3ª COMISSÃO PERMANENTE

PARECER N.º 3/III/2009

Assunto: Proposta de lei intitulada «*Lei de combate à criminalidade informática*».

I - Introdução

O Governo da Região Administrativa Especial de Macau apresentou, em 12 de Fevereiro de 2009, a proposta de lei intitulada «*Combate à criminalidade informática*», a qual foi no mesmo dia admitida pela Presidente da Assembleia Legislativa, nos termos regimentais.

A proposta de lei foi apresentada, discutida e votada na generalidade, em reunião plenária realizada no dia 23 de Fevereiro de 2009, tendo sido aprovada por maioria, com 19 votos a favor, 2 votos contra e 1 abstenção. Na mesma data, a proposta de lei foi distribuída a esta Comissão para efeitos de exame e emissão de parecer, nos termos do Despacho da Presidente da Assembleia Legislativa n.º 208/III/2009. Devido à complexidade técnica da proposta de lei, a Comissão necessitou de solicitar a prorrogação do prazo concedido pela

Presidente da Assembleia Legislativa para a apreciação na especialidade da proposta de lei, solicitação que foi gentilmente acolhida.

A Comissão, contando com o apoio de representantes do Governo, procedeu à análise da proposta de lei em reuniões realizadas nos dias 20 e 27 de Março, 1 de Abril, 21 e 25 de Maio e 17 de Junho de 2009. A par das reuniões da Comissão, foram realizadas reuniões de trabalho entre as assessorias da Assembleia Legislativa e do Governo, com vista ao aperfeiçoamento técnico da proposta de lei.

Dado o conteúdo da proposta de lei e a inclusão, no seu âmbito, de normas de natureza processual, a Comissão procedeu à auscultação da Associação de Advogados de Macau, em cumprimento do disposto no n.º 3 do artigo 30.º do Decreto-Lei n.º 42/95/M, de 21 de Agosto. Para tal, em 6 de Abril de 2009 foi enviado um ofício à referida Associação solicitando as suas opiniões relativas à proposta de lei em apreço. Até à data da assinatura do presente Parecer, a Comissão não recebeu qualquer comentário por parte da Associação de Advogados de Macau.

Em 27 de Maio de 2009, o Governo apresentou uma nova versão da proposta de lei que, em parte, reflecte as opiniões expressas no seio da Comissão e a análise técnico-jurídica efectuada pela assessoria da Assembleia Legislativa. Ao longo do presente Parecer, as referências aos artigos serão feitas com base na versão final da proposta de lei.

II – Apresentação

Nos termos da Nota Justificativa que acompanha a presente iniciativa legislativa, «*com o crescente avanço das tecnologias da informação, verifica-se uma vulgarização da utilização da informática e da internet, [mas também] 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. (...) [Esta] 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*».

Ainda de acordo com a Nota Justificativa, «*no ordenamento jurídico da RAEM (...) 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 (...)».

A presente iniciativa legislativa segue de perto a Convenção do Conselho da Europa sobre o Cibercrime, assinada em Budapeste a 23 de Novembro de 2001 e a legislação de prevenção e combate à criminalidade informática, nomeadamente do Interior da China, Hong Kong, Taiwan, Singapura, Portugal, Alemanha e Estados Unidos.

Na apresentação da proposta de lei, o proponente realça como aspectos fundamentais:

1. Em termos formais, a opção pela elaboração de uma lei especial em alternativa à inserção destes novos tipos de crime no Código Penal;

2. Quanto ao conteúdo material penal:
   (1) A tipificação de novos tipos de actos criminosos, nomeadamente os actos ilícitos de obtenção ou utilização ilegítima de dados informáticos, acesso ilegítimo a sistema informático, intercepção 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) A previsão da responsabilidade penal das pessoas colectivas, correspondendo às exigências das normas dos instrumentos de direito

internacional relativas à efectivação da responsabilidade penal das pessoas colectivas que pratiquem crimes informáticos.

(3) A previsão da agravação da pena em determinadas situações, por forma a reforçar a protecção da confidencialidade e a integridade de sistemas informáticos ou dados informáticos.

3. Quanto às disposições processuais penais, a atribuição às autoridades competentes de meios de investigação mais eficazes para o combate à criminalidade informática, incluindo:

(1) A previsão expressa da admissibilidade como prova do sistema informático, do suporte de armazenamento de dados informáticos e dos dados ou programas informáticos.

(2) A previsão de várias medidas necessárias e urgentes, quando houver razões para crer que os dados informáticos são relevantes para uma investigação criminal, nomeadamente 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.

A Nota Justificativa realça ainda o facto de «*na Proposta de Lei, não se [encontrarem] estipulados novos tipos de crimes que envolvam qualquer matéria relacionada com a liberdade de expressão, nem se impõem mais restrições à mesma, [dado 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*».

III – Apreciação genérica

1. Nas sociedades modernas, as tecnologias da informação e da comunicação desempenham um papel fundamental tanto ao nível do desenvolvimento económico, como da realização pessoal dos cidadãos. A nível económico, «torna-se cada vez mais evidente que o bem estar económico das nações depende da sua integração na economia global. À medida que o ciberespaço se torna o principal meio para o comércio, torna-se igualmente mais importante que haja uma plataforma legal segura para o comércio electrónico».[1] A nível pessoal, os computadores e a internet em particular, facilitam os contactos entre pessoas e o acesso a conteúdos de outra forma dificilmente alcançáveis, assim como representam uma plataforma de liberdade ao nível da expressão de ideias. Neste sentido, «a internet, enquanto espaço e veículo de comunicação, democratizou o discurso público e incentivou a troca de ideias. A divulgação generalizada do pensamento individual está hoje facilitada, tendo a internet permitido que o cidadão comum tenha deixado de ser um mero consumidor passivo, para poder assumir um papel mais activo de produtor de comunicação».[2] Devido às suas características, as tecnologias da informação e da comunicação são hoje um factor essencial no desenvolvimento da personalidade de muitos cidadãos, para quem *a distância deixou de ser um obstáculo e a globalização passou a ser um dado adquirido.*[3]

---

[1] Peter Grabosky, 'The Global Cyber-Crime Problem: The Socio-Economic Impact', in *Cyber-Crime – The Challenge in Asia*, Roderic Broadhurst & Peter Grabosky (eds.), Hong Kong University Press (2005), p. 50.
[2] Pedro Pereira de Sena, *Privatização da Censura: Liberdade de expressão e controlo de conteúdos na Internet*, Segundas Jornadas de Direito e Cidadania da Assembleia Legislativa de Macau, «Direitos Fundamentais – Consolidação e Perspectivas de Evolução», 20-22 de Outubro de 2008.
[3] Parecer da 3ª Comissão Permanente n.º 2/II/2005, respeitante à proposta de lei intitulada «*Documentos e assinaturas electrónicas*», disponível em http://www.al.gov.mo/lei/leis/2005/05-2005/parecer.pdf.

Tal como já anteriormente reconhecido por esta Comissão,[4] «à medida que a utilização das novas tecnologias se vai generalizando, aumenta igualmente o risco inerente ao seu uso. São conhecidos múltiplos casos de falhas nos sistemas de segurança que expõem os utilizadores da *internet* a novas formas de criminalidade: da violação da privacidade à utilização abusiva de dados pessoais, passando por fraudes de natureza patrimonial ou outros tipos de crimes. Ao "admirável mundo novo" das novas tecnologias junta-se um lado mais sinistro que impede ou dificulta uma plena utilização de todas as potencialidades que os novos meios de comunicação proporcionam. Torna-se, assim, indispensável reforçar a segurança inerente à utilização da *internet*».

2. O facto de as tecnologias da informação poderem ter uma utilização abusiva e ilícita (isto é, desconforme à lei) não permite concluir imediata e necessariamente que tais práticas sejam merecedoras de uma resposta penal. Para tal, a ordem jurídica exige que se identifiquem bens jurídicos merecedores de tutela penal, que as condutas em causa possam representar um risco para tais bens jurídicos penalmente relevantes e que o direito penal seja o último recurso de protecção desses bens jurídicos, a utilizar apenas quando os demais meios de tutela se mostram ineficazes (princípio da subsidiariedade do direito penal). [5]

No momento em que a Assembleia Legislativa é chamada a intervir no combate à criminalidade informática, a Comissão procedeu à análise dos factores acima elencados e, tendo verificado a existência de desvalor do resultado e da acção, assim como a conformidade com o princípio da

---

[4] *Idem.*

[5] *Vd.* 見劉守芬、葉慧娟：《網絡越軌行爲犯罪化正當性探討》，載張平主編《網絡法律評論》（第六卷），法律出版社 2005 年.

subsidariedade do direito penal, pode desde já afirmar que as condutas ilícitas no âmbito das tecnologias da informação reúnem os requisitos necessários para que haja uma reacção por parte do direito penal:

a) Ao nível dos bens jurídicos potencialmente afectados, tais condutas podem constituir perigo para bens jurídicos que tradicionalmente são merecedores de protecção da lei penal, tais como a honra, a liberdade pessoal, a liberdade e a autodeterminação sexual, a reserva da vida privada, o património ou a segurança nas relações jurídicas. Por outro lado, a relevância pessoal, social e económica de tais tecnologias permite que seja erigida a própria segurança informática como bem jurídico autónomo merecedor de tutela penal, visando garantir a segurança das redes de telecomunicações públicas e promover a confiança na sua utilização.[6]

b) Relativamente à susceptibilidade dos meios informáticos representarem perigo para bens jurídicos penalmente relevantes, é comummente reconhecido que as suas características, tais como a celeridade, rigor, fiabilidade, tecnicidade e adaptabilidade, lhes atribuem um carácter potencialmente insidioso e clandestino, fazendo de tais meios instrumentos adequados para pôr em perigo bens jurídicos fundamentais, penalmente tutelados.[7]

c) Quanto ao princípio da subsidariedade do direito penal, pode identificar-se uma tendência internacional no sentido de fazer operar este ramo do

[6] *Vd.* Lorenzo Picotti, 'Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l'informatique', in *La Cybercriminalité,* Revue Internationale de Droit Pénal, Vol. 77 (2006), pp. 525-568.
[7] *Vd.* Ricardo Mata y Martín, 'Criminalidad Informática: una introducción al Cibercrimen', in *Temas de Direito da Informática e da Internet*, Coimbra Editora (2004), pp. 197-236.

direito na protecção dos bens jurídicos passíveis de ser afectados pelas condutas ilícitas no âmbito das tecnologias da informação e da comunicação. Sendo certo que a segurança informática dispõe de mecanismos menos gravosos, que vão desde a arquitectura das próprias redes de comunicação à consagração de responsabilidade civil de intermediários de serviços de internet, passando por medidas adoptadas pelos próprios utilizadores no sentido de implementarem sistemas de auto-protecção, tais mecanismos por si só não têm o efeito dissuasor necessário que previna a utilização abusiva dos meios informáticos.

