COMPARAÇÃO DOS CRIMES DE INVASÃO ILEGAL DE COMPUTADORES NA CHINA, TAIWAN, HONG KONG E MACAU

Fong Pui Hong
Estudante do Curso de Mestrado em Direito em Língua Chinesa,
Faculdade de Direito da Universidade de Macau

1. Introdução

A natureza automática e a precisão do computador ajuda-nos a trabalhar. A sua natureza transnacional e rapidez facilitam a troca de informações. O computador está a tornar-se num instrumento cada vez mais importante. Porém, todas estas características tornam o computador um "ideal" instrumento e objecto de crime.

Para garantir a confiança da comunidade na utilização dos computadores e para proteger os direitos das pessoas sobre o seu computador, sistema e informações, tais como o direito ao sigilo e o direito à privacidade, muitos países criaram normas penais para combater a criminalidade informática[1].

A criminalidade informática refere-se a todos os crimes praticados através do sistema informático ou crimes que têm como objecto o sistema informático.

Os crimes de invasão que têm como objecto o computador são praticados com mais frequência nos sistemas de computador digital[2]. Este tipo de crime não só causa preocupação por parte da comunidade em relação à segurança do sistema informático, como também gera grandes riscos de perda, dano ou divulgação de informações e dados do computador invadido. Estes actos criminosos são praticados em segredo e pressupõem o uso de altas tecnologias. São actos

1 Pi Yong, "Teoria original do Direito da Segurança da Rede", Chinese People's Public Security University, 2008, pp. 445 a 484.

2 Benjamim Silva Rodrigues; com prefácio de Sara Antunes "Direito Penal: parte especial. 1, Direito penal informático-digital", Coimbra Editora, 2009, p. 281.

inter-regionais dificilmente investigáveis[3]. Portanto, é necessário analisar a regulamentação jurídica destes tipos de crime e a respectiva estratégia de combate.

Nesta apresentação vamos proceder à comparação dos regimes de combate à invasão ilegal de computadores da China, Taiwan, Hong Kong e de Macau, analisando especialmente os requisitos subjectivos e objectivos da constituição do crime para melhor compreender a implicação da regulamentação jurídica, de modo a adoptar as medidas de solução mais apropriadas e observar de forma global o sistema jurídico de diversos países para identificar as lacunas existentes[4].

2. Comparação do direito penal da China, Taiwan, Hong Kong e Macau em relação ao crime de invasão ilegal de computadores

(A) Finalidade e objecto de comparação

Não há crime sem lei e não há pena sem lei. Quando o agente pratica um acto proibido por lei, constitui um crime e deve ser sujeito a sanções. O direito penal para além de regular os actos criminosos, também estabelece uma série de condições necessárias para a constituição de um crime, os requisitos constitutivos.

De acordo com a doutrina de Macau, são três os elementos constitutivos do crime, sendo o primeiro a punibilidade. A seguir são a ilicitude e a imputabilidade, por sua vez dividida em quatro elementos, sendo eles a capacidade de responsabilidade, o dolo e a negligência, a consciência da ilicitude e a previsibilidade[5].

Na doutrina chinesa, os elementos constitutivos do crime abrangem em geral os elementos constitutivos das centenas dos crimes previstos no direito penal. Em primeiro lugar temos o elemento subjectivo do crime que inclui o sujeito do crime, pessoa singular ou colectiva; quanto ao aspecto subjectivo do crime, este abrange o dolo, a negligência, a culpa, a finalidade e o motivo; por outro lado, temos em primeiro lugar as condições objectivas que abrangem o aspecto objectivo do crime, incluindo neste certos pressupostos de crime, o tempo, o local, o método, o acto único, dois ou mais actos de diversa natureza e a repetição de actos da mesma natureza; em segundo lugar temos o objecto do crime que abrange o objecto, o resultado danoso e o bem jurídico; por último temos os factores de

3 Wang Mingyong, "Estudo da regulamentação dos crimes cibernéticos", in Liu Shangzhi, "Colectânea das teses da Conferência Nacional da Ciência e Tecnologia e Direito 2002", National Chiao Tung University, 2002, pp. 493 e 494.

4 Konrad Zweigert e Hein Kotz, "Introdução ao Direito Comparado", Law Press, 2005, pp. 21 a 44.

5 Zhao Guoqiang, "Estudo do Direito Penal de Macau (Direito Substantivo) ", Fundação Macau, 2005, pp. 5 a 8.

graduação, tais como a seriedade ou a gravidade da situação[6].

A doutrina de Taiwan por sua vez defende que os elementos constitutivos do crime são dois, sendo o primeiro deles o elemento subjectivo, incluindo o dolo, a negligência e a intenção; o segundo elemento é o elemento objectivo que abrange o objecto, agente, acto, situação do acto, tempo do acto, objecto do acto e resultado[7].

Em Hong Kong vigora o sistema de Common Law, centralizado na interpretação das leis por parte do juiz, ou seja, nos precedentes judiciários. A constituição do crime depende se o comportamento do réu violou a lei e se tinha intenção criminal, isto é, se o réu violou as leis penais com dolo ou negligência (sem ter em conta o resultado da sua acção), ou também, em certas situações, se o réu praticou o acto por negligência grosseira[8].

Através do direito comparado, podemos observar que diferentes locais têm diferentes formas de entender a constituição do crime. No entanto, podemos afirmar que existem certos elementos constitutivos do crime comuns em todas teorias do direito penal: elemento objectivo, certos pressupostos (tais como a autorização ou delegação), a prática da conduta e o objecto da acção (objecto e bem jurídico); o elemento subjectivo inclui o sujeito do acto, o dolo e a negligência. Este discurso terá como padrão o Direito de Macau e será feita uma comparação das diferenças dos aspectos regulados, discutindo os respectivos problemas.

(B) Comparação dos elementos constitutivos do crime de invasão ilegal de computadores

1. Regulamentação legal do crime de invasão ilegal de computadores

Na China, os crimes informáticos estão basicamente regulados no Capítulo VI "Crimes contra a Ordem de Administração Social" da Lei Penal da RPC. Nos termos do art. 285.º, alterado pela 7.ª Emenda do Código Penal, que estabelece o crime de invasão ilegal do sistema de informação de computadores[9]: Primeiro parágrafo - Quem, contra as disposições estabelecidas pelo Estado, interferir em assuntos nacionais, tais como sistemas de informática de tecnologia avançada ou sistemas de defesa nacional, deve ser punido com pena de prisão até 3 anos ou detenção criminal; Segundo parágrafo - Quem, violando disposições estatais,

---

6 Zhao Tingguang, Zhu Huachi, Pi Yong, "Condenação e determinação da pena dos crimes informáticos", Tribunal Popular, 2000, pp. 119 e 120.

