CRIMES VIRTUAIS

Edson Mafra Alves[*]
Elaine Beatriz Pedroso[**]

RESUMO

A informática tem se tornado o principal meio de comunicação entre os indivíduos, passando a ser indispensável nas organizações, visto que, através dela é possível realizar pesquisas, comunicar-se, fechar contratos, etc. Porém, muitas informações são confidenciais, e impõem a necessidade da utilização de *logins* e senhas, principalmente em transações bancárias em que há movimentação de dinheiro. Em conseqüência dessa dependência da informática que empresas e pessoas têm, surgiram indivíduos que têm por objetivo coletar informações importantes para conseguirem, de alguma forma, lucro. Esses indivíduos estudam, baixam programas da Internet, se atualizam, e invadem computadores à procura de senhas, saldos, transações e informações confidenciais. Estes são os chamados "*hackers*", que se dedicam a invadir computadores. Em distintas pesquisas, verificou-se que existem vários fatores que são vistos como ameaças aos sistemas de informática, como vírus, falhas na segurança física, funcionários, senhas disponibilizadas a qualquer um, utilização de *notebooks*, mensagens de *e-mails* desconhecidos, falta de conhecimento dos usuários, entre outros. Com tantas ameaças, torna-se cada vez mais difícil proteger-se de crimes. No entanto, na atualidade não há possibilidade de deixar de utilizar os meios eletrônicos, pois estes reduzem gastos, diminuem a necessidade de empregados, proporcionam rapidez e agilidade nos serviços realizados através do computador. Com o aumento de crimes virtuais, observou-se a necessidade de criar leis que protejam as pessoas prejudicadas ao utilizarem este meio eletrônico. A Lei nº 84 de 1999, dispõe sobre crimes de informática, suas penalidades e providências. Entre os crimes abordados nesta lei estão: utilização ou alteração de programas; acesso indevido ou não autorizado a computadores; alteração de senhas de entrada em programas sem autorização; obtenção de dados ou instruções constantes em computadores, sem autorização; violação de segredo armazenado; e veiculação de pornografia. Sendo que para cada crime, há uma penalidade e providência a ser tomada. Portanto, além de invasões, existem outros crimes cometidos em computadores particulares ou de empresas, realizados por *hackers* ou simplesmente pessoas que tenham acesso, como funcionários. Por isso, torna-se importante levar ao conhecimento da população a necessidade de tomar providências quanto à segurança de seus computadores e implementar o treinamento de pessoas confiáveis para utilizá-los, bem como promover a veiculação da Lei que penaliza aos que cometem crimes através de meios virtuais.

PALAVRAS-CHAVES: Crimes Virtuais; *Hackers*; Segurança da Informação; Leis; Computador; Informática; Penalidades.

ABSTRACT

Information technology has become the main means of communication among individuals and has become indispensable to any of enterprise. Through it people can communicate, conduct surveys, make deals, etc. However, much information is confidential and it is necessary to use passwords and logins, mainly in bank transactions in which there is money transference. As a result of people's dependence on information technology, many persons try to gather important information in order to, somehow, make a profit. These individuals study, download internet programs, up date themselves and invade computers in search of passwords, bank balances, transactions and confidential information. They are the so called "hackers", people who dedicate themselves to computer invasion. In different surveys, it was found that there are several factors which are regarded as threats to information technology systems, such as viruses, physical safety failures, indiscriminate availability

* Tecnologia de Processamento de Dados - Centro Universitário Filadélfia – UniFil.
** Docente da UniFil. Advogada. Especialista em Direito e Processo Penal pela Universidade Estadual de Londrina - UEL. Orientadora da presente pesquisa.

of passwords, the use of laptops, messages from unfamiliar e-mails, lack of users' awareness, among others. With so many threats, protection from crimes is becoming more and more difficult to achieve. In spite of this, nowadays there is no possibility of giving up the electronic means, for they lower costs, reduce the need for labor, provide speed and agility to the services rendered through the computer. New laws have become necessary, as a result of the rise in virtual crimes, in order to protect people who use the electronic means. Law # 84, enacted in 1999, concerns information technology crimes and establish penalties and steps to be taken. Among the crimes described by this law are: use or alteration of programs, unauthorized or undue access to computers, unauthorized changing of passwords to programs, unauthorized gathering of data or instructions stored in computers, violation of stored secrets and pornography distribution. For each crime there is a penalty and a step to be taken. In this way, besides invasions, there are other crimes committed against private or business computers by hackers or people with access to the computers, such as employees. In view of this, it is necessary to make the general public aware of the need to take measures concerning the safety of their computers and to implement the training of reliable persons to use them, and also promote the divulging of the law that penalizes those who commit crimes through virtual means.