Pelo exposto, a Comissão pode concluir pela necessidade de criminalizar as condutas que afectem ou utilizem as tecnologias da informação e da comunicação, a fim de salvaguardar bens jurídicos fundamentais do nosso sistema jurídico. Está, portanto, justificada a introdução no ordenamento jurídico de Macau de normas respeitantes ao que vulgarmente se designa de criminalidade informática.

3. A criminalidade informática pode ser entendida como *todo o acto em que um sistema informático serve de meio para atingir um objectivo criminoso ou em que o sistema informático é alvo desse acto.*[8]

Com base na definição apresentada, pode circunscrever-se o âmbito da intervenção legislativa ora empreendida através da identificação de duas categorias genéricas de crimes, delimitadas tendo em consideração o papel dos

[8] *Vd.* Garcia Marques & Lourenço Martins, *Direito da Informática*, Almedina (2000), p. 494.

sistemas informáticos [9] na conduta criminosa: crimes em que o sistema informático é o *instrumento do crime* e crimes em que o sistema informático é o *objecto do crime*.

3.1. A primeira categoria de ilícitos penais abrangida pelo conceito de criminalidade informática é composta por aqueles em que a ordem jurídica valoriza a utilização de meios informáticos no decurso do cometimento dos crimes por considerar que a utilização da informática representa um maior perigo para os bens jurídicos que pretende proteger. Nestes casos, está-se em presença de crimes de execução vinculada, em que a conduta tem de ser praticada através dos meios constantes especificamente do tipo penal.[10] Por a utilização da informática representar um perigo específico a ordem jurídica de Macau distingue no Código Penal, por exemplo, os crimes de burla (artigo 211.º) e de burla informática (artigo 213.º). Está-se em presença de condutas em que a utilização de um sistema informático é um instrumento do crime.

Apenas as situações acima descritas devem ser abrangidas pelo conceito de criminalidade informática. A generalidade dos tipos de crimes previstos no Código Penal [11] e em leis penais avulsas [12] está construída de uma forma

[9] Nos termos da definição constante da alínea 1) do artigo 2.º da proposta de lei, considera-se «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.*

[10] Tais são os casos dos crimes de falsificação informática e burla informática previstos, respectivamente, nos artigos 10.º e 11.º da proposta de lei.

[11] Nomeadamente os crimes de ameaça (art. 147.º), coacção (arts. 148.º e 149.º), tráfico de pessoas (art. 153.º-A), lenocínio (arts. 163.º e 170.º), difamação (art. 174.º), injúria (art. 175.º), ofensa à memória de pessoa falecida (art. 179.º), ofensa a pessoa colectiva que exerça autoridade pública (art. 181.º), devassa da vida privada (art. 186.º), divulgação de segredo (art. 189.º), extorsão (art. 215.º), incitamento à guerra (art. 229.º), incitamento ao genocídio (art. 231.º), discriminação racial [art. 233.º, nº2, b)], uso de atestado falso (art. 250.º), ofensa a sentimentos religiosos (art. 282.º), instigação pública a um crime (art. 286.º), apologia pública de um crime (art. 287.º), ameaça com prática de crime (art. 294.º), incitamento à alteração violenta

tecnologicamente neutra, o que faz com que a conduta criminosa possa ser praticada por qualquer forma, incluindo a utilização de sistemas informáticos. Nestes casos de tipos tecnologicamente neutros, a utilização de sistemas informáticos é penalmente irrelevante e equiparável à utilização de qualquer outro instrumento para a prática do crime.[13]

A título de exemplo, o crime de injúria (artigo 175.º do Código Penal) é praticado por quem imputar factos a outra pessoa, mesmo sob a forma de suspeita, ou lhe dirigir palavras, ofensivos da sua honra ou consideração, independentemente do meio através do qual tal imputação é feita. Sem prejuízo, no entanto, do ordenamento jurídico poder ter em consideração o meio utilizado para avaliar a dano produzido, como é o caso da agravação das penas determinada pelo artigo 177.º do Código Penal para ofensas praticadas através de meios que facilitem a sua divulgação.

Estes crimes não caem no âmbito da criminalidade informática por a utilização de tais meios ser penalmente irrelevante. Ainda que cometidos com recurso à utilização de meios informáticos, os bens jurídicos protegidos continuam os mesmos, não sendo necessária a criação de novos tipos penais para dar resposta efectiva a este novo modelo de criminalidade. [14]

---

do sistema estabelecido (art. 298.º), incitamento à desobediência colectiva (art. 300.º), ultraje aos símbolos do Território (art. 302.º), coacção contra órgãos do território (art. 303.º), ultraje de símbolos oficiais (art. 309.º), tirada de presos [art. 313.º, b)] ou violação de segredo de justiça (art. 335.º).

[12] Nomeadamente os crimes de branqueamento de capitais (art. 3.º da Lei n.º 2/2006), sedição e subtracção de segredo de Estado (arts. 4.º e 5.º da Lei n.º 2/2009), venda «em pirâmide» (art. 28.º-A da Lei n.º 6/96/M, de 15 de Julho), financiamento e incitamento ao terrorismo (arts. 7.º e 8.º da Lei n.º 3/2006), entre outros.

[13] *Vd.* José de Oliveira Ascensão, 'Criminalidade informática', in *Direito da Sociedade da Informação*, Vol. II, Coimbra Editora (2001), p. 203.

[14] *Vd.* Emeline Piva Pinheiro, *Crimes virtuais: Uma análise da criminalidade informática e da resposta estatal*, p. 25, disponível em http://www.pucrs.br/direito/graduacao/tc/tccII/trabalhos2006_1/emeline.pdf.

3.2. A par dos casos em que o sistema informático é um instrumento para a prática de crimes, outros há em que o próprio sistema informático é o objecto ou o alvo da actividade criminosa. Esta é a segunda categoria de crimes enquadráveis no conceito de criminalidade informática.

Em resposta ao reconhecimento da relevância dos sistemas informáticos na vida contemporânea e dos riscos[15] que eles enfrentam, é possível identificar a *segurança*, a *integridade* e a *confidencialidade* informáticas como bens jurídicos autónomos merecedoras de tutela penal.[16] Para que a sociedade possa aproveitar todas as potencialidades inerentes ao uso das tecnologias da informação e da comunicação é necessário que exista 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».[17] A vulgarização do uso das tecnologias na vida pessoal, social e económica faz com que qualquer sistema informático contenha um conjunto de informações preciosas sobre o seu utilizador e que haja quem pretenda aproveitar-se ilegitimamente do valor económico que o acesso e a manipulação de tal informação representa. É, portanto, necessário que a utilização dos sistemas informáticos seja feita de forma segura, que seja garantida a integridade dos dados informáticos neles contidos e que a sua utilização possa ser feita em respeito pela confidencialidade do seu conteúdo e do seu utilizador. É hoje sabido que através da utilização de programas informáticos específicos é possível que terceiros não autorizados tenham acesso a um sistema informático ou parte dele, particularmente quando ligado à internet. Deste facto podem

[15] Quanto aos tipos de riscos detectados na internet, *vd. Symantec Global Internet Security Threat Report – Trends for 2008*, Vol. XIV (2009), disponível em http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

[16] *Vd.* Lorenzo Picotti, 'Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l'informatique', *ob. cit.*, pp. 560-563.

[17] Nota justificativa.

resultar consequências com graus de perigosidade diferentes que vão desde o mero conhecimento da informação contida no sistema informático em causa, à elaboração de perfis de comportamento do seu utilizador comercialmente utilizáveis, à violação da correspondência electrónica ou à violação de medidas de segurança que protegem o sistema informático. De igual forma a propagação de programas maliciosos, nomeadamente vírus informáticos, visam a modificação ou destruição de dados informáticos, a afectação do funcionamento de programas informáticos ou a obstrução do normal funcionamento de um sistema ou programa informáticos.[18]

Os recentes desenvolvimentos tecnológicos, a autonomização de novos bens jurídicos tutelados pelo direito, a identificação de condutas específicas capazes de afectar tais bens jurídicos e o reconhecimento de que o enquadramento normativo existente é incapaz de lhes dispensar uma protecção necessária e adequada, faz com que seja imperioso a definição de novos tipos de crimes em que o sistema informático é o objecto da actividade delituosa, enquadráveis no âmbito do conceito de criminalidade informática.

4. A criminalização dos delitos informáticos é uma tendência internacional, sendo múltiplas as jurisdições onde existem normas penais específicas relativas à criminalidade informática.[19] O facto deste tipo de delinquência não conhecer fronteiras físicas ou políticas, faz com que seja de extrema importância uma relativa uniformização das normas penais que as diferentes ordens jurídicas se socorrem para combater a criminalidade informática.

---

[18] *Vd.* Esther Morón Lerma, *Internet y Derecho Penal: «Hacking» y otras Conductas Ilícitas en la Red*, 2ª ed., Editorial Aranzadi (2002), pp. 29-45.

