OS DESAFIOS DO CRIME CIBERNÉTICO[1]

SUSAN N. HERMAN[2]

Definindo o problema

O Departamento de Justiça dos Estados Unidos define o crime cibernético amplamente como "quaisquer violações de leis criminais que envolvam, para sua perpetração, investigação ou persecução, o conhecimento de tecnologia de computador." Essa ampla definição traz um número de diferentes tipos de problemas. Primeiro, computadores podem ser o objeto de um crime. Por exemplo, alguém pode roubar um computador ou um programa (*software*) de computador. Em segundo lugar, computadores podem ser o sujeito de um crime. Por exemplo, alguém pode introduzir um vírus ou invadir o computador de alguém e alterar os seus arquivos para danificar, ou para ganho pessoal ou financeiro. Terceiro, computadores podem servir como instrumento para o cometimento de um crime. Por exemplo, alguém pode usar um computador para invadir e comprometer um sítio da *Internet* (*website*). Computadores, especialmente "*websites*" e "*e-mails*" individuais, podem também conter provas do cometimento de todo tipo de crimes.

Muitos dos crimes cometidos dentro dessas categorias sobrepostas são, na verdade, apenas exemplos modernos de crimes tradicionais. O roubo de um computador, por exemplo, pode ser facilmente processado com base na legislação tradicional de roubo. O

[1] **Tradução** livre de Rafaela Dutra de Oliveira, aluna da UFRGS; revisão Professor Odone Sanguiné, com a colaboração de Laura Martins Miller e Érico Teixeira de Loyola.

[2] **Professora de Direito da Brooklyn Law School – New York.**

empregado de um banco que usa seu computador para desviar fundos do banco pode ser processado com base na legislação sobre apropriação indébita. Porém, nem sempre as leis criminais tradicionais se ajustarão ao crime de computador. Tentativas anteriores para aplicar leis criminais pré-existentes a crimes relativos a computador se revelaram freqüentemente desatualizadas. Algumas jurisdições tentaram processar '*hackers*'[3] que causaram danos alterando um sítio da *internet* atingido pelo crime de dano (*criminal mischief*). No entanto, as legislações relativas ao crime de dano foram elaborados para atos que causassem dano relativamente menor e geralmente classificavam tais infrações como pequenos delitos. O vasto alcance da Internet aumenta exponencialmente o dano potencial que um indivíduo pode causar com um ato danoso (em um mês recente, estatísticas mostraram que vírus introduzidos em computadores custaram US$ 3,5 bilhões, em despesa e em perda de produtividade). Quando as jurisdições tentaram processar os '*hackers*' com base em leis mais graves, por roubo de serviços, por exemplo, as Cortes se enredaram em refinamentos de interpretação da lei, discutindo se algo de valor havia sido roubado se o '*hacker*' acessasse erroneamente o computador de outro e simplesmente alterasse os arquivos sem proveitos financeiros. Os acusados poderiam levantar argumentos acerca do que os americanos chamam "legalidade" – isto é, se uma lei, neste tipo de persecução, estava sendo estendido além de uma interpretação razoável com a finalidade de abranger um novo comportamento, e se essa lei oportuniza-lhes, com uma antecedência justa, a informação de que aquela conduta particular era proibida. Definições clássicas de roubo, por exemplo, freqüentemente limitam a definição de roubo à privação física de outro de desfrutar de sua propriedade. Em um crime de computador, alguém pode, erroneamente, copiar um programa ou arquivo sem privar o seu dono do uso deste. Os acusados poderiam

[3] *Nota do revisor*: *hacker*: alguém que é capaz de usar ou modificar a informação no sistema de computador de outrem seu conhecimento ou permissão.

alegar que eles não privaram os donos de nada de valor e, portanto, não poderiam ser processados com base nas leis sobre crime de roubo.