KEYWORDS: Virtual crimes; *Hackers*; Information safety; Laws; Computer; Information technology; penalties.

INTRODUÇÃO

O mundo vem assistindo a uma grande popularização de microcomputadores e da Internet. Temos hoje a Internet como uma forma de comunicação que ganhou e vem ganhando, diariamente, um número maior de usuários, no menor tempo visto na história da humanidade.

A Internet oferece muitas oportunidades para o desenvolvimento da humanidade. É possível concluir que essa grande evolução é devida ao simples fato de que antigamente todo procedimento envolvendo comunicação era demorado, pois dependia de uma resposta de determinada pessoa. Hoje podemos ter tal resposta em questão de minutos (e porque não dizer segundos), tudo dependendo de um simples clique.

Nos serviços bancários eram necessários os famosos *office-boys,* que depois passaram a ser chamados de auxiliares de escritório; e agora, qual será o novo nome a ser dado a eles? Se é que ainda sobreviverão a essa nova tecnologia.

Nessa nova era em que vivemos, em questão de minutos podemos fazer diversas transações bancárias sem que haja necessidade de sairmos de nossas cadeiras ou de fazermos um mínimo esforço.

Devido ao crescimento desordenado da Internet e à falta de informação dos usuários, vem aumentando a cada dia os delitos pela Internet, os chamados "Crimes Virtuais". Estes estão se tornando constantes em nossa sociedade, causando um grande desconforto, pois não podemos nem mesmo confiar em nossas próprias máquinas. No entanto, pouco se conhece sobre os aspectos jurídicos relacionados a esses crimes, tornando a grande rede de computadores um local ideal para a prática de tais delitos.

DESENVOLVIMENTO

2.1. Importância do tema

Pode ser observado que não somente nas empresas de médio e grande porte, mas também em computadores pessoais, a segurança dos dados está se tornado uma exigência e não mais uma opção como antigamente, uma vez que qualquer vazamento de informações pode causar prejuízos, tanto pessoais como financeiros.

A segurança da informação não era tida como um foco principal, e os investimentos nessa área eram uma opção da empresa e não uma exigência legal. Mas com o crescimento da Internet e a informação sendo disponibilizada facilmente, os investimentos passaram a ser necessários, pois assim proporcionavam maior confiança para os usuários, agregando mais valor aos serviços prestados pela empresa.

Porém, mesmo com grandes investimentos em segurança, muitas vezes, passam despercebidos atos simples que podem causar transtornos, como por exemplo, o fato de se falar com uma pessoa ao telefone identificando-se como um gerente de sua conta bancária pessoal, fazendo simples perguntas e ao final solicitando que o interlocutor digite a sua senha no telefone. No momento em que menos se espera, percebe-se que foi vítima de um golpe chamado de "engenharia social".

A Internet oferece inúmeros recursos em que um simples acesso e/ou *download* de programa, permite que o 'agente do crime' instale-se no computador. Porém, facilmente encontram-se programas que ensinam a invadir outras máquinas e sistemas. Tendo em vista essa grande facilidade de acesso a tais programas, qualquer pessoa pode se dizer um *hacker* em potencial, pelo simples fato de poder utilizar um programa pronto, baixado através da Internet. Porém, os indivíduos que realmente são *hackers*, dedicam horas de suas vidas estudando códigos e buscando sempre aprender algo a mais no ramo escolhido, não ficando dependentes de programas ou pessoas.