[19] *Vd.* Pauline C. Reich (ed.), *Cybercrime & Security*, Oceana Publications (2009), e 皮勇：《網絡安全法原論》，中國人民公安大學出版社，2008年，第445-484頁.

A proposta de lei em apreço insere-se na linha das intervenções legislativas levadas a cabo noutras jurisdições, nomeadamente no Interior da China, Hong Kong, Taiwan, Singapura, Portugal, Alemanha e Estados Unidos e, tal como reconhecido na Nota Justificativa, foi elaborada com base na *Convenção sobre o Cibercrime* do Conselho da Europa.

A Convenção sobre o Cibercrime do Conselho da Europa foi assinada em Budapeste a 23 de Novembro de 2001 e vigora na ordem jurídica internacional desde 1 de Julho de 2004. Apesar de ser um instrumento de direito internacional celebrado no âmbito do Conselho da Europa, a ele podem aceder estados não membros desta organização internacional de âmbito regional. De momento, a Convenção de Budapeste foi assinada por 46 estados[20], estando em vigor, após os respectivos processos de ratificação, em 26 desses estados.[21]

É relevante o facto da proposta de lei ter sido elaborada com base no instrumento de direito internacional mais importante sobre a matéria da criminalidade informática. Mesmo não sendo parte da Convenção, não estando portanto a ela vinculada, a RAEM participa voluntariamente no processo de harmonização legislativa ao nível do direito penal material, que é um dos propósitos fundamentais desta iniciativa multinacional. Tal harmonização assume um papel determinante no combate a este novo tipo de criminalidade, uma vez que facilita a cooperação internacional na matéria, nomeadamente ao nível da cooperação judiciária em matéria penal.

[20] Quatro dos quais não membros do Conselho da Europa: África do Sul, Canadá, Japão e Estados Unidos da América.
[21] A convenção vigora nas ordens jurídicas dos seguintes países membros do Conselho da Europa: Albânia, Alemanha, Arménia, Bósnia Herzegovina, Bulgária, Croácia, Chipre, Dinamarca, Eslováquia, Eslovénia, Estónia, Finlândia, França, Holanda, Hungria, Islândia, Itália, Letónia, Lituânia, Antiga República Jugoslava da Macedónia, Moldova, Noruega, Roménia, Sérvia e Ucrânia. Vigora ainda nos Estados Unidos da América, país não membro do Conselho da Europa.

Ao criminalizar as condutas atentatórias da segurança, integridade e confidencialidade informáticas e ao fazê-lo em termos semelhantes aos das demais ordens jurídicas, Macau adopta instrumentos legais que permitem uma mais eficaz investigação dos crimes, a maior parte dos quais tem contactos com múltiplas ordens jurídicas. De facto, «quando as leis de um país criminalizam certas condutas relacionadas com a informática e as leis de outros países não o fazem, a cooperação na investigação de um crime e a punição do seu autor podem ser impossíveis. Isto é, quando um criminoso transmite as suas comunicações através de três, quatro ou cinco países antes de alcançar as suas vítimas, a inadequação da legislação de apenas um desses países pode, com efeito, escudar esse criminoso de ser perseguido pelos aplicadores da lei em todo o mundo».[22] A existência, na generalidade das ordens jurídicas, de um certo grau de uniformização das normas penais que criminalizam as condutas ilícitas relacionadas com a informática, tal como almejado pela Convenção sobre o Cibercrime, elimina um dos mais importantes obstáculos ao pleno funcionamento dos mecanismos de cooperação judiciária internacional no combate a tais delitos. Esta cooperação pressupõe um acordo entre jurisdições quanto aos valores merecedores de protecção penal, expresso pelo princípio da dupla punibilidade, segundo o qual *a infracção que motiva o pedido de cooperação deve ser punível com uma reacção criminal pela legislação da parte requerente e pela legislação da parte requerida*.[23] A uniformização do direito penal material no âmbito da criminalidade informática reflecte a existência de tal acordo.

---

[22] Peter Csonka, 'The Council of Europe Convention on Cyber-Crime: A Response to the Challenge of the New Age', in *Cyber-Crime – The Challenge in Asia, ob. cit.* (2005), p. 306.

[23] Artigo 6.º, n.º 1, da Lei n.º 6/2006. Quanto ao âmbito de aplicação do princípio da dupla punibilidade em Macau, *vd.* Parecer da 1ª Comissão Permanente n.º 2/III/2006, respeitante à proposta de lei intitulada «*Lei da Cooperação Judiciária em Matéria Penal*», disponível em http://www.al.gov.mo/lei/leis/2006/06-2006/parecer.pdf.

5. Para que uma ordem jurídica possa proteger-se contra crimes relacionados com a informática, é necessário um enquadramento legislativo básico, o qual envolve o direito penal material, o direito processual relativo a buscas e apreensões, assim como o direito probatório.[24] O mero recurso ao direito penal material, apesar de importante, pode não ser suficiente para um eficaz combate à criminalidade informática. A especificidade dos meios técnicos associados à prática de delitos informáticos faz com que estes sejam «de difícil investigação, pelo que os métodos tradicionais de combate à criminalidade (...) se revelam insuficientes face ao carácter virtual dos actos praticados na internet».[25] A par da rapidez de difusão de mensagens na internet, do elevado grau do 'anonimato' da autoria do crime, da existência de poucas provas físicas da prática do crime e da facilidade da sua destruição, é sabido que a criminalidade informática apresenta sérias dificuldades ao nível da investigação, as quais têm expressão nos seguintes aspectos:[26]

1) Dificuldade em descobrir o agente da infracção;
2) Dificuldade investigatória colocada pelos novos meios tecnológicos;
3) Novas técnicas da prática de crimes;
4) Generalização das técnicas de uso de códigos secretos informáticos;
5) Dificuldade de medir o tempo exacto de actuação ilícita;
6) Não colaboração da vítima.

5.1. Para além de introduzir na ordem jurídica de Macau novos tipos de crime, a proposta de lei contém normas processuais penais que visam a facilitação da investigação da criminalidade informática e de crimes cometidos

[24] Peter Grabosky, 'The Global Cyber-Crime Problem: The Socio-Economic Impact', *ob. cit.* (2005), p. 50.
[25] Nota Justificativa.
[26] *Vd.* Fong Man Chong, *Do Mundo Real ao Mundo Virtual – Alguns aspectos jurídico-criminais da vida cibercomunitária*, Instituto de Estudos Jurídicos Avançados da Faculdade de Direito da Universidade de Macau (2005), pp. 141-147.

por meio de sistemas informáticos, assim como a criação de um regime especial de recolha e conservação de prova em suporte electrónico da prática de quaisquer crimes.

A Comissão admite a necessidade de previsão de normas processuais penais específicas para a criminalidade informática. Tais normas devem proceder à adaptação dos métodos tradicionais de investigação criminal às novas tecnologias, particularmente tendo em vista a facilidade de ocultação de identidade do autor do crime e de destruição de provas em suporte digital.

Sendo evidente que nas sociedades modernas existe uma tensão constante entre os direitos individuais e a necessidade de segurança, essa tensão faz-se sentir ainda com maior acuidade quando o fenómeno a combater ultrapassa o padrão de criminalidade tradicional. No entanto, a dificuldade do combate a este tipo de criminalidade e as particularidades dos meios técnicos de que se socorre não podem justificar uma derrogação dos princípios estruturantes do sistema jurídico vigente na RAEM. É, pois, imperativo que a proposta de lei alcance um equilíbrio entre, por um lado, os valores da segurança e da justiça, reflectidos na eficácia na investigação criminal, e por outro, o respeito pelos direitos, liberdades e garantias das pessoas. A Comissão considera adequado que se prevejam medidas específicas de combate a tais fenómenos criminosos, sem que no entanto se justifique, de modo algum, um regime próximo do "estado de excepção" que permita que tal combate seja feito fora do quadro geral de regras de um Estado de Direito. É este, aliás, o enquadramento da actividade de segurança interna da RAEM, no âmbito da qual o combate à criminalidade se insere.[27]

[27] *Vd.* Lei n.º 9/2002 e Parecer da 2ª Comissão Permanente n.º 4/II/2002, relativo à proposta de lei intitulada «*Lei de Bases da Segurança Interna da Região Administrativa Especial de Macau*».

5.2. No decurso do debate na especialidade da presente proposta de lei foram suscitadas dúvidas quanto às normas processuais penais nela contidas e aos poderes atribuídos às autoridades competentes para procederem a uma investigação mais eficaz da criminalidade informática. Por um lado, devido à incerteza quanto à relação estabelecida entre o regime especial constante da proposta de lei e o regime geral supletivo do Código de Processo Penal. Por outro lado, devido ao receio de que o regime especial ora proposto pudesse representar uma restrição abusiva dos direitos, liberdades e garantias dos cidadãos constitucionalmente consagrados.

5.2.1. Relativamente à relação entre a proposta de lei e o Código de Processo Penal, a Comissão teve a oportunidade de confirmar junto do proponente a sua intenção legislativa. Foi reiterada a ideia segundo a qual a proposta de lei não pretende derrogar as regras gerais relativas aos meios de obtenção de prova, nomeadamente quanto à competência para proceder a buscas, apreensões e intercepção ou gravação de conversações ou comunicações feitas através de sistemas informáticos ou telemáticos. Está assim garantida, como regra, a competência das autoridades judiciárias para proceder a tais actos e o regime de garantias que a lei processual penal dispensa para tutelar segredos legalmente protegidos. [28] O regime de conservação expedita de provas previsto na proposta de lei destina-se tão-só a permitir que as provas em formato digital da prática de crimes sejam preservadas. A previsão da possibilidade de tais medidas urgentes serem determinadas pelos órgãos de polícia criminal [designadamente a Polícia Judiciária, a quem, nos termos da alínea 10) do n.º 1 do artigo 7.º da Lei n.º

[28] *Vd.* Paulo Dá Mesquita, *Direcção do Inquérito Penal e Garantia Judiciária*, Coimbra Editora (2003).

