Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual

Luciana Boiteux

Mestre em direito pela Universidade do Estado do Rio de Janeiro. Doutoranda em direito penal e criminologia pela Universidade de São Paulo. Diretora do Grupo Brasileiro da Associação Internacional de Direito Penal. Advogada criminal no Rio de Janeiro.

Sumário: 1. Introdução – 2. Evolução legislativa dos crimes informáticos – 3. Por uma política criminal para delitos informáticos: 3.1 Aspectos criminológicos da delinqüência informática; 3.2 Da necessidade de uma política criminal para crimes informáticos; 3.3 Medidas de prevenção no campo da informática – 4. Aspectos internacionais dos crimes informáticos e a Convenção Européia sobre Crimes Cibernéticos: 4.1 Características internacionais dos crimes informáticos; 4.2 A Convenção Européia sobre Crimes Cibernéticos; 4.3 Conceitos e objetivos preconizados pela Convenção Européia sobre Crimes Cibernéticos; 4.4 Dos crimes informáticos previstos; 4.5 Medidas processuais-penais recomendadas; 4.6 Cooperação Penal Internacional – 5. Conclusão – Bibliografia.

Resumo: O presente artigo discute medidas de prevenção e a real necessidade de criminalização de condutas, na busca de refletir sobre uma política criminal para delitos informáticos, traçando um panorama da Convenção Européia sobre Crimes Cibernéticos.

Palavras-chave: crimes de informática; política criminal; direito penal internacional.

1. Introdução

As transformações no campo da informática e das telecomunicações nas últimas décadas foram impressionantemente rápidas. Enquanto no início do século XX as notícias sobre a guerra na Europa somente chegaram no interior do Brasil mais de um mês depois, em setembro de 2001 o mundo todo pode acompanhar o ataque às torres do World Trade Center ao vivo e a cores, quase que simultaneamente.

De fato, especialmente nos últimos cinqüenta anos, a evolução da sociedade foi muito acelerada e a globalização reestruturou profundamente as nossas formas de viver, sob a forma individual e coletiva, a vários níveis: economia, relações pessoais, cultura, tradição, política, e ciência e tecnologia.[1] A informática aproximou as pessoas e as nações, sendo que hoje a maioria da população já faz parte da aldeia global, embora muito ainda há de se fazer para democratizar esses avanços tecnológicos e assim conseguir reduzir o abismo entre ricos e pobres, que paradoxalmente aumentou ainda mais com a globalização.[2]

O conceito de ciberespaço (*cyberspace*), ou espaço virtual alcançado pela rede mundial de computadores, a Internet, que reduziu as distâncias e aproximou as pessoas, foi concebido como uma nova dimensão espacial que transcende fronteiras, e permite a todos aqueles conectados à rede imediato contato com qualquer lugar do mundo em segundos, independentemente de fronteiras ou meios de transporte.

Assim, as relações sociais e a economia mundial se adaptaram eficazmente a essa nova era, que possibilitou um intenso crescimento econômico nos países desenvolvidos, tendo sido facilitadas as relações comerciais entre os países. Novos tipos de empresas foram criados, tal como provedores de Internet, empresas

1. Sobre o tema do impacto da globalização, v.: GIDDENS, Anthony. *O mundo na era da globalização*. Lisboa: Presença, 2000.

2. Para aprofundamento do tema dos impactos da globalização sobre as pessoas, veja a análise de: BAUMAN, Zigmund. *Globalização*: as conseqüências humanas. Rio de Janeiro: Jorge Zahar, 1999.

de telecomunicações, empresas fabricantes de *hardware* e *software*, além das chamadas "pontocom", que existem apenas virtualmente na Internet geradas na época de grande expansão de negócios *on line*, que com um pequeno investimento inicial se transformaram e se valorizaram da noite para o dia, muito embora esta bolha tenha estourado recentemente. Essa nova realidade virtual não poderia ter acontecido antes da criação do computador e de sua evolução tecnológica, especialmente de transmissão, processamento e armazenamento de dados e imagens em velocidades cada vez maiores.

Nos dias de hoje convivemos normalmente com o comércio virtual, pagamentos e autenticações bancárias pela Internet, banco eletrônico, transações bancárias internacionais *on line*, certidões oficiais pela rede, salas de bate-papo virtual, sexo virtual, jornais *on line*, além de jogos eletrônicos e cassinos virtuais, tendo havido uma radical mudança de comportamento, pois a vida cotidiana se transformou com o auxílio da informática. A própria linguagem dessa nova era da realidade virtual global também mudou, tendo a língua inglesa sido ainda mais simplificada, e criados termos específicos para facilitar a comunicação global.[3] O uso da comunicação eletrônica, ou *e-mail*, é comum, assim como o acesso à Internet é fácil e rápido; há milhões de *websites* (sítios na rede), além das ferramentas de buscas que em menos de um minuto vasculham a rede e localizam arquivos específicos; o uso de computadores em empresas, bancos, escritórios e pelo governo mostra-se atualmente imprescindível. Ninguém mais se imagina podendo sobreviver sem um computador, tão grande que se tornou a dependência de nossa sociedade das tecnologias.

A base destas transformações radicais do modo de vida das pessoas, com a redução das distâncias, a otimização do tempo e o espetacular aumento da capacidade de comunicação, está na incrível evolução da tecnologia da

3. Como se pode observar no presente texto, no qual foi necessária a utilização de diversas palavras em inglês.

informática, com computadores cada vez mais potentes, e também pela criação da Internet, que simplificou e agilizou a troca de informações entre os computadores.

Diante disso, não se mostra surpreendente e nem um pouco inesperado que, a partir das transformações da sociedade e das relações pessoais, profissionais e financeiras, os comportamentos socialmente danosos também se adaptassem a essa nova era. O crime é um fato social, portanto perfeitamente natural que também se transformasse com as alterações da sociedade em que se insere.

Assim, diante da facilidade das comunicações e do incremento das tecnologias, nota-se hoje em dia que as conseqüências de determinado ato delituoso praticado com o uso de computadores na esfera local, ou via Internet, podem ser bem mais amplas e perigosas do que antes, já que não há restrição de fronteiras ou limitações geográficas no chamado ciberespaço. Exemplos comuns são a distribuição de vírus que afetam vários países ao mesmo tempo, sem que se consiga controlar ou mesmo detectar sua origem, e desfalques eletrônicos por meio do uso fraudulento dos sistemas de computadores de bancos, envolvendo quantias elevadas. Sobre este tema, Ricardo M. Mata y Martín aduz que "la aparición de los instrumentos informáticos con una serie de características específicas hacen de ellos un factor criminógeno de primer orden".[4]

Portanto, diante disso, deve ser analisado a melhor forma de se lidar com esses novos tipos de delinqüência, levando em consideração que quando qualquer fato social novo se aproxima do entorno do direito, novos desafios e necessidades são criados, havendo sempre um momento transitório de perplexidade, tal como esse que nos encontramos agora. Isso porque o direito é conservador e nunca acompanhou nem tem condições de seguir de perto as grandes transformações sociais, que sempre estão na frente do legislador. A aproximação entre a realidade e o direito sempre foi um desafio, em todos os ramos, civil, constitucio-

4. *Delincuencia informática y derecho penal.* Madrid: Edisofer SL, 2001. p. 11-12.

nal, mas especialmente no direito penal, que, por ser concebido como forma de controle social, sofre ainda mais pressões e cobranças.

Especificamente nessa área, nota-se a pressão exercida pela sociedade, representada pelos meios de comunicação, para ampliar ainda mais o controle social, que vem acompanhada de mensagem política pregando o aumento urgente de crimes e penas, sob a justificativa de que a situação está fora de controle por culpa "da ausência de legislação específica sobre o tema", o que supostamente "impediria as autoridades de resolver o problema". Se o fato que causa comoção social já está previsto em lei como crime, a solução proposta passa a ser a de "aumentar as penas, que são muito leves". Trata-se de verdadeira falácia, que, muito embora sem base lógica ou eficaz, é incentivada pela mídia e pelos políticos de plantão.

Nosso objetivo com o presente estudo, portanto, é buscar uma maior reflexão sobre os delitos informáticos, de forma a estudá-los como sendo uma conseqüência previsível da evolução da tecnologia de computação, na busca de encontrar uma solução para reduzir seus impactos danosos sobre a sociedade.

O enfoque a ser dado será crítico quanto à necessidade de criação de novos tipos penais, por considerarmos acima de tudo que o direito penal deve ser aplicado somente como *ultima ratio*, razão pela qual teremos bastante cautela para evitarmos o lugar comum das propostas de criminalização descontrolada de condutas influenciadas pelo discurso do direito penal simbólico.

Portanto, a base de nossa argumentação estará na análise concreta do fenômeno da criminalidade com o uso de computadores, levando em conta a necessidade de se equilibrar a idéia de repressão penal às condutas mais graves com a garantia e o respeito aos direitos humanos, à liberdade de expressão e de circulação, especialmente no que se refere ao mais democrático e livre espaço de comunicação mundial – Internet.

São, portanto, objetivos do presente trabalho: a) o debate sobre questões de política criminal, por meio da reflexão sobre estratégias de prevenção deste tipo de conduta que expõe a vulnerabilidade de sistemas informáticos; b) a análi-

se da legislação internacional sobre crimes de computador, diante da característica transnacional do fenômeno, de forma a contribuir para a discussão e o aprimoramento da legislação brasileira sobre crimes de informática.

Por outro lado, não constituem objeto do presente estudo os tipos penais específicos, ou o estudo dogmático ou jurisprudencial dos chamados delitos informáticos, mas nosso foco estará essencialmente em discutir em termos gerais uma política criminal deste tipo de delito, mais especificamente sugerindo medidas de prevenção, para depois traçar um panorama da legislação internacional existente sobre o tema, de modo a sustentar nossa tese de que os delitos informáticos devem ser tratados pelo legislador como inseridos em um contexto que transcende as fronteiras nacionais.

Para tanto, traçaremos inicialmente um breve histórico dos crimes informáticos, depois abordaremos questões de política criminal e medidas de prevenção, para finalmente discorrermos sobre questões ligadas à de criminalização de condutas na esfera internacional.