7 Lu Yingjie, "Nova Teoria do Direito Penal", Sharing Culture, 2008, pp. 1 a 4, 14, 15, 42, 69 e 82.

8 Chen Hung-yee ...[etc], "Introdução do Direito de Hong Kong", Joint Publishing (Hong Kong), 2009, pp. 173 e 174.

9 A designação dos crimes consagrada na Lei Penal da RPC é feita pelas regras de determinação da designação dos crimes da Lei Penal aplicadas pelo Tribunal Popular.

aceder ilegitimamente a sistema informático de informação outro que não o descrito no parágrafo anterior ou utilizar outros meios técnicos para obter os dados aí armazenados, processados ou transmitidos, ou exercer controlo ilegal sobre o referido sistema informático de informação, se as circunstâncias forem graves, deve ser condenado em pena de prisão até 3 anos ou detenção criminal, e/ou em pena de multa. Se as circunstâncias forem extremamente graves, deve ser condenado em pena de prisão de termo fixo de 3 a 7 anos e em pena de multa.

Em Macau, os crimes informáticos estão regulados na Lei n.º 11/2009, Lei de combate à criminalidade informática, publicada no Boletim Oficial n.º 27, de 6 de Julho de 2009. O art. 4.º que regula o "acesso ilegítimo a sistema informático" estabelece que: "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". Por outro lado, o art. 12.º que regula a agravação da pena prevê que: "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 (...) são agravadas de um terço nos seus limites mínimo e máximo. (...) ".

Em Hong Kong, este tipo de crime está regulado pelo "Computer Crimes Ordinance". No entanto, a lei não estabelece o crime de invasão ilegal. Este tipo de crime é punido através do crime de acesso não autorizado a computadores por via de telecomunicações ou crime de utilização de computadores com má fé, etc.[10]. A primeira lei corresponde ao seu Capítulo 106, "Telecommunications Ordinance", Secção 27A, e estabelece o seguinte: "Quem, por via de telecomunicação, conscientemente faz com que um computador desempenhe qualquer função para obter o uso não autorizado de qualquer programa ou sistema de dados, comete um crime e é sujeito a condenação a multa de $20000". Por outro lado, a Secção 161 que consagra o "Crimes Ordinance" prevê que: "(1) Quem obtém acesso a um computador – (a) com intenção de cometer um crime; (b) com intenção fraudulenta; (c) com intenção de lucro para si ou para terceiro; ou (d) com intenção de causar perda para terceiro, no momento da conduta ou em qualquer momento futuro, comete um crime e é sujeito a condenação a prisão por 5 anos (...)".

O Código Penal de Taiwan regula no seu art. 36.º o crime contra o uso de computador. No art. 358.º regula o crime de invasão de computadores ou equipamentos relacionados e estabelece o seguinte: "Quem, sem motivo

10 Zhao Bingzhi, Yu Zhigang, "Estudo comparativo da criminalidade informática", Law Press, 2004, p. 68.

justificado, invadir o computador ou equipamento relacionado de terceiro, por meio de utilização da palavra-passe da conta de terceiro, quebra de meios de protecção de computadores ou aproveitamento das lacunas do sistema informático, é condenado a prisão até 3 anos, detenção e/ou pena de multa até 100000". O art. 360.º regula a agravação da pena e estabelece que: "quando os crimes dos três artigos anteriores forem praticados contra computador ou equipamento relacionado de órgãos públicos, a pena será aumentada a metade".

2. Comparação do elemento objectivo constitutivo do crime

Tal como referido anteriormente, o elemento objectivo inclui o pressuposto, a conduta, o objecto e o bem jurídico.

a) Comparação do pressuposto

Na China, os pressupostos que objectivamente implicam a constituição do crime são a violação das leis estatais, isto é, a violação das leis que protegem a segurança do sistema informático[11], tais como o Estatuto da Protecção da Segurança do Sistema de Informação de Computadores da RPC, as Medidas de Administração da Protecção da Segurança da Rede Internacional do Sistema de Informação de Computadores, etc.

Em Macau, os pressupostos específicos que objectivamente constituem um crime são a falta de autorização e a violação de medidas de segurança.

A falta de autorização significa a falta de legitimidade, portanto, a falta de autorização implica o acesso ilegítimo[12].

No âmbito da protecção de informações, a autorização refere-se ao responsável por garantir os recursos protegidos por um sistema informático (incluindo arquivos, programas de computador, dispositivos de hardware e outras funções do sistema) apenas sejam utilizados por utentes autorizados. Utente refere-se à pessoa que utiliza o sistema informático através de uma interface, programas de computador ou outros dispositivos[13].

Autores portugueses defendem que os requisitos da autorização para o acesso devem ser definidos com antecedência ou ao mesmo tempo, caso contrário, o acesso irá tornar-se ilegítimo.

---

11 De acordo com o art. 3.º do Estatuto da Protecção da Segurança do Sistema de Informação de Computadores da RPC: a protecção da segurança do sistema de informação de computadores consiste em proteger a segurança dos computadores e os respectivos equipamentos, a segurança de instalações (incluindo a Internet), a segurança das condições de funcionamento, proteger a segurança das informações, garantir o funcionamento normal dos computadores, garantindo o funcionamento seguro do sistema de informação dos computadores.

12 Parecer n.º 3/III/2009 da 3.ª Comissão Permanente da Assembleia Legislativa da RAEM (versão chinesa), p. 24.

13 http://pt.wikipedia.org/wiki/Autoriza%C3%A7%C3%A3o

Devemos estabelecer limites à autorização? O legislador entende que o acesso autorizado nunca constitui crime. Segundo autores portugueses, o acesso autorizado implica o consentimento da realização de actos ilegítimos. Mas esta situação causa inevitavelmente prejuízos ao sujeito passivo (ou seja, aquele que autoriza), portanto, deve ser sujeita a restrições. Consideramos que podemos aplicar o regime de consentimento estabelecido no art. 37.º do Código Penal, isto é, se aquele que autoriza tem o direito de dispor os interesses jurídicos em causa, o acto que a pessoa autorizada e legitimada pratica não ofende por si os bons costumes e a declaração é feita de forma séria, livre e esclarecida, a autorização é existente, caso contrário, é considerada não feita. Por exemplo, o administrador do sistema informático do Banco A autoriza B para aceder ao sistema para adquirir informações. Esta autorização não é eficaz, porque A não tem poderes para autorizar. Por outro lado, o fornecimento da palavra-chave também é uma forma de autorização. Este acto promove a invasão ilegal, reduzindo o efeito das normas do direito penal. Assim, o sistema legal japonês e o art. 1030.º do Código Penal dos EUA regularam este tipo de acto, atribuindo-lhe responsabilidade criminal[14]. Portanto, é necessário estabelecer limites sobre o regime da autorização.