Com isso, o crescimento dos crimes virtuais é nítido, podendo o cidadão sofrer ataques de todas as formas possíveis, tais como furto de senhas de bancos através de programas de "*KeyLoger*". Ou programas de "*Sniffer*" em redes de *Cyber*-cafés, faculdades, redes corporativas ou particulares, para capturar todo o tráfego da rede; ou ainda métodos de "F*ishing Scam*" para enviar cópias idênticas de *sites* de banco para o *e-mail* da vítima, solicitando a troca de senha.

Mas muitas vezes esses crimes virtuais não são causados somente por programas ou por vírus que circulam pela grande rede de computadores. Os crimes podem ser perpetrados pelos próprios funcionários da empresa, como é mostrado na reportagem abaixo.

> [...] Ameaça interna – "Nenhum sistema é completamente seguro e a Internet permite a exploração das falhas existentes", continua Scudere. Grande parte delas é interna: a maioria dos ataques a sistemas é feita por usuários autorizados. Segundo a Módulo Security Systems, empresa brasileira especializada em segurança de sistemas, a principal ameaça, depois dos vírus, é o funcionário insatisfeito, que se vinga da empresa ou de um superior
>
> (TERRA, 2005).

Devido ao grande aumento de crimes virtuais, também tem crescido a criação de novos tipos de delitos, como é citado no texto abaixo.

> [...] Não é só o volume de crimes virtuais que preocupa. "É possível que novos tipos de crimes possam ocorrer", previne Mauro Marcelo. "Ainda não se ouviu falar em homicídios, mas, se alguém invadir o sistema de um hospital, pode alterar a medicação de um paciente." Apesar dessa perspectiva, e da polícia ainda não ter quadros especializados, o policial é otimista. Para ele, mesmo quando trabalhosos, os casos de crimes virtuais são de fácil solução. "Qualquer ação na Internet exige um provedor", explica. Para chegar aos autores, a polícia dispõe de várias ferramentas e táticas, como programas que traçam a origem de mensagens ou quem hospeda os sites. "Não existem provedores piratas, todos são registrados. É por isso que os criminosos virtuais, por mais inteligentes e bem preparados que sejam, sempre deixam vestígios e, mais cedo ou mais tarde, são apanhados." (TERRA, 2005).

Por fim, neste artigo será desenvolvida uma análise crítica de alguns tipos de crimes de informática presentes no Projeto de Lei 84/99, abordando alguns tópicos referentes a criminosos de informática e o que faz com que esses indivíduos se motivem para agir assim.

2.2. Criminosos da Informática

Atualmente, é praticamente um engano se pensar que os crimes virtuais são cometidos por especialistas, visto que, com a evolução dos meios de comunicação, o aumento de equipamentos, o crescimento da tecnologia e, principalmente, a acessibilidade aos sistemas disponíveis, qualquer pessoa pode ser um criminoso de informática. Tendo um mínimo de conhecimento e acesso a grande redes de computadores, torna-se um indivíduo potencialmente capaz de cometer delitos.

Segundo Mauro Marcelo de Lima e Silva, chefe do Setor de Crimes pela Internet da polícia de São Paulo (www.modulo.com.br, 2005):

> O perfil do criminoso, baseado em pesquisa empírica, indica jovens, inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, "uma brincadeira."

Na Tabela 1, podem ser vistos os criminosos mais famosos do mundo.

Tabela 1 – Criminosos mais Famosos.

Kevin David Mitnick (EUA)

O mais famoso *hacker* do mundo. Atualmente em liberdade condicional, condenado por fraudes no sistema de telefonia, roubo de informações e invasão de sistemas. Os danos materiais que causou são incalculáveis.

Kevin Poulsen (EUA)

Amigo de Mitnick, também especializado em telefonia, ganhava concursos em emissoras de rádio. Ganhou um Porsche por ser o 102º ouvinte a ligar, mas na verdade ele tinha invadido a central telefônica, o que foi fácil demais para ele.

Mark Abene (EUA)

Inspirou toda uma geração a “fossar” os sistemas públicos de comunicação - mais uma vez, via telefonia. E sua popularidade chegou ao nível de ser considerado uma das 100 pessoas mais “espertas” de New York. Trabalha atualmente como consultor em segurança de sistemas.