5/2006, está atribuída a competência exclusiva para realizar a investigação dos crimes relacionados com a informática], antes mesmo de receberem ordem da autoridade judiciária competente, tem natureza excepcional. Esta intervenção 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). Havendo consonância entre a Comissão e o proponente quanto à relação de especialidade entre a proposta de lei e o Código de Processo Penal, a Comissão diligenciou no sentido da intenção legislativa subjacente à proposta de lei ficar claramente expressa no seu articulado.

5.2.2. Relativamente à restrição dos direitos, liberdades e garantias dos cidadãos, a Comissão entende que a proposta de lei não representa um entorse aos princípios fundamentais do ordenamento jurídico da RAEM, nem contém mecanismos que, em virtude da sua mera consagração legal, possam pôr em causa direitos, liberdades e garantias consagrados na Lei Básica, nomeadamente ao nível da liberdade de expressão, da privacidade e da confidencialidade das comunicações. Neste aspecto, a proposta de lei parece apta a atingir o equilíbrio entre os diferentes valores em presença:

a) Em primeiro lugar, a proposta de lei não pretende limitar a liberdade de expressão dos cidadãos. Ao nível do direito material penal, a Nota Justificativa dá especial enfoque a este aspecto, afirmando que «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». Já quanto ao direito processual penal, os poderes de investigação previstos na proposta de lei são justificados para o combate da criminalidade em causa, com as suas características e especificidades. As medidas de conservação de provas não legitimam a intercepção do conteúdo informativo das mensagens ou comunicações transmitidas através dos sistemas informáticos.

Em Macau, a Lei Básica consagra o direito à liberdade de expressão (artigo 27.º) e determina que tal direito não pode ser restringido excepto nos casos previstos na lei e com respeito, nomeadamente, pelo Pacto Internacional sobre os Direitos Civis e Políticos (artigo 40.º). Este, regulando a matéria em termos idênticos, determina no seu artigo 19.º que o exercício da liberdade de expressão pode ser sujeito a restrições que, devem, todavia, ser expressamente fixadas na lei e que sejam necessárias ao respeito dos direitos ou da reputação de outrem ou à salvaguarda da segurança nacional, da ordem pública, da saúde e da moralidade públicas. Assim, a liberdade de expressão no ambiente digital deve ter o âmbito e estar sujeita aos limites que existem em geral, para qualquer ambiente ou meio de comunicação.[29]

b) Em segundo lugar, a proposta de lei respeita a privacidade dos cidadãos. As medidas nela previstas reportam-se à conservação expedita dos

[29] *Vd.* Mark Turner, 'Liberté d'expression, censure et intégrité sur l'Internet', in *Les Droits de l'homme dans de cyberspace*, Unesco/Economica (2005), pp. 31-46.

dados informáticos em geral, mas as medidas que podem ser entendidas como sendo mais gravosas dizem respeito apenas aos dados de tráfego.[30] Estes são uma espécie de descrição do percurso de uma comunicação nas redes, desde o ponto de partida até ao seu destino, em que se possibilita a identificação de que um terminal de computador, num determinado dia e a uma determinada hora, acedeu à internet por via de um determinado endereço de IP. Os dados de tráfego são gerados por computadores na cadeia de comunicação de forma a encaminhar uma comunicação desde a sua origem até ao seus destino. São portanto elementos auxiliares da comunicação propriamente dita e não revelam o conteúdo da comunicação, nem permitem saber nada mais sobre outras eventuais comunicações que o indivíduo tenha efectuado, nem tão pouco revelar hábitos repetidos, padrões de comportamento, atitudes e outras informações que permitem inferir informação pessoal da esfera privada do indivíduo. [31] Assim, sendo fundamental para a investigação da criminalidade informática a informação fornecida pelos dados de tráfego para que se proceda à reconstrução do percurso da comunicação, a obtenção de tal informação não contende com a esfera de protecção do direito à privacidade do indivíduo, consagrado nos artigos 30.º e 32.º da Lei Básica e com expressão em variada legislação avulsa.[32]

---

[30] Nos termos da alínea 5) do artigo 2.º, «dados de tráfego» *são 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.*

[31] *Vd.* Pedro Verdelho, 'A Reforma Penal Portuguesa e o Cibercrime', in *Revista do Ministério Público*, Ano 27, n.º 108 (2006), pp. 117-120 e Relatório Explicativo da Convenção do Conselho da Europa sobre o Cibercrime (pontos 28-31), disponível (versão portuguesa) em http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf.

[32] Quanto ao *princípio da protecção jurídica da privacidade* no ordenamento jurídico de Macau *vd.* Parecer da 3ª Comissão Permanente n.º 3/II/2005, relativo ao projecto de lei intitulado «*Lei da protecção dos dados pessoais*», disponível em http://www.al.gov.mo/lei/leis/2005/08-2005/paracer.pdf.

c) Por fim, a proposta de lei não viola o direito ao sigilo dos meios de comunicação consagrado no artigo 32.º da Lei Básica. Este direito visa prevenir o conhecimento abusivo do conteúdo das comunicações, qualquer que seja o meio pelo qual elas se efectuem, uma vez que «na sociedade moderna onde se desenvolve rapidamente a indústria informática, a troca de informações e qualquer forma de comunicação constitui um recurso social muito importante».[33] Este direito pode, contudo, sofrer restrições: por um lado, o próprio artigo 32.º prevê a possibilidade de restrição do direito ao sigilo das comunicações em casos de inspecção dos meios de comunicação pelas autoridades competentes, de acordo com as disposições da lei, e por necessidade de segurança pública ou de investigação em processo criminal; por outro lado, o artigo 40.º da Lei Básica reconhece a admissibilidade legal para a consagração de normas restritivas de direitos no ordenamento jurídico de Macau, desde que prevista na lei e desde que não seja contrariado o disposto no Pacto Internacional sobre os Direitos Civis e Políticos, no Pacto Internacional sobre os Direitos Económicos, Sociais e Culturais, bem como nas convenções internacionais de trabalho, aplicáveis em Macau por força do disposto no parágrafo 1º do mesmo artigo 40º.[34]

Os mecanismos previstos na proposta de lei não permitem o acesso das autoridades policiais ao conteúdos das comunicações transmitidas através de sistemas informáticos ou telemáticos, seja correio electrónico, mensagens SMS,[35] conversações através de sistema VOIP[36] ou outras.[37]

---

[33] Iong Wan Chong, *Anotações à Lei Básica de Macau*, Associação de Divulgação da Lei Básica de Macau (2005), pp. 83-85.
[34] Quanto ao regime de restrição de direitos em Macau, *vd.* Parecer da 2ª Comissão Permanente n.º 4/II/2002, relativo à proposta de lei intitulada «*Lei de Bases da Segurança Interna da Região Administrativa Especial de Macau*».
[35] "Short Message System".

Tal acesso, a existir, deve seguir o regime constante do Código de Processo Penal para as escutas telefónicas: o artigo 175.º do Código procede à extensão de tal regime legal *às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone*. Assim, a possibilidade de efectuar a monitorização dos conteúdos das comunicações digitais situa-se fora do âmbito da presente proposta de lei e existe no ordenamento local apenas para dar resposta a situações de ameaça à segurança interna particularmente graves. Só assim se justifica que, perante tais ameaças, os direitos individuais de certas pessoas possam ceder perante o valor da segurança colectiva ou dos direitos à segurança e tranquilidade de toda a população.[38]

5.2.3. Importa realçar o facto de o regime processual constante da proposta de lei dizer respeito à preservação expedita de dados informáticos no âmbito de um processo penal em concreto. Preservar dados significa manter dados quando estes já existem e se encontram armazenados, estando assim protegidos de tudo quanto seja passível de causar a alteração ou deterioração da qualidade ou do estado actual. A preservação de dados consiste na actividade que permite conservar intactos e seguros os dados armazenados num sistema informático.

As medidas especiais previstas no artigo 16.º aplicam-se a dados armazenados que foram já recolhidos e arquivados pelos detentores dos dados,

---

[36] "Voice Over Internet Protocol".

[37] *Vd.* Armando Veiga/Benjamim Silva Rodrigues, *Escutas telefónicas – Rumo à Monitorização dos Fluxos Informacionais e Comunicacionais Digitais*, 2ª ed., Coimbra Editora (2007).

[38] O controle das comunicações informáticas pode igualmente ser feito ao abrigo do artigo 18.º da Lei n.º 9/2002 (*Lei de Bases da Segurança Interna da Região Administrativa Especial de Macau)*, quando em presença de fortes indícios de perturbação da segurança interna por acção de actividades criminosas, seguindo os termos do Código de Processo Penal. *Vd.* Parecer da 2ª Comissão Permanente n.º 4/II/2002, relativo à proposta de lei intitulada «*Lei de Bases da Segurança Interna da Região Administrativa Especial de Macau*».

tais como os fornecedores de serviços. As referidas medidas não se aplicam, pois, à recolha em tempo real nem à conservação de futuros dados de tráfego ou ao acesso em tempo real ao conteúdo das comunicações.[39] Por outro lado, as medidas ora previstas dizem respeito à investigação de um caso particular e só perante as circunstâncias desse caso em concreto pode ser analisada a necessidade da sua adopção.

5.2.4. Pelas razões expostas, a Comissão considera que a proposta de lei não contém normas violadoras dos direitos, liberdades e garantias dos cidadãos. Contudo, tem também consciência que o combate à criminalidade com características especiais – tanto a criminalidade informática como a criminalidade organizada, transfronteiriça, de "colarinho branco" ou o terrorismo – leva a queos aplicadores da lei possam ter a tentação de se arrogarem de poderes também eles especiais que não têm correspondência no texto da lei ou na intenção legislativa. A Comissão considera não ser intenção legislativa a existência de um sistema de monitorização generalizada dos conteúdos publicamente disponíveis nos sistemas informáticos e telemáticos ou das comunicações através deles transmitidas. As medidas de prevenção da criminalidade informática e telemática devem ser adoptadas apenas para fins de investigação policial, limitando-se ao necessário para prevenção de um perigo concreto ou repressão de uma infracção determinada, não podendo ter funções de prevenção geral. A Comissão confia que os aplicadores da futura lei de combate à criminalidade informática terão presentes os princípios orientadores de um Estado de Direito como critério para ajuizar o âmbito da sua actuação.