O crime cibernético (*computer crime*) possui, em alguns aspectos, caráter freqüentemente diferente dos crimes tradicionais abrangidos por leis proibindo condutas como roubo ou fraude. Crimes cometidos por meio de computador não estão restritos por limites físicos ou, até mesmo, temporais da mesma forma que o crime tradicional normalmente o é. Um ladrão de banco pode roubar apenas um número finito de bancos em uma semana. Se há algum limite de número de computadores que uma pessoa pode infectar com um vírus em determinado período, é, no entanto, uma imagem astronômica. O risco de programas de computador serem roubados ou copiados é maior do que o risco de roubo físico de um item de propriedade pessoal, uma vez que essas "subtrações" por meio de computador freqüentemente não são detectáveis. Alguém cujo carro ou carteira é subtraída saberá do furto e será capaz de informá-lo. A vítima também poderá ser capaz de descrever o gatuno ou fornecer pistas de sua identidade. Se os agentes de crimes de computadores realmente acreditam que eles não serão capturados e que não é nem mesmo provável que os seus crimes serão descobertos, eles não serão tão facilmente detidos. Por causa do vasto potencial de custo de um crime de computador, algumas leis adotaram propostas que enfatizam a prevenção antes que a prisão e punição de tais crimes. Além disso, dada a natureza da '*Internet*', noções tradicionais de jurisdição geográfica tornaram-se ultrapassadas e inúteis. Um crime pode ser iniciado em uma cidade, município ou País, mas atingir alvos em todo o mundo. E assim a tradicional suposição nos Estados Unidos de que os estados estarão na vanguarda da persecução de crimes contra seus cidadãos não tem sustentação. Enquanto os estados podem processar os roubos tradicionais, é recomendável estabelecer leis federais rígidas criando um tratamento uniforme aos crimes de

computador. Apesar de muitos estados americanos possuírem leis específicas sobre a persecução de crimes cibernéticos, e de aplicarem as suas tradicionais leis criminais a vários crimes envolvendo computadores, o problema do crime cibernético tornou-se amplamente o tema da legislação e execução federais especiais. O trabalho do governo federal nessa área pode ser geralmente considerado como o de mais alto nível de desenvolvimento.

A Lei – básica: Lei de Proteção à Infra-estrutura Nacional da Informação de 1996

Quando os Estados Unidos decidiram confrontar diretamente o problema do crime de computador, durante a década de 1980, o Congresso não revisou sistematicamente o código criminal e atualizou as possíveis centenas de leis que poderiam ser aplicadas a um crime relacionado a computador se eles fossem modificados. Ao invés disso, o Congresso criou um expansivo esquema estatutário federal, começando com a Lei anti-pirataria e acesso e abusivo de Computador ('*Counterfeit Access Device and Computer Fraud Abuse Act of 1984*'). Os principal objetivo era definir novos crimes nos quais os computadores eram os sujeitos dos crimes, onde não existisse nenhuma outra lei criminal análoga. A lei federal foi alterada desde então. A principal Lei Federal abrangendo agora o crime cibernético visando computadores é a Lei de Proteção da Infra-estrutura da informação ('*National Information Infrastructure Protection Act of 1996*'). Os objetivos dessa Lei são a proteção da confidencialidade, integridade e disponibilidade de dados e sistemas. A Lei, codificada na 18ª Seção, n. 1030, do Código dos Estados Unidos da América, proíbe sete diferentes tipos de condutas contra "computadores protegidos" (uma definição ampla, que inclui qualquer computador conectado à *Internet*). As referências legais ao comércio inter-

estadual são explicadas pelo fato de que o governo federal somente limitou jurisdição comparativamente aos estados, e uma das principais fontes dessa jurisdição é o impacto no comércio inter-estadual. Os sete tipos de condutas proibidas são, em síntese:

1. Acessar arquivos de computador sem autorização e transmitir informação governamental confidencial, 1030(a)(1),

2. Obter, sem autorização, informação de instituições financeiras, dos Estados Unidos, ou de computadores privados usados em comércio inter-estadual, 1030(a)(2),

3. Intencionalmente, acessar computadores do Departamento dos Estados Unidos da América, ou de escritório privado, 1030(a)(3),

4. Acessar um computador protegido sem autorização com a intenção de fraudar e obter algo de valor, 1030(a)(4),

5. Conscientemente causar a transmissão de um programa, código ou comando e, como resultado, causar intencionalmente dano a um computador protegido, ou intencionalmente acessar um computador protegido e causar dano, mesmo se o dano não é intencional, 1030(a)(5) conforme modificado pela recente Lei Anti-terrorismo (‘*USA Patriot Act*’). (Este é um crime graduado e outras subseções dessa proibição tratam da conduta indiferente e negligente, com diferentes, graduados limites dos requisitos de dano).