A chamada "violação de medidas de segurança" consiste na ultrapassagem de dispositivos de protecção da segurança do sistema informático, por exemplo, quebrar a palavra-passe.

Em Taiwan, a chamada "sem razão justificativa" corresponde à falta de razão legítima (tal como direitos), isto é, à falta de exclusão de ilicitude, incluindo a exclusão de ilicitude legal ou extralegal. O acto de invasão não constitui crime quando a sua ilicitude é excluída[15].

Na nossa opinião, existem aspectos comuns entre os pressupostos específicos na China e em Taiwan, porque qualquer exclusão da ilicitude deve ser prevista expressamente na lei, portanto, a falta de exclusão de ilicitude pode ser considerada como uma forma de violação da lei. A diferença reside no facto de em Macau, o pressuposto consistir na autorização, ao passo que na China e em Taiwan, o pressuposto consiste na lei, isto é, a invasão que viola as leis estatais constitui um crime, independentemente da autorização da vítima. O que acontece se o acto não é permitido por lei mas é autorizado pela vítima? Podemos afirmar que quando a autorização satisfaz as condições do consentimento para a exclusão da ilicitude, o agente autorizado terá legitimidade para praticar o acto e, consequentemente, o acto não será considerado crime. No entanto, dado que

14 Liu Shangchi, "Colectânea das teses da Conferência Nacional da Ciência e Tecnologia e Direito 2002", National Chiao Tung University, 2002, pp. 511 e 512.

15 Gan Tiangui, "Teoria do Direito Penal = Criminal law: specific provisions", San Min Book, 2009, pp. 418 a 423.

a segurança do sistema é também um direito e interesse legítimo do titular, a sua opinião deve ser considerada, permitindo-lhe que, em certas circunstâncias, possa autorizar a utilização do sistema informático por parte de terceiro.

b) Comparação da conduta

Na China, quanto aos elementos da conduta, em primeiro lugar temos a obtenção e a visita não autorizada de contas e o acesso não autorizado a recursos do sistema de informação de computadores[16]. Em segundo lugar, para além dos actos de invasão, temos também actos de obtenção. De acordo com a teoria criminal da China, obtenção geralmente pode ser feita por subtracção, espionagem ou suborno. A subtracção refere-se ao acto de obtenção de dados do computador através de métodos secretos. Dado que as duas últimas formas só podem ser feitas através de pessoas, o acto de obtenção de dados apenas pode ser praticado por subtracção. Por último, o controlo ilegal do sistema informático também pode constituir crime. O controlo consiste na diminuição ou eliminação da capacidade de uso material ou disposição do sistema de informação de computadores por parte do seu proprietário, por exemplo, a criação de uma "botnet" para praticar actos criminosos[17].

Normalmente estes actos são praticados através da utilização de contas falsas ou através de ataques por tecnologia informática[18].

Em Macau, a conduta proibida apenas abrange o "acesso". O Parecer da Assembleia Legislativa refere que o termo "acesso" se entende como sendo a entrada no todo ou numa parte de um sistema informático e a penetração noutro sistema informático, acessível através de redes de telecomunicações públicas, ou num sistema informático na mesma rede.

Autores portugueses consideram que o acesso abrange a simples penetração e a invasão do sistema informático, através da quebra de medidas ou meios de segurança, por motivos de entretenimento ou diversão, sem intenção de controlo ou destruição. Também há casos jurisprudenciais onde se refere que o acesso refere-se ao acto de penetração sem consentimento ou autorização[19].

Quando à forma ou método concreto do acto, o Parecer da Assembleia

16 Pi Yong, "Estudo Comparativo da Criminalidade Informática", Chinese People's Public Security University, 2005, p. 121; Yu Zhigang, "Medidas de resolução judicial de problemas da criminalidade informática", Jilin People's Publishing House, 2001, p. 135.

17 http://jcy.zhenjiang.gov.cn/fzxc/200912/t20091214_253997.htm

18 Yu Zhigang (editor), Shi Tingan (vice-editor), "Medidas de resolução judicial de problemas da criminalidade informática", Jilin People's Publishing House, 2001, p. 139.

19 Decisão do Tribunal de Segunda Instância, Processo n.º 112/2003 (versão em língua chinesa), p. 16.

Legislativa divide-o em dois tipos. O primeiro tipo é o acesso feito através da violação de medidas de segurança do sistema informático, por exemplo a descodificação de palavra-chave ou de desencriptação dos conteúdos. O segundo tipo refere-se a todas outras formas de acesso, dado que a lei não regula em especial outras formas de acesso. Segundo autores portugueses, o acto de invasão pode ser dividido entre invasão ilegal com intenção de lucro, invasão legal perigosa, onde a invasão é feita aproveitando-se das lacunas ou deficiências das medidas de segurança do sistema informático e invasão ilegal por motivos de curiosidade.

Em Hong Kong, a constituição do crime depende apenas da conduta e da intenção de praticar o crime. Assim, os elementos da conduta regulada na Secção 27A do Capítulo 106 são, quanto ao aspecto negativo, a falta de autorização, isto é, a falta de um acto que legitima o uso de dados ou programas do computador, portanto, o suspeito não tem poderes para praticar o acto. O crime é praticado através da telecomunicação. A telecomunicação consiste na transferência de informações entre dois lugares diferentes, por via do uso da tecnologia electrónica, por exemplo, canais de transmissão de dados baseados em tecnologia digital (especialmente computadores). De acordo com a lei, esta é a única maneira de praticar o crime. "Fazer com que um computador desempenhe qualquer função" consiste na execução da função de tratamento de dados ou de programas do sistema informático tal como lhe foi indicado pelo agente. Por último, o "uso" de programas ou dados informáticos refere-se à transferência ou utilização do computador e dos respectivos programas ou dados. Por outro lado, os elementos da conduta regulada na Secção 161 da mesma lei incluem o acto de acesso, isto é, o acesso ao computador feito através de qualquer forma[20].

Em Taiwan, o crime pode ser praticado de três formas: utilização da palavra-passe de terceiro sem motivo justificado, isto é, a utilização da palavra-passe de identificação de terceiros para utilização do computador; quebra de medidas de protecção do computador, eliminando as medidas de protecção, através do uso da força física, tal como a destruição do dispositivo de vigilância do computador, ou através do uso da força não-física, por exemplo, a quebra da restrição do problema de administração da conta do computador. As medidas de protecção incluem os dispositivos de hardware e software. Finalmente, é de referir que o aproveitamento das lacunas do sistema informático consiste na invasão pacífica e não destruidora, através da lacuna do sistema. A condição objectiva do crime é preenchida através da invasão de equipamentos informáticos por meio de uma

20 Inter-departmental Working Group on Computer Related Crime of Hong Kong SAR Government, "Inter-departmental Working Group on Computer Related Crime Report" (versão chinesa), Setembro de 2000, p. 43.

destas formas. "Invasão" significa lesão por penetração[21]. Alguns autores entendem que a invasão corresponde à utilização não autorizada.