[39] *Vd.* Relatório Explicativo, *ob. cit.*, pontos 149-169.

IV – Apreciação na especialidade

Para além da apreciação genérica apresentada no ponto anterior, a análise efectuada na Comissão teve como propósito, nos termos do artigo 117.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.

Durante a apreciação na especialidade, a Comissão contou com a estreita colaboração do proponente. As principais questões levantadas durante a apreciação na especialidade e as mais relevantes alterações introduzidas são as seguintes:

1. - Objecto (Artigo 1.º)

A inclusão de uma norma relativa ao objecto da lei visa permitir a percepção imediata do âmbito material do conjunto de normas incluídas no diploma legislativo. Assim considerou-se que a redacção do artigo 1.º da versão inicial da proposta de lei, que se limitava a repetir o título da lei, não cumpria a função inerente a uma norma de objecto. Na nova redacção esclarece-se que o objecto desta iniciativa legislativa é a tipificação dos crimes informáticos (direito material penal) e a criação de um regime de recolha de prova em suporte electrónico da prática de crimes (direito processual penal).

2. - Definições (Artigo 2.º)

A inclusão de uma norma com definições visa estabelecer a unidade de interpretação do diploma, através da criação de conceitos operatórios uniformes que vinculem o intérprete no âmbito do acto normativo. Na matéria respeitante às tecnologias da informação justifica-se o uso de definições pela alta tecnicidade de conceitos próprios da ciência e da técnica informática, servindo o artigo das definições para orientar o intérprete e o aplicador da lei quanto ao sentido da terminologia utilizada. Por esta razão, a proposta de lei contém um artigo referente a definições, as quais seguem de perto as definições constantes na Convenção de Budapeste sobre o Cibercrime.

Nos termos da alínea 1) do artigo 2.º, «sistema informático» é 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.

Na nova versão da proposta de lei foram introduzidas algumas alterações na redacção desta definição. Em particular, foi eliminada a enumeração exemplificativa dos dispositivos capazes de fazerem o tratamento automatizado de dados.[40] Em primeiro lugar, devido ao facto de tal enumeração ter em conta apenas as tecnologias actualmente conhecidas, perdendo actualidade à medida que novos dispositivos surjam no mercado, o que conduziria à desactualização da enumeração e da própria lei. Através da sua eliminação pretendeu-se atribuir à lei um carácter o mais tecnologicamente neutro possível. Por outro lado, os

[40] A definição de sistema informático constante da versão inicial da proposta de lei era «qualquer dispositivo isolado ou grupo de dispositivos interligados ou relacionados, nomeadamente computadores pessoais autónomos, agendas digitais e pessoais, descodificadores digitais, vídeo-gravadores pessoais e telemóveis, em que um ou mais de entre eles desenvolvem, em execução de um programa, o tratamento automatizado dos dados informáticos».

dispositivos nela mencionados poderiam suscitar dúvidas de interpretação e levar a uma aplicação menos correcta da lei, em particular a referência a telemóveis. Estes, enquanto meros instrumentos que permitem a comunicação de voz através de tecnologia analógica, não estão abrangidos no âmbito de aplicação da presente lei. Assim, não só os tipos penais ora consagrados, como as medidas processuais adoptadas, não têm aplicação às comunicações telefónicas, enquanto tais. Contudo, os recentes desenvolvimentos tecnológicos permitem aos telemóveis o desempenho de um conjunto de funções que vão para além da comunicação da voz. Quando tenham funções de tratamento de dados, os aparelhos designados como telemóveis deixam ser "telefones móveis" para passarem a ser "terminais informáticos móveis". Nesta função, estão incluídos na definição de sistema informático. Por fim, a eliminação da enumeração de dispositivos deveu-se também ao facto de a própria Convenção de Budapeste não conter qualquer exemplificação das aplicações tecnológicas abrangidas pela definição de sistema informático.

É válida para a compreensão da definição constante da proposta de lei a explicação do conceito apresentada pelo Conselho da Europa no Relatório Explicativo da Convenção sobre o Cibercrime. Assim, um sistema informático é «um equipamento composto por *hardware* e *software* desenvolvidos para o tratamento automático de dados digitais. Poderá incluir dispositivos de entrada, saída e armazenamento. Poderá funcionar independentemente ou estar ligado em rede com outros dispositivos semelhantes. O termo 'automático' significa sem a intervenção directa do Homem e a expressão 'tratamento de dados' significa que os dados no sistema informático são operados através da execução de um programa de computador».

A definição de sistema informático faz apelo ao conceito de dados informáticos, os quais estão definidos na alínea 2) do artigo 2.º (a qual não

sofreu qualquer alteração) como sendo *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.* Esta definição assenta na definição de dados adoptada pela Convenção, a qual acolheu o conceito de dados da Organização Internacional da Normalização (ISO). Dela decorre que dados informáticos são a tradução em linguagem binária, isto é, linguagem processável por um computador, de factos, informações ou de conceitos.[41]

Ao nível das definições, a nova versão da proposta de lei procedeu à eliminação da definição de "dados relativos ao conteúdo", constante da alínea 6) do artigo 2.º da versão inicial da iniciativa legislativa. Os dados de conteúdo são os dados informáticos relativos ao conteúdo informativo de uma comunicação ou de uma mensagem. Uma vez que o conceito não tem expressão ao longo do articulado[42] procedeu-se à sua eliminação. A este respeito importa salientar que as medidas especiais previstas no artigo 16.º permitem a conservação expedita de todos os dados informáticos[43] mas não permitem o acesso aos dados de conteúdo sem ser no âmbito do regime previsto no Código de Processo Penal. A medida que permite o acesso a certos dados informáticos, prevista na alínea 2) do n.º 1 do artigo 16.º, diz respeito tão-só aos dados de tráfego. Assim, a inclusão de uma definição relativa aos dados de conteúdo poderia induzir o intérprete-aplicador em erro, no sentido das medidas especiais poderem também abranger o acesso ao conteúdo informativo da comunicação, quando não é essa a intenção legislativa.

---

[41] *Vd.* Pedro Verdelho, 'Cibercrime', in *Direito da Sociedade da Informação*, Vol. IV, Coimbra Editora (2003), p. 361.
[42] Com excepção da referência que lhe é feita, a título incidental, na alínea 4) do artigo 2.º ao fazer-se a delimitação negativa do conceito de "dados de base".
[43] 1ª parte da alínea 1 do n.º 1 do artigo 16.º.

3. - Direito subsidiário (Artigo 3.º)

No decurso da análise do artigo 3.º, foi ponderada a necessidade da sua inclusão no articulado da lei.

Em relação ao disposto no n.º 1, a previsão de que «aos crimes previstos na presente lei são subsidiariamente aplicáveis as normas do Código Penal» é redundante face à disposição geral constante no artigo 8.º do Código Penal. Este determina que «salvo disposição em contrário, o preceituado no presente Código é aplicável subsidiariamente aos factos puníveis por legislação de carácter especial». Assim, e em rigor, não é necessário que a lei especial repita o que a lei geral afirma, a menos que o pretenda afastar.[44] No entanto, considerou-se que a referência à aplicação subsidiária do Código Penal poderia contribuir para uma melhor compreensão da relação de especialidade que esta proposta de lei tem em relação à lei penal geral.

Relativamente ao n.º 2, pretende-se salvaguardar os demais crimes relacionados com a protecção de sistemas informáticos específicos, nomeadamente os crimes que visam punir os atentados à segurança dos circuitos integrados dos documentos de identificação e de viagem, assim como as respectivas bases de dados, previstos no artigo 14.º da Lei n.º 8/2002 (Regime do bilhete de identidade de residente da RAEM) e no 15.º da Lei n.º 8/2009 (Regime dos documentos de viagem da RAEM).

[44] *Vd.* José de Oliveira Ascensão, 'Criminalidade informática', *ob. cit.*, p. 205.

4. - Acesso ilegítimo a sistema informático (Artigo 4.º)

O Relatório Explicativo da Convenção do Conselho da Europa sobre o Cibercrime[45] esclarece que o crime de acesso ilegítimo a sistema informático abrange basicamente a infracção relativa às perigosas ameaças e atentados à segurança (isto é, confidencialidade, integridade e disponibilidade) dos sistemas informáticos. A necessidade de protecção reflecte os interesses de organizações e indivíduos em gerir, operar e controlar os seus sistemas informáticos de forma livre e tranquila. O meio mais viável de prevenção do acesso não autorizado é, evidentemente, a introdução e o desenvolvimento de medidas de segurança eficazes. Contudo, uma resposta abrangente terá igualmente que englobar a ameaça e a utilização de medidas contempladas no direito penal.

O termo "acesso" entende-se como sendo a entrada no todo ou numa parte de um sistema informático (*hardware*, componentes, dados armazenados no sistema instalado, directorias, dados de tráfego e dados relativos ao conteúdo). "Acesso" inclui a penetração noutro sistema informático, acessível através de redes de telecomunicações públicas, ou num sistema informático na mesma rede, tal como uma rede de área local (LAN) ou *intranet* no seio de uma organização (rede privada de uma empresa, por exemplo).

O acesso só é punível se for feito "sem autorização", residindo nesta falta de consentimento a sua ilegitimidade. Isto significa que não existe crime se o acesso for autorizado pelo proprietário ou outro titular do direito sobre o sistema ou parte do mesmo (como por exemplo, para efeitos de teste, protecção ou reparação do sistema informático em questão). Além disso, não existe criminalização associada ao facto de se aceder a um sistema informático que

[45] Relatório Explicativo, *ob. cit.*, pontos 44-50.

permite o acesso livre e aberto ao público, uma vez que tal acesso se faz com direito.