6. Com a intenção de fraudar, traficar senhas que poderiam permitir acesso não autorizado a computador do governo, ou afetar o comércio inter-estadual ou estrangeiro, 1030(a)(6), e

7. Transmitir, no comércio inter-estadual ou estrangeiro, qualquer ameaça de causar dano a um computador protegido com a intenção de extorquir algum valor.

Estudantes de direito penal e promotores, ao analisar cuidadosamente os diversos elementos dessas leis perceberão as respostas do legislador às questões mais fundamentais e comuns no direito criminal: quando um crime deve depender da intenção do agente, e quando deve depender da extensão do dano causado? como devem os crimes serem classificados? Com base no "*National Information Infrastructure Protection Act*" (NIIPA), as penas variam principalmente com base no fato de se a pessoa condenada é um criminoso iniciante ou reincidente. Por exemplo, a violação da primeira seção, 1030(a)(1), possui pena máxima de dez anos para o réu primário, e de 20 anos para o reincidente. A lei também distingue nas suas penas entre a conduta que envolve simplesmente o acesso impróprio a um computador e aquela conduta cujo acesso é usado para propósitos nocivos, aumentando a pena máxima prevista em cinco anos se o crime foi cometido para obter ganho financeiro ou vantagem comercial. As diretrizes federais para imposição de penas ("*Federal Sentencing Guidelines*") também regulam as punições para condenações com base nessas e outras leis, dependendo da variedade de fatores não arrolados nas próprias leis.

Exemplos de Persecuções Criminais

Eis alguns exemplos de casos em que o Departamento de Justiça processou com base nesta e outras leis.

O "'*Hacker*' Profissional" (*The Career Hacker*). Kevin Mitnick admitiu ter invadido computadores por quase toda sua vida, não para lucro financeiro, mas para provar

que ele era capaz de fazê-lo. Ele foi preso e condenado pela primeira vez por fraude de computador em 1989 e recebeu uma condenação permanecendo em liberdade condicional sob a condição de que não mais usasse tecnologia. Quando foi descoberto que violou esta condição por possuir um 'telefone celular clonado' (um telefone celular ligado à conta de outra pessoa), ele foi condenado a vinte e dois meses de prisão. Depois de sua soltura, ele retornou à sua atarefada agenda de invasor de computadores e tornou-se o criminoso de computadores mais procurado do mundo. Capturado e processado novamente em 1999, ele admitiu sua culpa por quatro acusações de fraude eletrônica, duas acusações de fraude em computador, e uma acusação de interceptação ilegal de comunicação telefônica. Dessa vez, ele foi condenado a quarenta e seis meses de prisão. Durante os dois anos e meio entre suas prisões, Mitnick admitiu ter invadido sistemas de computador e roubado a propriedade de softwares pertencentes a grandes empresas. Ele admitiu ter cometido esses crimes usando uma variedade de ferramentas, incluindo telefones celulares clonados, programas "farejadores" colocados nos sistemas do computador da vítima e programas de *hacker*. Ele até admitiu ter alterado os sistemas do computador da Universidade da Califórnia e ter armazenado lá seus programas obtidos desonestamente. Ele também roubou *e-mails*, sistemas monitorados de computador, e imitou empregados de suas empresas alvo, incluindo Nokia, na sua tentativa de conseguir o programa que estava sendo desenvolvido por essas companhias[4].

'O vingador" (*The Avenger*). Andrew Garcia tinha sido um administrador de sistemas de uma grande empresa de tecnologia na Califórnia. Ele foi despedido pela empresa e, duas semanas depois, ele usou as senhas da companhia para invadir a rede de

[4] Para maiores informações, veja *United States v. Kevin Mitnick, Press Release, U.S. Department of Justice, August* 9, 1999, disponível em http://www.cybercrime.gov/mitnick.htm.

computadores e eliminar dados importantes. Esse ato causou a queda da rede e danificou as operações estrangeiras da firma. Garcia foi considerado culpado por acessar um computador protegido e ter, com indiferença, causado dano, e foi sentenciado a um ano de prisão[5].

"O extorsionista profissional" (*The International Extortionist*). Oleg Zezev, um cidadão do Cazaquistão, invadiu computadores pertencentes a Bloomberg LLP e roubou informações confidenciais sobre a companhia e seus clientes e, então, usou essas informações para tentar extorquir US$ 200.000 do fundador da empresa, Michael Bloomberg (que depois se tornou prefeito de Nova Iorque). Ele foi preso depois que os oficiais do FBI rastrearam o *e-mail* da ameaça de extorsão até uma conta de *e-mail* do *Hotmail*. Apesar de Zezev ter registrado a conta com um nome falso, o FBI foi capaz de usar os registros de acesso para rastrear a conta e chegar à empresa para a qual Zezev trabalhava. Bloomberg então mandou um *e-mail* a Zezev dizendo que pagaria o dinheiro solicitado, mas somente se Zezev se encontrasse com ele e com seus especialistas em computador em Londres para explicar como Zezev tinha acessado as informações. Quando Zezev chegou a Londres para o encontro, ele foi preso. Depois de um julgamento de três semanas e meia, ele foi condenado por conspiração para cometer extorsão, tentativa de extorsão, ameaça de extorsão e invasão de computador, e recebeu uma condenação de cinqüenta e um meses, uma das mais longas penas que foram impostas por atividades de crime cibernético.

Outras leis federais

[5] Veja *United States v. Andrew Garcia*, Press Release, U.S. Department of Justice, February 2004, disponível em http://www.cybercrime.gov/garciaSent.htm.

Além do NIIPA e de leis criminais tradicionais que, às vezes, englobam crimes de computador, há outras leis criminalizando aspectos específicos do crime de computador. Por exemplo, a Lei de proteção à privacidade das comunicações Eletrônicas ('*Electronic Communications Privacy Act of 1986*') tem como objetivo o problema da invasão, atualizando proibições federais pré-existentes contra interceptações de comunicações eletrônicas e proibindo a obtenção, alteração ou prevenção de acesso autorizado a "depósito" eletrônico, incluindo *e-mail*. Apesar dessa lei ter sido usada para processar *hackers*, a sua função principal tem sido a de fortalecer a privacidade dos usuários de computadores, e de permitir aos funcionários públicos usarem fiscalização eletrônica na investigação de crime de computador.

Outras leis federais lidam com o problema específico da violação de direitos autorais. A pirataria de aplicações de computadores pessoais resultaram, nos Estados Unidos, em perdas de mais de US$ 1,8 bilhão em um único ano (2001). A Lei de Violação de Direitos Autorais, Seção 17, 506 (a) do Código dos Estados Unidos (alterada pela Lei de combate à subtração eletrônica ('*No Electronic Theft Act*'), proíbe a cópia e distribuição ilegais de programa ou outro material por computador se um direito autoral válido existir, o acusado infringe o direito autoral, agindo intencionalmente, e o acusado dentro de cento e oitenta dias reproduz no mínimo dez cópias de um ou mais trabalhos registrados com um total de prejuízo de US$ 2.500. Essa lei reflete uma tentativa de contemplar os casos mais sérios de pirataria e não de utilizar fontes federais para processar toda pessoa que copia um programa de computador de um amigo. A Lei de proteção dos Direitos Autorais da era digital ('*Digital Millennium Copyright Act of 1998*'), seções 17, 1201 – 1205 do Código dos Estados Unidos, bane o uso de computadores e outros meios eletrônicos com o intuito de infringir direitos autorais em trabalhos tradicionais. Essa lei visa não o ato da pirataria,

mas o tráfico de tecnologia ou dispositivos especialmente concebidos ou produzidos para contornar as medidas tecnológicas utilizadas para proteger direitos autorais de obras registradas. Em decorrência do fato de os serviços de *Internet* poderem ser usados, sem o conhecimento ou participação de seus administradores, para tais propósitos, o ato dá uma garantia de defesa se os provedores não sabem ou não se beneficiam do uso dos seus serviços.

A Lei Nacional contra apropriação ilicita de propriedade (‘*National Stolen Property Act*’), seção 18, 2314 do Código dos Estados Unido, proíbe o transporte de comércio inter-estadual de qualquer bem avaliado em US$ 5.000 ou mais, o qual foi sabidamente apropriado ou obtido de forma fraudulenta, incluindo transferências de fundos fraudulentos de computador. Leis acerca de fraude de correio eletrônico que proíbem o uso de mensagens ou comunicações de rede entre Estados para barrar um esquema fraudulento de obter dinheiro ou propriedade de bens, têm sido aplicadas pelas Cortes para o caso de crimes cibernéticos.

Em três ocasiões distintas, o Congresso já aprovou legislação buscando proibir pornografia infantil e a publicação na internet de materiais que pudessem ser inapropriados para crianças. Todo, ou parte de cada uma dessas leis foi considerada inconstitucional pelas Cortes, geralmente porque as definições das condutas eram vagas e poderiam ter conseqüências não intencionais de criminalizar a publicação de uma série de materiais por e para adultos, incluindo informações sobre abortos, postadas por várias bibliotecas, e

comunicações entre adolescentes homossexuais, ou poderia intimidar as pessoas de postarem tais materiais expressamente protegidos constitucionalmente[6].

Problemas de execução

Por sua própria natureza, crimes cibernéticos são difíceis de serem investigados. Muitas vítimas não denunciam crimes cibernéticos simplesmente porque elas não sabem que estes ocorreram. Outras vítimas, especialmente empresários, talvez não queiram informar que foram vítimas porque eles não querem que o público ou seus clientes saibam que o seu sítio da *Internet* ou seus registros empresariais não são seguros. Os perpetradores podem permanecer anônimos e serem difíceis de rastrear. Mesmo se um *hacker* for rastreado em um computador particular, o dono do computador pode negar ter sido a pessoa que utilizou o computador para um propósito ilícito. Os dados podem ser criptografados e difíceis de ler. Há soluções tecnológicas para alguns desses problemas (como o descubridor de chave "*loggers*"[7], que podem rastrear dados digitados ('*keystrokes*') feitos em um determinado computador, mesmo se o que foi digitado não foi salvo). Muitos promotores não têm familiaridade suficiente com a tecnologia envolvida para serem capazes de compreender os desafios tecnológicos envolvidos no rastreamento de *hackers*, piratas de programas de computador e outros criminosos de computador.

[6] Veja *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) (invalidando a Lei de Comunicações Decentes ('*Communications Decency Act of 1996*') na medida em que proibia a transmissão de materiais indecentes ou manifestamente ofensivos a menores através da *Internet*); *Ashcroft* v. *ACLU*, 124 S. Ct. 2783 (2004) (injunção preliminar contra a Lei de Proteção à criança que acessa a Internet ('*Child Online Protection Act of 1998*'), que proibía a distribuição comercial de material que é nocivo a menores por meio da *Internet*, foi afirmado porque o governo não havia demonstrado que mecanismos filtradores seriam uma alternativa menos restritiva para servir aos propósitos do Congresso; o caso foi arquivado para maiores procedimentos); *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) (encontrou disposições inconstitucionais na Lei de Prevenção à Pornografia Infantil ('*Child Pornography Prevention Act of 1996*'), a qual criminalizava a produção, distribuição e recepção de imagens sexuais de crianças criadas por computador – imagens que poderiam não ser de crianças – por ser vago e abrangente).

[7] *Nota do revisor*: *Logger* – dispositivo que reconstrói tudo que foi digitado, mesmo que não tenha sido salvo.

Regras de prova, algumas vezes, precisam ser adaptadas à prova gerada pelo computador, e às vezes os promotores precisam aprender como adaptar regras de prova quando recolhe e usa prova obtida de computadores.

O problema da perícia tem sido tratado nos Estados Unidos por meio da criação de agências federais ou suas divisões com especialistas que podem utilizar os avanços tecnológicos às suas técnicas de investigação, e que podem ajudar os agentes responsáveis pela aplicação da lei local e estadual, e laboratórios forenses regionais. O FBI, por exemplo, tem uma nova divisão de crime cibernético, cujo papel é coordenar investigações de crimes de computador. O Departamento de Justiça tem uma divisão uma divisão especial chamada CCIPS (pronunciado como '*Seesips*'), o que significa Seção de Crime de Computador e Propriedade Intelectual. Os procuradores dos Estados Unidos, os promotores federais locais, formaram uma unidade especial chamado CHIP (*Computador Hacking and Intellectual Property*) para fornecer treinamento especializado e para coordenar os seus esforços.

Há uma série de situações em que uma pessoa sem experiência pode atrapalhar um inquérito. Se um computador está ligado, por exemplo, desligá-lo pode alterar ou perder alguns dos dados no disco rígido, e, assim, corromper os dados. O investigador pode resolver este problema fazendo uma cópia 'somente leitura' ('*read-only*') do disco rígido e deixar o disco rígido original rodando sozinho. Há questões sobre como estabelecer uma adequada cadeia de guarda para provar que a informação recuperada a partir de um computador é exata e confiável. Legisladores bem intencionados também cometeram erros devido à sua falta de conhecimento técnico. Por exemplo, legisladores que visaram a

proteger os usuários de *Internet*, inadvertidamente implementaram legislação que proíbe a utilização de proteções de uma rede de '*firewalls*'[8].

Envolvimento do setor privado e alternativas de direito não criminal

Os Estados Unidos da América descobriram que uma grande parte da sua infra-estrutura vital – telecomunicações, energia, serviços de emergência, a *Internet*, sistemas financeiros – é gerido pelo setor privado. Em 1998, o Presidente Bill Clinton emitiu uma instrução ordenando agências federais e membros do setor negocial a formarem o Centro Nacional de Proteção de Infra-estrutura, uma organizada coligada para avaliar e investigar ameaças à infra-estrutura da informação. Em 1992, a Aliança de Programas de Computadores Empresariais, grupo comercial da indústria de *software*, começou um programa internacional de execução de direitos autorais, envolvendo tanto associações comerciais nacionais de *softwares* como associações comerciais e de aplicação da lei, para encontrar métodos de prevenção de pirataria de programas de computador. Esses esforços já resultaram em uma queda significativa, embora certamente não a eliminação, de pirataria de programas de computador[9]. A Força Tarefa de Segurança da Pátria ('*Homeland Security Partnership Task Force*'), uma outra coligação governamental/privada, também visa prevenir delitos de computador recomendando as melhores práticas, através da fixação de normas de segurança cibernética, e utilizando ferramentas de varredura de códigos para identificar defeitos de programas de computador. A Lei contra fraude abusiva de computador ('*Computer Fraud Abuse Act*') prevê recursos civis que particulares e empresas podem aplicar para procurar danos, como uma alternativa ao processo penal. Alguns analistas sugeriram que fazer os distribuidores de programas de

[8] *Nota do revisor*: dispositivo que barra o acesso a determinado sítio/arquivo no computador.
[9] Vide *http://www.bsa.org*.

computador responsáveis suscetíveis por permitir a pirataria dos seus produtos poderia resultar no investimento da indústria em prevenção, a um nível que não está agora em seus melhores interesses econômicos. Outros notaram que fornecendo uma indenização para os danos civis para as vítimas poderia fazer com que estas ficassem mais dispostas a denunciar os crimes de computador, se elas pudessem esperar alguma compensação financeira e controlar os seus próprios procedimentos legais.

Esforços internacionais

A maioria dos países industrializados alterou a sua legislação para fornecer proteção à privacidade, para processar os crimes econômicos, e para proteger a propriedade intelectual. Muitos países adotaram leis semelhantes à Lei de Fraude e Abuso de Computador direcionadas ao acesso não autorizado e à manipulação de dados e sistemas. Além disso, muitos países concluíram que, pelas mesmas razões que os Estados Unidos da América pensavam que uma abordagem nacional, coordenada e uniforme para o crime de computador era desejável, a cooperação internacional também o seria. Além de fornecer cooperação nas investigações e processos, ter uniformes fontes legislativas também facilita a coleta de dados sobre o crime cibernético e sobre que mecanismos de execução estão provando serem efetivos.

Em 23 de Novembro de 2001, os Estados Unidos da América e trinta e três outros países (principalmente europeus, além de Japão, África do Sul, e Canadá), em reunião em Budapeste, assinaram o Tratado do Conselho da Europa sobre '*cybercrime*'. Este tratado obriga os seus signatários a (1) criar leis materiais tratando do crime cibernético, (2) fornecer aos seus agentes da aplicação da lei autoridade suficiente para efetivamente investigar crimes cibernéticos, incluindo mecanismos de autorização para procurar e

apreender computadores, e habilitá-los a ordenar aos provedores da *Internet* a preservarem registros em conexão com uma investigação e (3) oferecer cooperação internacional para outros países signatários em seus esforços de combate ao crime cibernético. Embora os Estados Unidos tenham assinado este Tratado, este ainda não é uma lei eficaz nos Estados Unidos da América porque ainda não foi ratificado pelo Senado. A situação é a mesma na maioria dos outros países signatários.

Críticas

Finalmente, uma palavra sobre algumas das ramificações das liberdades civis e questões levantadas no âmbito da Constituição dos Estados Unidos da América pelo Tratado e pela legislação nacional. Alguns críticos do tratado do Conselho da Europa estão preocupados com o fato de o Tratado não exige a 'dupla incriminação'. Em outras palavras, o País A pode ser solicitado a ajudar o país B para investigar as ações que constituem crime no país B, mas não no País A. Alemanha, por exemplo, incriminou a conduta de negar a realidade histórica do holocausto. Nos Estados Unidos, tal afirmação, como muitas formas de 'discurso de ódio' ('*hate speech*'), que violariam as leis de alguns países, seria uma expressão constitucionalmente protegida sob a Primeira Emenda. O Departamento de Justiça norte-americano responde que há uma exceção no Tratado permitindo aos países membros declinarem o pedido de realizarem vigilância quando solicitados a fazê-lo se entenderem que isso prejudicaria os 'interesses fundamentais' da nação, o que poderia ser interpretado de forma a incluir a liberdade de expressão constitucionalmente protegida. A Primeira Emenda também provou ser um grande obstáculo às tentativas do Congresso de limitar a exposição das crianças a material pornográfico porque se revelou difícil esboçar um lei que limitasse o acesso das crianças

sem limitar também o acesso de adultos aos materiais que estes têm o direito de ver ou remeter pelo Correio.

A Quarta Ementa da Constituição norte-americana limita a capacidade do governo de realizar buscas ou apreensões na ausência de um mandado de busca baseado numa provável causa e assinado por um magistrado imparcial. A lei antiterrorismo ('*USA Patriot Act*'), ao proporcionar maiores poderes investigatórios para o governo federal, incluindo permissão governamental de obrigar provedores da *Internet* a fornecer informações sem um mandado judicial baseado numa causa provável, está testando os limites da Quarta Emenda de um modo que os tribunais americanos ainda não examinaram.

Bibliografia

The website of the cybercrime unit of the US Department of Justice, http://www.cybercrime.gov, é um repositório de leis, jurisprudência, e outras informações aplicativas sobre rastreamento de *hackers* de computador, etc. Other sources of information on US federal government efforts: COMPUTER CRIME & INTELL. PROP. SECTION - CRIMINAL LAW, U.S. DEP'T OF JUSTICE, PROSECUTING INTELL. PROP CRIMES, http://www.usdoj.gov/criminal/cybercrime; National Institute of Justice, US Dep't of Justice, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 2 (1989); Stephen P. Heymann, *Legislating Computer Crime*, 34 HARV. J. ON LEGIS. 373 (1997); U.S. Sentencing Commission, *Computer Fraud Working Group, Report Summary of Findings* (1993); U.S. Copyright Office, *Summary, The Digital Millennium Copyright Act of 1998*, http://lcweb.loc.gov/copyright/legislation/dmca,pdf; the Congressional Research Service, também disponível *online*, fornece análises úteis de diversas leis federais. Ferramentas úteis a respeito da pesquisa sobre computadores é oferecida em http://www.cybercrime.gov/searchmanual.htm.

Other useful websites and periodicals: Business Software Alliance, http://www.bsa.org, incluindo *Seventh Annual BSA Global Software Piracy Study* (2002); http://www.attrition.org (onde os hackers podem se 'vangloriar' de suas próprias ações); Cyber-Rights and Cyber-Liberties, http://www.cyber-rights.org/cybercrime; CYBERSPACE LAW, uma revista incluindo um artigo sobre *Coordinated Efforts to Attack Cybercrimes* in volume 3, No. 1 (1998); FED. COMM. L.J., incluindo um artigo sobre *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?* in volume 50 at 117 (1997); COMPUTER LAW, incluindo um artigo de Clifford Miller, *Electronic Evidence - Can You Prove the Transaction Took Place?*, in volume 9, No. 5 (1992); COMPUTER AND INTERNET LAWYER, incluindo um artigo de Michael R. Levinson & Christopher E. Paetsch, *The Computer Fraud and Abuse Act: A Powerful New Way to Protect Information*, in volume 19 at 11 (2002) (propondo um direito privado de ação relativo à fraude em computador); e WEEK, incluindo um artigo sobre *IT Laws Defy Reality: When eight states propose laws that make it illegal to use a network firewall, it would nice if working IT professionals could laugh it off*, in volume 20, issue 15, 2003 WL 5735177 (destacando o problema de ter legisladores não familiarizados com o estágio teconológico); GOVERNMENT COMPUTER NEWS, incluindo um artigo sobre *Civil Law Might Beat Criminal Law at Protecting IT*, in volume 22, No. 7, 2003 WL 10987002 (propondo que tornar os distribuidores responsáveis pelas falhas em seus programas de computador seria mais efetivo que o direito criminal).

Some interesting articles: Neil Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003 (2001) (especialmente recomendado); Elizabeth Tutmarc, *The War on Cyberterror: Why Australia Should Examine the U.S. Approach to Critical Infrastructure Protection*, 123 PACIFIC RIM L. & POLICY J. 743 (2004) (discutindo a abordagem norte-americana sobre a cooperação entre os setores público/privado e propondo a adoção de similar abordagem na Austrália); Robert Ditzion, Elizabeth Geddes & Mary Rhodes, *Computer Crimes*, 40 AMERICAN CRIM. L. REV. 285 (2003); Amy Knoll, *Any Which Way*

but Loose: Nations Regulate the Internet, 4 TULANE J. INT'L & COMP. L. 275 (1996); Marc D. Goodman, *Why the Police Don't Care about Computer Crime*, 10 HARV. J. LAW & TECH. 465 (1997); John T. Soma, et al, *Transnational Extradition for Computer Crime: Are New Treaties and Laws Needed?*, 34 HARV. J. ON LEGIS. 317 (1997); Fred & Christine Galves, *Ensuring the Admissibility of Electronic Forensic Evidence and Enhancing Its Probative Value at Trial*, 19 CRIMINAL JUSTICE at 37 (Spring 2004).

Books: Jody Westby, INTERNATIONAL GUIDE TO COMBATING CYBERCRIME (American Bar Association 2003); Stanley S. Arkin, et al, PREVENTION AND PROSECUTION OF COMPUTER AND HIGH TECH. CRIME (1991).

Information on International Efforts: Council of Europe Convention on Cybercrime, disponível em http:conventions.coe.int/Treaty; REV. INT'L DE DROIT PENAL (periodical), incluindo *AIDP - Preliminary Colloquium, Computer Crime and Other Crimes Against Information Technology*, in volume 64 at 49 (1993), and Cole Durham, *The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm*, General Report for the AIDP Colloquium, in volume 64 at 79 (1993)..