Através da observação dos elementos da conduta segundo diferentes teorias penais de diferentes locais, podemos concluir que existem dois tipos de actos que preenchem o tipo de crime: actos de meios e actos de finalidade.

O primeiro tipo abrange a violação de medidas de segurança de computadores, a execução de qualquer função por meio de telecomunicação ou computador, a utilização da palavra-passe, a quebra de instalações e o aproveitamento de lacunas. Na nossa opinião, dado a natureza oculta e técnica da criminalidade informática, os tipos e as formas de criminalidade informática são inevitavelmente infinitas e variáveis, por isso a regulamentação dos actos de meios deve cobrir múltiplas situações. Assim, defendemos que as regulamentações na China e em Macau e a Secção 161 de Hong Kong são mais preferíveis. A norma da China sobre a invasão do sistema de informação de computadores relacionada com os interesses estatais não pressupõe a prática de actos específicos. O art. 4.º do regime de Macau apenas regula os actos de violação das medidas de segurança de computadores e outras acções. A Secção 161 de Hong Kong abrange qualquer forma de actuação. A Secção 27A do Capítulo 106 apenas se aplica aos actos de execução de funções do computador através de telecomunicações e o art. 358.º de Taiwan apenas abrange três tipos de actos criminosos.

Os elementos da conduta na China também incluem o acesso a dados e o controlo ilegal do sistema informático. Na nossa opinião, estes dois tipos de actos devem ser tratados de forma independente. Este problema será discutido posteriormente.

Os actos de finalidade incluem o acesso, a invasão e o uso. Na China e em Taiwan, a lei refere-se à "invasão", ao passo que em Hong Kong, o conceito utilizado é o "uso", e em Macau, o acesso. A nosso ver, a doutrina da China é preferível, embora à primeira vista o acesso ao computador apenas inclua a invasão. Se o agente após a invasão do computador pratica outros actos criminosos, pratica vários crimes. Mas quando a invasão é praticada, os recursos do sistema informáticos passam a estar sob o controlo do agente e este pode emitir qualquer ordem ao sistema. Portanto, os actos de finalidade, para além de terem efeito do acesso, também têm o efeito de utilização de recursos do sistema informático.

No direito penal de Hong Kong, o elemento negativo do crime corresponde à falta de autorização. A sua concepção é idêntica à de Macau.

Quanto à questão de saber se o crime pode ser praticado sob a forma de omissão, entendemos que sim. Quando um terceiro pratica um crime informático com o conluio da pessoa que tem o dever de manutenção e administração do

21 Chen Huansheng, Liu Bingjun, "Prática do Direito Penal", San Min, 2006, p. 556.

computador e o dever de garantia da respectiva segurança[22], a omissão dessa pessoa também deve ser considerado como parte do acto criminoso. Portanto, também constitui crime.

Por outro lado, os actos subsequentes ao acto de invasão, isto é, os actos criminosos praticados após o acto de invasão, devem ser identificados tendo em conta a função do acto de invasão no seio do crime. Se a invasão for apenas um meio e o objectivo do acto for a prática de outros crimes, por exemplo, se a invasão do sistema informático for meio para adquirir segredos do Estado, a situação deve ser tratada como um concurso de crimes. Neste caso o crime é único e deve ser condenado com uma pena mais grave. Se simultaneamente ou sucessivamente a invasão e os outros crimes forem praticados como um objectivo, a situação deve ser tratada como um concurso material de vários crimes. Por exemplo, se após a invasão surge uma nova intenção criminosa de aquisição de dados do computador.

c) Comparação do objecto

Na China, o primeiro tipo de objecto do crime é o sistema informático de informação relacionado com interesses estatais, incluindo assuntos de Estado, instalações de defesa nacional e sistemas de tecnologia avançada. O segundo tipo de objecto corresponde ao sistema de informação de computadores não abrangido pelo primeiro tipo e os respectivos dados. De acordo com o art. 2.º do Estatuto da Protecção da Segurança do Sistema de Informação de Computadores da RPC, "sistema informático de informação" abrange o computador e os respectivos equipamentos, instalações (incluindo a internet), é um sistema que procede à recolha, processamento, armazenamento, transmissão e pesquisa de informações segundo determinados objectivos e regras.

Dados informáticos são informações digitalizadas que o computador trata. Existem informações numéricas e não numéricas, tais como sons e imagens. No entanto, todas as formas de informações são expressadas no computador através de determinados dados.

Em Macau, o objecto do crime corresponde à totalidade ou a parte de um sistema informático[23]. O art. 2.º da Lei n.º 11/2009 define o sistema informático como sendo "qualquer dispositivo isolado ou grupo de dispositivos interligados ou relacionados, em que um ou mais de entre eles desenvolve, em execução de

22 Cai Haining, "Fronteiras do Direito sobre Rede de Informação e Novas Tecnologias, 2009/ Elaboração da Organização do Comité Especial das Redes de Informação e Novas Tecnologias da Associação Nacional dos Advogados da China", Law Press, 2009, p. 80 a 83.

23 De acordo com o art. 12.º da lei referida, que regula a agravação da pena, se o objecto do crime for o sistema informático de órgãos públicos ou entidades públicas, as penas são nos seus limites mínimo e máximo.

um programa, o tratamento automatizado de dados informáticos".

Em relação a Hong Kong, a Secção 27A do Capítulo 106 regula como objecto "qualquer programa ou sistema de dados". O "Computer Crimes Ordinance" não define o conteúdo de "programa" e "dados". No entanto, o art. 59.º, "interpretation", do Capítulo 200 do "Crimes Ordinance" estabelece: "(1) Nesta parte, "propriedade" significa – (...) (b) qualquer programa ou dado, realizado num computador ou armazenado num computador, independentemente de o programa ou o dado ter natureza tangível ou não." No que toca ao objecto do crime regulado na Secção 161, o termo "computador", tendo em conta a legislação vigente em Hong Kong, é definido no art. 22A do "Evidence Ordinance", Capítulo 8, no art. 26A do "Inland Revenue Ordinance", Capítulo 112, e no art. 19.º do "Business Registration Ordinance", Capítulo 310 como: "equipamento para armazenamento, processamento ou pesquisa de informações".

De acordo com o entendimento oficial[24], por enquanto o significado de sistema informático ainda não está definido na lei, por isso a sua interpretação é feita pelo juiz no caso concreto. O Capítulo 553, "Electronic Transactions Ordinance " estabelece o conceito de "sistema de informações": "(a) tratamento de informações; (b) registo de informações; (c) registo ou armazenamento das informações noutro sistema de informação situado em qualquer outro lugar ou tratamento das informações de outra forma no mesmo sistema "; e (d) pesquisa de informações (independentemente de as informações serem registadas ou armazenadas no respectivo sistema ou noutro sistema de informação situado noutro lugar).