O tipo subjectivo apenas admite o dolo directo (intenção), não sendo possível a punição de acessos ilegítimos efectuados por forma negligente. Contudo, o tipo exige, como dolo específico, que o acesso seja feito com "qualquer intenção ilegítima". Assim, para haver crime basta que o agente saiba que está a aceder ilegitimamente a uma sistema informático, ou parte dele, sem autorização e o faça com qualquer intenção ilegítima, isto é, contrária à lei. Na nova versão da proposta de lei alterou-se o elemento subjectivo, eliminando-se a referência à intenção de obtenção de dados informáticos, pelo facto de tal intenção fazer parte de um crime autónomo, a saber o crime previsto no artigo 5.º.

Por força do elemento subjectivo do tipo, possibilita-se o concurso entre o crime de acesso e outros crimes cometidos após se ter tido acesso ao sistema, nomeadamente os crimes de obtenção, utilização ou disponibilização de dados informáticos (artigo 5.º), intercepção ilegítima (artigo 6.º), dano a dados informáticos (artigo 7.º), obstrução de sistema informático (artigo 8.º), falsificação informática (artigo 10.º) ou burla informática (artigo 11.º).

Caso o acesso seja feito através da violação de medidas de segurança que protejam o sistema informático, como sejam os casos de descodificação de palavras-chave ou de desencriptação dos conteúdos, passa a estar-se em presença de um crime de acesso ilegítimo qualificado, dada a especial censurabilidade da conduta, com o correspondente agravamento da pena aplicável, que é o dobro da do crime simples.

O crime simples é semi-público: o procedimento penal depende de queixa, tendo legitimidade para a sua apresentação o titular do sistema violado. Considerou-se adequado deixar à vontade da vítima o exercício do direito de

queixa por poder haver situações em que o conhecimento público da vulnerabilidade do sistema informático poder causar mais prejuízos ao seu titular do que a própria conduta criminosa. No entanto, no crime qualificado já haverá razões de interesse público para que o crime seja público. Na prática, contudo, será improvável que as autoridades judiciárias tenham conhecimento da prática de um crime de acesso ilegítimo qualificado sem a existência de uma queixa por parte do titular do sistema.

5. – Obtenção, utilização ou disponibilização ilegítima de dados informáticos (Artigo 5.º)

O crime previsto no artigo 5.º é uma inovação da lei de Macau face à generalidade das experiências legislativas, ao nível do direito comparado, relativas à criminalidade informática e face à lista de crimes prevista da Convenção de Budapeste. Esta, no entanto, representa apenas um consenso mínimo e não impede que as legislações nacionais classifiquem como crimes outras condutas.[46]

O crime visa proteger a privacidade e a autodeterminação informacional de cada pessoa. O tipo objectivo do crime previsto no artigo 5.º é a obtenção, utilização e colocação à disposição de outrem de dados informáticos alheios. Pretende-se, portanto, proteger a confidencialidade dos dados informáticos, mesmo quando o agente tenha tido acesso a tais dados de forma legítima, isto é, com autorização. Independentemente da legitimidade do acesso, se o agente não tiver autorização do titular dos dados não pode obtê-los, utilizá-los ou colocá-los à disposição de outrem.

[46] *Vd.* Relatório Explicativo, *ob. cit.*, ponto 34.

O termo "obtenção" diferencia-se do "acesso" e implica que os dados tenham sido transferidos para a disponibilidade do agente, seja através da subtracção, seja por meio de cópias desses dados. O facto relevante é que, através da obtenção, o agente passa a ter o controlo sobre dados dos quais não é titular. A "utilização" implica que o agente faça uso desses dados, ou seja, que deles tire partido. Contudo, não é intenção legislativa a inclusão no tipo deste crime o mero uso pessoal de dados informáticos alheios. Assim, para efeitos do n.º 1 do artigo 5.º, "utilização" implica que o agente se aproveite desses dados *quando em contacto com terceiros*, haja ou não benefício económico. Abrange-se, assim, as situações de distribuição, isto é, o acto de envio ou partilha com terceiros, ou de venda de dados alheios. A "colocação à disposição de outrem" reporta-se à disponibilização, isto é, a conduta de tornar os dados alheios acessíveis por um número indeterminado de terceiros, nomeadamente através do seu carregamento para sítios da rede (*upload*).

Nos termos do n.º 2, o crime de obtenção, utilização ou disponibilização ilegítima de dados informáticos é qualificado em virtude da especial protecção dispensada a certos tipos de dados. Assim, caso se trate de dados sensíveis[47] ou de qualquer tipo de segredo ao qual a lei dispense protecção (nomeadamente segredo profissional, de justiça, médico, de Estado ou da Região, religioso ou comercial), a pena a aplicar é elevada para o dobro da do crime simples. Em ambas as situações está-se na presença de um crime semi-público.

Foi intenção de reunir no tipo de crime em análise a punição da utilização de dados informáticos, a qual estava na versão inicial da proposta de lei repartida em vários artigos. Razão pela qual foi eliminada a agravação, prevista no n.º 2 do artigo 6.º da versão inicial da proposta de lei, para os casos de

[47] No conceito adoptado pelo artigo 7.º da Lei n.º 8/2005 – Lei de protecção de dados pessoais.

utilização de dados obtidos através de intercepção ilegítima. Considerou-se ser mais adequado tratar todos os casos de utilização abusiva de dados informáticos da mesma forma, em vez de diferenciar tal utilização em função da forma de obtenção dos dados. Tanto mais que as molduras penais aplicáveis eram substancialmente diferentes. [48]

6. – Intercepção ilegítima de dados informáticos (Artigo 6.º)

Este crime visa proteger o direito à exclusividade e à privacidade na comunicação de dados em resultado da protecção que ao sigilo das comunicações é dispensada pelo artigo 32.º da Lei Básica. Da mesma forma que estão interditas escutas e gravações de conversas telefónicas entre indivíduos, esta norma impede que a comunicação de dados informáticos dentro de um sistema informático ou entre sistemas seja interceptada ilegitimamente.[49]

A intercepção é o acto destinado a captar informações contidas num sistema informático através de meios técnicos. «A intercepção por "meios técnicos" refere-se à escuta, monitorização ou vigilância do conteúdo das comunicações, à obtenção de conteúdo dos dados quer directamente, através do acesso e utilização do sistema informático, quer indirectamente, através da utilização de dispositivos electrónicos de intercepção de mensagens ou de escuta clandestina. A intercepção poderá igualmente envolver a gravação. Os meios técnicos englobam os equipamentos técnicos ligados a linhas de

[48] Pena de prisão até 5 anos ou pena de multa até 600 dias (para o caso do n.º 2 do artigo 6.º da versão inicial) e, nos demais casos, prisão até 1 ano ou pena de multa até 120 dias (crime simples) e pena de prisão até 2 anos ou pena de multa até 240 dias (crime qualificado).

[49] De acordo com o Relatório Explicativo, *ob. cit.*, ponto 55, «a comunicação sob a forma de transmissão de dados poderá ter lugar no interior de um único sistema informático (por exemplo, o fluxo de dados que é enviado da CPU para o monitor ou impressora), entre dois sistemas informáticos pertencentes à mesma pessoa, dois computadores em comunicação entre si, ou entre um computador e uma pessoa (por exemplo, através do teclado)».

transmissão, bem como dispositivos de recolha e gravação de comunicações sem fio. Poderão incluir o uso de sofware, "passwords" e códigos. O requisito da utilização de meios técnicos constitui uma condição restritiva a fim de evitar a sobrepenalização». [50] Os meios técnicos podem ser electromagnéticos, acústicos, mecânicos ou outros.

O n.º 2 do artigo 6.º (à semelhança do previsto nos artigos 7.º, 8.º 10.º e 11.º) prevê a punibilidade da tentativa. Aquando da análise na especialidade da proposta de lei foi ponderada necessidade e a adequação de se punir a tentativa da prática de certos crimes, tendo em consideração o grau de perigo que tal tentativa representa para os bens jurídicos protegidos. Assim, seguindo o critério fixado na Convenção de Budapeste na delimitação dos crimes que devem prever a punibilidade da tentativa, a nova versão da proposta de lei previu-a expressamente para os crimes de intercepção ilegítima, dano a dados informáticos, obstrução de sistema informático, falsificação informática e burla informática. Nos diversos casos de crimes agravados, quando o limite máximo da pena é superior a 3 anos de prisão, aplica-se a regra geral sobre a punibilidade da tentativa, consagrada no artigo 22.º do Código Penal.

7. – Dano a dados informáticos (Artigo 7.º)

O crime previsto no artigo 7.º visa assegurar aos dados informáticos uma protecção semelhante àquela de que gozam os bens corpóreos relativamente aos danos ocasionados de forma deliberada. [51] Neste caso, os interesses jurídicos protegidos são a integridade e o adequado funcionamento ou a correcta

[50] Relatório Explicativo, *ob. cit.*, ponto 53.
[51] *Vd.* Artigo 206.º (dano) do Código Penal.

utilização dos dados informáticos armazenados. [52] A nível do elemento subjectivo, exige-se apenas um dolo genérico.

Para a compreensão dos diferentes actos previstos no n.º 1 do artigo 7.º atente-se que ««danificação" e "deterioração" enquanto actos de sobreposição referem-se em particular a uma alteração negativa da integridade ou do conteúdo informativo dos dados ou programas. A "eliminação" de dados corresponde à destruição de bens corpóreos, uma vez que os suprime e os torna irreconhecíveis. A "supressão" de dados informatizados significa todo e qualquer acto no sentido de impedir ou extinguir a disponibilização dos dados à pessoa que tem acesso ao computador ou ao suporte no qual os dados se encontravam armazenados. O termo "alteração" significa a modificação dos dados existentes».[53]

O crime de dano comporta uma forma qualificada em função do valor do prejuízo patrimonial causado (n.ºs 3 e 4). Os conceitos de "prejuízo patrimonial elevado" e "prejuízo patrimonial de valor consideravelmente elevado" são concretizados nos termos das alíneas a) e b) do artigo 196.º do Código Penal. A alínea 2) do n.º 4 consagra uma forma qualificada do crime de dano, não em função do valor do prejuízo causado, mas em função da natureza dos dados danificados (dados com importante valor científico, artístico ou histórico ou com significado importante para o desenvolvimento tecnológico ou económico).

