CRIMES NA INTERNET

* James Nogueira Bueno
** Vânia Maria Bemfica Guimarães Coelho

Resumo

Este trabalho apresenta a dimensão ética contida nos espaços e suportes informacionais trazido à realidade do profissional da informação.

Saliente, os conceitos de crimes praticados “com” e “contra” o computador, ao concluir que os crimes informáticos não podem mais deixar de ser uma preocupação social, carecendo de tipificação em nosso ordenamento jurídico.

Aponta para a necessidade de uma reflexão ética, por parte dos profissionais da informação, a fim de poderem, de forma legítima, atuando não apenas como meros disponibilizadores de informações, mas como valiosos colaboradores das instâncias jurídicas que visam a garantir tais direitos.

Palavra-chave: crime; internet; ética profissional; informação.

1. Desenvolvimento

O surgimento dos crimes informáticos, que começou na década de 1960, época em que apareceram na imprensa e na literatura científica os primeiros casos de uso do computador para a prática de delitos, constituídos, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados em matérias jornalísticas. Somente na década seguinte é que se iniciariam os estudos sistemáticos e científicos sobre essa matéria, com emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial.

A partir de 1980, o aumento de ações criminosas que passaram a incidir em manipulações de caixas bancárias, pirataria de programas de computador, abusos nas telecomunicações etc., revelando vulnerabilidade que os criadores do processo não haviam previsto.

---

* Acadêmica do Curso de Direito da Faculdade de Direito de Varginha.
**Professora titular da cadeira de Direito Processual Penal da Faculdade de Direito de Varginha.

Essa criminalidade, conta com as mesmas características da informatização global, logo a delinqüência correspondente, ainda que em graus distintos, também está presente em todos os continentes.

Nesse contexto, observa-se que, como fator criminógeno, cabe reconhecer que a informática permite não só o cometimento de novos delitos, como potencializa alguns outros tradicionais (estelionato, por exemplo). Há, assim, crimes cometidos com o computador e os cometidos contra o computador, isto é, contra as informações e programas nele contidos.

Pode-se observar que, enfatiza crimes cometidos contra computador, ou seja, contra as informações e programas nele contidos, bem como contra as informações ou dados em trânsito por computadores, com o dolo específico de ameaça e de fraude, não abordando aqueles crimes praticados com o computador, mas cujo bem protegido pelo ordenamento jurídico e diverso, como por exemplo, a pedofilia.

O crime virtual puro seria toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas. Crime virtual misto seria aquele em que o uso da internet é condição para efetivação da conduta, embora o bem jurídico visado seja diverso do informático, como, por exemplo, as transferências ilícitas de valores em uma *homebanking*, onde o racker retira de milhares de contas correntes, diariamente, pequenas quantias que correspondem a centavos e as transfere para uma única conta. Embora esses valores sejam ínfimos para o correntista, que, na maioria das vezes, nem se dá conta do furto, representam para o cibercriminoso uma expressiva quantia em seu montante. Por derradeiro, crime virtual comum seria utilizar a internet apenas como instrumento para a realização de um delito já tipificado pela lei penal. Assim, a Rede Mundial de Computadores acaba por ser apenas mais um meio para a realização de uma conduta delituosa. Se antes, por exemplo, o crime como o de pornografia infantil era instrumentalizado por meio de vídeos ou revistas, atualmente, dá-se por salas de bate-papo, ICQ, como também pela troca de fotos por e-mail entre pedófilos e divulgação em sites. Mudou a forma, mas a essência do crime permanece a mesma.

Os crimes de informática se distinguem em duas categorias:

1 - os atos dirigidos contra um sistema de informática, por qualquer motivo, verdadeiro núcleo da criminalidade informática, por se tratarem de ações que atendem contra o próprio material informático (suportes lógicos ou dados dos computadores);

2 - os atos que atendem contra outros valores sociais ou outros bens jurídicos, cometidos através de um sistema de informática, que compreenderiam todas as espécies de infrações previstas em lei penal.