Em Taiwan, o objecto do crime é o computador ou respectivo equipamento de terceiro. O Código Penal e o direito penal subsidiário não definem o significado de conceitos tecnológicos como computador, sistema informático ou Internet. "Dado que hoje em dia a tecnologia de informação desenvolve rapidamente, não é fácil a definição de conceitos tecnológicos como "computador", "sistema informático" e "Internet". Para evitar lacunas e a desactualização futura das leis, adoptamos o método de legislação do "Computer Misuse Act" do Reino Unido, não procedendo à definição dos conceitos mencionados"[25]. Alguns autores entendem que o termo "terceiro" mencionado duas vezes no art. 358.º refere-se todos aqueles que não o agente, que pode ser uma única pessoa ou pessoas diferentes. Por exemplo, A utiliza, sem razão justificativa, a palavra-passe de B para invadir

24 Este grupo de trabalho foi criado para realizar os objectivos do Governo da RAEHK – garantir a actualização das leis e medidas de combate à criminalidade informática.

25 Projecto de alteração de algumas disposições do Código Penal de Taiwan (parte da criminalidade de rede informática), versão aprovada em 3 de Junho de 2003, ponto 4 da anotação do artigo 358.º.

o sistema que C forneceu a B. Computador é um dispositivo electrónico capaz de interpretar e executar ordens de programas informáticos, capaz de realizar operações de entrada, saída, cálculo e lógica. É composto por um dispositivo de entrada, processador, dispositivo de saída e dispositivo de armazenamento; os "equipamentos relacionados" são dispositivos não estruturais do computador. São apenas equipamentos de auxílio, tais como um modem.

Por outro lado, de acordo com o art. 361.º, quando o crime for praticado contra computador ou equipamento relacionado de órgãos públicos, a pena será aumentada. Dado que a invasão do sistema informático de órgãos públicos provoca a divulgação de segredos de Estado, pondo em risco a segurança nacional.

Em suma, o objecto deste tipo de crime é principalmente o sistema informático, computador, equipamentos relacionados, dados e programas. Na nossa opinião, a regulamentação do objecto da China e de Macau são mais dignos de adopção, pois, dado que a invasão do sistema informático é feita normalmente pela pura invasão de piratas informáticos ("hackers") por motivos de curiosidade em relação ao funcionamento do sistema. Diferente é a invasão feita por "crackers", que praticam o acto com intenção de destruir o sistema informático invadido[26]. Portanto, o objecto do crime é o sistema informático e não outros objectos.

O sistema informático pode ser definido subjectiva ou objectivamente, tendo em conta, respectivamente, a finalidade ou o objecto. Em Macau, a finalidade do sistema informático é o tratamento de dados informáticos por parte do utente (que pode ser uma pessoa singular ou colectiva), onde esse tratamento não requer a intervenção da força manual e é feita de acordo com instruções capazes de permitir ao sistema informático indicar, executar ou produzir determinada função, tarefa ou resultado; no regime chinês, a finalidade do sistema informático é idêntica à de Macau, isto é, a respectiva execução também terá de cumprir instruções específicas; por outro lado, o termo "utilização", na China e em Macau, revela que basta a utilização numa única vez para que a situação seja abrangida pela lei; por último, quando o sistema informático é utilizado para outros fins que não o tratamento de dados, tais como a reciclagem de resíduos, o regime legal não é aplicável.

A definição de sistema de informações de Hong Kong não é razoável, porque apenas realça a finalidade do sistema, ignorando o respectivo objecto. Pois para além do sistema informático, certas máquinas também podem realizar os fins acima mencionados, tais como o dispositivo de armazenamento de dados (USB). Por outro lado, a falta de definição do objecto também leva a problemas de obstrução da investigação.

Autores de Taiwan definem como computador uma ferramenta que contém

26 Un Man Ivone Kuok "O direito penal informático: o cibercrime na "INTERNET", University of Macau, 1997, p. 27.

dispositivos de hardware e software, cuja operação necessita da força humana, portanto, o computador em si não é capaz de praticar um crime. No entanto, a lei de Taiwan não estabelece a definição de conceitos como computador e sistema informático. Isto leva a que seja o juiz que procede à definição no caso concreto, desempenhando simultaneamente o papel de juiz e legislador. É claro que o juiz deve sempre preencher as lacunas, mas a falta de definição de conceitos pode causar problemas de qualificação do caso e dificuldades de investigação.

Assim, através da comparação, podemos concluir que o sistema informático consiste no tratamento de dados feita segundo programas e objectivos específicos. Se o sistema não for utilizado para tratamento de dados, a definição não é preenchida. Além disso, o sistema informático pode ser constituído por um ou uma série de dispositivos.

d) Comparação do bem jurídico

O bem jurídico é um importante interesse comum da sociedade. O direito penal só intervém quando outros meios legais não foram aptos para proteger o bem jurídico.

Na China, este tipo de crime protege dois tipos de bens jurídicos. O primeiro deles é o sistema informático de informação relacionado com interesses estatais. Envolve a protecção da ordem e segurança da administração do sistema informático de informação, o regime de segredo de Estado e de assuntos nacionais, sistema de defesa nacional e o funcionamento normal do sistema de tecnologia avançada. O segundo tipo relaciona-se com outros sistemas não abrangidos pelo primeiro e corresponde à protecção da segurança do sistema informático de informação[27]. Hoje em dia o computador tornou-se numa ferramenta cada vez mais importante, amplamente utilizada. A criação do computador contribuiu para a troca de informações, o aumento da eficiência do trabalho e, portanto, o computador deve ser tratado como um bem jurídico autónomo protegido pelo direito penal.

Em Macau, o bem jurídico protegido é a segurança do sistema informático e a necessidade de utilização do próprio sistema informático. Por outro lado, autores portugueses referem que este tipo legal de crime é baseado numa nova concepção – "Inviolabilidade do domicílio informático"[28], tendo como fim proteger a privacidade, confidencialidade e integridade do sistema informático[29], por outras palavras, proteger o acesso a informações do computador por parte do

27 "Regras complementares sobre o estabelecimento dos crimes da Lei Penal da RPC pelo Supremo Tribunal Popular e Suprema Procuradoria Popular (D)", ponto 2, (6).

28 Sobre este conceito, *vide* "Relatório do Comité Europeu de Problemas Criminais" e "Recomendação (89) 9, do Comité de Ministros do Conselho da Europa.

29 Benjamim Silva Rodrigues, ob., cit., p. 284.

proprietário legítimo[30].

Em relação a Taiwan, o crime destina-se a proteger a segurança da utilização do computador. Há uma concorrência de bens jurídicos: segurança da informação da comunidade e segurança de segredos e propriedades individuais. Dado que o primeiro envolve direitos e interesses legítimos da maioria, a sua violação provoca maior danos e causa maior perigo e destruição, por isso o primeiro constitui o bem jurídico principal e o segundo o bem jurídico secundário.

A determinação do bem jurídico influencia a política criminal e, consequentemente, o poder legislativo e judicial. Na nossa opinião, a teoria criminal de Macau e de Taiwan são preferíveis, porque em relação à prevenção geral, é capaz de proteger a segurança das informações do sistema informático e, em relação à prevenção especial, protege a segurança de segredos e da propriedade individuais. O problema na China reside na regulamentação do sistema informático de informação do segundo tipo, onde apenas engloba a aquisição de dados e os actos de controlo ilegais. O bem jurídico protegido é apenas a segurança do sistema, pondo de lado os direitos da vítima sobre os dados e os direitos e interesses sobre a utilização e o controlo do computador. Dado que o computador tem uma variedade de capacidade de operação, substituindo a tradicional trabalho baseado na força humana, a sua utilização tornou-se popular[31]. Portanto, é necessária uma protecção das espectativas razoáveis da comunidade e de cada indivíduo em relação ao estado de segurança do sistema informático[32]. Assim, os direitos da vítima poderão constituir um bem jurídico autónomo?

Na China, a questão de saber se os dados informáticos poderão constituir um bem jurídico autónomo e um objecto autónomo depende do estabelecimento de um novo crime. A nosso ver, se os dados podem tornar-se independentes do sistema informático de informação, a sua violação deve ser tratada como um crime autónomo.

De acordo com as "Regras complementares sobre o estabelecimento dos crimes da Lei Penal da RPC pelo Supremo Tribunal Popular e Suprema Procuradoria Popular (D)", aprovada para resolver o problema da aplicação do estabelecimento dos crimes da "Proposta de alteração da Lei Penal (G)", o crime de acesso ilegal ao sistema informático de informação e o crime de controlo ilegal do sistema informático de informação são crimes alternativos. São três as principais razões. Primeiro porque o crime estabelecido pelo n.º 1 do art. 9.º da "Proposta

30 José Francisco de Faria Costa, "Algumas Reflexões sobre o estatuto dogmático do chamado "Direito Penal Informático", Revista Jurídica da Universidade Moderna, Ano 1.º, n.º 1, 1998: (1-511): "47-63":52.

31 Cai Dunming, "Teoria do Direito Penal", San Min Book, 2008.

32 Zeng Shuyu, "Conhecimento por gráficos: Direito Penal", Sharing Culture, 2007.

de alteração da Lei Penal (G)" (ou seja, o art. 285.º da Lei Penal) é um crime de constituição complexa, incluindo dois meios alternativos: obtenção de dados armazenados, processados ou transmitidos no sistema informático de informação e exercício do controlo ilegal sobre o sistema informático de informação. Durante o processo de cometimento do crime, o agente pode utilizar autonomamente cada um destes meios ou pode utiliza-los subsequentemente. Nestes casos, o agente pratica o acto com dolo e o objecto do crime é a segurança do sistema informático de informação. Sendo bastante prejudicial para a sociedade, e dado que preenche as condições gerais de aplicação do crime alternativo, não deve ser visto como um crime autónomo. Em segundo lugar, se os crimes previstos neste artigo forem estabelecidos como dois crimes autónomos, quando o agente simultaneamente obtém os dados informáticos e controla ilegalmente o sistema, deve ser punido por dois crimes. Isto contraria a natureza de *última ratio* do direito penal e causa uma inconformidade manifesta com pena estabelecida no n.º 1 do art. 285.º (pena máxima de três anos de prisão). Em terceiro lugar, a consideração dos crimes como crimes autónomos pode levar a que, no caso concreto, o crime seja aplicado separada ou conjuntamente.

Porém, afirmamos que a questão pode ser discutida. Em relação ao primeiro ponto acima referido, temos as seguintes conclusões: primeiro, os direitos do utente sobre os dados informáticos e o direito ao controlo material do sistema informático podem constituir um bem jurídico autónomo relativamente à segurança do sistema informático de informação. Em Macau e Hong Kong existe uma regulamentação destinada a proteger especificamente o sistema informático pessoal, diferente da protecção de dados informáticos e do sistema informático nacional. A *ratio legis* subjacente é o gozo pessoal do direito à privacidade, autodeterminação e exclusividade sobre os dados informativos e o sistema informático. Esta posição foi adoptada pela Convenção sobre o Cibercrime. Por outro lado, os dados em si têm natureza de propriedade e são disponíveis. Autores chineses consideram que dados informáticos são um tipo de propriedade fictícia (tal como moeda fictícia) e também têm um valor de uso, valor de troca e liquidez, portanto, podem ser considerados como "outros bens"[33], nos termos do art. 92.º da Lei Penal. No entanto, o legislador ainda não procedeu à interpretação desta questão. Concordamos com esta posição, porque se considerarmos que a propriedade fictícia tem natureza de propriedade, podemos aplicar o crime de violação da propriedade através do uso de computadores, tal como o crime de roubo através de computadores estabelecido no art. 287.º, de modo a garantir a indemnização da vítima. Em Macau, o art. 7.º da Lei n.º 11/2009 reflecte a consideração dos dados

33 Liu Shangzhi, "Colectânea das teses da Conferência Nacional da Ciência e Tecnologia e Direito 2002", National Chiao Tung University, 2002, p. 80 a 83.

informáticos como propriedade, pois, apenas o valor da propriedade pode ser tida em conta para avaliar o montante do prejuízo patrimonial (saber se é um valor elevado ou consideravelmente elevado). Além disso, a pena será mais elevada quando os danos causados à vítima forem mais graves; é claro que a vítima pode intentar uma acção civil de indemnização por perdas e danos. Em Hong Kong, a Secção 59 do Capítulo 200, e em Taiwan, os artigos 359.º[34] e 360.º também consideram os dados informáticos como propriedade. Defendemos esta posição, porque os dados e as informações têm um significado específico e particular para o utente do computador. São direitos e interesses deste. Portanto, no momento da lesão surge o direito à reclamação dos danos. Assim, os dados e informações têm valor pessoal e económico, portanto, os interesses sobre os dados devem ser protegidos pelo direito penal. Por outro lado, se o sistema informático for objecto de controlo ilegal, é sinal de que o proprietário perde o direito à utilização e controlo do seu sistema. A não protecção da perda parcial do direito à utilização causada por actos de invasão não é uma solução adequada. A natureza superior e a automaticidade do sistema informático levam a que o trabalho do ser humano seja cada vez mais atribuído ao computador. Basta uma simples invasão do computador para causar ao utente uma ameaça séria, quanto mais a privação do direito de utilização causado pelo controlo ilegal de piratas informáticos. Como devemos lidar com a invasão de sistemas informáticos de áreas importantes, como o sistema financeiro ou de transporte?

Segundo, os dados e o sistema informático podem ser objectos de crime autónomos. Tal como mencionado anteriormente, como os dois envolvem importantes interesses jurídicos, o objecto do crime pode não ser apenas os dados armazenados ou o sistema informático controlado ilegalmente.

Terceiro, o art. 285.º não protege apenas a segurança do sistema informático de informação. Nestas situações o agente tem como finalidade a obtenção de dados ou o controlo ilegal do sistema. Se além da invasão existir outros fins criminosos, o crime não é o da invasão, mas outro[35]. Assim, a invasão é apenas um meio,

34 Este artigo estabelece o crime de destruição de registos electromagnéticos. Segundo este artigo, quem obtém, eliminar ou alterar sem motivo justificativo o registo electromagnético do computador de terceiro ou de equipamentos relacionados, causando danos ao público ou a terceiro, é punido com pena de prisão até 5 anos, detenção e/ou multa até 200 mil patacas. Outro artigo estabelece o crime de interferência no computador ou equipamentos relacionados, segundo o qual quem interferir no computador de terceiro ou nos equipamentos relacionados através de programa informático ou outros meios eletromagnéticos, sem motivo justificativo, causando danos ao público ou a terceiro, é punido com pena de prisão até 3 anos, detenção e/ou pena de multa até 100 mil patacas.

35 Zhao Tingguang, Zhu Huachi, Pi Yong, "Condenação e determinação da pena dos crimes informáticos", Tribunal Popular, 2000, p. 181.

sendo a obtenção de dados e o controlo ilegal o objecto do acto. Portanto, na nossa opinião, os dados informáticos e o sistema em si podem autonomamente constituir objecto do crime. Os direitos e as legítimas espectativas do proprietário podem constituir um bem jurídico autónomo.

Da interpretação dos dois pontos acima mencionados, podemos afirmar que o crime de acesso a informações e de controlo ilegal do sistema protegem dois bens jurídicos independentes, por isso a punição destes dois tipos de forma de acto é apropriada, tendo em conta a teoria do direito penal e a teoria do concurso de crimes. Quando as informações do sistema informático que envolve interesses estatais referido no art. 285.º sejam obtidas e o sistema em si também seja controlado ilegalmente, é difícil imaginar que a situação não seja tratada como um concurso de crimes.

Por fim, através da interpretação dos três pontos acima mencionados, podemos concluir que os órgãos legislativo e judicial delimitaram claramente o objecto dos diferentes crimes, isto é, o bem jurídico e o objecto protegidos, possibilitando uma maior eficácia e qualidade na identificação do caso e na determinação do caminho a seguir na investigação, segundo os factos e o direito.

3. Comparação das condições subjectivas da constituição do crime

As condições subjectivas incluem o sujeito, o dolo, a negligência e a intenção.

a) Comparação do sujeito

O sujeito é aquele que, de acordo com a lei, é criminalmente responsável, cuja idade deve exceder determinado limite, e deve ter um estado mental normal. Dado que a idade da imputabilidade criminal de difere consoante os lugares e a criminalidade informática tem natureza inter-regional, o agente pode ter imputabilidade criminal no lugar A e não o ter no lugar B. A imputabilidade em razão da idade é decisiva para saber se o agente tem capacidade para responder criminalmente. O direito penal de diversos países exige a imputabilidade para que o agente tenha responsabilidade criminal. Devido ao limite de tempo, não nos vamos debruçar sobre este assunto.

Na China, o sujeito do crime é um sujeito geral, isto é, uma pessoa singular, membro da sociedade. Nos termos do art. 17.º da Lei Penal, dado que o crime de invasão ilegal do sistema informático de informação não pertence aos crimes de ofensa graves previstos no n.º 2 do mesmo artigo, a idade para que uma pessoa possa ser criminalmente responsável é de 16 anos. De acordo com o art. 30.º, as pessoas colectivas só serão responsabilizados criminalmente quando a lei assim o determina. No entanto, a lei não estabelece que as pessoas colectivas podem ser sujeitos deste tipo de crime.

Em Macau, o sujeito do crime poderá ser uma pessoa singular ou pessoa colectiva. Nos termos do art. 18.º do Código Penal, os menores de 16 anos são inimputáveis. De acordo com o art. 13.º da Lei n.º 11/2009, as pessoas colectivas, ainda que irregularmente constituídas, e as associações sem personalidade jurídica são responsáveis pelos crimes previstos nesta lei. A responsabilidade das pessoas colectivas não exclui a responsabilidade individual dos respectivos agentes.

Em Hong Kong, o "Juvenile Offenders (Amendment) Ordinance 2003" estabelece que a idade da imputabilidade criminal é de 10 anos. Quanto à questão da responsabilidade criminal das pessoas colectivas, não existe nenhuma disposição legal a este respeito.

Em relação a Taiwan, não há nenhuma limitação especial em relação ao sujeito do crime em questão[36]. O art. 18.º da lei penal estabelece que a idade mínima para a responsabilidade criminal é de 14 anos. Quanto às pessoas colectivas, a situação é idêntica à de Hong Kong.

Através da comparação, podemos concluir que a idade mínima de responsabilidade criminal entre os quatro locais é de 10 anos a 16 anos. Por outro lado, apenas o direito penal de Macau estabelece a possibilidade de pessoas colectivas serem sujeitos do crime. Defendemos que a pessoa colectiva pode ser sujeito do crime, porque objectivamente, ela é composta por recursos humanos e financeiros, é lhe atribuída personalidade jurídica, tendo portanto recursos e condições suficientes para praticar o crime em questão. Dado que o número de membros da pessoa colectiva é plural, o crime por ela praticado causa riscos mais graves do que o crime praticado por uma pessoa singular; por outro lado, a finalidade da pessoa colectiva é a realização do interesse colectivo ou comum. A sua vontade depende da maioria dos seus membros, portanto, os membros com intenções ilegítimas podem causar a formação da intenção criminosa da pessoa colectiva, bastando satisfazer a condição da maioria. Mesmo que o crime seja praticado por um membro em falsa representação da pessoa colectiva, a responsabilidade criminal desta última não deixa de existir, porque os órgãos da pessoa colectiva têm o dever de fiscalização. Neste caso, a responsabilidade criminal deve-se à falta de fiscalização[37].

b) Comparação sobre o dolo e a negligência

36 Chen Qianwan, "Análise do Direito Penal", WenSheng Book Store, 2009, p. 409.

37 Esta solução manifesta-se no nº 1 do art.13º da Lei nº 11/2009: "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".