Os aspectos processuais-penais também serão analisados, por consideramos que o mais importante no combate aos efeitos deletérios da utilização de computadores para a prática de crimes, além da prevenção, deve estar na efetiva possibilidade de elucidação dos delitos, por meio da utilização de métodos e instrumentos processuais especializados que permitam a investigação destas ações criminosas, assim como maior capacitação da perícia especializada

Para ilustrar tal questão, traçaremos um panorama da Convenção Européia sobre Crimes Cibernéticos[5] (ECC – *European Convention on Cybercrime*), assinada em Budapeste, Hungria, em 23.11.2001, que é o mais atualizado e completo instrumento internacional já elaborado sobre o tema, para depois trazermos nossa conclusão.

5. Ressalte-se que a terminologia utilizada pela Convenção, *cybercrime*, traduzível por "crimes cibernéticos", constitui o termo mais adequado e atual para representar este fenômeno, mas no presente trabalho optamos por usar a expressão "crimes informáticos", muito embora mais antiga, de significado mais restrito, por ser esta a mais utilizada no Brasil.

Após essas considerações iniciais, traremos um breve histórico dos delitos de informática, a fim de situar a evolução da legislação penal sobre o tema.

2. Evolução legislativa dos crimes informáticos

Segundo a literatura especializada,[6] foi em 1960 que surgiram os primeiros casos de abusos no uso de computador, com a manipulação de dados, sabotagem, espionagem e abuso ilegal de sistemas de computadores. Naquela época chegava-se mesmo a ter dúvidas se se tratavam de realidade ou ficção, visto que ainda era muito incipiente sua ocorrência.

Por meio dos primeiros estudos empíricos sobre o tema, com a utilização de métodos criminológicos que foram conduzidos na metade dos anos 70, verificou-se um número limitado de casos de crimes praticados com a utilização de computadores. A conclusão a que se chegou naquela oportunidade foi a de que a maioria dos crimes permanecia não detectada ou então não era divulgada. Naquela ocasião, foram investigados os primeiros casos espetaculares, noticiados pela imprensa com destaque.

A partir de 1980, houve uma mudança radical na visão pública e científica sobre o tema. Foram detectados, além das ocorrências já noticiadas, novos casos de pirataria de programas, manipulação de valores nos caixas eletrônicos, além de abusos nas telecomunicações – o que revelou para o público em geral a vulnerabilidade da "sociedade da informação", e levou à discussão sobre a necessidade de se privilegiar a segurança e de se tentar controlar esses tipos de condutas consideradas lesivas ao meio social. Observar-se a partir daí o início da tipificação legal de algumas condutas ligadas à informática.

6. Sobre a evolução histórica dos delitos informáticos, remetemos o leitor ao vol. 64 da *Revue Internationale de Droit Penal*, n. 1/2, 1993, que publicou os relatórios nacionais elaborados para o colóquio preparatório realizado em Wurzbürg, Alemanha, em 05.08.1992, pela Associação Internacional de Direito Penal.

A criminalização do novo fenômeno do abuso no uso dos computadores chegou às legislações penais em meados da década de 80, nos Estados Unidos, com a edição do *Crime Control Act*, de 1984, seguido pelo *Computer Fraud and Abuse Act*, de 1986, que previam cinco categorias de ilícitos informáticos. A Alemanha foi o segundo país a editar leis penais nesta esfera, ao introduzir a legislação de 15.05.1986, que ficou conhecida como *Computer Kriminalität*, no que foi seguida pela França por meio da Lei Godfrain, de 05.01.1988, depois incorporada ao Código Penal francês, e pela Itália (Lei 547, de 23.12.1993), que adaptou seu Código Penal à nova criminalidade informática.[7] Já a Espanha incluiu delitos informáticos na reforma do Código Penal de 1995.[8]

Na década passada, ou seja, a partir de 1990, os casos mais comuns constatados incluíam ilícita transferência de fundos, atuação de *hackers* na violação de sistemas e distribuição de vírus, o que levou as sociedades industrializadas a se organizarem, visando a tomar providências no âmbito internacional, tendo em vista os efeitos da globalização e a massificação do uso dos sistemas de computadores e da Internet como rede de comunicação.

Neste momento surgiram as primeiras comissões européias para o estudo da delinqüência informática, devendo ser destacada a atuação da Associação Internacional de Direito Penal (AIDP), que foi precursora na reunião de especialistas para estudar o tema. Nesse sentido, podemos citar o colóquio preparatório realizado na Alemanha em 1992, cujos anais foram publicados em 1993.[9]

7. MARTÍN, Ricardo M. Mata y. Op. cit., p. 12.

8. Para ter acesso a outras legislações estrangeiras sobre crimes informáticos, v.: <http://www.mosstingrett.no/info/legal.html>.

9. Posteriormente, essas recomendações serviram de base para a discussão na Mesa Redonda organizada no XVI Congresso Internacional de Direito Penal que ocorreu no Rio de Janeiro em 1994. Mais recentemente, os mesmos especialistas que fizeram parte da comissão que elaborou a Convenção Européia sobre *Cybercrime* se reuniram novamente no Colóquio Preparatório da AIDP realizado em Atenas, Grécia, em abril de 2003, cujas conclusões serão levadas ao XVIII Congresso Internacional da AIDP, a ser realizado em Beijing, China, em setembro de 2004.

No Brasil, o tema dos crimes informáticos foi inicialmente tratado pela doutrina como uma questão de direito penal econômico, pois inicialmente era considerada prioritária a proteção de programas de computadores, certamente por pressões das empresas multinacionais, tendo sido editada uma legislação que os colocou sob a égide das leis de direitos autorais (Lei 7.646, de 18.12.1987).[10]

Posteriormente, alargou-se o rol dos delitos praticados por meio do computador, com a edição da Lei 8.137/1990, que define os crimes contra a ordem tributária, tendo sido criminalizada a conduta de *utilizar ou divulgar programas de processamento de dados* para fins de sonegação fiscal, no art. 2.º, V. Algum tempo depois, em 1995, com a Lei 9.100, foram previstos tipos penais tais como o acesso indevido a sistema de *tratamento automático de dados utilizados pelo serviço eleitoral, com fim de alterar a apuração ou a contagem dos votos* (art. 67, VII), e a *alteração de programa de computador para provocar resultado diverso do esperado em sistema de votação eletrônica* (inc. VIII do mesmo artigo).

Mais recentemente, com a edição da Lei 9.983, de 14.07.2000, que alterou e incluiu alguns artigos no Código Penal Brasileiro, foram criados novos dispositivos destinados à proteção específica de dados e de sistema de informações, tais como crimes próprios de funcionários públicos que modifiquem ou alterem sistemas informáticos da Administração Pública (art. 313-B do CP), e punindo também a divulgação de informações sigilosas de bancos de dados oficiais (art. 153, § 1.º-A, do CP), além do art. 325, § 1.º, I, do mesmo diploma legal.

Finalmente, no momento atual, em que o espaço cibernético, ou virtual, é cotidianamente explorado por pessoas de todas as nacionalidades, observa-se não só o aumento da percepção de delitos já detectados anteriormente, como também maior incidência de condutas delituosas praticadas com o uso de computadores. Nesse sentido, podemos apontar a pornografia infantil, que foi facilitada

10. Especificamente sobre a proteção da propriedade intelectual de programas de computador, foram editadas em nosso País posteriormente as Leis 9.609/1998 e 9.610/1998.

pela revolução da tecnologia de imagens e pelo aumento de velocidade na transmissão de informações, o jogo ilegal por meio de Internet, que criou verdadeiros cassinos virtuais, além do chamado ciberterrorismo, sem ainda evidências concretas de sua ocorrência.

Sobre este ponto, especialmente depois dos atentados de 11.09.2001 nos Estados Unidos, com a edição do *Patriotic Act*, que praticamente terminou com a privacidade nas telecomunicações com o objetivo declarado de combater o terrorismo, e que acabou por impor maciço controle social sobre a população em geral, podemos afirmar que a concepção do chamado espaço cibernético como um dos maiores instrumentos da democracia e da liberdade de comunicação está se transformando, uma vez que até mesmo a Internet está cada vez mais controlada pelo aparato punitivo.

Dentro desta constatação, há quem sustente a necessidade de serem criminalizadas várias condutas que envolvem sistemas de computadores, estando em trâmite no Congresso Brasileiro diversos projetos de lei sobre o tema.[11] De fato, nota-se que a tendência atual em nosso País é a de se optar pelo aumento na criminalização de delitos informáticos, dentro da concepção do direito penal simbólico, deixando-se de lado a adoção de medidas de prevenção, ou a previsão legal de ilícitos administrativos ou extra-penais em geral.

Infelizmente, isso vem ocorrendo não só no Brasil, mas também em outros países do mundo, havendo uma tendência cada vez mais repressora do ponto de vista da política criminal adotada com a criminalização de novas condutas no campo da informática.

Com o presente estudo, iremos nos posicionar contrariamente a essa tendência, razão pela qual passaremos a analisar a necessidade da adoção, em primeiro lugar, de medidas preventivas extra-penais, deixando o direito penal como *ultima ratio* também nos crimes informáticos, como veremos a seguir.

11. Podem ser citados aqui os Projetos de Lei 137/1989; 152/1991; 597/1991; 22/1996; 1.713/1996; 3.258/1997; 3.943/1997; 6.210/2002; Projeto de Lei do Senado 76/2000.

3. Por uma política criminal para delitos informáticos

Essa nova realidade surgida com o incremento da informática implica na necessidade de analisar os novos fatos socialmente nocivos que decorrem do abuso do uso de computadores, para depois termos condições de avaliar as repercussões jurídico-penais que possam destes decorrer. Neste estudo, optaremos por analisar tal fenômeno inicialmente sob a ótica da Política Criminal e da Criminologia, dentro da perspectiva da Ciência Global do Direito Penal.[12]

3.1 Aspectos criminológicos da delinqüência informática

Muito embora não tenhamos condições nesse momento de realizar uma abordagem criminológica profunda, mostra-se necessário tecer algumas considerações iniciais sobre os crimes informáticos enquanto fenômenos empíricos, de modo a conhecer melhor a situação fática, para depois compreendermos os métodos de prevenção.

Estudos criminológicos já realizados sobre esse fenômeno apontam essencialmente para uma heterogeneidade das condutas agrupadas sobre a mesma nomenclatura de delitos informáticos. Realmente, uma fraude eletrônica é uma conduta bastante diferente de um envio de *e-mail* contendo pornografia infantil, mas ambos são categorizados dentro do conceito de crimes informáticos.