John Draper (EUA)

Praticamente um ídolo dos três acima, introduziu o conceito de *Phreaker*, ao conseguir fazer ligações gratuitas utilizando um apito de plástico que vinha de brinde em uma caixa de cereais. Obrigou os EUA a trocar de sinalização de controle nos seus sistemas de telefonia.

Johan Helsingius (Finlândia)

Responsável por um dos mais famosos servidores de *e-mail* anônimo. Foi preso após se recusar a fornecer dados de um acesso que publicou documentos secretos da Church of Scientology na Internet. Tinha para isso um PC 486 com HD de 200Mb, e nunca precisou usar seu próprio servidor.

Vladimir Levin (Rússia)

Preso pela Interpol após meses de investigação, durante os quais ele conseguiu transferir 10 milhões de dólares de contas bancárias do Citibank. Insiste na idéia de que um dos advogados contratados para defendê-lo é, na verdade, um agente do FBI.

Robert Morris (EUA)

Espalhou "acidentalmente" um *worm* que infectou milhões de computadores e fez boa parte da Internet parar em 1988. Ele é filho de um cientista, chefe do National Computer Security Center, parte da Agência Nacional de Segurança.

Fonte: (UNIV, 2005)

2.3. Motivação dos *hackers*

Alexandre Jean DAOUN e Renato M. S. Opice BLUM dividem a motivação dos *hackers* em cinco aspectos: (Aspectos Jurídicos Relevantes, p.122):

> 1) Aspecto Social – Cuidam de ganhar ascensão no grupo social em que vivem, através de ataques bem sucedidos a redes importantes ou sites famosos, e com sua posterior pichação, ganham destaque dentro da comunidade underground, sendo mais considerados pelo grupo e com isso ganhando acesso a informações de ponta, pois não há poder sem informação;
>
> 2) Aspecto técnico – O fim perseguido, é a demonstração das falhas dos sistemas que, segundo os hackers, foram deixadas propositalmente pelos criadores dos programas;
>
> 3) Aspecto político – São os que têm fortes convicções políticas. Utilizam invasão dos sistemas para "passar seus ideais". São pequenos focos politizados e atuantes que brigam por uma causa e se expressam no meio eletrônico;
>
> 4) Aspecto laboral – Compreendem indivíduos que buscam um emprego, mostrando que são melhores que aqueles que desenvolvem o sistema invadido. Incluem-se também os que são contratados pela promessa de prêmio por colocarem à prova os novos mecanismos de segurança informatizados;
>
> 5) Aspecto governamental internacional – Envolve os atos praticados por um governo contra outro. É o avanço da tecnologia de um país sobre a de outro. Sabemos que tal tendência, iniciada com a chamada 'guerra fria', transcendeu a Guerra do Golfo. É a tendência natural de substituição gradual de armamentos pesados por tecnologias de ponta.

O mundo das invasões se divide em diversos grupos, dentre eles:

Hackers: são pessoas ou especialistas com capacidade muito superior ao normal que têm uma grande capacidade de achar falhas (*Bug*) em um sistema ou programa qualquer e consertá-las; ou avisar os seus respectivos desenvolvedores. Hoje em dia, a imagem deles é muito destorcida pela mídia.

Crakers: ao contrário dos *hackers* são os criminosos mais temidos da grande rede de computadores. São movidos pelo dinheiro e fama. Sempre estão à procura de alguma brecha na segurança das redes para roubar dados e interferir em *sites*. A maioria dos *crakers* mantém *sites* com programas e códigos fontes para exploração de brechas. O diferencial nos *crackers* é a solidariedade; quando algo novo é descoberto, um novo programa é feito ou alterado, eles disseminam, para causar um dano maior.

Hacktivistas: na verdade são os *crakers* envolvidos em movimentos políticos ou ideológicos. O surgimento da categoria não foi direcionado para fins lucrativos, mas sim para promover as suas causas.

Carders: são especialistas em criar programas para gerar números de cartão de crédito, possibilitando a qualquer um fazer compras em *sites* de comércio eletrônico sem pagar, é claro.

Phreakers: especializados em telefonia. Fazem parte de suas principais atividades as ligações gratuitas, tanto locais como interurbanas, reprogramação de centrais telefônicas e instalação de escutas.