Na China, alguns autores defendem que este tipo de crime apenas pode ser praticado com dolo directo. O dolo directo significa que o agente tem a intenção de invadir o computador, sabendo que se trata de um sistema informático nacional ou de terceiro e sabendo que não tem direito de acesso ao sistema. Além disso, a negligência não pode constituir o crime dado que nos termos do art. 15.º da Lei Penal, a responsabilidade criminal nos crimes negligentes depende da previsão específica da sua punibilidade e depende do resultado danoso.

O Parecer da Assembleia Legislativa da RAEM refere que o acesso ilegal pressupõe uma intenção ilegítima, por isso, o crime apenas pode ser praticado com dolo directo.

Em relação a Hong Kong, a lei estabelece que só constitui crime quando o agente tem intenção criminosa. A Secção 27A do Capítulo 106 e a Secção 161 exigem que o crime seja praticado com dolo. O dolo significa a existência de intenção (determinação) de praticar o acto ou a consciência, no momento da prática, de que o acto provoca necessariamente o resultado. O "Computer Crimes Ordinance" exige o conhecimento da forma da prática do acto (fazer com que um computador desempenhe qualquer função) e a intenção de atingir o resultado (o uso da informação). Além disso, de acordo com o art. 60.º do "Crimes Ordinance", quem, sem razão justificativa ou desconsiderando o resultado, utiliza abusivamente o computador, incluindo a modificação, eliminação ou adicionamento de dados informáticos, pratica um crime. Assim, a desconsideração da prática do acto também pode constituir um crime. A "desconsideração", ou "imprudência", refere-se à situação em que o agente, não tendo intenção de praticar o crime, prevê a possibilidade de produção do resultado danoso e mesmo assim pratica o acto.

Autores de Taiwan afirmam que o crime de invasão de computadores apenas pode ser praticado com dolo, isto é, subjectivamente o agente conhece que não tem poderes para utilizar equipamentos de terceiro e, sem consentimento do titular do direito, decide praticar a invasão. O agente pode ter dolo directo ou indirecto[38].

Através da análise comparativa das disposições, existem semelhanças entre o conceito de desconsideração de Hong Kong e o conceito de dolo eventual do direito chinês[39], onde o agente sabendo que o resultado da acção pode constituir um crime, actua aceitando a produção do resultado. No entanto, na nossa opinião, os crimes informáticos não incluem o dolo eventual, porque a natureza deste tipo de crime requer certos conhecimentos para a quebra dos meios de segurança do sistema, tal como a descodificação, especialmente no que toca ao sistema informático nacional altamente protegido, onde necessita maior conhecimento

38 Gan Tiangui, "Teoria do Direito Penal = Criminal law: specific provisions", San Min Book, 2009, p. 418 a 423.

39 De acordo com a definição de dolo estabelecida no n.º 3 do art. 13.º do Código Penal de Macau.

tecnológico e profissional. Portanto, o agente deve ter total conhecimento dos meios de acção e do respectivo resultado.

O direito penal dos diferentes locais não prevê o crime na forma negligente. Nós concordamos com esta solução. O crime de invasão é cometido por acção. É consumado quando se reúnem os elementos objectivos do crime, independentemente da existência de resultados perigosos. Pelo contrário, os crimes negligentes dependem da ocorrência do resultado.

c) Comparação da intenção

A intenção refere-se ao resultado que o agente pretende alcançar com o acto criminoso. Difere do dolo, isto é, do conhecimento do resultado danoso.

Neste aspecto, o direito chinês requer que o agente tenha intenção de invasão, isto é, que tenha uma "mentalidade de pirata informático", uma "mentalidade anormal", como curiosidade em relação ao sistema informático, curiosidade intelectual ou desejo de causar um mal.

Em Macau, a lei exige uma intenção ilegítima. A nota justificativa não define o conceito de intenção ilegítima. Autores portugueses referem que esta intenção consiste na aquisição de interesses ou benefícios ilegítimos para si ou para terceiro[40].

Em Hong Kong, a Secção 27A do Capítulo 106 não exige o elemento da intenção, não havendo necessidade de provar a intenção criminosa ou desonesta. Quanto à Secção 161, a lei exige a intenção ilegal de praticar outros crimes, adquirindo benefícios para si ou para terceiro, ou a intenção desonesta de causar danos a terceiro[41].

A lei penal de Taiwan não regula a intenção.

Podemos observar que a lei da China, de Macau e a Secção 161 de Hong Kong, "Access to computer with criminal or dishonest intent" regularam a intenção, ao passo que a lei de Taiwan e a Secção 27A do Capítulo 106 de Hong Kong, "Unauthorized access to computer by telecommunications", não regularam. Na nossa opinião, os elementos da intenção devem estar completamente definidos na lei, pois, a prática de um acto por curiosidade, por exibição ou por aquisição ilegal de dinheiro ou de benefícios são todas situações diferentes[42]. Estas situações influenciam a determinação da medida da pena e os dados necessários para a investigação. Imaginem uma invasão por motivos de aquisição benefícios ilegais e uma invasão por simples curiosidade, qual delas é mais censurável e

40 A "A Lei da Criminalidade Informática" - Lei, n.º 109/91, lei de Portugal destinada ao combate à criminalidade informática, também reflecte a posição acima mencionada.

41 *Vide* rodapé 29, p. 42.

42 Liu Shangchi, "Colectânea das teses da Conferência Nacional da Ciência e Tecnologia e Direito 2002", National Chiao Tung University, 2002, p. 511 e 512.

mais perigosa? Por isso não basta regular um ou alguns dos tipos de intenção. A regulamentação deve ter em conta todas as situações.

3. Conclusão

A tecnologia de informação está a desenvolver-se a um ritmo cada vez maior. Surgem novas formas de praticar o crime e o objecto é cada vez mais vasto (por exemplo, telemóveis que podem aceder à Internet). Isto requer que os elementos constitutivos do crime de invasão do sistema informático, e mesmo de outros crimes informáticos, sejam abrangentes e actuais. Segundo as estatísticas, até agora, 95% da criminalidade informática não é denunciada ou descoberta pela vítima[43]. A falta de denúncia por parte da vítima dificulta a prevenção e o combate deste tipo de crime. Mas de qualquer forma, a investigação criminal deve respeitar os direitos fundamentais do suspeito e as regras do direito processual, não podendo utilizar meios ilegais. Só assim é que a investigação criminal consegue cumprir o princípio da legalidade e o princípio da subsidiariedade, isto é, a ofensa do bem jurídico protegido pela lei apenas constitui crime e será punida quando preenche os pressupostos que a lei penal estabelece.

43 Cf. Jorge Rangel, traduzido por Li Changsan: "As novas tecnologias, a sociedade da informação e o direito", Instituto Internacional de Macau, 2000, p. 62.