Por outro lado, não há dúvidas de que estes tipos de condutas que envolvem o uso de computadores acarretam por si só um aumento de sua potencialidade lesiva ao bem jurídico protegido, pelo alcance e rapidez proporcionados pelo espaço cibernético, ao mesmo tempo em que a investigação é bastante difícil, diante do tipo de evidência a ser buscada, pois envolve o uso de avançada tecnologia.

Os chamados crimes informáticos, portanto, são condutas anti-sociais alçadas à condição de fatos típicos por decisão de política criminal, diante da

12. Nesse sentido, v.: MARTÍN, Ricardo M. Mata y. Op. cit., p. 24.

constatação da sua gravidade e necessidade de interferência do direito penal. Contudo, dentro da mesma categoria de delitos, encontram-se diversas condutas que em comum possuem apenas a circunstância de que são utilizados para sua prática sistemas de computador.

Na literatura sobre o tema tem sido destacado o elemento criminógeno do processamento eletrônico de dados, por várias circunstâncias, dentre elas a grande capacidade de armazenamento de dados, enorme velocidade de trabalho e rapidez nas operações, além da flexibilidade e possibilidades de aplicação diversas, inclusive com relação às falhas na segurança dos sistemas de operação mais vendidos no mercado. Acrescente-se a estas a dificuldade de rastreamento das operações ilícitas, além da elevada rentabilidade do ganho obtido pelo agente e a facilidade de se esconder o produto do crime, mesmo no caso de desvio de altos valores.

Ressalte-se, ainda, o fato de que a prática, qualquer lugar do mundo, de um delito via computador pode gerar efeitos em locais distantes e diferentes entre si, dificultando a localização do agente.

Ao mesmo tempo, sob a ótica da repressão penal, os altos custos da investigação podem, em alguns casos, torná-la desvantajosa para a vítima, assim como a preocupação de empresas e instituições financeiras com sua credibilidade no mercado que pode ser afetada como a divulgação de deficiência nos sistemas de informática, razão pela qual seus representantes legais optam por ressarcir a vítima, ou mesmo arcar com seu próprio prejuízo, ao invés de comunicar os crimes às autoridades para que sejam investigados.

Assim como as empresas mais atingidas pelo problema evitam oficializar os crimes de que foram vítimas, com receio de expor a vulnerabilidade de seus sistemas, as empresas fabricantes de sistemas informáticos também são vítimas das ações danosas, tal como se vê nas notícias de vírus dirigidos à Microsoft, maior fabricante mundial de programas de computador.

Ao analisar aspectos fenomenológicos dos delitos informáticos, nos informa Ricardo Martín que "importantes complicaciones para el descubrimiento

y la investigación de los hechos en y mediante el ordenador, de forma que puede en ocasiones no ser raro que muchos de los casos no lleguen nunca a detectarse".[13] Nesse sentido, muito embora não se tenha notícia de pesquisas sobre os delitos informáticos que não chegam ao conhecimento das autoridades no Brasil, dados coletados pelo FBI indicam que somente chegam ao conhecimento das autoridades americanas 1% (um por cento) dos casos, em relação aos quais somente em 3% (três por cento) são proferidas sentenças condenatórias, ou seja, de cada 22.000 autores destes delitos, somente um deles resultaria condenado pelos tribunais, conforme a análise do Prof. Ulrich Sieber.[14]

Portanto, diante dessa realidade, nos cabe analisar aspectos de política criminal, de forma a tentar encontrar a melhor forma de lidar com o problema.

3.2 Da necessidade de uma política criminal para crimes informáticos

No panorama visto acima, constatada a cada vez maior visibilidade do fenômeno, e considerando o fator criminógeno representado pelos sofisticados sistemas informáticos, que levam à maior danosidade social e o alcance global das condutas, pretendemos discutir uma política criminal para crimes de informática.

Há necessidade de se adotarem medidas de prevenção a este tipo de criminalidade, por meio da utilização de métodos não-penais com o objetivo de prevenir a prática de crimes, ao invés de optar-se pela mera previsão legal de tipos especiais, diante do reconhecimento de que o direito penal não serve à finalidade de impedir a prática de delitos.

13. Op. cit., p. 27.

14. Dados citados por: SIEBER, Ulrich. "Criminalidad informática: peligro y prevención". In: MIR PUIG (Org.). *Delincuencia informática*. Barcelona: PPU, 1992. p. 94. Apud MARTIN, Ricardo M. Mata y. Op. cit., p. 27.

A sociedade atual depende muito dos sistemas de informática, que já fazem parte do dia-a-dia das pessoas. Como já dito acima, as próprias características tecnológicas e a amplitude e rapidez na manipulação de dados e informações constituem um fator criminógeno de primeira ordem.

Assim, no combate a esses tipos de condutas socialmente nocivas praticadas mediante abuso da liberdade na operação de sistemas de computadores, essencial se mostra atuar antes da efetiva prática do delito, por meio de uma estratégia compreensiva e integrada de prevenção e controle, que não pode ser baseada exclusivamente em medidas repressivas, mas sim deve combinar medidas preventivas voluntárias para usuários de computadores, a aplicação de sanções administrativas e também medidas educativas, com o intuito de inibir e desestimular a prática de condutas socialmente reprováveis por parte dos potenciais infratores. Por certo que nos casos mais graves, caso seja atingido um bem jurídico constitucionalmente relevante, não se descarta a utilização do direito penal, porém como *ultima ratio*.

Quando se tem em mente uma abordagem de prevenção de crimes, conforme bem colocado pelo criminólogo Ken Pease, devemos partir de alguns pressupostos: i) os diversos comportamentos reunidos sob a nomenclatura de "crimes" são bastante diferentes entre si, razão pela qual não há como se pensar em técnicas universais de prevenção; ii) porque uma ação é considerada como crime, isso não significa dizer que a melhor forma de prevenir sua prática seja por meio da polícia e dos tribunais. Deve ser entendido o comportamento em análise para que se possa determinar quais as mudanças que devem ser realizadas para tentar prevenir sua ocorrência; iii) o objetivo do direito penal é moralmente problemático, pois uma sociedade em que mais se consegue prevenir práticas criminosas não é necessariamente o local mais agradável de se viver. Daí se depreende que os limites e restrições impostos às pessoas com o intuito de prevenir a prática de crimes devem ser ponderados com o dano causado pela própria prevenção ao crime.[15]

15. PEASE, Ken. "Crime prevention". In: MAGUIRE, Mike; MORGAN, Rod; REINER, Robert (Org.). *The Oxford Handbook of Criminology*. 2. ed. Oxford: Clarendon, 1997. p. 963.

Nesse sentido, com relação aos crimes informáticos, devemos analisar se a sociedade se tornaria mais segura caso as pessoas conseguissem adotar técnicas de prevenção eficazes, tal como deixar de usar computador. Será que se voltássemos a usar papel ao invés de arquivo eletrônico, carta ao invés de e-mail, entrássemos na fila do banco ao invés de acessar a conta pela internet estaríamos mais seguros? Por certo que sim, pois estaríamos reduzindo nossa exposição ao fator criminógeno que constitui o uso de computadores certamente, mas certamente isso não levaria à melhoria da qualidade de vida.

O fato é que hoje não há mais como se pensar na sociedade em que vivemos sem o uso de computadores, não há como se negar que somos todos atualmente dependentes da tecnologia. Assim, para buscarmos a melhor forma de prevenção, pensada como sendo a interrupção de mecanismos que causem eventos criminosos, a questão será como fazê-lo, sem que nos prejudiquemos ainda mais, já que impensável seria o retorno a procedimentos arcaicos de manipulação de dados e informações.

A teoria criminológica aponta para três grandes perspectivas de prevenção: *estrutural*, que consistiria na prevenção por meio de mudanças sociais e econômicas, defendida normalmente na esfera da política social, por meio da redução das desigualdades sociais para se reduzir a prática de crimes; *psicológica*, por meio da mudança no comportamento dos potenciais ofensores por meio do controle ou reforma; e *circunstanciais*, ou seja, que o controle do crime pode ser alcançado por modestos ajustamentos das circunstâncias que envolvem a prática do delito, tal como os alinhamentos sociais e locais nos quais determinado crime ocorre.[16]

No estudo a que nos propomos não trataremos da perspectiva estrutural da prevenção, até porque nosso foco está em cima da delinqüência informática, que está interligada às esferas mais economicamente desenvolvidas da sociedade. Nos dedicaremos, portanto, ao propósito de analisar a prevenção do crime do

16. PEASE, Ken. Crime prevention. Op. cit.

ponto de vista da chamada *prevenção primária* – no sentido de reduzir a oportunidade objetiva para a prática de delitos informáticos, ou seja, a terceira perspectiva descrita anteriormente.

No entanto, mostra-se relevante desde logo chamar a atenção para a inexistência de pesquisas de campo para detectar a incidência e os tipos de ações danosas por meio de computador mais praticadas em nosso País, pois somente a partir de pesquisas empíricas é que será possível detalhar estratégias e prever seus impactos no campo, razão pela qual abordaremos nesse momento medidas preventivas gerais, coletadas de experiências de outros países, mas que podem servir de base para a realidade brasileira. Deve ser ressaltada ainda a necessidade de levantamento de dados oficiais desse tipo de criminalidade, que ainda se mostra incipiente em nosso país.

Veremos então as grandes linhas de prevenção de crimes informáticos que entendemos essenciais serem adotadas dentro de uma estratégia de política criminal integrada.

3.3 Medidas de prevenção no campo da informática

Inicialmente, não há como se falar em delitos praticados por computador sem se falar em medidas de segurança tecnológicas, não no sentido de medida punitiva destinada a não imputáveis, tal como prevista em nosso Código Penal, mas sim como tradução da expressão *security measures*, encontrada na literatura especializada.

Assim, mostra-se essencial como medida de prevenção o aumento da segurança nos sistemas de computadores por meio da criação de leis que incentivem tais medidas – por exemplo, linhas de pesquisas em universidades, cooperação estatal com a iniciativa privada – que constitui um dos métodos mais eficazes de controle dos crime de informática.

Sobre este tema, mostra-se essencial unir os esforços que as indústrias e empresas de tecnologia já vêm tomando, com medidas governamentais de incen-

tivo, incluindo o desenvolvimento de melhores protocolos de segurança de computadores, o fechamento das chamadas "*trap doors*", ou "*back-doors*", que se caracterizam por uma falha do sistema que o deixa vulnerável à intromissão de *bugs* tanto para espionar como para alterá-lo e causar dano à sua estrutura, além do desenvolvimento de técnicas de criptografia mais complexas e seguras.