2.4. Principais ameaças

Segundo a 9ª Pesquisa Nacional de Segurança da Informação, realizada em outubro de 2003, o vírus de computador continua sendo, o maior causador de problemas nos sistemas de informática de uma empresa. Conforme a pesquisa da Modulo, 66% das invasões são causadas por vírus, e 78% dos entrevistados entendem que os problemas com vírus, no ano de 2004, vão aumentar.

Em segundo lugar, entre os maiores causadores de problemas situa-se a insatisfação do funcionário com 53%. Em terceiro figura a divulgação indevida de senhas dos funcionários, com 51%. Funcionários sem nenhum conhecimento e totalmente despreparados, sem noção dos danos que podem ser causados, não tomam os devidos cuidados com suas senhas e, de boa-fé, as entregam a pessoas não autorizadas.

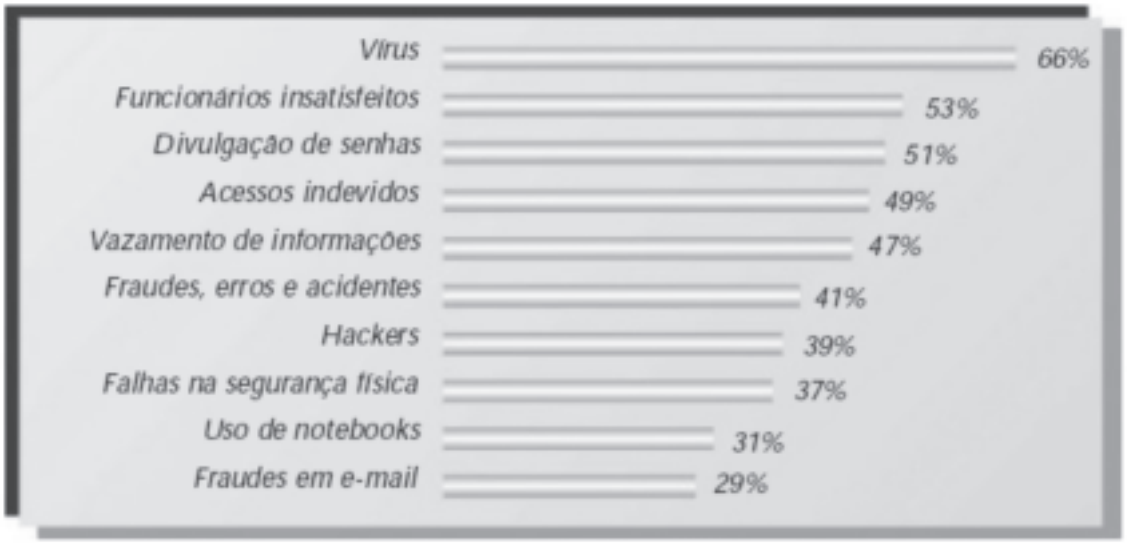

Figura -1: 9ª Pesquisa Nacional sobre Segurança da Informação.
Fonte: Modulo Security Solutions – E-security Magazine.
Outubro de 2003 (Modulo, 2005).

Conforme mostrado na Figura 1, a grande causa dos problemas de segurança que hoje afligem as empresas é relativa a vírus e funcionários insatisfeitos. No entanto, entre as ameaças mais freqüentes de falhas de segurança, estão aquelas que ocorrem pela 'porta da frente', isto é, a divulgação de senhas e o acesso ou o uso indevido por funcionários da própria empresa. Foi possível observar nesta pesquisa que a grande preocupação não é mais com *hackers*, ficando em 7º lugar, com 39%.

2.5. Legislações penais para crimes de informática

Atualmente, o Brasil está caminhando para a criação de uma legislação especifica para os crimes de informática através da Lei nº 84/99. Enquanto se estuda leis atualizadas, algumas outras leis e artigos estão sendo utilizados por autoridades para efetuar a prisão dos criminosos virtuais.

Segundo o *site* da Modulo Security, foi publicado um artigo no *site* da Polícia Civil do Estado do Rio de Janeiro, onde podem ser verificadas algumas das legislações que a Delegacia de Repressão aos Crimes de Informática (DRCI) utiliza para autuar os criminosos virtuais.

