SILVA, José Afonso da. *Curso de direito constitucional positivo*. São Paulo: Malheiros, 1996.

SUPLICY, Martha. A responsabilidade das TVs. *Folha de S.Paulo*, 24/11/97.

TOURINHO, Arx. A família e os meios de comunicação. *Revista da Procuradoria-Geral da República*, n. 6.

DOS CRIMES POR COMPUTADOR

Túlio Lima Vianna*

"Os computadores dominam o mundo, nós dominamos os computadores; logo, dominaremos o mundo" (GhOsT InVaDeR).[1]

Sumário

1 INTRODUÇÃO

O estudo interdisciplinar da Informática e do Direito apresenta-se como tarefa bastante árdua já que se baseia em dois ramos do conhecimento humano absolutamente distintos: de um lado, os números, a exatidão, a máquina, a Informática; do outro, as letras, a dialética, o homem, o Direito.

* Bacharel em Direito pela Faculdade de Direito da UFMG (turma de agosto de 1999).

1 Com esse irônico silogismo, o *hacker* Ghost Invader inicia seu *ezine* (*eletronic magazine*) *UHF – Unit Hacker Force* (jan/98). O arquivo-texto com o conteúdo do *ezine* pode ser baixado em http://members.xoom.com/ – XOOM/blackouthp/zines.htm

Cada qual aparenta para o outro ser um universo hermético, só acessível àqueles que se dispuserem a dedicar uma vida inteira ao estudo exclusivo daquela matéria. Mas se é verdade que não se pode exigir do homem moderno o conhecimento eclético que detinham Platão e Aristóteles, também é certo que as ciências humanas, e em especial o Direito, devem acompanhar as evoluções tecnológicas.

O surgimento de crimes realizados com o auxílio de computadores só vem confirmar essa necessidade. Ao Direito caberá criar normas que disciplinem esse novo poder que surge travestido de máquina. Para isso, Informática e Direito terão de se abrir um para o outro, pois, caso contrário, a sociedade estagnar-se-á, arraigando-se na segurança fornecida pelo Direito, ou caminhará para o caos na velocidade estonteante da evolução tecnológica.

O Direito brasileiro só agora parece despertar para essa urgente necessidade de criação de normas legais que disciplinem os crimes cometidos por meio de computadores. Nossa legislação não está conseguindo acompanhar a velocidade das inovações tecnológicas, e o princípio constitucional do *nullum crimen, nulla poena sine lege* proíbe expressamente que se crie crime por analogia. A doutrina também parece ignorar o problema e se detém diante das dificuldades que os conceitos técnicos da ciência da computação impõem ao estudo das questões legais pertinentes ao assunto. A jurisprudência, por outro lado, pouco se pronunciou a esse respeito, talvez porque a polícia, de modo geral, também não estejam tecnicamente preparadas para investigações de delitos cometidos por computador.

Nosso objetivo aqui será, principalmente, o de despertar nos operadores do Direito o interesse pelo estudo interdisciplinar da ciência jurídica e da informática, como forma de coibir os crimes cometidos com o auxílio de computadores.

Tais crimes apresentam-se de várias formas, destacando-se dentre eles a violação dos direitos autorais sobre *softwares*, o furto de tempo[2] e o dano

2 "No Estado americano de Virgínia, o Código Penal considera *propriedade* o tempo do computador ou de serviços de processamento de dados e, portanto, incrimina seu uso não autorizado" (REIS, Maria Helena Junqueira. *Computer crimes* – Criminalidade na era dos computadores, p. 30).

causado pelos famosos vírus de computador. Com o surgimento da Internet – rede mundial de computadores – o número desses crimes aumentou significativamente, como bem lembra Maria Helena Junqueira Reis:

> "A gama de delitos que podem ser perpetrados pela Internet é quase infinita. A lista inclui o mau uso dos cartões de crédito, ofensas contra a honra, apologia de crimes, como racismo, ou incentivo ao uso de drogas, ameaças e extorsão, acesso não autorizado a arquivos confidenciais, destruição e falsificação de arquivos, programas copiados ilegalmente e até crime eleitoral (propaganda não autorizada por exemplo) ,dentre outros."[3]

Evidentemente, pela própria limitação do espaço, não nos será possível abordar aqui todos eles. Escolhemos, então, três, por sua simplicidade técnica[4] e pela presença de legislação nacional vigente que cuida do tema, ainda que de forma incompleta.[5]

2 DA VIOLAÇÃO DE *EMAILS*

2.1 Do objeto

Email ou *eletronic mail* (correio eletrônico) é um termo usado para designar toda mensagem enviada através de uma rede de computadores para uma caixa postal eletrônica.

3 *Op. cit.*, 1996. p. 53.

4 Por se tratar de um artigo dirigido aos operadores do Direito, sempre que houver necessidade de esclarecimentos quanto a questões técnicas relacionadas aos delitos faremos uma breve explanação.

5 Vale lembrar que no universo da informática tudo evolui de forma muito rápida, e é possível que, quando este artigo vier a ser publicado, muitas das novas tecnologias aqui descritas estejam superadas e, conseqüentemente, novos delitos relacionados a computadores já tenham surgido.

O *modus operandi* dos *emails* é bastante simples. Alguém, a partir de um computador ligado a uma rede, redige uma mensagem num editor de *emails* e a envia para a caixa postal eletrônica do destinatário. Essa caixa postal nada mais é do que um arquivo de dados armazenado em um servidor que guarda todas as mensagens do usuário. Assim, quando este desejar acessar sua correspondência, deverá conectar-se ao servidor e "baixar" suas mensagens, ou seja, pedir ao servidor que envie as mensagens lá armazenadas para o seu computador. Nesse momento, deverá informar seu *login*, que é o nome pelo qual é conhecido na rede, e sua senha de acesso. O servidor irá então checar os dados, e só liberará o acesso às mensagens se estiverem corretos. Note-se que, no envio de um *email*, três computadores participam do processo: o remetente, que envia a mensagem; o servidor, que armazena a mensagem até que o destinatário a procure; e o destinatário, que busca a mensagem no servidor e a exibe para leitura.

Durante todo esse processo, porém, pessoas não autorizadas podem ter acesso a esses *emails*. Tais indivíduos acabaram ficando conhecidos pelo grande público como *hackers*, devido ao uso equivocado da palavra pela imprensa. Trata-se, na verdade, de denominação pouco técnica, fazendo-se necessária uma breve análise terminológica.