Há necessidade de se combinarem medidas técnicas de segurança voluntárias, a serem adotadas por usuários de computadores, juntamente com medidas compulsórias exigidas das empresas de tecnologia, para proteção dos usuários.

Na prática, a implementação de medidas preventivas como essas se mostra muito mais eficaz para se deter a ocorrência de crimes de informática do que leis penais incriminadoras. As próprias empresas vítimas de ataques sabem disso, tanto é que a maioria dos casos de invasões de sistemas, quebra de privacidade e transferências ilegais é resolvida internamente, sem que se dê maior publicidade, justamente por meio do aprendizado da técnica utilizada pelo agente e aprimoramento dos seus sistemas.

Sobre este ponto, merece ser chamada a atenção para o seguinte paradoxo: são justamente os eventos danosos aos computadores que acabam levando ao aumento da segurança e ao aperfeiçoamento dos sistemas informáticos.

Assim, a prática de delitos por meio do uso da informática em geral deve ser entendida como um produto direto da forma deficiente pela qual os sistemas informáticos vêm operando atualmente, o que leva diretamente à necessidade de se incentivar seu aperfeiçoamento, ao invés de se refletir exclusivamente acerca de medidas repressivas que somente irão atuar depois do dano já causado.

No caso de vírus, o mesmo autor da contaminação vende o antivírus, sendo certo que em vários casos se teve notícia de que a empresa vítima do golpe depois acabou contratando o *hacker* responsável para trabalhar para ela, visando ao aprimoramento de seu sistema.

Tais considerações mostram-se de extrema relevância especialmente em nosso País, no qual há que se incentivar a pesquisa nacional e o intercâmbio edu-

cacional com países desenvolvidos, pois dependemos da importação de tecnologias do exterior, e pouco investimos em pesquisa tecnológica, o que nos torna ainda mais vulneráveis à prática delituosas deste tipo.

Portanto, nossa sugestão seria justamente adotar-se como medidas de prevenção ao crime informático o incentivo à pesquisa em segurança informática e a exigência de padrões de segurança e controle pelas empresas, especialmente no caso de bancos e instituições financeiras.

Podemos ainda apontar para a necessidade de se aumentar a responsabilidade administrativa das empresas fabricantes de sistemas e dos provedores de Internet, de forma a, uma vez identificado o meio pelo qual foi possível a ação delituosa, que se exija de tais empresas, sob pena de multa e até de fechamento definitivo, a adoção de medidas que impeçam a repetição de tal ato, ainda que estas não tenham tido ligação subjetiva com o ilícito praticado. O controle administrativo, neste caso, seria muito mais eficaz do que a imposição de responsabilidade penal dos provedores de Internet que vem sendo proposta por alguns, diante da própria estrutura do processo penal que se mostra muito menos ágil em todos os aspectos, até porque requer maiores garantias na condução dos procedimentos e na aplicação da pena.

O incentivo à criação de associações de empresas e a auto-regulamentação por parte dos prestadores de serviços, por meio da criação de canais diretos de reclamações dos usuários com empresas privadas e autoridades são outras medidas a serem implementadas como prevenção. Especialmente no caso do *spam*, entendemos que sua prática não deve ser criminalizada, pois a melhor solução para o problema é a interferência estatal na coordenação de medidas preventivas entre as empresas prestadoras de serviço de *e-mail* e seus usuários, para se evitar a prática e punir imediatamente os abusos, por meio da detecção mais rápida da prática do envio massivo de mensagens indesejáveis pela rede mundial de computadores, o que vem causando enorme prejuízos. A adoção de filtros anti-*spam*, que vêm sendo aprimorados a cada dia, igualmente constituem medidas eficazes

na prevenção deste tipo de ação extremamente danosa aos usuários de *e-mail*. Ressalte-se, ainda, que tais medidas de segurança podem vir a ser extremamente lucrativas para as empresas dedicadas a essa atividade preventiva, conforme noticiou a revista *The Economist*.[17]

Do ponto de vista educacional, devem ser aumentados os esforços para se estabelecerem valores éticos na comunidade dos usuários de computadores e desenvolvimento de responsabilidade profissional. No caso de delitos informáticos, a educação preventiva tem uma importância enorme, sendo certo que o papel de incentivar a educação para desenvolver a consciência da segurança e moralidade social no uso dos computadores pode ser desenvolvido pelas universidades e cursos técnicos.

Além disso, sendo muito comum o envolvimento de profissionais de informática em delitos envolvendo computadores, por se tratar de atividade altamente especializada, que requer dedicação e experiência, uma proposta preventiva seria exigir-se o registro desses profissionais em entidades associativas, que poderiam exercer o poder disciplinar de fiscalização de seus membros e também reforçar o cumprimento de padrões éticos por meio da elaboração de um Código de Ética Profissional.[18]

Com tais recomendações, não temos a pretensão de esgotar a enumeração das medidas necessárias, mas sim de fomentar o debate sobre o tema dos delitos informáticos sob a ótica preventiva, e não repressiva.

No nosso entender, não basta apenas se discorrer sobre elementos típicos de crimes sem antes se analisar em profundidade o fenômeno real com que se está lidando. Por certo que tais medidas não são perfeitas ou infalíveis, bem como não se tem ainda estudos que provem sua eficácia, porém as chances destas evitarem

17. *The Economist*. "E-mail spam: filter it out". 19.10.2002, p. 61.

18. Conforme já referido nas Recomendações da AIDP que foram apresentadas no Congresso Internacional de 1984, vide nota n. 9 supra.

a incidência de crimes certamente são maiores do que as medidas repressivas, que somente serão aplicadas após a prática da ação e com o dano já causado.

Temos de reconhecer, no entanto, que mesmo nos países mais desenvolvidos que possuem as mais avançadas tecnologias de segurança, os especialistas vêm entendendo que o legislador deve criminalizar apenas as condutas mais graves devendo as medidas preventivas vir acompanhadas de mecanismos apropriados de aplicação da lei e de investigação, para que se consiga eficazmente combater e controlar esse tipo de criminalidade.

Outro elemento muito importante que vem sendo discutido na Europa e nos Estados Unidos é a necessidade de se adotar uma política criminal internacional harmônica, tendo em vista o caráter internacional dos chamados *cybercrimes*.

Em resumo, podemos concluir que a prevenção dos crimes que envolvem computadores mostra-se essencial para o bom funcionamento da sociedade da informação, que mais do que nunca exige um alto grau de eficiência e rapidez nas transações comerciais e depende socialmente do bom funcionamento de seus sistemas informáticos, sendo necessária a adoção de uma estratégia compreensiva e integrada para a prevenção e controle deste tipo de criminalidade, que não pode ser baseada exclusivamente em medidas legais, mas sim deve combinar medidas técnicas de segurança voluntárias, a serem adotadas por usuários de computadores, e a previsão legal de medidas mais leves ou mais repressivas dependendo da gravidade da lesão causada pela conduta, visando tanto à educação quanto a impedir as práticas lesivas de potenciais infratores.[19]

Por fim, mostra-se essencial destacar, na busca de soluções para se controlar esse tipo de crime a necessidade de maior colaboração e uniformização da legislação no âmbito mundial.

19. SIEBER, Ulrich. "Computer crimes and other crimes against information technology". *Revue Internationale de Droit Pénal*, Paris, vol. 64, p. 67-77, 1993.

4. Aspectos internacionais dos crimes informáticos e a Convenção Européia sobre Crimes Cibernéticos

4.1 Características internacionais dos crimes informáticos

Nas mais recentes discussões e elaborações legislativas sobre delitos informáticos, concluiu-se que não há como se pensar em soluções nacionais, devendo ser discutido o assunto no âmbito internacional, por se tratar de fenômeno influenciado diretamente pela globalização, normalmente praticado com a ultrapassagem de fronteiras, com interdependência de ações praticadas em diversos locais. Sem dúvida, há necessidade urgente de se facilitar a cooperação internacional como meio eficaz de combate a esse tipo de criminalidade.

Uma das razões mais freqüentemente apontadas pelos estudiosos para a harmonização da legislação (penal e extra-penal) é justamente a ampla mobilidade e a livre circulação de dados através de sistemas informáticos, tal como ocorre quando um agente pratica um crime usando um computador de um país, enquanto os resultados ocorrem em diversos outros locais sujeitos a diferentes legislações. Além disso, a existência de redes mundiais de telecomunicações internacionais que cruzam o território de vários países e a característica básica da Internet, meio mais usado de comunicação entre computadores, que ultrapassa fronteiras nacionais, reforçam ainda mais essa conclusão.

Devemos chamar atenção para o fato de que no mundo todo são usados praticamente os mesmos programas de computadores importados dos Estados Unidos, razão pela qual as medidas de segurança a serem adotadas devem ser globais. Além disso, menciona-se igualmente a necessidade de leis internacionais que protejam os direitos de autores de programas de *software*.

Assim sendo, diante da complexidade da questão e da característica global dos delitos informáticos, a existência de leis nacionais diversas com o objetivo

de prevenir tais delitos poderia levar à criação de paraísos criminais (chamados de *data heavens* ou *computer crime heavens*).[20]

Sem dúvidas, na atualidade, a mobilidade e a ausência de possibilidade de controle de informações faz com que soluções no campo do direito informático sejam indispensáveis, assim como, com relação às leis processuais, a harmonização dos poderes nacionais de coerção constitui importante fator de controle, prevenção e combate às infrações praticadas por meio de computadores.

Como conclusão decorrente dos fatores acima apontados, além de táticas de prevenção, a adoção de acordos e tratados de cooperação internacional, e a troca de informações entre os diversos países, constituem condição essencial para o bom andamento de investigações de crimes de computadores.

Desta forma, o funcionamento e a eficácia dos instrumentos internacionais de assistência mútua perpassam pela uniformização das legislações nacionais, assim como preconizado pelo Conselho da Europa na elaboração da Convenção sobre Crimes Cibernéticos, realizada em Budapeste em 2001, pois um Estado a que se requer assistência somente pode levar adiante medidas admitidas na sua própria legislação nacional, bem como diante do princípio da dupla criminalidade que constitui a base da cooperação internacional. Utilizando as palavras de um dos maiores especialistas em delitos informáticos, o Prof. Ulrich Sieber, da Universidade de Munich, *as soluções nacionais para as questões dos delitos de computadores devem ser banidas para os arquivos do passado*.[21]

Sob este ponto, no relatório explicativo da Convenção, foi explicitada a preocupação dos especialistas europeus que "a nova tecnologia desafia conceitos legais. Informações e comunicações circulam mais facilmente pelo mundo. Fronteiras não constituem mais limitações a esse movimento contínuo. Criminosos podem estar

20. Paraísos criminais seriam locais nos quais provedores se instalariam e seriam beneficiados por legislações mais brandas, que não punissem crimes informáticos, em alusão aos conhecidos paraísos fiscais de taxas e impostos que atraem as companhias internacionais interessadas em reduzir seus custos.