Na Tabela 2 figuram aspectos da legislação veiculada pelo *site* da Policia Civil do Rio de Janeiro.

Tabela 2: Legislações do *site* da Policia Civil do Rio de Janeiro.

Inserção de dados falsos em sistema de informações	Art.313-A do C. P.
Adulteração de dados em sistema de informações	Art.313-B do C. P.
Crimes contra a segurança nacional	Art.22 / 23 da Lei 7.170/83
Interceptação de comunicações de informática	Art.10 da Lei 9.296/96
Interceptação de E-mail comercial ou pessoal	Art.10 da Lei 9.296/96
Crimes contra software "Pirataria"	Art.12 da Lei 9.609/98

Fonte: (POLICIA CIVIL, 2005).

2.6. Diferença entre crime comum e crime puro

A diferença entre crime comum e crime puro de informática é de grande importância, pois assim é possível fazer uma melhor análise dos projetos de lei. Para que ocorra um crime puro de informática são necessários dois elementos: que o crime seja cometido contra dados e com o uso de equipamentos de informática.

Um exemplo de crime puro de informática é aquele em que uma pessoa, utilizando-se de um computador e de um acesso à Internet, invade outro computador e rouba um banco de dados. Neste caso, estão presentes os dois elementos necessários para a caracterização do crime de informática.

Um exemplo de crime comum seria aquele onde uma pessoa, com o objetivo de destruir um banco de dados gravado em um disquete, quebra-o com as mãos. O delito praticado seria o de dano, já que o disquete sofre avarias, ficando sem utilidade para o fim a que se destinava.

2.7. Análise do Projeto de Lei 84/99

> Seção I: Dano a dado ou programa de computador
>
> Art. 8º. Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.
>
> Pena: detenção, de um a três anos e multa.

Neste artigo, o legislador pune quem apagar, destruir, modificar ou, de qualquer forma, inutilizar, total ou parcialmente, dado ou programa de computador. Pode ser visto que este é um crime puro de informática.

> Seção II: Acesso indevido ou não autorizado
>
> Art. 9º. Acessar de forma indevida ou não autorizada, computador ou rede de computadores.
>
> Pena: detenção, de seis meses a um ano e multa.

Neste artigo, o legislador pune quem acessar de forma indevida ou não autorizada, computador ou rede de computadores, pois ao ter acesso indevido sem a senha do usuário, fica caracterizado que o indivíduo violou a segurança e/ou de uma pessoa ou empresa.

> Seção VI: Criação, desenvolvimento ou inserção em computador de dados ou programas com fins nocivos
>
> Art. 13. Criar, desenvolver ou inserir, dados ou programas em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador, ou de qualquer forma, dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.
>
> Pena: *reclusão, de um a quatro anos e multa.*

No Artigo 13, o legislador pune quem criar, desenvolver ou inserir, dados ou programas em computador ou rede de computadores, de forma indevida ou não autorizada. *Enquadra-se aqui qualquer inserção dos programas de sniffer, keyloger, fishing scam e* vírus ou outros programas que possam causar qualquer prejuízo de indisponibilidade a empresa ou a um computador pessoal.

> Seção VII: Veiculação de pornografia através de rede de computadores
>
> Art. 14. Oferecer serviço ou informação de caráter pornográfico ou de sexo explícito, em rede de computadores, sem exibição prévia, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescente.
>
> Pena: detenção, de um a três anos e multa.

No Artigo 14, o legislador pune quem oferece um serviço de pornografia ou de sexo explícito, quando, ao se acessar a página, não se vê uma mensagem dizendo que o *site* é impróprio para menores. Lembrando que este não é simplesmente um crime puro de informática, mas na legislação geral é considerado crime, conforme consta no Estatuto da Criança e Adolescente.

> Art. 15. Publicar em rede de computadores cenas de sexo explícito ou pornográficas, envolvendo criança ou adolescente.
>
> Pena: reclusão, de dois a seis anos e multa.

No Artigo 15 do projeto de lei 84/99 o legislador pune quem divulgar na rede de computadores cenas de sexo explícito ou pornográficas envolvendo criança ou adolescente. