, aceder à totalidade ou a parte de um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2. Quando o acesso for conseguido através da violação de medidas de segurança, o agente é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.

3. No caso previsto no n.º 1, o procedimento penal depende de queixa.

Artigo 5.º

Obtenção, utilização ou disponibilização ilegítima de dados informáticos

1. Quem, sem autorização e com qualquer intenção ilegítima, obtiver, utilizar ou colocar à disposição de outrem dados informáticos que não lhe sejam destinados, contidos num sistema

informático ou num suporte de armazenamento de dados informáticos, ao qual tenha tido acesso ainda que legítimo, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2. O agente é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias quando os dados informáticos referidos no número anterior sejam relativos à vida privada da pessoa, designadamente a intimidade da vida familiar ou sexual, à saúde, à raça ou à origem étnica, às convicções políticas, religiosas ou filosóficas, ou ainda a segredo legalmente protegido.

3. O procedimento penal depende de queixa.

Artigo 6.º

Intercepção ilegítima de dados informáticos

1. Quem, sem autorização e através de meios técnicos, interceptar dados informáticos em transmissões não públicas dentro de um sistema informático, a ele destinadas ou dele provenientes, incluindo emissões electromagnéticas provenientes de um sistema informático que veicule esses dados, é punido com pena de prisão até 3 anos ou com pena de multa.

2. A tentativa é punível.

Artigo 7.º

Dano a dados informáticos

1. Quem, sem autorização, danificar, deteriorar, alterar, suprimir, eliminar ou adicionar dados informáticos ou, por qualquer forma, lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou com pena de multa.

2. A tentativa é punível.

3. Se o prejuízo patrimonial causado for de valor elevado, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.

4. A pena é a de prisão de 2 a 10 anos se:

1) O prejuízo patrimonial causado for de valor consideravelmente elevado; ou

2) Os dados informáticos referidos no n.º 1 possuírem importante valor científico, artístico ou histórico, ou significado importante para o desenvolvimento tecnológico ou económico.

5. Nos casos previstos nos n.os 1 e 2, o procedimento penal depende de queixa.

Artigo 8.º

Obstrução de sistema informático

1. Quem, por qualquer forma, obstruir gravemente o funcionamento de um sistema informático, nomeadamente através da introdução, transmissão, danificação, deterioração, alteração, supressão ou eliminação de dados informáticos, é punido com pena de prisão até 3 anos ou com pena de multa.

2. A tentativa é punível.

3. Se o prejuízo patrimonial causado for:

1) De valor elevado, o agente é punido com pena de prisão de 1 a 5 anos;

2) De valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 10 anos.

Artigo 9.º

Dispositivos ou dados informáticos destinados à prática de crimes

1. É punido com pena de prisão até 3 anos ou com pena de multa, quem produzir, importar, exportar, vender, distribuir ou colocar à disposição de outrem:

1) Dispositivo ou programa informático concebido ou adaptado essencialmente para a prática de um dos crimes previstos nos artigos 4.º a 8.º; ou

2) Senha, chave secreta ou dados informáticos similares que permitam o acesso à totalidade ou a parte de um sistema informático destinados à prática de um dos crimes previstos nos artigos 4.º a 8.º

2. O disposto no número anterior não se aplica aos casos em que as acções referidas visam proceder a ensaios autorizados, à protecção dos sistemas informáticos ou a outros fins que não sejam ilícitos.

Artigo 10.º

Falsificação informática

1. Quem, com intenção de provocar engano nas relações jurídicas, introduzir, alterar, suprimir ou eliminar dados informáticos ou, por outra forma, interferir num tratamento informático de dados, quando esses dados sejam susceptíveis de servir como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado, ou bem assim, os utilize para os fins descritos, é punido com pena de prisão até 3 anos ou com pena de multa.

2. Na mesma pena incorre quem utilizar documento produzido a partir de dados informáticos que tenham sido objecto dos actos referidos no número anterior, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo para si ou para terceiros.

3. A tentativa é punível.

4. O agente é punido com pena de prisão de 1 a 5 anos se os factos referidos nos n.os 1 e 2:

1) Forem praticados por funcionário no exercício das suas funções;

2) Respeitarem a documento de especial valor, qualificado como tal nos termos da lei; ou

3) Respeitarem a assinatura electrónica qualificada ou a documento ao qual tenha sido aposta assinatura electrónica qualificada.

Artigo 11.º

Burla informática

1. É punido com pena de prisão até 3 anos ou com pena de multa quem, com intenção de obter enriquecimento ilegítimo para si ou para terceiro, causando prejuízo patrimonial a outrem:

1) Introduzir, alterar, suprimir ou eliminar dados informáticos;

2) Interferir no resultado de tratamento de dados informáticos;

3) Estruturar incorrectamente programa informático; ou

4) Intervier no funcionamento de sistema informático.

2. A tentativa é punível.

3. Se o prejuízo patrimonial causado for:

1) De valor elevado, o agente é punido com pena de prisão de 1 a 5 anos;

2) De valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 10 anos.

4. Nos casos previstos nos n.os 1 e 2, o procedimento penal depende de queixa.

Artigo 12.º

Agravação da pena

1. Se os crimes previstos na presente lei envolverem dados ou sistemas informáticos dos órgãos executivo, legislativo ou judicial ou de outras entidades públicas da Região Administrativa

Especial de Macau (RAEM), as penas previstas nos artigos 4.º a 11.º são agravadas de um terço nos seus limites mínimo e máximo.

2. O disposto no n.º 2 do artigo 177.º e na alínea b) do artigo 192.º do **Código Penal** é aplicável aos crimes neles indicados, cometidos através da Internet quando esta seja utilizada como meio de ampla difusão.