2.2 Do sujeito ativo

Hacker[6] é um termo de origem inglesa derivado do verbo *to hack* (cortar, cavar), que originalmente significava alguém que fabrica móveis utilizando um machado. No jargão da informática, pode ser traduzido livremente por "fuçador". É o indivíduo que se dedica a explorar os detalhes de sistemas programáveis. Profundo conhecedor de computadores, o *hacker* em geral domina muito bem o uso de sistemas operacionais como o Linux e o Windows, e programa em linguagens como *C* e *Assembly*, dentre outras. A especialidade dos *hackers*, no entanto, são as redes de computadores, em especial, a Internet.

Atualmente, com a popularização dos microcomputadores, o termo *hacker* acabou servindo para designar o intruso virtual que tenta obter acesso a informações confidenciais através de espionagem, por meio de quebra de segurança nas redes. Não se deve, porém, usar a palavra nesse sentido, pois os intrusos virtuais são, na verdade, denominados *crackers*.

Cracker[7] é o indivíduo que utiliza seus conhecimentos técnicos para "quebrar" todo e qualquer tipo de barreira de segurança. Numa definição simplista, poderíamos dizer que é o *hacker* "do mal". Os *crackers* podem ter como objeto de seus crimes a quebra do sistema de segurança de programas ou o acesso ilícito a informações armazenadas em computadores. Limitaremos, no entanto, nosso estudo ao acesso não autorizado a *emails*, que é uma das modalidades do acesso ilícito a computadores.

2.3 Dos fatos

Há uma falsa idéia dominante dentro do próprio mundo da informática de que os *crackers* agem durante a transmissão dos *emails* de um computador para o outro, obtendo, assim, uma cópia dessas mensagens. Nada mais equivocado. Na verdade, os *crackers* conseguem acessar os servidores e as caixas postais dos usuários, tendo, assim, acesso a todas as suas mensagens. Mas como conseguem esse acesso? Basicamente através da senha do próprio usuário ou, em alguns casos, da senha do administrador do sistema (*root*). Analisemos, *en passant,* o modo de agir dos *crackers*.

É fato notório a displicência com que os usuários criam suas senhas. A maioria preocupa-se tão-somente em criar uma combinação fácil de ser me-

6 Pronuncia-se "réquer".

7 Pronuncia-se "créquer".

morizada, sem pensar que, com isso, será também de fácil dedução por parte de pessoas mal-intencionadas. Muitos chegam ao extremo de usar como senha o mesmo nome do *login*. E os *crackers*, melhor do que ninguém, sabem disso. Assim, grande parte das invasões é cometida pela simples dedução da senha da vítima. Se o *login* de determinado usuário é *batman*, naturalmente a primeira senha que o *cracker* irá tentar para obter acesso ao sistema será *robin*. E, na maioria das vezes, obterá sucesso. Datas de nascimento, sobrenomes e nomes de pessoas próximas, como filhos e cônjuge, também são senhas bastante previsíveis. Se o *cracker* tiver acesso a essas informações do usuário, certamente irá tentá-las como primeira opção para descobrir a senha. É o que eles denominam ironicamente de "engenharia social".

Mas nem tudo é dedução no mundo dos *crackers*. Quando a lógica falha, eles recorrem à força bruta. Para tanto, criam programas que funcionam na base da tentativa e do erro, que são capazes de montar todo tipo de combinação de letras e números. O sistema funciona bem para senhas de até seis caracteres, mas é muito lento, pois as tentativas são feitas em períodos curtos e bem espaçadas para não despertar suspeitas. No Brasil, é um método muito difundido, pois as senhas, em geral, são simples, e dificilmente os computadores possuem sistema de proteção.

Outro método bastante comum é a invasão do servidor. Esta técnica requer conhecimentos avançados em informática, pois nesse caso o *cracker* não utiliza uma senha falsa, mas força sua entrada no servidor a partir de falhas no sistema operacional, através de métodos que, devido à sua complexidade, não nos cabe detalhar aqui. Após invadir o servidor, os *crackers* obtêm o arquivo que contém todos os *logins* e as senhas de acesso (em geral o /etc/passwd). Evidentemente esse arquivo estará criptografado, mas os *crackers* já criaram programas capazes de descriptografar a maioria das senhas. Baseiam-se tais programas num dicionário de senhas criado com palavras geralmente usadas para tal fim. Assim, o programa criptografa cada uma das palavras do dicionário de senhas e as compara com as senhas do arquivo conseguido no servidor. No momento em que encontra a igualdade, terá encontrado a senha do usuário. Notem que o processo é bastante rápido, pois o *cracker* copia o arquivo do

servidor e realiza toda a operação *off-line*, isto é, desconectado da rede, portanto, sem risco de ser rastreado posteriormente.

Um terceiro método bastante interessante é o uso de programas semelhantes a vírus, denominados *Trojan Horses* ou Cavalos de Tróia. Em lugar de destruir programas ou arquivos, os *trojan* monitoram a digitação do *login* e da senha da vítima e os gravam num pequeno arquivo que fica oculto no sistema. Quando o usuário se conecta à rede, o *trojan* envia um *email* para seu criador com o arquivo que contém o *login* e a senha do usuário.

Existe ainda uma infinidade de outros métodos cuja análise excederia os limites deste trabalho. Passemos, pois, à análise da legislação pertinente.

2.4 Do direito

A Constituição Federal de 1988 declara, no art. 5º, XII, que "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 (grifo nosso)."

O legislador constituinte mostrou-se atento às tendências dos modernos meios de comunicação e incluiu na norma constitucional a proteção à comunicação de dados. Os *emails* claramente enquadram-se nessa categoria, já que são uma forma de envio de dados através de uma rede de computadores.

O legislador de 1940, no entanto, não tinha como prever a existência de redes de computadores. Assim, na redação do art. 151 do nosso Código Penal, não consta qualquer expressão que sirva para tipificar o crime de violação de *emails*.[8]

8 "Art. 151. Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:
Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa.
§ 1º Na mesma pena incorre:

O Código Brasileiro de Telecomunicações (Lei n. 4.117 de 27 de agosto de 1962), no entanto, em seu art. 56, tipifica o crime de violação de *email*:

> "Pratica crime de violação de telecomunicações quem, transgredindo lei ou regulamento, exiba autógrafo ou qualquer documento ou arquivo, divulgue ou comunique, informe ou *capte*, transmita a outrem ou utilize o *conteúdo*, resumo, significado, interpretação, indicação ou efeito de *qualquer comunicação dirigida a terceiro* (Grifos nossos)."

O Dicionário Aurélio Eletrônico V.2.0 define captar:

> "[Do lat. *captare*.] V. t. d. **1.** Atrair, granjear, conquistar, empregando meios capciosos; **2.** Atrair, granjear, provocar, suscitar; **3.** Aproveitar ou colher nas nascentes (água corrente); **4.** Apanhar, colher; apreender, compreender."

O mesmo dicionário dá, entre outros significados, o seguinte conceito de comunicação: "Ato ou efeito de emitir, transmitir e receber mensagens por meio de métodos e/ ou processos convencionados, quer através da linguagem falada ou escrita, quer de outros sinais, signos ou símbolos, quer de aparelhamento técnico especializado, sonoro e/ou visual."

Ora, clara está a tipificação do crime. A violação de *emails* nada mais é do que a conquista de uma mensagem eletrônica pelo emprego de meios capciosos. O agente efetivamente apanha ou colhe a mensagem no servidor sem autorização legal ou de regulamento. Assim, estará ele sujeito às penas do art. 58 da citada Lei n. 4.117/62:

> "Nos crimes de violação da telecomunicação, a que se referem esta Lei e o art. 151 do Código Penal, caberão, ainda, as seguintes penas:
>
> I – para as concessionárias ou permissionárias as previstas nos arts. 62 e 63 se culpados por ação ou omissão e independentemente da ação criminal;
> II – para as pessoas físicas:
>
> a) 1 (um) a 2 (dois) anos de detenção ou perda de cargo ou emprego, apurada a responsabilidade em processo regular, iniciado com o afastamento imediato do acusado até decisão final;
> b) para autoridade responsável por violação da telecomunicação, as penas previstas na legislação em vigor serão aplicadas em dobro;
> c) serão suspensos ou cassados, na proporção da gravidade da infração, os certificados dos operadores profissionais e dos amadores responsáveis pelo crime de violação da telecomunicação."

A Lei n. 9.296, de 24 de julho de 1996, em seu art. 10, veio, aparentemente, aumentar a pena do crime de violação de *emails*:

> "Constitui crime realizar *interceptação* de comunicações telefônicas, de *informática* ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
> Pena: reclusão, de dois a quatro anos, e multa (grifos nossos)."

A interpretação da ação típica de interceptar pode, no entanto, nos levar a duas idéias bem diferentes. O que seria interceptar? Se o autor lesse a mensagem no servidor deixando-a intacta para que o real destinatário a recebesse, estaria cometendo a ação de interceptar ou, para tanto, teria de impedir que a mensagem chegasse intacta a seu legítimo destinatário?

I – quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói;

II – quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas;

III – quem impede a comunicação ou a conversação referidas no número anterior;

IV – quem instala ou utiliza estação ou aparelho radioelétrico, sem observância de disposição legal.

§ 2º As penas aumentam-se da metade, se há dano para outrem.

§ 3º Se o agente comete o crime, com abuso de função em serviço postal, telegráfico, radioelétrico ou telefônico:

Pena – detenção, de 1 (um) a 3 (três) anos.

§ 4º Somente se procede mediante representação, salvo nos casos do § 1º, IV, e do § 3º".

Mais uma vez vale recorrer ao *Dicionário Eletrônico Aurélio V.2.0:*

"Interceptar: [De *intercepto* + -ar2.] V. t. d. 1. Interromper no seu curso; deter ou impedir na passagem; 2. Cortar, interromper; 3. Reter, deter, empolgar (o que era destinado a outrem); 4. Servir de, ou constituir obstáculo a."

A partir de uma interpretação gramatical da lei, somos obrigados a concluir que só haverá o crime definido no art. 10 da Lei n. 9.296 quando, e somente quando, o autor impedir que a mensagem chegue intacta a seu destinatário. Se o *cracker* simplesmente acessa o servidor e lê os *emails,* sem modificá-los ou apagá-los, evidentemente, não está interceptando as mensagens, que chegarão ilesas a seu legítimo destinatário. A ação de interceptar envolve necessariamente a idéia de interrupção do curso da mensagem, o que, definitivamente, não ocorre com a simples leitura desta. Além do mais, há um princípio básico de hermenêutica que determina que as leis penais devem ser interpretadas restritivamente.

Daí entendermos que só se pode aplicar o citado artigo nos casos em que o *cracker* impedir que a mensagem chegue a seu destinatário ou a altere de qualquer forma. Quando, porém, o *cracker* se limitar a ler o conteúdo do *email*, ou apenas copiar a mensagem para seu computador, deixando a original intacta, os dispositivos a serem aplicados são os arts. 56 e 58 do Código Brasileiro de Telecomunicações.

2.5 Da prova

Tipificado o crime, surge-nos então o problema da prova. Para entendermos melhor a questão, fundamental é que se faça uma breve síntese da estrutura da Internet.

Computadores trabalham eminentemente com números. Quando alguém digita www.algumacoisa.com.br em seu programa navegador *(browser),* esse nome será associado a um número que denominamos endereço IP (*Internet*

Protocol). O DNS – *Domain Name System* (Sistema de Nomes de Domínio) – é o serviço que faz essa associação. Todos os domínios da Internet estão registrados em algum servidor DNS. Quando um servidor não tem condições de determinar um IP, transfere a solicitação para outro, até que o número correto seja encontrado.

Para facilitar essa localização, convencionou-se o uso de sufixos indicativos da localização geográfica do site e da atividade a que está ligado. Assim, os endereços DNS usam sufixos com a sigla do país: br, para Brasil; uk, Reino Unido; fr, França; etc. Da mesma forma os endereços DNS têm terminações que indicam a atividade relacionada: com, comercial; edu, educacional; gov, governo; org, organizacional sem fins lucrativos; etc. Os dois sufixos são importantes, pois facilitam a tradução do nome digitado pelo número correspondente ao endereço IP.

Mas, afinal, o que vem a ser o endereço IP? Trata-se de quatro seqüências de números separadas por pontos. Cada número pode variar de 0 a 255, portanto, 12.345.6.78 pode ser um endereço IP. Obviamente não pode haver duplicidade de endereços, pois é este número que individualizará cada máquina na Internet.

Em poucas palavras, podemos dizer que, ao se digitar www.algumacoisa.com.br no computador, o programa procurará na rede uma lista com os nomes de domínios brasileiros (sufixo *br*), em seguida selecionará aqueles do ramo comercial (sufixo *com*) para só então fazer a tradução do nome do domínio para seu endereço IP, que pode ser algo como 12.345.6.78. Por fim, com o endereço IP na memória, irá conectar-se à máquina desejada.