As penas previstas tanto para o crime de dano informático na forma simples, como na forma qualificada têm correspondência com os crimes de dano, simples e qualificado, previstos nos artigos 206.º e 207.º do Código Penal.

---

[52] *Vd.* Relatório Explicativo, *ob. cit.*, ponto 60.

[53] *Idem*, ponto 61. A introdução de códigos dolosos, tais como vírus e rotinas como os chamados "cavalos de Tróia", encontra-se abrangida por este crime, da mesma maneira que a modificação dos dados resultantes deste acto.

8. – Obstrução de sistema informático (Artigo 8.º)

O crime previsto no artigo 8.º tem como finalidade a penalização do impedimento intencional da utilização legítima de sistemas informáticos. O interesse jurídico protegido reside no interesse dos operadores e utilizadores de sistemas informáticos em que os mesmos apresentem um funcionamento adequado. Por "obstrução " entende-se todo e qualquer acto que interfira com o correcto funcionamento do sistema informático, o qual poderá ter lugar através da introdução, transmissão, danificação, deterioração, alteração, supressão ou eliminação de dados informáticos.[54]

A nova versão da proposta de lei procedeu à redução da pena prevista para este crime (em vez de pena de prisão até 5 anos ou pena de multa até 600 dias o crime passa a ser punido com pena de prisão até 3 anos ou com pena de multa). Esta alteração visou proceder a uma uniformização das penas dos diferentes crimes previstos nesta lei quando considerados na sua forma simples.[55] Visou, também, introduzir uma diferenciação entre a punição da forma simples do crime de obstrução (n.º 1) e a da sua forma qualificada (n.º 3). Tal não acontecia na versão inicial da proposta de lei uma vez que havia uma coincidência entre a moldura penal máxima entre as duas formas do crime (5 anos), havendo apenas uma diferenciação ao nível da moldura penal mínima.

[54] *Idem*, pontos 65-66.
[55] Os crimes previstos nos artigos 6.º a 11.º são todos punidos, na sua forma simples, com pena de prisão até 3 anos ou com pena de multa.

9. – Dispositivos ou dados informáticos destinados à prática de crimes (Artigo 9.º)

O crime em análise consagra como infracção penal distinta e independente a prática intencional de certos actos relativos a dispositivos ou dados informáticos que sirvam para cometer os crimes contra a confidencialidade, integridade e disponibilidade dos sistemas ou dados informáticos. Os bens jurídicos protegidos são os mesmos que obtêm protecção ao abrigo dos artigos 4.º a 8.º, mas este crime prevê a antecipação da protecção penal desses bens jurídicos, punindo as transacções que visem tornar tais dispositivos acessíveis a quem pretenda cometer crimes informáticos. O regime ora introduzido é equivalente ao crime previsto no artigo 263.º do Código Penal para as transacções sobre instrumentos destinados à violação de comunicações.

O n.º 1 do artigo 9.º exige um dolo específico: a prática de qualquer um dos actos nele previstos tem de reportar-se a dispositivos ou dados concebidos ou adaptados essencialmente para a prática de crimes informáticos. Refira-se ainda que a mera posse não é punível e que os conceitos de "distribuição" e de "colocação à disposição de outrem" devem ser entendidos como o acto de enviar dados para terceiros e o acto de colocação de dispositivos *online* para utilização de terceiros, respectivamente.[56]

10. – Falsificação informática (Artigo 10.º)

O crime de falsificação informática visa dispensar aos documentos electrónicos o mesmo tipo de protecção que os artigos 244.º e 245.º do Código Penal dispensam aos documentos tangíveis, isto é, em suporte de papel.

[56] *Vd.* Relatório Explicativo, *ob. cit.*, ponto 72.

A falsificação informática consiste na criação ou alteração não autorizada de dados informáticos por forma a que os mesmos se revistam de um valor probatório diferente, afectando as relações jurídicas que se baseiem na autenticidade da informação veiculada por esses dados.[57] Exige-se, portanto, que os dados falsificados «sejam susceptíveis de servirem como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado. Tenta-se mais uma vez proteger a segurança e credibilidade do tráfico jurídico, em especial dos meios de prova, pois é este o bem jurídico que é violado quando através de um meio de prova falsificado se provoca um engano nas relações jurídicas. Assim sendo, só estaremos perante um crime de [falsificação] informática quando o "documento" falsificado é susceptível de ser utilizado como meio de prova».[58] A disposição em causa aplica-se «aos casos em que os dados manipulados não são transportados para um texto impresso, mas são directamente empregados para outros tratamentos informáticos, como, por exemplo, em transacções bancárias, em operações contabilísticas e até em pagamentos. Pode tratar-se de levar um computador a reagir a um documento falso como se se tratasse de um verdadeiro, exactamente como no caso de levar um pessoa a aceitar como verdadeiro um documento falso».[59]

Tanto no crime de falsificação informática (n.º 1), como no de uso intencional de documento falsificado (n.º 2), a lei exige um dolo específico: que haja a intenção de provocar engano nas relações jurídicas (n.º 1) ou que haja a intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo para si ou para terceiros (n.º 2).

---

[57] *Idem*, ponto 81.
[58] Helena Moniz, *O Crime de Falsificação de Documentos – Da Falsificação Intelectual e da Falsidade em Documento*, Coimbra Editora (1999), pp. 270-271.
[59] Manuel António Lopes da Rocha, 'A Lei da Criminalidade Informática', in *Legislação – Cadernos de Ciência de Legislação*, n.º 8, Instituto Nacional de Administração (1993), p. 72.

Ambos os crimes compreendem uma forma qualificada em função da especial qualidade do agente, do especial valor do documento falsificado (o que remete para a classificação feita pelo artigo 245.º do Código Penal) ou da segurança inerente ao uso de assinatura electrónica qualificada (nos termos do disposto na Lei n.º 5/2005).

A redução da pena efectuada pela nova versão da proposta de lei visa, à semelhança da pena prevista para o crime de obstrução de sistema informático, proceder a uma harmonização sancionatória dos diversos crimes informáticos. Considerou-se, igualmente, que a falsificação informática devia ser punida nos mesmos termos em que o é a falsificação de documentos no Código Penal. Assim, após a redução da pena tal como constava da versão inicial, a falsificação de documentos, na sua forma simples, é punida com uma pena até 3 anos de prisão ou com pena de multa, independentemente da natureza do documento falsificado. Atinge-se, desta forma, uma maior harmonia no sistema penal.

11. – Burla informática (Artigo 11.º)

O crime de burla informática previsto no artigo 11.º é um crime contra o património: visa proteger o património de quem sofre um prejuízo patrimonial em virtude da burla (e não de quem é o proprietário ou o utente dos dados ou sistemas informáticos). O tipo ora previsto é semelhante ao do artigo 213.º do Código Penal, ora revogado, sendo dele retirado a vertente da utilização não autorizada de dados informáticos, conduta constante do artigo 5.º da proposta de lei. Os actos abrangidos pelo tipo objectivo prendem-se com manipulações informáticas que tenham uma intenção fraudulenta, deles resultando perdas patrimoniais de terceiros e caso o agente tenha agido com a intenção de obter

vantagem lucrativa ilícita para si próprio ou para terceiros. A referência à interferência no resultado de tratamento de dados informáticos [alínea 2) do n.º 1] visa garantir que todas as formas relevantes de manipulação se encontram abrangidas, cobrindo actos tais como as manipulações de *hardware*, os actos que impedem as saídas para a impressora, assim como os actos que afectam o registo ou o fluxo de dados, ou a sequência pela qual os programas são executados.[60] A estruturação do programa informático é incorrecta [alínea 3) do n.º 1] quando ela é contrária à finalidade do programa informático, produzindo as novas instruções resultados objectivamente contrários à finalidade do programa.[61]

A burla informática distingue-se do crime de burla geral, previsto no artigo 211.º do Código Penal, por ser um crime de execução vinculada. Enquanto que o crime de burla geral pode ser cometido por qualquer meio de erro ou engano sobre os factos que o agente astuciosamente provocou, o crime de burla informática tem de ser cometido através de algum dos meios descritos no n.º 1.[62]

12. – Agravação da pena (Artigo 12.º)

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,

[60] *Vd.* Relatório Explicativo, *ob. cit.*, ponto 87.
[61] *Vd.* Paulo Pinto de Albuquerque, *Comentário do Código Penal*, Universidade Católica Editora (2008), comentário ao artigo 221.º, p. 609.
[62] *Vd.* Manuel Lopes Maia Gonçalves, *Código Penal Português Anotado e Comentado*, 17ª ed. (2005), anotação ao artigo 221.º, p. 769.

pretendendo-se «reforçar a protecção da confidencialidade e a integridade de sistemas informáticos ou dados informáticos».[63]

O n.º 2 procede a uma equiparação material da internet a meios de comunicação social, para os efeitos do n.º 2 do artigo 177.º e da alínea b) do artigo 192.º do Código Penal. Estas duas normas prevêem que a prática através de meios de comunicação social dos crimes de difamação e injúria (artigo 177.º) e dos crimes contra a reserva da vida privada previstos nos artigos 184.º a 189.º do Código Penal (artigo 192.º) é punida de uma forma agravada por força do alargamento do impacto nocivo da ofensa decorrente do número alargado de pessoas com acesso à conduta típica. O conceito de "meio de comunicação social" abrange a imprensa, a rádio e a televisão. Apesar de haver uma tendência para também fazer abranger a internet nesse conceito,[64] poderiam ser suscitadas dúvidas quanto ao âmbito do conceito. Assim, para evitar dúvidas na interpretação da lei, o n.º 2 do artigo 12.º da proposta de lei vem equiparar a internet aos demais meios de comunicação social. Esta equiparação é feita, no entanto, apenas quando a internet seja utilizada como meio de ampla difusão das condutas típicas dos crimes em causa. Ou seja, quando sirva para uma difusão generalizada das condutas injuriosas, caluniosas ou devassadoras. Assim, a agravação não funciona quando a internet seja utilizada para a mera distribuição (através de correio electrónico, por exemplo), mas já o será quando servir para a disponibilização de conteúdos que constituam os tipos de crime em causa (através do carregamento para sítios da internet, por exemplo). No primeiro caso não se estará perante uma ampla difusão da conduta criminosa, ainda que tenha sido utilizada a internet.

[63] Nota Justificativa.
[64] *Vd.* Luís Brito Correia, *Direito da Comunicação social*, Vol. I, Almedina (2000), pp. 22-24 e Paulo Pinto de Albuquerque, *ob. cit.*, anotação ao artigo 183.º, p. 502.

Note-se, ainda, que os termos da agravação efectuada pelo artigo 178.º do Código Penal terá também aplicação, ainda que de forma indirecta, quando os crimes de difamação e injúria forem cometidos através da internet e se reportarem a uma das pessoas referidas na alínea h) do n.º 2 do artigo 129.º do Código Penal: O facto do artigo 178.º agravar as penas dos artigos 174.º, 175.º e 177.º faz com que a difamação e injúria através da internet de funcionário, docente, examinador público, testemunha ou advogado, no exercício das suas funções ou por causa delas, sejam punidas com as penas previstas no n.º 2 do artigo 177.º (devido ao meio utilizado), elevadas de metade nos seus limites mínimos e máximo, por força do artigo 178.º (devido à especial qualidade da vítima).

13. – Disposições processuais penais – disposição geral (Artigo 14.º)

A redacção do artigo 14.º foi alterada no sentido de clarificar o âmbito do regime processual consagrado na presente iniciativa legislativa. Assim, pretende-se criar um regime especial relativo à obtenção e conservação de prova para:

1) Os crimes previstos na lei de combate à criminalidade informática;
2) Os crimes previstos no Código Penal e demais legislação penal avulsa caso sejam cometidos por meio de sistema informático;[65]
3) Todos os crimes, no que diz respeito à recolha de prova em suporte electrónico.[66]

[65] Pense-se, por exemplo, no crime de difamação praticado no internet. Para uma lista não exaustiva dos crimes que podem ser cometidos com recurso a sistemas informáticos *vd.* notas 11 e 12 ao presente Parecer.
[66] Assim, por exemplo, o disposto na presente iniciativa legislativa é aplicável às apreensões de correspondência electrónica trocada no âmbito da prática de um crime de ameaça ou de corrupção.

As normas previstas nos artigos 15.º e 16.º têm natureza especial face às do Código de Processo Penal (CPP), sendo este aplicável em tudo o que não esteja especialmente previsto nesta lei. Assim, mantém-se, como regra, a aplicação do disposto na lei processual penal geral.

14. – Apreensões (Artigo 15.º)

A versão inicial deste artigo continha uma regra que previa a admissibilidade dos sistema informáticos, suportes de armazenamento de dados informáticos e dados ou programas informáticos como prova para efeitos processuais penais. Tendo em consideração o princípio da legalidade da prova (artigo 112.º do CPP), segundo o qual são admissíveis as provas que não forem proibidas por lei, e não estando proibida a obtenção e a utilização dos sistemas informáticos, suportes de armazenamento de dados informáticos e dados ou programas informáticos como prova, considerou-se desnecessária a previsão de tal norma. A eliminação do n.º 1 do artigo 15.º da versão inicial da proposta de lei em nada afecta a admissibilidade em juízo das provas em suporte electrónico ou a possibilidade de os sistemas e dados informáticos poderem ser utilizados para efeitos probatórios. O valor probatório das reproduções por meios electrónicos está, aliás, consagrado no artigo 153.º do CPP.

O n.º 1 do artigo 15.º da nova versão da proposta de lei possibilita, como meio de obtenção de prova, a apreensão de sistemas informáticos, de suportes de armazenamento de dados informáticos e de dados informáticos, de forma directa ou por meio de cópia. Estende-se às provas electrónicas, portanto, o regime constante dos artigos 163.º, 168.º e 169.º do CPP.[67]

[67] Relativamente às apreensões de material electrónico, *vd.* Fong Man Chong, 'Recurso às Novas Tecnologias no Processo Penal', in *Actas da Conferência Internacional do Processo Penal – Os desafios do Século XXI*, Centro de Formação Jurídica e Judiciária (2007), pp. 247-277, e Pedro Verdelho, 'A

O n.º 5 do artigo 15.º esclarece que às apreensões de correio electrónico ou de outras formas de comunicação particular sob a forma electrónica, por exemplo através de SMS, se aplica o Código de Processo Penal (artigos 164.º e 235.º), não havendo qualquer especialidade de regime relativa a este aspecto. Mantém-se, assim, válida a garantia judiciária para este tipo de intervenções, sendo exigida a intervenção do juiz de instrução neste tipo de apreensões. Enquanto que os órgãos de polícia criminal têm competência para efectuar apreensões no âmbito de um processo penal, não o poderão fazer quando as apreensões digam respeito a correspondência em forma electrónica, entendida esta de forma lata.

De igual forma, as apreensões de provas electrónicas em escritório de advogado ou em consultório médico, em estabelecimento bancário ou relativas a segredo legalmente protegido seguem o regime geral previsto na lei processual penal (artigos 165.º a 167.º do CPP), funcionando plenamente a garantia judiciária aí prevista. O mesmo se passando no que diz respeito à intercepção do conteúdo das comunicações electrónicas – o artigo 175.º do Código de Processo Penal procede à extensão do regime legal das escutas telefónicas (artigos 172.º a 174.º do CPP) às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone.

15. – Medidas especiais (Artigo 16.º)

O ponto 5.2 da apreciação genérica do presente Parecer já teve oportunidade de analisar o regime constante do artigo 16.º da proposta de lei. Em sede de apreciação na especialidade cumpre salientar que as alterações de

obtenção de prova no ambiente digital', in *Revista do Ministério Público*, Ano 25, n.º 99 (2004), pp. 117-136.

redacção visaram, sobretudo, reforçar a ideia de que a competência para a prática dos actos aí previstos é atribuída à autoridade judiciária, especificamente ao Ministério Público. Este, no âmbito dos seus poderes de direcção do inquérito penal, pode ordenar a prática das medidas especiais previstas no n.º 1 do artigo 16.º. Justamente por serem especiais, incumbe ao Ministério Público um dever especial de fundamentação da necessidade da sua adopção. A nova versão da proposta de lei enfatiza, aliás, a necessidade de o Ministério Público presidir à diligência sempre que isso seja possível.

A intervenção dos órgãos de polícia criminal é admitida, nos mesmos termos em que o é pelo CPP nos demais casos, em situações de urgência na obtenção e conservação da prova. Uma vez mais, realça-se o carácter excepcional desta intervenção, não devendo a mesma ser adoptada a título de regra. Quando os órgãos de polícia criminal adoptem as medidas especiais sem prévia autorização judiciária, necessitam que as mesmas sejam validadas no prazo de 72 horas, sob pena de nulidade. O regime previsto nos n.ºs 2 e 3 do artigo 16.º para a adopção das medidas especiais no âmbito da lei de combate à criminalidade informática é idêntico ao previsto nos n.ºs 3 a 5 do artigo 163.º do CPP para as apreensões. Também aí se prevê a competência geral da autoridade judiciária, a possibilidade de intervenção urgente dos órgãos de polícia criminal e a validação judicial no prazo de 72 horas.

O n.º 4 do artigo 16.º consagra a figura da impugnação judicial da ordem de remoção de dados informáticos considerados ilegais, nos termos da alínea 5) do n.º 1. Neste caso, a autoridade judiciária faz um pré-juízo sobre a legalidade dos dados em questão e determina que os mesmos fiquem inacessíveis ao público em geral, por forma a fazer parar a violação dos bens jurídicos relevantes. Devido ao facto desta medida poder, na prática, limitar a liberdade de expressão constitucionalmente garantida, a lei consagra a possibilidade de sindicância da

decisão judicial, determinando que a adopção da medida prevista na alínea 5) do n.º 1 possa ser impugnável perante o juiz de instrução criminal. O titular deste direito de impugnação não é apenas o destinatário da ordem de remoção – o prestador de serviço de Internet –, mas também quem é afectado por essa ordem, ou seja, o titular dos dados removidos. O prazo de 10 dias para a impugnação é idêntico ao previsto no Código de Processo Penal para a impugnação das apreensões (artigo 163.º, n.º 6, com a redacção dada pelo n.º 2 do artigo 6.º do Decreto-Lei n.º 55/99/M, de 8 de Outubro). O facto de se prever a figura da impugnação judicial apenas para as situações da alínea 5) do n.º 1 não prejudica a aplicação subsidiária do disposto no Código de Processo Penal para a impugnação das apreensões efectuadas ao abrigo da presente iniciativa legislativa.

V –Conclusão

Em conclusão, apreciada e analisada a proposta de lei, a Comissão:

a) é de parecer que a proposta de lei reúne os requisitos necessários para apreciação e votação, na especialidade, pelo Plenário;

b) sugere que, na reunião plenária destinada à votação na especialidade da presente proposta de lei, o Governo se faça representar, a fim de poderem ser prestados os esclarecimentos necessários.

Macau, 17 de Junho de 2009.

A Comissão,

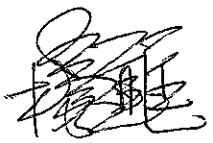
Cheang Chi Keong
(Presidente)

Philip Xavier
(Secretário)

Ho Teng Iat

Kou Hoi In

Victor Cheung Lup Kwan



Iong Tou Hong

José Maria Pereira Coutinho

Leong On Kei

Lee Chong Cheng