21. SIEBER. Ulrich. "Computer crimes...", cit., p. 77.

em lugares completamente diversos dos locais onde seus atos produzem efeitos. Contudo, leis nacionais têm sua aplicação limitada a um território específico. Desta forma, soluções para os problemas citados devem ser adotadas pelo direito internacional, sendo necessária a adoção de adequados instrumentos legais internacionais".

No mesmo sentido são as conclusões de estudo recente da ABA – American Bar Association, que preconizam a importância de uma comissão internacional para tratar do tema da *cyberlaw* em geral, incluindo os delitos informáticos, para o estudo de uma legislação capaz de transpor *de forma célere as fronteiras geográficas dos países.*[22]

A partir desta constatação, passaremos a analisar em maiores detalhes a referida Convenção Européia, com o objetivo de situar o público brasileiro nas questões tratadas por tal instrumento internacional, que muito tem a contribuir para o aperfeiçoamento de nossa legislação, de modo a atualizá-la de acordo com os padrões atualmente fixados no âmbito internacional. Deve ser lembrado, igualmente, que não se trata de propor a reprodução de legislações estrangeiras para incorporá-las ao nosso sistema jurídico de forma acrítica, mas sim de se discutir os termos elaborados por especialistas no campo do direito penal informático em relação a um tipo de criminalidade com características internacionais.

4.2 A Convenção Européia sobre Crimes Cibernéticos

A Convenção Européia sobre Crimes Cibernéticos de 2001,[23] elaborada pelo Conselho da Europa (*Council of Europe*), órgão intergovernamental que

22. Cf.: GUEIROS JR., Nehemias. "*Cyberlaw*: novas regras terão que ser globais". *Revista Justilex*, ano 2, n. 18, p. 26, jun. 2003.

23. A situação atual da Convenção é a seguinte: seu texto está aberto para assinatura aos Estados membros e não-membros que participaram da sua elaboração (Canadá, Japão, África do Sul e EUA). Até outubro de 2003, apesar de quase todos os países membros já terem assinado, apenas Albânia, Croácia e Estônia haviam ratificado o tratado. Portanto, seu texto ainda não está em vigor, o que ocorrerá quando houver cinco ratificações, incluindo pelo menos três Estados membros do Conselho da Europa.

engloba 45 Estados membros, incluindo os 15 membros da União Européia, mas que não se confunde com ela, é o instrumento internacional mais amplo e atual sobre o tema e foi produzido em conjunto pelos maiores especialistas de diversas nacionalidades.

Na realidade, trata-se do primeiro tratado internacional sobre crimes cometidos por meio de sistemas de computadores, lidando particularmente com a segurança de redes de computadores, violações de direitos autorais, fraude por meio de computadores e pornografia infantil. Contém ainda uma série de poderes e procedimentos que permitirão a adoção de medidas investigatórias dirigidas a sistemas informáticos, inclusive interceptação de dados.

O objetivo de tal Convenção, como expressamente declarado em seu preâmbulo, é o de buscar uniformizar a legislação européia, por meio de uma política criminal comum, para proteger a sociedade dos crimes cibernéticos, recomendando a legislação apropriada e buscando facilitar e agilizar a cooperação internacional por meio da adoção de tipos legais e procedimentos penais uniformes.

Apesar de não se tratar de uma Convenção internacional, mas sim européia, de acordo com seu art. 37, há a possibilidade de países não-membros e que não tenham participado de sua elaboração aderirem a seus termos. Para tanto, o Comitê de Ministros do Conselho da Europa, desde que com o consenso dos países signatários da Convenção, poderá convidar qualquer Estado a fazê-lo.

De fato, a elaboração da Convenção foi uma conquista, diante das inúmeras divergências surgidas entre os países-membros que participaram de sua elaboração, sendo que sua futura entrada em vigor facilitará muito a adoção de políticas criminais comuns e também a uniformização das legislações nacionais.

4.3 Conceitos e objetivos preconizados pela Convenção Européia sobre Crimes Cibernéticos

Na Convenção Européia sobre Crimes Cibernéticos, foi definido o termo espaço cibernético (*cyberspace*) como um tipo de espaço comum, utilizado pelos

usuários da rede mundial de computadores (Internet) ao se conectarem aos serviços de comunicação e informação, para propósitos legítimos, mas que também podem estar sujeitos a abusos.

Em termos dogmáticos, os crimes cibernéticos ou crimes informáticos são delitos cometidos contra a integridade, disponibilidade e confidencialidade dos sistemas informáticos e redes de telecomunicações, bem como consistem no uso de redes de serviço para cometer crimes tradicionais através da Internet. Essa característica de ultrapassar fronteiras, por exemplo, em crimes praticados pela Internet, está em conflito com a competência e atuação territorial das autoridades nacionais.

Diante destas características, os especialistas europeus chegaram à conclusão de que somente um instrumento internacional que fosse vinculante aos países signatários poderia ter a necessária eficiência na luta contra esse novo fenômeno, e que uma Convenção deveria ser elaborada não somente para criar novos tipos penais (direito penal substantivo), mas também deveria prever questões de processo penal, harmonizar procedimentos de direito penal internacional e estabelecer acordos referentes à tecnologia da informação.

São objetivos da referida Convenção: i) harmonizar as legislações penais substantivas, elementos do delito e outras provisões conexas sobre delitos de informática; ii) promover alterações nas legislações processuais nacionais de forma a conceder poderes de investigação e persecução criminal necessários para combater delitos praticados com o uso de sistemas de computador, ou nos demais tipos de delitos nos quais as provas devam ser obtidas mediante meios eletrônicos; iii) estabelecer um regime rápido e efetivo de cooperação internacional.

Em termos gerais, no que diz respeito à sua estrutura, a Convenção de Budapeste está dividida em quatro capítulos. O primeiro trata da terminologia, e define os termos mais básicos tais como *"sistema de computador"* (computer system), *"dados de computador"* (computer data), *"provedor de serviços"* (service provider) e *"fluxo de dados"* (traffic data), com o intuito de harmonizar as definições, conforme seu art. 1.º.

No capítulo seguinte, estão previstas medidas a serem tomadas no âmbito das legislações nacionais, tais como leis penais substantivas e regras de processo e investigação penal. Também se recomenda a criminalização de determinadas condutas mais graves, que envolvam computadores, estando definidos nove crimes divididos em quatro diferentes categorias cuja tipificação é recomendada.

4.4 Dos crimes informáticos previstos

Os crimes indicados na Convenção são todos dolosos, havendo referência expressa em seu texto ao princípio da ofensividade, pois tão somente se indica a opção de criminalização das ações mais graves envolvendo o abuso no uso de computadores.

Desta forma, estão descritos roteiros que servirão como base para as alterações das leis nacionais, sendo certo que não se exige dos Estados-parte que eles copiem a descrição dos delitos do texto convencional, mas, ao aderirem ao tratado, estes se comprometem a adotar definições equivalentes em seus sistemas jurídicos. Optou-se pela concepção de crimes informáticos em sentido estrito, baseando-se no consenso mínimo obtido entre as partes signatárias do texto normativo europeu.

O primeiro título dispõe sobre crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computadores, estando previstos os seguintes crimes propriamente informáticos, ou seja, condutas em que o sistema informático é objeto material da ação: "acesso ilegal à integralidade ou a parte de sistema de computadores sem autorização" (*illegal access* – art. 2.º);[24] "interceptação ilegal" (*illegal interception* – art. 3.º);[25] "interferência ou dano em

24. Este crime pode ser cometido pela violação das medidas de segurança, com a intenção de obter dados de computadores ou outra intenção desonesta, estando tal sistema de computador conectado ou não a uma rede de computadores.

25. Trata-se de interceptação sem autorização, por meios técnicos, de transmissões privadas de dados, envolvendo um sistema de computadores, incluindo emissões eletromagnéticas de um sis-

dados de computador" (*data interference* – art. 4.º);[26] "interferência em sistemas" (*system interference* – art. 5.º).[27] A Convenção também recomenda em seu art. 6.º a tipificação de alguns atos preparatórios tal como o "uso indevido de dispositivos" (*misuse of devices*).[28]

O Título 2 do Capítulo 2 prevê as duas ofensas relacionadas com computadores, ou seja, crimes já tipificados nas legislações penais comuns, mas que podem ser praticados tendo como meio sistemas informáticos. São eles: falsificação eletrônica ou praticada por meio de computadores (*computer-related forgery* – art. 7.º)[29] e fraude informática (*computer-related fraud* – art. 8.º).[30]

A seguir, no Título 3, são tratadas as ofensas relacionadas à pornografia infantil, tema esse muito em voga na atualidade, diante do aumento de sua per-

tema de computadores capacitado para processar tais dados. Pode a ofensa ser cometida com intenção desonesta em sistemas conectados a outros sistemas de computação (rede).

26. Estão previstas no referido artigo as ações de danificar, apagar, deteriorar, alterar ou suprimir dados de computadores sem autorização, podendo ser exigido para a configuração do delito que a conduta tenha resultado em grave lesão.

27. A tipificação se refere à restrição ao bom funcionamento de um sistema de computadores, sem autorização, por meio de inserção, transmissão, dano, exclusão, deterioração ou supressão de dados.

28. As condutas previstas são: produzir, vender, comprar para uso, importar, distribuir ou tornar disponível: i) dispositivo, incluindo programa de computador, desenhado ou adaptado com especial propósito de cometer qualquer das ofensas previstas nos arts. 2.º a 5.º acima; ii) senha de computador, código de acesso ou informação similar que em todo ou em parte permita o acesso a sistema de computador. Em ambas deve haver intenção de cometer qualquer das ofensas estabelecidas nos arts. 2.º a 5.º. Pune-se também a posse de um dos itens referidos acima (i e ii) com intenção de cometer as ofensas previstas nos arts. 2.º a 5.º, podendo ser exigida pela lei que uma quantidade mínima de tais itens esteja na posse da pessoa para que possa ser atribuída responsabilidade criminal.