Da mesma forma que os provedores possuem endereços IPs, os usuários comuns, ao conectarem suas máquinas à Internet, também necessitaram de um endereço IP, pois é através dele que as informações solicitadas chegam até o computador. Seus endereços IPs, no entanto, não são fixos como se poderia imaginar inicialmente. Na realidade, a maioria dos IPs são dinâmicos, ou seja, variam conforme a conexão do usuário. O que ocorre é que os provedores de acesso à Internet possuem IPs fixos, mas os usuários que se conectam a eles por um *modem*, através de uma linha telefônica, acabam tendo um número de IP

diferente a cada conexão. Assim, hoje posso ter como endereço IP 123.456.7.89, e amanhã, ao conectar-me com o mesmo provedor, meu número poderá ser 123.456.7.98 (no caso de conexão com o mesmo provedor altera-se apenas o número final, que varia de 0 a 255).[9]

O estudo do endereço IP é fundamental para a resolução do problema das provas no crime de interceptação de *emails*. O endereço IP funciona como o número de identidade da máquina no universo virtual. Isso porque, quando se acessa uma caixa de *email*, a maioria dos provedores grava em um pequeno arquivo a data, a hora e o endereço IP do acesso.

Assim, se o IP for fixo, ter-se-á chegado ao foco da ação e será relativamente simples processar o autor de um acesso não autorizado. No caso dos IPs dinâmicos, a pesquisa é mais complicada. Como os três números iniciais do IP dinâmico indicam o provedor de acesso, fácil será descobrir qual o provedor do autor. Mas os grandes provedores têm centenas de usuários. Como se encontrar entre eles o autor?

Todas as vezes que alguém se conecta a um provedor de acesso à Internet é exigido antes da conexão um *login* (nome pelo qual se identifica o usuário) e uma senha de acesso. Logo que a permissão de acesso é concedida, é gravado um arquivo no provedor com o *login* do usuário, a data e hora de sua conexão e o IP usado nesta conexão. Ora, sabendo-se a data e a hora do delito e o endereço IP do autor, é relativamente fácil chegar-se ao autor, requisitando-se informações ao provedor. No entanto, *crackers* experientes não utilizam sua conta de acesso à Internet para cometer seus delitos virtuais. Não será difícil para um *cracker* conseguir um *login* e senha falsos para se conectar sem ser rastreado, ou até mesmo permitir que o rastreamento ocorra, apenas direcionando-o para uma outra pessoa.

Alguns provedores já possuem identificadores de chamadas telefônicas (bina) e gravam, no momento da conexão de seus usuários, não só seus *logins*,

9 Cf. MACHADO, Carlos (Ed.). Soluções – Help desk. *Info Exame*, São Paulo, a-13, n. 150, p. 150.

data/hora e IP, mas também o número do telefone pelo qual foi feita a conexão. Isso diminui bastante a chance de *crackers* usarem senhas falsas para se conectarem, já que agora bastará autoridades localizar o dono do número do telefone para ter bons indícios do autor do crime.

Mas os *crackers* são, às vezes, mais sofisticados e utilizam computadores portáteis (*laptops*), conectados a telefones públicos para cometer seus delitos virtuais. Nesse caso, o identificador de chamadas telefônicas de nada valerá, já que se trata de telefone público e, como as senhas são falsas, não se poderá chegar ao responsável pela conta.

2.6 Do futuro

O problema da segurança na Internet vem recebendo tratamento privilegiado no desenvolvimento de novas tecnologias. Muitas empresas interessadas em aumentar suas vendas pela Internet têm interesse no aumento da segurança e estão investindo altas somas em dinheiro para que isso ocorra o mais rapidamente possível.

Vários sistemas de criptografia vêm sendo desenvolvidos para garantir a segurança do tráfego de mensagens pelas redes. A idéia primária da criptografia é utilizar um código para cifrar a mensagem e torná-la ilegível para qualquer pessoa que tiver acesso a elas nos servidores. Somente o verdadeiro destinatário, munido do mesmo sistema, conseguiria decodificar o texto para poder lê-lo. Tornar-se-ia inviável para os *crackers* descriptografar mensagens inteiras, pois se, como vimos, descriptografar senhas é uma tarefa relativamente fácil, o mesmo não se pode dizer da descriptografia de mensagens inteiras. Pelos atuais métodos, tal tarefa poderia levar anos, ou quem sabe décadas, tornando assim quase impossível qualquer êxito da tentativa.[10]

10 Cf. MACHADO, Carlos (Ed.) Soluções – Help desk. *Info Exame*, São Paulo, a. 13, n. 150, p.152.

Por outro lado, a Intel lançou recentemente seu processador Pentium III, que, se não chegou a empolgar pelo desempenho, por ser uma mera evolução do Pentium II, em matéria de segurança revelou-se uma verdadeira revolução. Isso porque a Intel gravou internamente um número de série no processador, que pode ser lido por um programa apropriado. Além de dificultar a venda de processadores adulterados (prática comum no Brasil), o número de série poderá ser usado para identificar as máquinas na Internet.

O problema é que o número de série despertou preocupações quanto à privacidade. O usuário já não poderá mais navegar anonimamente pela rede, pois sua identidade poderá ser facilmente revelada pelo processador. A Intel foi obrigada, então, a voltar atrás, e distribuiu um programa que permite ao usuário habilitar ou desabilitar a leitura do número de identificação.[11]

O sistema aparentemente é perfeito. O usuário poderia desabilitar o número de série do processador para navegar anonimamente pela Internet sem o constrangimento de, por exemplo, visitar uma página de conteúdo erótico sabendo que sua identidade digital o denunciaria. Por outro lado, quando precisasse acessar seu *email*, seria exigido dele que habilitasse o número de série do processado e, somente após a checagem do número de série seria permitido o acesso aos *emails*. Da mesma forma, as compras pela Internet através do número de cartões de crédito passariam a exigir a habilitação do número de série do processador.

Restaria, no entanto, uma pequena lacuna, originada do fato de o computador não ser usado apenas por uma pessoa. É comum que, várias pessoas da família utilizem a mesma máquina para acessar a Internet. Dessa forma, pessoas diferentes teriam a mesma identidade digital, já que o número de série do processador da máquina seria o mesmo. Ainda assim haveria uma efetiva diminuição dos crimes por computadores em rede, e estes seriam bem mais fáceis de serem identificados, já que os autores estariam reduzidos aos usuários de determinada máquina.

11 Cf. GREGO, Maurício. A terceira geração do *pentium*. *Info Exame*, São Paulo, a. 14, n. 156, p. 53.

3 DA VIOLAÇÃO DE DIREITOS AUTORAIS SOBRE *SOFTWARE*

A violação dos direitos autorais sobre *software* é o delito relacionado a computadores mais em voga atualmente, talvez devido às grandes pressões exercidas pela indústria internacional do *software*.

O objeto material desses crimes é o programa de computador, ou *software*, cuja definição legal é dada pela Lei n. 9.609, de 19 de fevereiro de 1998:

> "Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados."

Em poucas palavras, poderíamos definir o programa de computador como um conjunto ordenado de instruções dadas à máquina que faz com que ela realize determinada tarefa.

A violação de direitos de autor de programa de computador está tipificada, na legislação brasileira, no art. 12 da citada lei.[12] A norma abrange três figuras

12 "Art. 12. Violar direitos de autor de programa de computador:
Pena – Detenção de seis meses a dois anos ou multa.
§ 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
Pena – Reclusão de um a quatro anos e multa.
§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
§ 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
I – quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
II – quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.
§ 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação."

bem distintas, conhecidas no jargão da informática por pirataria, *warez* e *crackz*, não fazendo qualquer distinção entre elas e dando a impressão de ter sido criada com o fim exclusivo de coibir apenas a primeira.

3.1 Da pirataria

Pirataria é a reprodução de programas de computador em meio físico (um disquete, um CD-R, etc) sem autorização do autor, sendo irrelevante para caracterizá-la o *animus lucri faciendi*. O que caracteriza a pirataria é a consubstanciação de programa de computador em meio físico, sem qualquer autorização. A pirataria exige conhecimentos técnicos, ainda que mínimos, por parte do autor que realiza uma cópia do programa do meio físico original para outro meio físico conhecido como virgem. Tal crime é extremamente comum no Brasil. A revista *Info Exame* de janeiro de 1999 traz números impressionantes:

> "A Associação Brasileira de Empresas de *Software* (ABES) estima que a indústria da informática perca 913 milhões de reais por ano com o uso de programas piratas. Segundo um estudo da Price Waterhouse, 68% dos *softwares* em operação no Brasil são ilegais. Mais de vinte pessoas foram presas em flagrante ao longo de 1998 por fraude de *copyright* digital. A ABES espera que, com essas ações, as irregularidades caiam a patamares de 60%." [13]

Atribui-se como causa desses índices o alto preço dos programas de computador, em relação à renda média brasileira (a maioria dos *softwares* custa mais que um salário mínimo). Além disso, é opinião corrente entre os usuários que grandes empresas internacionais de *software* estimulam o uso de programas piratas em países subdesenvolvidos para que, após as pessoas se habituarem a usá-los, elas (empresas) reivindiquem seus direitos autorais. A crescente diminuição dos preços de aparelhos gravadores de CDs-Rs só vem intensificar o problema, já que qualquer pessoa com conhecimentos médios de informática é capaz de criar cópias idênticas de programas originais com esses aparelhos.

13 País de Piratas? *Info Exame*, São Paulo, a. 13, n. 154, jan. 1999.

Mas a pirataria não é a única forma de se violar os direitos autorais sobre *softwares*, sendo muito comum no exterior a conhecida como *warez*, que começa a chegar ao Brasil.

3.2 Do *warez*

Warez é a prática de se disponibilizar na Internet, ou por qualquer outro tipo de conexão entre computadores, programas completos que podem ser copiados integralmente do servidor para outra máquina.

A origem do termo é a palavra inglesa *wares* (mercadoria), trocando-se o s pelo sufixo z, que na gíria do submundo da Internet serve para identificar tudo aquilo que é ilegal.

Os autores desses crimes geralmente se aproveitam de servidores gratuitos de espaço para *homepages* e ali criam o ponto de distribuição de suas "mercadorias". Assim, qualquer pessoa no mundo, ligada à Internet, que saiba seu endereço poderá ter acesso aos programas sem o pagamento de direitos autorais.

O *warez* difere da pirataria, pois neste não há a consubstanciação do programa em meio físico. A prática ainda é pouco comum no Brasil, talvez devido à baixa velocidade de conexão na Internet brasileira, o que torna inviável o *download*[14] de programas muito grandes.

Outra característica interessante do *warez* é a ausência, na maioria absoluta dos casos, do *animus lucri faciendi*. Trata-se de um crime cometido por

14 Transferência de arquivos entre dois computadores ligados em rede, na qual um deles "baixa" de um servidor uma cópia idêntica de um arquivo lá armazenado.

uma concepção ideológica de que as empresas de *software* abusam de seus direitos autorais cobrando valores exorbitantes por eles.

Ao contrário da pirataria, em que o exame de corpo de delito é a prova por excelência, já que nesta há sempre a consubstanciação do programa em meio físico, no *warez* a questão é bem mais complexa, pelo próprio modo *sui generis* da ação. Os autores desse crime criam contas com dados falsos em servidores que oferecem hospedagem gratuita de *home pages*. Como esses servidores em geral possuem milhares de usuários, não há como controlar tudo aquilo que é divulgado em suas páginas. Assim, passam a disponibilizar em suas páginas programas completos para *download*, na grande maioria das vezes gratuitamente. Com isso as páginas de *warez* chegam a ficar meses funcionando, permitindo que milhares de pessoas descarreguem de lá programas completos sem qualquer ônus. Tais páginas somente são retiradas do ar quando os responsáveis pelo servidor são comunicados, por terceiro, sobre a ilegalidade.

Como os dados da conta são falsos, o único meio de se chegar ao autor da página é através do endereço IP, que fica gravado no momento da criação da conta no servidor; porém, na maioria absoluta das vezes, os *crackers* utilizam contas falsas para criar esse tipo de página, tornando impossível o seu rastreamento.

3.3 Dos *crackz* e *key makerz*

Crackz são pequenos programas criados por *crackers*, capazes de transformar programas de demonstração, como *sharewares* e *demos*, em programas completos.

Sharewares[15] são programas *try before you buy* (experimente antes de comprar), ou seja, o autor fornece uma cópia de demonstração do programa

15 Não se deve confundi-los com os *freewares*, que são programas de distribuição livre e podem ser copiados à vontade.

que funciona normalmente por certo período de tempo (em geral trinta dias), depois do qual o programa pára de funcionar e passa a requisitar do usuário um número de série (*serial number*) para voltar a funcionar normalmente. Esse número de série deve ser obtido pelo registro do programa com o conseqüente pagamento dos direitos autorais, o que em geral é feito pela própria Internet, através de pagamento por cartão de crédito.

Demos são programas de demonstração com limitações de recursos. Tais limitações podem variar desde as mais essenciais (como salvar e imprimir) até algumas que pouco acrescentam ao programa. Os programas *demos*, em sua maioria, não podem ser registrados, devendo ser adquiridos nas lojas, mas alguns, assim como os *sharewares*, aceitam o registro pela Internet, destravando-se o programa através de um número de série. Os *demos* não possuem limitação de tempo, podendo ser usados indefinidamente pelo usuário, sempre com recursos limitados.

Os *crackz* nada mais são do que pequenos programas que permitem romper as travas de segurança que limitam o uso do programa em determinadas funções (*demos*) ou por determinado período (*sharewares*). Assim, com o uso dos *crackz*, os programas deixam de exigir o número de série e passam a funcionar como se tivessem sido efetivamente registrados. Ocorre, pois, uma apropriação indébita de cópias de programas que foram cedidas pelo autor a título de demonstração.

Números de séries são criados a partir do nome completo do usuário registrado. Quando um usuário registra um *software*, os computadores da empresa detentora dos direitos autorais sobre o programa criam, a partir do nome completo do registrante, um número de série personalizado. Esse número deverá ser digitado no programa a ser registrado, juntamente com o nome completo do usuário. Assim, o programa checará se aquele número corresponde àquele nome e, em caso positivo, passará a funcionar como registrado.

No entanto, determinados *crackers* conseguem descobrir o código que relaciona as letras do nome do usuário ao número de série do programa e criam geradores de números seriais (*key makerz* ou *key generatorz*), que geram números de série personalizados exatamente iguais ao que os computadores da

empresa detentora dos direitos autorais criariam no momento do registro. Isso possibilita a qualquer pessoa, com a simples digitação de seu nome completo no *key maker*, a obtenção de uma senha que não só destrava o programa, mas também "registra" seu nome como se o registro tivesse sido realmente obtido.

Diferem os *crackz* dos *key makerz*, pois, enquanto que com o uso dos primeiros o programa simplesmente ignora a necessidade do uso de senha, com a utilização dos segundos o programa efetivamente "registra" o usuário, passando o nome dele a constar no programa como usuário registrado.

A diferença em matéria probatória é essencial. Um simples exame pericial pode comprovar facilmente o uso de *crackz* para burlar o sistema de segurança do programa, pois este lhe altera o código original. Já os *key makerz*, como são *softwares* independentes do original, podem ser facilmente apagados após a geração da senha, que poderá ser anotada até mesmo num pedaço de papel, servindo como "prova" de que aquele programa foi "devidamente registrado".

4 DA CRIAÇÃO, DIVULGAÇÃO E DISSEMINAÇÃO DE VÍRUS

4.1 Da doença

A palavra vírus deriva do latim e significava originalmente "veneno". O termo acabou sendo usado pelas Ciências Biológicas para designar diminutos agentes infecciosos, visíveis apenas ao microscópio eletrônico, que se caracterizam por não terem metabolismo independente e sua capacidade de reprodução ser apenas no interior de células hospedeiras vivas.[16]

16 "Quando um vírus entra em contato com uma célula hospedeira, acopla-se a ela através da cauda e perfura a membrana celular por meio de ação enzimática. Então, o ácido nucléico viral é injetado no interior da bactéria, passando a interferir no metabolismo bacteriano de maneira a comandar a síntese de novos ácidos nucléicos virais, à custa da energia e dos componentes químicos da célula vítima. Paralelamente, e ainda utilizando a célula hospedeira como fonte de energia e de matéria-prima, o ácido nucléico do vírus comanda a síntese de várias outras moléculas que, ao se juntarem, de maneira ordenada, definem a formação de novos vírus. [...]. Uma vez formadas, as novas unidades virais promovem a ruptura da membrana bacteriana (*lise*) e os novos vírus liberados podem infectar outra célula, recomeçando um novo ciclo (PAULINO, Wilson Roberto. *Biologia atual* – Seres vivos, fisiologia e embriologia, p.19-20)."

Assim como os vírus biológicos, os vírus de computadores são programas que infectam outros programas, causando-lhes uma série de danos e reproduzindo-se a partir do programa hospedeiro. O homem criou os vírus de computador à imagem e semelhança de seus homônimos biológicos. São programas extremamente pequenos, escritos geralmente em Assembly, C ou Pascal, capazes de reproduzir através da contaminação de disquetes que, se colocados em outros computadores, acabam infectando-os também. Também já foram criados vírus mutantes (produzem cópias um pouco diferentes das originais para tentar burlar os programas antivírus) e vírus que se reproduzem pela Internet (como o famoso Happy 99, que anexa uma cópia de si mesmo em todos os *emails* enviados pela máquina infectada).

Os vírus, talvez, sejam a ameaça a computadores mais temida pelos usuários pouco experientes, que sequer acreditam que algum *cracker* possa invadir seus computadores, mas, com certeza, temem o ataque de vírus.

Além disso, não são raros os casos de pessoas bem instruídas que temem ver seus organismos infectados por vírus de computador. A desinformação sobre o assunto é tamanha que já se propôs ação reclamatória trabalhista em que se pretendia receber adicional de periculosidade porque o reclamante trabalhava com computadores infectados por vírus.[17] É bom deixar claro que, apesar da lógica de funcionamento dos vírus de computadores ser análoga à dos vírus biológicos, não há a menor possibilidade de que um programa de computador venha a infectar um organismo vivo causando-lhe qualquer tipo de doença.

17 Cf. Processo n. 00950/95 – 14ª Junta de Conciliação e Julgamento de Belo Horizonte.

4.2 Dos sintomas

Podemos dizer que há duas fases bem marcantes na ação dos vírus: a contaminação e o ataque.

A contaminação é o momento da infecção do sistema, ou seja, ocorre quando o programa "vírus" se instala em um computador. Nessa fase, a maioria dos vírus não causa qualquer dano, permanecendo escondidos, aguardando a ocasião de contaminar novas máquinas.

Em seguida vem o ataque, que pode ocorrer até mesmo meses após a contaminação. O ataque só ocorre numa determinada combinação de fatos muito específicos: pode ser apenas uma determinada data, uma certa quantidade de execuções, ou uma combinação de eventos desse tipo. Nesse momento, o vírus causa todo o estrago que seu autor o programou para fazer. Alguns vírus atacam, por exemplo, quando os dias 13 caem numa sexta-feira (para lembrar apenas dois exemplos o Jerusalém e NXeram). Se o usuário não ligar o micro nestas datas, jamais conhecerá as conseqüências do ataque de tais vírus. Em outras palavras: um computador pode estar contaminado 365 dias por ano, mas só numa determinada situação será atacado pelo vírus.[18]

4.3 Do remédio

Na legislação brasileira não há um tipo penal que cuide especificamente da criação, divulgação e disseminação de vírus de computador. Analisemos, porém, cada uma dessas ações separadamente.

A criação é o processo que vai da elaboração do código fonte até a compilação final do programa que gera o vírus acabado. No Brasil, não há qualquer dispositivo que tipifique tal conduta, fazendo-se necessária a criação de uma norma que incrimine a criação de vírus, pois tal ação constitui evidentemente crime de perigo concreto.

18 Cf. BECEIRO, Francisco Panizo. *Help desk* – Portal das dicas. Internet. http://users.sti.com.br/helpdesk/

A divulgação é a ação de tornar público o acesso ao vírus fazendo-se a advertência de que se trata de programa ardiloso capaz de causar danos aos dados armazenados no computador. É feita em geral pela Internet em *home pages* de *crackers*, onde se pode baixar exemplares de vírus com instruções para a sua disseminação. Não há qualquer dispositivo em nossa legislação que incrimine tal conduta especificamente, mas consideramos que ela pode ser perfeitamente enquadrada no delito de incitação ao crime disciplinado no art. 286 do Código Penal:

"Incitar, publicamente, a prática de crime:
Pena – detenção, de 3 (três) a 6 (seis) meses, ou multa."

O grande problema é que os *crackers* normalmente têm o cuidado de advertir os visitantes de suas páginas que a disseminação de vírus constitui crime, recomendando que todo material lá encontrado seja utilizado apenas com fins de estudo. Assim, em geral, desconfigura-se a presença do dolo, sendo, pois, urgente a criação de um tipo específico que cuide dessa matéria, considerando a divulgação de vírus como crime de perigo concreto.

A disseminação é a difusão do vírus com o intuito de infectar as máquinas com o programa, causando-lhes assim um dano material. Pode-se dar por qualquer meio, seja através de disquetes contaminados, ou mesmo por uma rede de computadores, como no caso típico da Internet.

A disseminação de vírus de computadores, apesar de não ter um dispositivo que trate exclusivamente sobre ela, pode ser enquadrada no crime de dano, disciplinado no art. 163 do Código Penal brasileiro:

"Destruir, inutilizar ou deteriorar coisa alheia:
Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa.

Schönke-Schröder lecionam que "o objeto da tutela jurídica é a preservação do valor da coisa para o proprietário, protegendo-se não só o seu valor substancial ou intrínseco como também o mero valor de utilidade".[19]

19 SCHÖNKE, Adolf, SCHRÖDER, Horst. *Strafgesetzbuch Kommentar.* 16. ed. Munique: Beck Verlag, 1976. § 303, I, *apud* FRAGOSO, Heleno Cláudio. *Lições de direito penal* – Parte especial § 382, p. 338.

Ora, os dados armazenados em um disco rígido de computador têm um valor-utilidade significativo para seu proprietário. A destruição, inutilização ou deterioração desses dados por um vírus de computador constitui, pois, crime de dano. Evidentemente, o vírus jamais pode ser considerado autor do dano, pois, na verdade, é apenas o meio do qual se vale o verdadeiro autor para atingir o fim danoso. O sujeito ativo nesses casos é, portanto, o disseminador do vírus.

Quando o disseminador do vírus não foi seu próprio criador, não se poderá falar necessariamente em co-autoria, já que para que esta se configure é necessário existir uma cooperação consciente recíproca, expressa ou tácita entre os agentes, resultante de acordo prévio ou de um entendimento repentino, surgido durante a execução.

Vejamos um exemplo curioso: Tício, desenvolvedor de um famoso programa antivírus, cria um vírus de computador simplesmente com o intuito de testar a nova versão de seu antivírus. Mévio, *cracker* bastante conhecido no submundo da Internet, invade o computador de Tício e copia esse novo vírus, disseminando-o pela Internet. Evidentemente que, nesse caso, somente Mévio responderá pelo crime de dano, já que Tício não poderá jamais ser punido a título de dolo; e ainda que no caso houvesse negligência por parte do criador do vírus, o crime de dano não admite a modalidade culposa.

Note-se que a mera criação do vírus não pode, pela legislação atual brasileira, ser considerada crime algum. É imprescindível que o vírus efetivamente cause um dano qualquer, para que criador e disseminador possam ser responsabilizados pelo dano.

Há que analisar-se também o elemento subjetivo do crime. Vários autores entendem que o dolo específico, no caso, o ânimo de causar prejuízo (*animus nocendi*), é essencial no crime de dano. Entendemos, como Fragoso, que "se há vontade e consciência de destruir, inutilizar ou deteriorar, há, evidentemente, vontade de causar dano, e, pois de prejudicar".[20]

20 FRAGOSO, Heleno Cláudio. *Op. cit.*, § 385, p. 340.

Não há, portanto, que se falar em dolo específico no crime de disseminação de vírus. Não há necessidade de que o agente tenha a vontade de provocar um efetivo prejuízo para a vítima; basta que haja a intenção de destruir ou inutilizar dados ou programas contidos no seu computador.

Vale ressaltar ainda que, por força do art. 167 do Código Penal, o crime de dano e, conseqüentemente, a disseminação de vírus, é de ação penal privada; só se procede mediante queixa.

Como o crime de dano é de natureza material, deixa vestígios, uma vez que seus efeitos permanecem no tempo. Indispensável será, pois, o exame do corpo de delito para sua comprovação, não podendo supri-lo a prova testemunhal ou a confissão do acusado.

O problema é que, muitas vezes, os vírus formatam o disco rígido. A formatação é o ato de se apagar todos os dados existentes no disco e pode ser realizada pelo usuário pelo simples comando *format c:*. Após a formatação, o disco fica num estado semelhante ao de sua saída da fábrica, sendo impossível para a perícia técnica determinar se a causa da formatação foi um comando do próprio usuário ou de um vírus, pois, com a formatação, todos os dados e programas existentes no disco são apagados, inclusive o próprio vírus.

É praticamente impossível condenar atualmente alguém por crime de dano causado por vírus de computador. Os programadores dos vírus não assinam seus programas, e a divulgação por meio da Internet garante um anonimato praticamente perfeito, tornando quase impossível a prova da autoria. Além disso, há uma limitação técnica da perícia que impede a comprovação da materialidade do crime quando os vírus formatam os discos rígidos.

4.5 Da profilaxia

O problema dos crimes de vírus está intimamente ligado ao acesso direto aos computadores. O Direito só poderá punir os criminosos da era digital se se puder comprovar a autoria dos delitos. Mas como isso será possível?

É comum nos sistemas operacionais que trabalham com redes (Unix, Linux, Windows NT, etc.) a exigência de um *login* e de uma senha para todos aqueles que tenham acesso ao sistema. Assim, o nome do usuário fica registrado em um arquivo, juntamente com a data e a hora em que ele acessou o sistema.

O ideal seria que os sistemas operacionais, para todas as ações que importassem a perda ou a modificação de dados, registrassem a data, a hora e o responsável pela modificação (no caso do usuário, *o login*; no caso de um programa, o nome do *software*). Este arquivo controlador das modificações deveria ser "somente leitura" para todos os programas e usuários (inclusive para o administrador do sistema). Seu acesso para gravação só deveria ser realizado pelo sistema operacional nos momentos em que houvesse o *apagamento* ou uma modificação de determinado arquivo para o registro das alterações. Dessa forma, ter-se-ia um histórico das modificações e ficaria bem mais fácil o controle dos arquivos perdidos ou modificados. No caso de um vírus que corrompe aos poucos os dados, o usuário perceberia o problema e seria fácil apagar o arquivo indicado como corruptor do sistema.

Evidentemente que, no caso de uma formatação, o sistema não funcionaria, pois, como esta apaga todos os arquivos, o próprio arquivo de registro das modificações seria apagado também.

O uso de *logins* e senhas falsas para obter acesso ao sistema também seria um grande problema, mas, quanto a isso, a indústria da informática já acena com soluções revolucionárias que irão aumentar a segurança de acesso a computadores. A tecnologia de reconhecimento de íris, desenvolvida por empresas como a IriScan (www.iriscan.com), de New Jersey, permite que, após capturadas por uma câmera, as imagens da íris sejam processadas por um IrisCode e armazenadas num servidor. Depois, basta que o usuário olhe para um leitor especial para que o reconhecimento seja realizado.

Empresas como a Veridicom (www.veridicom.com), da Califórnia, desenvolveram sensores que reconhecem a impressão digital. Trata-se de uma espécie de *scanner* capaz de ler a impressão digital da pessoa e compará-la com dados armazenados em seus arquivos.

Os reconhecimentos de voz e facial também estão em fase de testes e em breve poderão estar disponíveis no mercado.[21]

Todos esses recursos aumentarão a segurança do acesso a computadores e permitirão um instrumental probatório muito maior para as discussões, nos tribunais, sobre o problema dos vírus.

5 CONCLUSÃO

Por mais entusiasmantes que nos pareçam os intrumentos criados pela moderna tecnologia no intuito de garantir a segurança no universo dos computadores, não acreditamos que eles sejam a solução definitiva do problema.

O número de série do processador *Pentium III* e as tecnologias de reconhecimento de íris e de impressão digital possuem o grande mérito de fornecer ao Direito um instrumental probatório mais efetivo; porém, julgamos que não se pode confiar que a solução para os crimes relacionados a computadores esteja exclusivamente nas mãos de técnicos em informática, capazes de criar mecanismos de segurança perfeitos. Seria, no mínimo, utópico supor que a simples tecnologia seja suficiente para coibir delitos virtuais.

É bem provável que *crackers* desenvolvam métodos para fraudar o sistema de segurança baseado no número de série do processador *Pentium III*. Também já se especula sobre lentes de contatos e dedeiras capazes de burlar a segurança dos mecanismos de reconhecimento de íris e de impressões digitais.

Lembremo-nos das palavras de Freud: "As criações humanas são de fácil destruição. A ciência e a técnica que as construíram podem ser aplicadas também no seu aniquilamento."[22]

21 MILITELLO, Kátia. O preigo está dentro de casa. *Info Exame*, São Paulo, ano 13, n. 147, p. 130, jun. 1998.

22 CLARET, Martin. (Ed.). *O pensamento vivo de Freud*, p.108.

Assim, acreditamos que o Direito não poderá se furtar à difícil tarefa de disciplinar o uso dessas novas tecnologias. Para tanto, é preciso que os operadores do Direito aceitem o desafio de um estudo interdisciplinar da informática e da ciência jurídica. Assim como no estudo do Direito Econômico é essencial ao jurista bons conhecimentos da Ciência Econômica, imprescindível também que, no estudo dos crimes por computador, o jurista domine os conceitos fundamentais da Ciência da Computação.

No estudo interdisciplinar da Informática e do Direito, caberá a este criar normas que disciplinem o uso das modernas tecnologias, e, àquela, oferecer o instrumental probatório para a efetivação de tais normas.

6 BIBLIOGRAFIA

BARATA ELÉTRICA. Internet: *http://www.geocities.com/SiliconValley/Bay/5617/* 1994. (Ezine).

BECEIRO, Francisco Panizo. *Help desk;* portal das dicas. Internet: *http://users.sti.com.br/helpdesk/* ult. atual. 17 de março de 1999.

CLARET, Martin. (Ed.). *O pensamento vivo de Freud*. Rio de Janeiro: Ediouro, 1986. 110 p.

FRAGOSO, Heleno Cláudio. *Lições de direito penal* – Parte especial: arts. 121 a 212 do CP. 7. ed. Rio de Janeiro: Forense, 1983. 615 p.

GREGO, Maurício. A terceira geração do *pentium*. *Info Exame*, São Paulo, a. 14, n. 156, p. 52-54, mar. 1999.

LACERDA, Carlos Augusto (Ed.); GEIGER, Paulo (Ed.); BARROSO, Márcio Ellery Girão (*software*). *Dicionário Aurélio Eletrônico* – V.2.0. Rio de Janeiro: Nova Fronteira, 1996.

MACHADO, Carlos. (Ed.). Soluções – Help desk. *Info Exame*, São Paulo, a. 13, n. 150, p.152-154, set. 1998.

MILITELLO, Kátia. O perigo está dentro de casa, *Info Exame*, São Paulo, a. 13, n. 147, p.128-131, jun. 1998.

PAÍS de piratas? *Info Exame*. São Paulo, ano 13, n. 154, Caderno I, não paginado, jan. 1999.

PAULINO, Wilson Roberto. *Biologia atual*: seres vivos, fisiologia, embriologia. 4. ed. São Paulo: Ática, 1990. v. 2, 328 p.

RANGEL, Paulo. Breves considerações sobre a Lei n. 9.296/96 – Interceptação telefônica. *Revista Forense*, Rio de Janeiro, v. 344, p. 217-224, out./dez. 1998.

REIS, Maria Helena Junqueira. *Computer crimes* – A criminalidade na era dos computadores. Belo Horizonte: Del Rey, 1996. 62 p.

ROCHA, Fernando Antônio Nogueira Galvão da. Criminalidade do computador. *Revista Jurídica do Ministério Público*, Belo Horizonte, a. 27, v. 19, p. 75-98, 1996.

SIQUEIRA FILHO, Élio Wanderley de. Escuta telefônica – comentários à Lei n. 9.296/96. *Revista Forense*, Rio de Janeiro, v. 340, p. 99-106, out./dez. 1997.

UHF. Internet: http://members.xoom.com/–XOOM/blackouthp/zines.htm 1998. (Ezine).