Há delitos informáticos puros, “em que o sujeito visa especificamente ao sistema de informática em todas as suas formas”, incluindo software, hardware, dados e sistemas, bem como meios de armazenamento, e delitos informáticos mistos, “em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático”, como por exemplo, a prática de homicídio por meio da internet, com a mudança a distância de rota de um avião.

Dentre os “vírus” o Cavalo de Tróia (trojan horse) é uns dos mais comuns. O usuário pode recebe-lo de várias maneiras, na maioria das vezes ele vem anexado a algum e-mail. Este vem acompanhado de mensagens bonitas que prometem mil maravilhas se o arquivo anexado for aberto. Uma vez aberto o arquivo, o trojan horse se instala no computador do usuário. Na maioria das vezes, tal programa ilícito vai possibilitar aos hackers o controle total da sua máquina. Poderá ver e copiar todos os arquivos do usuário, descobrir todas a senhas que ele digitar, formatar seu disco rígido, ver a sua tela e até mesmo ouvir sua voz se o computador tiver um microfone instalado.

Considerando-se que boa parte dos computadores é dotada de microfones ou câmaras de áudio e vídeo, observar-se que o cavalo de tróia permite a possibilidade de se fazer escuta ambiente clandestina, arma poderosa nas mãos de criminosos que visam à captura de segredos industriais.

O delito eletrônico, em sentido amplo, é qualquer conduta criminógena ou criminal em cuja realização haja o emprego da tecnologia eletrônica como método, meio ou fim, em um sentido estrito, qualquer ato elícito penal em que os computadores, suas técnicas e funções desempenham um papel como método,

meio ou fim. Complementando sua definição, classifica os delitos eletrônicos em três categorias:

a Os que utilizam a tecnologia eletrônica como método, ou seja, condutas criminais onde os indivíduos utilizam métodos eletrônicos para obter um resultado ilícito;

b Os que utilizam à tecnologia eletrônica como meio, ou seja, condutas criminais em que para a realização de um delito utilizam o computador como meio;

c Os que utilizam a tecnologia eletrônica como fim, ou seja, condutas dirigidas contra a entidade física do objeto ou máquina eletrônica ou seu material com o objeto de danificá-lo.

2. Conclusão

Como se pode observar, a dimensão criminal ora verificada na internet não apenas conserva os aspectos tradicionalmente preconizados pelo Direito Penal, como traz à tona peculiaridades desse novo contexto. Assim, condutas igualmente lesivas, mas ainda não-consideradas crimes, por dependerem de regulamentação específica, como é o caso do dano praticado contra informações e programas contidos em computador, proliferam em ritmo acelerado, e por vezes incontrolável.

Desse modo, questões como a propagação deliberada de vírus informáticos, destruindo sistemas inteiros e levando à impossibilidade de acesso à informação (direito constitucional protegido), não podem mais deixar de ser uma preocupação inerente ao profissional da informação, visto incorporarem-se a seu próprio fazer.

Portanto, uma reflexão ética a mais se incorpora ao métier desse profissional, qual seja, aquela de buscar, pelas formas que lhe forem legitimamente acessíveis, propiciar que o acesso e a recuperação de informações se façam em moldes consonantes com a estrutura jurídica estabelecida, atuando não apenas como um mero disponibilizador de informações, mas como um valioso colaborador das instâncias jurídicas que visam garantir tais direito.

3. Referencias bibliográficas

CORREA, Gustavo Testa. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 2000. 135 p. p. 43.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Décimo Congresso sobre Prevenção de Delito e Tratamento do Delinqüente**. Disponível em: http://www.onu.org/. Acesso em 11 out. 2007.

PAESANI, Liliana Minardi, **Direito e Internet: liberdade de informação privacidade e responsabilidade civil**. São Paulo: Atlas, 2000. 141 p. p. 25.

PINHEIRO, Reginaldo César. **Os crimes virtuais na esfera jurídica brasileira**. São Paulo: IBCCrim, v. 101, p. 18-19, abr 2001 (separata).