Artigo 13.º

Responsabilidade penal das pessoas colectivas

1. As pessoas colectivas, ainda que irregularmente constituídas, e as associações sem personalidade jurídica são responsáveis pelos crimes previstos na presente lei quando cometidos, em seu nome e no interesse colectivo:

1) Pelos seus órgãos ou representantes; ou

2) Por uma pessoa sob a autoridade destes, quando o cometimento do crime se tenha tornado possível em virtude de uma violação dolosa dos deveres de vigilância ou controlo que lhes incumbem.

2. A responsabilidade das entidades referidas no número anterior não exclui a responsabilidade individual dos respectivos agentes.

3. Pelos crimes referidos no n.º 1 são aplicáveis às entidades aí referidas as seguintes penas principais:

1) Multa;

2) Dissolução judicial.

4. A pena de multa é fixada em dias, no mínimo de 100 e no máximo de 1 000.

5. A cada dia de multa corresponde uma quantia entre 100 patacas e 20 000 patacas.

6. Se a multa for aplicada a uma associação sem personalidade jurídica, responde por ela o património comum e, na sua falta ou insuficiência, solidariamente, o património de cada um dos associados.

7. A pena de dissolução judicial só é decretada quando os fundadores das entidades referidas no n.º 1 tenham tido a intenção, exclusiva ou predominante, de, por meio delas, praticar os crimes aí previstos ou quando a prática reiterada de tais crimes mostre que a entidade está a ser utilizada, exclusiva ou predominantemente, para esse efeito, quer pelos seus membros, quer por quem exerça a respectiva administração.

8. Às entidades referidas no n.º 1 podem ser aplicadas as seguintes penas acessórias:

1) Proibição do exercício de certas actividades por um período de 1 a 10 anos;

2) Privação do direito a subsídios ou subvenções outorgados por serviços ou entidades públicos;

3) Injunção judiciária;

4) Publicidade da decisão condenatória a expensas do condenado, num jornal de língua chinesa e num jornal de língua portuguesa dos mais lidos na RAEM, bem como através de edital, redigido nas referidas línguas, por período não inferior a 15 dias, no local de exercício da actividade, por forma bem visível ao público.

9. As penas acessórias podem ser aplicadas cumulativamente.

10. A cessação da relação laboral que ocorra em virtude da aplicação da pena de dissolução judicial ou de qualquer das penas acessórias previstas no n.º 8 considera-se, para todos os efeitos, como sendo resolução do contrato de trabalho sem justa causa por iniciativa do empregador.

CAPÍTULO III

Disposições processuais penais

Artigo 14.º

Disposição geral

Na investigação e nos actos processuais relativos a processos por crimes previstos na presente lei e por crimes cometidos por meio do sistema informático, assim como na recolha de prova em suporte electrónico pela prática de qualquer crime, observam-se as regras constantes do **Código de Processo Penal** e legislação complementar, com as especialidades previstas nos artigos seguintes.

Artigo 15.º

Apreensões

1. Podem ser efectuadas apreensões de sistema informático, de suporte de armazenamento de dados informáticos e de dados informáticos ou feita uma cópia dos dados informáticos susceptíveis de servir como prova e constantes do sistema informático ou do suporte de armazenamento de dados informáticos, sendo a cópia junta aos autos, restituindo-se o respectivo sistema informático ou o suporte de armazenamento de dados informáticos.

2. A cópia a que se refere o número anterior é feita em duplicado, sendo este selado e conservado, a fim de preservar a integridade dos dados informáticos armazenados.

3. O levantamento do selo só é possível quando autorizado ou ordenado por despacho judicial e desde que haja fundadas dúvidas sobre a autenticidade da cópia efectuada.

4. Ao levantamento do selo aplica-se o disposto no artigo 169.º do **Código de Processo Penal**.

5. O disposto nos artigos 164.º e 235.º do **Código de Processo Penal** é aplicável, com as necessárias adaptações, à apreensão de correio electrónico ou de qualquer outra forma de comunicação particular sob a forma electrónica, quer estas tenham ou não sido recebidas pelo seu destinatário.

Artigo 16.º

Medidas especiais

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:

1) Ordenar a conservação expedita dos dados informáticos, devendo o prestador de serviços de Internet preservar a integridade desses dados informáticos por um período considerado necessário até um máximo de 90 dias e fornecer os dados de tráfego suficientes para a identificação dos fornecedores de serviços no âmbito da Internet e da via através da qual a comunicação foi efectuada;

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;

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.

2. 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.

3. Nos casos referidos no número anterior, a 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.

4. A ordem emitida ao abrigo do disposto na alínea 5) do n.º 1 é impugnável por qualquer titular de interesse pessoal, directo e legítimo, no prazo de 10 dias, perante o juiz de instrução criminal.

5. Os dados informáticos obtidos ou conservados ao abrigo do disposto no n.º 1 são, conforme os casos, destruídos, restituídos a quem de direito ou restituídos à situação jurídica anterior à adopção da respectiva diligência, em caso de recusa de validação da diligência por parte da autoridade judiciária competente ou decorrido o prazo legal sem que a validação tenha sido efectuada.

6. A recusa do cumprimento das ordens previstas nos n.os 1 e 2 constitui crime de desobediência qualificada nos termos do n.º 2 do artigo 312.º do **Código Penal**.

CAPÍTULO IV

Disposições finais

Artigo 17.º

Revogação

É revogado o artigo 213.º do **Código Penal**.

Artigo 18.º

Entrada em vigor

A presente lei entra em vigor 30 dias após a data da sua publicação.

Aprovada em 24 de Junho de 2009.

A Presidente da Assembleia Legislativa, Susana Chou.

Assinada em 26 de Junho de 2009.

Publique-se.

O Chefe do Executivo, Ho Hau Wah.