29. A descrição típica sugerida é a inclusão, alteração, exclusão ou supressão de dados de computador, que resultem na inautenticidade dos dados com a intenção de se fazer passar, ou sendo utilizado para fins legais como se autêntico fosse, mesmo se a informação não é diretamente legível e/ou inteligível. Pode-se exigir intenção de defraudação ou outra intenção semelhante, para a atribuição da responsabilidade criminal.

30. Neste art. 8.º, está prevista a ação de causar lesão a bens de uma pessoa por meio das seguintes práticas: i) inclusão, alteração, exclusão ou supressão de dados de computadores; ii) interferência no funcionamento de sistema de computador; em ambos os casos com intenção fraudulenta ou desonesta, e sem autorização, tendo como objetivo a obtenção de vantagem econômica para si ou para outrem.

cepção e pela facilidade de manipulação e circulação de imagens através da rede mundial de computadores.

Nas discussões que antecederam a elaboração dos termos da Convenção, houve muitas divergências com relação ao tema da pornografia infantil, pois existia um grupo proponente de medidas mais duras de inclusão como crime a mera posse de material pornográfico envolvendo crianças ou adolescentes, enquanto que outros consideravam inconstitucional esta proibição diante do direito fundamental à privacidade. Assim, a redação dos termos da Convenção acabou sendo feita de forma a tentar conciliar as duas vertentes, ou seja, constou como imposição a criminalização somente daqueles tópicos em que não havia divergências, enquanto que outros tipos, como a criminalização da mera posse, ficou como uma faculdade para os países membros, conforme se abstrai da redação do art. 9.º, que trata dos crimes relacionados à pornografia infantil (*offenses related to child pornography*).[31]

Assim, de acordo com o art. 9.º, os Estados-parte poderão se reservar ao direito de não criminalizar a mera posse de material pornográfico envolvendo crianças (§ 1.º, *d*) e também as hipóteses de imagens não reais, e/ou simulações, envolvendo adultos ou representações e imagens não reais, criadas artificialmente que representem menores em práticas sexuais (vide § 2.º, *b* e *c*).

Por fim, o Título 4 trata de crimes relacionados à violação de direitos de autor em geral, ou crimes contra a propriedade intelectual envolvendo progra-

31. Estão previstos os seguintes tipos relacionados à pornografia infantil, praticados mediante o uso de sistemas de computadores: a) produzir pornografia infantil com o propósito de distribuição; b) oferecer ou tornar disponível pornografia infantil; c) distribuir ou transmitir pornografia infantil; d) adquirir pornografia infantil para si ou para outrem; e) ter em seu poder pornografia infantil no sistema de computadores ou em qualquer meio de arquivo externo de computação (exemplos: disquete ou CD). O § 2.º deste mesmo artigo define como pornografia infantil material que demonstre visualmente: a) um menor engajado em conduta sexualmente explícita; b) pessoa aparentando ser menor de idade em conduta sexualmente explícita; c) imagens realistas representando menor engajado em conduta sexualmente explícita, sendo certo que o termo menor, para fins deste parágrafo, significa pessoas com menos de dezoito anos de idade, podendo os Estados-parte exigir um limite de idade de até dezesseis anos.

mas de *software*, sendo recomendadas a criminalização de condutas intencionais, com objetivos e em escala comercial praticadas por meio do uso de computadores para a pirataria de *software*. No entanto, está também prevista ressalva para alguns Estados que poderão optar por promover medidas não penais para lidar com a questão, ao invés de criminalizar tais condutas.

Há ainda outras questões controvertidas que não foram resolvidas pelos *experts* da Convenção, diante das inúmeras divergências entre os países signatários, tais como o jogo ilegal pela Internet e o terrorismo cibernético, ainda objetos de debate. Preferiu-se deixar tais condutas de fora da Convenção, para que cada Estado decida por conta própria decidir criminalizá-las ou não.

Por outro lado, optou-se intencionalmente por não criminalizar o *spam*, tendo em vista as conclusões de que medidas outras, não penais, seriam a melhor forma de cuidar do recebimento de mensagens indesejáveis.[32]

Com relação à responsabilidade penal da pessoa jurídica (*corporate liability*) diante da divergência entre os países, tal como ocorreu em outras convenções internacionais elaboradas recentemente, a Convenção Européia no seu art. 12, § 4.º apenas indica que sua responsabilização poderá ser criminal, civil ou administrativa.

Posteriormente, foi assinado um Protocolo Adicional à Convenção de Budapeste, em 28.01.2003, que recomenda a criminalização de atos de racismo e xenofobia cometidos por meios de computador, visando harmonizar suas legislações para combater o conteúdo da informação que circula pela rede tais como: disseminação de material racista e xenófobo (art. 3.º); ameaça motivada por racismo ou xenofobia (art. 4.º); insultos ou crimes contra a honra motivados por racismo ou xenofobismo (art. 5.º); denegação, minimização grosseira, aprovação ou justificação de genocídio ou crimes contra a humanidade (art. 6.º).

32. A Convenção aborda ainda questões da parte geral de direito penal em seus arts. 11 a 13, tal como concurso de agentes, participação e tentativa, que não oferecem maiores novidades, mantendo a linha tradicional das legislações nacionais.

4.5 Medidas processuais-penais recomendadas

Desde 1992, já havia uma preocupação da comunidade internacional com relação à necessidade de previsão de medidas adequadas à apuração desse tipo de criminalidade de alta especialização tecnológica, pois para tornar eficazes as investigações neste campo faz-se necessária a previsão legal de procedimentos específicos de busca e apreensão, coleta, congelamento e interceptação de dados de computadores, assim como a busca no ambiente em rede de sistemas.

Por outro lado, também já se preocupavam os juristas com a necessidade de utilização dessas novas técnicas de investigação de forma equilibrada, garantindo-se proteção adequada aos direitos fundamentais, especialmente ao direito à privacidade, exigindo-se a ponderação entre o grau de lesividade ou gravidade do delito a ser investigado, com a restrição de direitos atingidos pela investigação. Desta forma, somente se deve admitir a violação do sigilo dos dados de computador para fins de apuração dos delitos mais graves.

Tais recomendações influenciaram fortemente a elaboração da Convenção Européia, tendo sido previstas no texto convencional medidas processuais a serem adotadas pelas legislações nacionais com o propósito de investigação criminal não só dos crimes informáticos propriamente ditos, como também de delitos comuns cometidos por meio de um sistema de computadores, ou aqueles cujas evidência a serem obtidas estejam na forma eletrônica. Trata-se de procedimentos específicos que visam atualizar a legislação processual para a era da informática, e fornecer aos operadores do direito meios rápidos e eficazes para reprimir as condutas ilícitas e descobrir seus autores.

Um dos maiores desafios na esfera do combate à criminalidade informática é justamente a dificuldade de identificação do agente criminoso e coleta de evidências, diante da volatilidade dos dados eletrônicos, que podem ser facilmente alterados, movidos ou apagados em segundos, sendo o segredo e a rapidez essenciais para a investigação.

A Convenção Européia em estudo, portanto, adaptou medidas processuais tradicionais para o meio ambiente da tecnologia, além de ter criado outras inéditas, especificamente destinadas a um tipo específico de dados de computadores a serem buscados, impondo, ao mesmo tempo, as salvaguardas do art. 15, relativas à proteção aos direitos humanos e liberdades individuais. Recomendou-se aos países a exigência de autorização judicial ou outra supervisão independente das medidas procedimentais previstas, além da fundamentação específica para limitar o objeto e a duração dos poderes de investigação concedidos, especialmente diante da possível violação de interesses legítimos de terceiros.

As medidas processuais recomendadas têm por objetivo permitir a obtenção e coleta de dados em investigações criminais específicas. Chegou-se a discutir a possibilidade de se impor obrigações gerais para serviços de provedores para a coleta e manutenção em seus arquivos, de fluxos de dados por um certo período a ser fixado, como medida preventiva visando futura investigação de crimes, que não foram incluídos no texto final por falta de consenso entre os especialistas.

Em termos gerais, estes procedimentos de investigação e obtenção de evidências referem-se a todos os tipos de dados, entre eles "fluxo de dados" ("*traffic data*"), que são aqueles que representam as conexões entre os computadores, contendo informações sobre o caminho percorrido; "dados com informações" ("*content data*"), ou seja, o próprio conteúdo da informação; e dados pessoais do assinante (*subscriber data*), tais como nome, endereço e número de acesso, que ficam armazenados no banco de dados dos provedores (§ 3.º do art. 18).

A possibilidade de aplicação de medidas para obter evidência eletrônica, portanto, dependerá da natureza e da forma dos dados e do procedimento.

São medidas processuais recomendadas pela Convenção Européia: i). *determinação ou ordem de preservação de dados armazenados em sistemas de com-*

putadores" ("*expedited preservation of stored computer data*"),[33] com duração de até noventa dias, que permite às autoridades pleitear posteriormente uma ordem de abertura ou revelação (*disclosure*) de tais dados, o que seria equivalente à nossa quebra de sigilo (art. 16); ii) *ordem de preservação e parcial abertura de fluxo de dados* ("*expedited preservation and partial disclosure of traffic data*")[34]; iii) *ordem de fornecimento de dados às autoridades* ("*production order*" – art. 18)[35]; iv) *busca e apreensão para acessar sistemas e dados de computadores*, incluindo meios de armazenamento de dados eletrônicos (*CD-rom*, disquetes e similares – art. 19)[36]; v) *obtenção, coleta ou gravação em tempo real de fluxo de dados* ("*real-time collection of traffic data*" – art. 20)[37]; vi) *interceptação de dados* (de conteúdo)

33. Trata-se de um tipo de apreensão no qual o detentor de dados específicos, inclusive fluxo de dados, que estejam armazenados em seu sistema, está obrigado a preservá-los por um prazo maior de tempo, evitando-se, dessa forma, a possibilidade de modificação ou perda. Tal medida permitirá ao detentor dos dados continuar a utilizar normalmente seu sistema, desde que preservando determinadas informações de interesse da investigação, tendo como contrapartida a obrigação de manter confidencial tal fato, evitando-se que o investigado tome conhecimento.

34. Esta medida tem por objetivo preservar e revelar (*disclosure*) as informações referentes ao fluxo de dados no sistema, permitindo o acesso das autoridades às informações sob a forma eletrônica, do caminho percorrido pelo usuário, mesmo havendo um ou mais provedores envolvidos em tal transmissão, de forma a se chegar até seu destino final. As medidas previstas nos arts. 16 e 17 se aplicam aos dados armazenados que já tenham sido coletados pelos seus detentores, tais como provedores de acesso à rede.

35. Na medida prevista no artigo 18, a autoridade competente ordena que lhe sejam fornecidos dados específicos armazenados em computadores, incluindo os dados pessoais dos assinantes contidos nos arquivos dos provedores fornecidos por ocasião do contrato, além de outras informações sobre tipos de equipamentos utilizados e outras provisões técnicas que auxiliem as autoridades nas investigações. Neste caso, a autoridade não busca ou apreende, mas ordena que informações sejam fornecidas por terceiros que estejam na posse destas sob a forma de dados.

36. Neste tipo de medida investigativa, as autoridades poderão ter acesso, congelar ou bloquear um sistema de computadores ou qualquer meio de armazenamento de dados, assim como fazer cópias dos dados contidos nos computadores, ou mesmo tornar inacessível ou remover tais dados do sistema.

37. No caso do artigo 20, enquanto os dados são transmitidos pelo computador, a autoridade poderá ter acesso simultâneo à rota percorrida por tais informações, ou ainda compelir o provedor a fazê-lo, podendo ser gravadas tais informações obtidas. Esse procedimento visa apenas identificar a circulação das informações, mas não seu conteúdo, o que poderá ser objeto da medida prevista no art. 21.

("*interception of content data*") transmitidos por meio de comunicação eletrônica, em tempo real (art. 21).[38]

Desta forma, os Estados-parte da Convenção, após a ratificação, estarão obrigados a adotar em seu sistema jurídico tais medidas acima previstas, ou outras que se façam necessárias de acordo com suas leis nacionais, estabelecendo os poderes e procedimentos necessários em uma investigação criminal de delitos que envolvam o uso de computadores ou sistemas.

Há ainda uma outra questão interessante a ser abordada. Está explícito nos termos na Convenção que as partes devem incorporar à sua legislação a possibilidade de que a informação obtida por meios digitais ou eletrônicos seja usada como evidência perante a Corte em procedimentos penais, independentemente da natureza do crime. Contudo, há duas exceções a essa regra, quais sejam as medidas previstas no arts. 20 e 21 (coleta de fluxo de dados e interceptação de dados), consideradas excepcionais, e assim aplicáveis apenas aos crimes mais graves, pelo alcance e intrusão causada pela medida, razão pela qual as partes podem prever limitações em suas leis nacionais.

Mostra-se importante chamar a atenção para o art. 15, que prevê garantias ou salvaguardas, com o objetivo de ponderar as necessidades da persecução penal com a proteção dos direitos humanos, bem como sua adaptação às leis nacionais, que irão prever as condições específicas de deferimento destas medidas, incluindo a necessidade de autorização judicial, a exigência de certas condições e limitações, bem como respeitando-se parâmetros comuns já previstos em convenções internacionais de direitos humanos. Por isso, está expressamente prevista a incorporação às leis nacionais do princípio da proporcionalidade, ou seja, que os poderes conferidos às autoridades investigadoras e as ordens por elas proferi-

38. Poderíamos também chamar tal medida de "grampo", ou interceptação de dados transmitidos entre computadores. A ordem da autoridade neste caso permite coletar e gravar os dados transmitidos, ou compelir o provedor a fazê-lo com seus meios técnicos, prestando assistência às autoridades.

das devem ser proporcionais à natureza do crime investigado, devendo estar previstos requerimentos razoáveis que limitem a busca e apreensão exclusivamente aos casos em que se mostre necessária.

Há uma clara preocupação por parte dos especialistas que elaboraram a Convenção com o impacto de tais medidas em interesses de terceiros, incluindo os provedores, sendo requerido aos Estados-parte que utilizem os meios apropriados para minimizar seus efeitos, incluindo o respeito às vítimas e o direito à privacidade, assim como a necessidade de se evitar a interrupção no fornecimento dos serviços aos consumidores.

A previsão de tais medidas técnicas nas legislações nacionais[39] poderá tornar mais ágeis e eficazes as investigações nos crimes envolvendo sistemas e computadores. No nosso entender, muito mais importante do que criminalizar novos tipos penais informáticos é se estabelecer meios procedimentais específicos de coleta de provas, sem os quais as autoridades não conseguirão chegar aos autores dos delitos.

Além da previsão legal de medidas processuais para se obter a evidência em crimes informáticos, mostra-se essencial que se tenha também uma polícia técnica desenvolvida, com pessoas capacitadas e treinadas no campo da

39. Com relação ao direito brasileiro, merecem ser trazidas algumas breves considerações. De acordo nossa Constituição Federal, art. 5.º, XII, "é *inviolável o sigilo* da correspondência e das comunicações telegráficas, *de dados* e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal". A esse respeito foi editada a LC 9.296/1996, que regula as hipóteses de quebra de sigilo das comunicações. Quanto à possibilidade de interceptação do fluxo em sistemas de informática e telemática, a doutrina brasileira se divide, pois há quem considere inconstitucional a quebra de sigilo de dados, sob o argumento de que somente se admite a interceptação de comunicações telefônicas. Nesse sentido: GRECO FILHO, Vicente. *Interceptação telefônica*. São Paulo: Saraiva, 1996. p. 11; e GRINOVER, Ada Pellegrini. "Regime brasileiro das interceptações telefônicas". *Revista de Direito Criminal* 17/115. Em sentido contrário, Luiz Flávio Gomes. *Interceptação telefônica*. São Paulo: RT, 1997. p. 176 . Não nos parece lógico que haja alguma diferença de conteúdo ou significado entre as comunicações telefônicas e aquelas realizadas por meio de dados, que possa ter levado o legislador a considerar a tutela do sigilo de dados absoluta, razão pela qual nos filiamos ao entendimento que admite a quebra de sigilo de dados, desde que na forma e com as garantias previstas na lei.

informática e que dominem as novas tecnologias, além de bem equipadas com computadores de última geração, para que possam periciar e avaliar os dados coletados, tendo em vista o alto grau de especialização deste tipo de atividade.[40]

Por fim, a Convenção recomenda ainda critérios de atribuição de jurisdição, visando a permitir que todos os países possam exercer sua jurisdição sobre os delitos informáticos, ampliando seu alcance, além de sugestões para resolução de conflitos de jurisdição, conforme se vê no art. 22, e seu § 4.º.

4.6 Cooperação Penal Internacional

A Convenção Européia em estudo contém importantes provisões referentes a assistência, extradição e cooperação mútua, mesmo para casos em que não haja base legal (tratado ou reciprocidade) entre as partes envolvidas, de forma a tornar cada vez mais ampla a cooperação entre os Estados-parte na persecução penal aos delitos envolvendo computadores.

Em seus termos, encontra-se expressamente permitida a comunicação via fax ou *e-mail*, de forma a agilizar a comunicação entre as partes, evitando-se os meios diplomáticos como tradicionalmente se fazia (art. 25, § 3.º).

Há também instruções expressas para que as partes designem uma autoridade central ou autoridades responsáveis para receber e enviar pedidos de assistência mútua, assim como executar tais requisições ou transmiti-las às autoridades competentes (art. 27, § 2.º).

40. No caso da realidade brasileira, devemos sempre ter em conta que há uma crônica falta de investimentos em perícia técnica, o que nos permite concluir que de nada adiantará a previsão legal de medidas cautelares como as que analisamos acima, se não houver peritos e equipamentos adequados à investigação de delitos com utilização de tecnologia mais avançada. No Estado do Rio de Janeiro, por exemplo, na investigação de crimes informáticos as autoridades policiais acabam tendo de solicitar a colaboração universidades, inclusive de outros Estados, diante de sua incapacidade de realizar certas perícias especializadas. A sugestão que fazemos nesse sentido é o estreitamento da colaboração entre esses órgãos, bem como a separação dos órgãos técnicos de perícia da estrutura da Polícia Civil, para órgãos científicos independentes, como já ocorre em São Paulo, tendo em vista que as funções exercidas são muito diferentes.

A preocupação da Convenção em agilizar a cooperação internacional na investigação de delitos informáticos levou à previsão expressa de requerimento de cooperação por meio de medidas cautelares, visando preservar a evidência para futuras requisições, por um período não inferior à sessenta dias (arts. 29 e 30).

Constou dos termos do texto convencional, inclusive, a possibilidade de acesso direto transnacional a dados armazenados em computadores, sem a necessidade de ser requerida assistência mútua, desde que haja consentimento, ou quando sejam públicos (art. 32). Admite-se também que se possa acessar ou receber dados armazenados em computadores diretamente, desde que a autoridade do local onde esses dados se encontrem consinta e se tenha autorização judicial para abrir tais informações à outra parte por meios eletrônicos.

5. Conclusão

A aproximação do direito aos novos fatos sempre será um desafio, pois as transformações sociais sempre estarão à frente das leis. No caso do direito penal, especialmente, os avanços tecnológicos de nossa época estão levando a uma mudança de paradigma, constituindo os crimes informáticos um exemplo disso.

Há de se ter em mente que o desenvolvimento da tecnologia levou a mudanças radicais na sociedade, porém, ao mesmo tempo em que os computadores facilitaram muito a vida das pessoas, o outro lado da moeda é o abuso no uso da informática por meio da prática de atos danosos socialmente por meio das novas tecnologias facilitadoras. Isso porque, como vimos, a utilização de sistemas de computadores constitui um fator criminógeno de primeira ordem.

De fato, as particularidades inerentes às novas tecnologias se traduzem no âmbito da criminalidade que projetam. Ao mesmo tempo em que pessoas de diferentes países se comunicam por meio de computadores em tempo real, usam telefones celulares, *laptops* e passam *e-mails*, essa mesma tecnologia pode ser uti-

lizada para praticar crimes com amplas conseqüências danosas, além de muito mais difíceis de serem investigados.

Diante desta constatação, concluímos que se mostra muito mais adequada e eficaz a implementação de medidas preventivas de segurança e de aperfeiçoamento das tecnologias de proteção de sistemas, com a adoção de medidas não-penais, administrativas e voluntárias, para se lidar com o fenômeno dos delitos informáticos.

Por sua vez, o direito penal somente deverá atuar como *ultima ratio* também no campo na informática, sendo que a pena somente deve ser aplicada em situações extremas, respeitando-se o princípio da ofensividade e da subsidiariedade, razão pela qual somente as condutas mais graves devem ser levadas à esfera repressiva penal.

Diante isso, consideramos desnecessária a edição de nova legislação que preveja especificamente delitos informáticos, visto que mais de noventa por cento das condutas delituosas neste campo já estão previstas no Código Penal e em leis especiais, restando ainda a serem criminalizados tão-somente menos de dez por cento, no caso de delitos em que o sistema de computadores seja o único bem jurídico a ser protegido.[41]

Consideramos que o maior desafio atual com relação à criminalidade informática está, acima de tudo, nas graves deficiências de prevenção das novas formas de violações a bens jurídicos protegidos pelo ordenamento. Não há como se pensar apenas em criminalizar, mostrando-se a prevenção ainda como a melhor estratégia, especialmente no Brasil, com seus contrastes e iniqüidades sociais, onde o direito penal nunca foi nem será capaz de resolver os problemas decorrentes das ações delituosas danosas ao meio social, nem é capaz de evitá-las.

41. O presente artigo foi elaborado antes da edição da Lei 10.766/2003 que alterou o art. 241 do Estatuto da Criança e do Adolescente, prevendo expressamente sua prática por meio da rede mundial de computadores.

Assim, concluímos ser mais importante do que discutir a necessidade de alteração da legislação penal atual – até porque praticamente todas as condutas já estão criminalizadas, com raras exceções – a reflexão sobre quais medidas preventivas devem ser tomadas, a fim de minimizar o risco, diante da constatação do fator criminógeno do uso de computadores.

As dificuldades encontradas pelos operadores do direito no combate e prevenção aos crimes de informática não serão solucionadas simplesmente por meio da tipificação penal generalizada de novas condutas, ainda que consideradas como danosas ao meio social. Além da prevenção, há de se ter em conta que a apuração de delitos informáticos, de estrutura complexa, é especialmente problemática, diante das dificuldades na apuração e investigação deste tipo de delito, o que requer agilidade, conhecimento técnico, amplo uso de tecnologia e altos investimentos em perícia técnica.

Para isso, mostra-se fundamental a previsão legal de procedimentos específicos de colheita de evidências envolvendo computadores, além do incremento da cooperação internacional, pautada na harmonização de delitos diante dos reflexos internacionais deste tipo de criminalidade, que ultrapassa fronteiras através do fluxo livre de informações pela rede.

Porém, neste momento em que pensamos em novos paradigmas no horizonte do direito penal, mostra-se igualmente necessária a manutenção das conquistas do Garantismo, tomando-se como exemplo o modelo europeu consubstanciado na Convenção Européia sobre Crimes Cibernéticos, que ao lado de novas medidas processuais compromete-se com a proteção dos direitos humanos fundamentais, incluindo o direito à intimidade e à vida privada, que devem ser ponderados com os interesses públicos da investigação no caso concreto.

Com relação aos elementos transnacionais ou internacionais dos crimes informáticos, deve-se ter em conta a importância da agilidade da cooperação internacional e a otimização dos procedimentos, o que pode ser feito por meio da

elaboração de acordos de cooperação mútua para se alcançar resultados, assim como a adoção de medidas comuns de prevenção.

O que precisa ser estudado é a implementação de medidas preventivas concomitantemente com medidas legais restritivas ou punitivas cabíveis nos casos mais graves.

Ao mesmo tempo, devemos chamar a atenção para o perigo da utilização do direito penal enquanto instrumento punitivo para incrementar o controle do Estado sobre a população, especialmente quando se trata do mais democrático e livre meio de comunicação que já foi criado – a Internet.

Outro ponto a ser refletido é qual o tipo de sociedade que queremos, diante do exemplo dos Estados Unidos após o *Patriotic Act*, editado sob a emergência dos atentados de 11.09.2001, que acabou com a privacidade das comunicações em território americano a pretexto de combater o terrorismo. Afinal, a utopia de Bentham da prisão onde os presos ficariam sob vigilância 24 horas é facilmente concretizada com as novas câmeras de vídeo, e o panóptico tal como idealizado por ele é a Prisão de Guantânamo hoje.

Desta forma, com relação à escolha das medidas processuais de investigação desse tipo delito, assim como referido na Convenção Européia sobre Crimes Cibernéticos, deve ser garantido o equilíbrio entre os interesses da repressão e o respeito aos direitos humanos fundamentais, incluindo o direito de todos à liberdade de expressão, que inclui a liberdade de buscar, receber e compartilhar informações e idéias de todos os tipos, independentemente de fronteiras, além do direito à intimidade e privacidade, e ao sigilo de dados, todos garantidos pela nossa Constituição.

A criminalização de condutas e a agilização dos procedimentos investigatórios não devem ser utilizadas como subterfúgio para limitar a liberdade de expressão e de comunicação que é a essência da rede de computadores Internet, uma das maiores conquistas da humanidade.

Com as novas tecnologias criou-se um verdadeiro paradoxo: liberdade mais ampla de comunicação e de expressão, de organização (vide passeatas e movimentos sociais que se utilizam das novas tecnologias), mas ao mesmo tempo essa tecnologia é cada vez mais utilizada para vigiar e controlar pessoas, assim como para praticar delitos.

Dentro desta reflexão, essencial o aprofundamento da reflexão sobre o tema dos crimes informáticos não só sob a ótica do direito penal, mas sim das ciências criminais em geral, e incluir um enfoque criminológico, de modo a se compreender a ampla realidade do fenômeno de modo amplo, auxiliado pela política criminal, no estudo de métodos de prevenção, e questionar a necessidade de criminalização de determinadas condutas. Esse estudo deve ser feito levando-se em conta a realidade brasileira inserida no contexto global da sociedade da informação, procurando-se minimizar os riscos de condutas danosas ao meio social, mas sem abrir mão de princípios, garantias e liberdades individuais, o que constitui nosso maior desafio hoje.

Bibliografia

BAUMAN, Zigmund. *Globalização*: as conseqüências humanas. Rio de Janeiro: Jorge Zahar, 1999.

BUSCH, Cristina. *Computer-based crimes against intellectual property*. 2003. Trabalho apresentado no AIDP Colloquium on Cybercrime, Atenas, Grécia, abril de 2003.

COUNCIL OF EUROPE. *Convention on cybercrime*. Disponível em: <www.conventions.coe.int/treaty/em>.

FAGGIOLI, Gabriele. *Computer crimes*. Napoli: Esselibri, 1998.

GIDDENS, Anthony. *O mundo na era da globalização*. Lisboa: Presença, 2000.

GOMES, Luiz Flávio. Crimes informáticos: primeiros delitos e aspectos criminológicos e político-criminais. Disponível em: <www.direitocriminal.com.br>.

_____. *Interceptação telefônica*. São Paulo: RT, 1997. p. 176.

GOMEZ, Pedro J. Montano. Delitos informáticos y los tipos que exigen la cosa ajena mueble. In: PENTEADO, Jaques de Camargo (Coord.). *Justiça criminal moderna*. São Paulo: RT, 2000. p. 334-348.

GONÇALVES, Maria Eduarda. *Direito da informação:* novos direitos e formas de regulação na sociedade da informação. Coimbra: Almedina, 2003.

GOUVEA, Sandra. *O direito na era digital:* crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997.

GRECO FILHO, Vicente. *Interceptação telefônica.* São Paulo: Saraiva, 1996.

GUEIROS JR., Nehemias. *Cyberlaw*: novas regras terão que ser globais. *Revista Justilex*, ano 2, n. 18, p. 26, jun. 2003.

ICOVER, David; SEGER, Karl; VONSTORCH, William. *Computer crime:* a crime fighter's handbook. Sebastopol, CA: O'Reilly & Associates, 1995.

KASPERSEN, Henrik W. K. *Gathering electronic evidence*. 2003. Trabalho apresentado ao AIDP Colloquium on Cybercrime, Atenas, Grécia, abril de 2003.

_____. *The evolution of cybercrime*: where does it end? Trabalho apresentado ao 13th World Congress on Criminology, Rio de Janeiro, agosto de 2003.

LERMA, Esther Morón. *Internet y derecho penal: hacking* y otras conductas ilícitas en la red. Pamplona: Aranzadi, 1999.

MARTÍN, Ricardo M. Mata y. *Delincuencia informática y derecho penal.* Madrid: Edisofer S.L., 2001.

NOVECK, Beth Simone. *Self-regulation, user protection and media competence.* Trabalho apresentado no European Forum on Harmful and Illegal Cybercontent. Strasbourg, Council of Europe, 28.11.2001.

PARKER, Donn B. *Fighting computer crime*. New York: Wiley Computer, 1998.

PEASE, Ken. Crime prevention. In: MAGUIRE, Mike; MORGAN, Rod; REINER, Robert (Org.). *The Oxford Handbook of Criminology*. 2. ed. Oxford: Clarendon, 1997. p. 963-995.

PIRAGOFF, Donald K. Computer crimes and other crimes against information technology in Canada. *Revue Internationale de Droit Pénal*, Paris, vol. 64, p. 201-250, 1993.

_____. *International cooperation in combating cyber-crime and cyber-terrorism*. Trabalho apresentado ao AIDP Colloquium on Cybercrime, Atenas, Grécia, abril de 2003.

RAHAL, Flavia; GARCIA, Roberto Soares. Crimes e Internet: breves notas aos crimes praticados por meio da rede mundial e outras considerações. *Boletim IBCCrim*, São Paulo, vol. 9, n. 110, p. 8-9, jan. 2002.

ROQUE, Sergio Marcos. Crimes de informática e investigação policial. In: PENTEADO, Jaques de Camargo (Coord.). *Justiça criminal moderna*. São Paulo: RT, 2000. p. 309-333.

SIEBER, Ulrich. Computer crimes and other crimes against information technology. *Revue Internationale de Droit Pénal*, Paris, vol. 64, p. 67-77, 1993.

VIANO, Emilio C.. Computer crimes and criminal law: international approaches and dilemmas. Trabalho apresentado ao AIDP Colloquium on Cybercrime, Atenas, Grécia, abril de 2003.

SILVA, Rita de Cássia Lopes da. *Direito penal e sistema informático*. São Paulo: RT, 2003.

THE ECONOMIST. "E-mail spam: filter it out". p. 61, 19.10.2002.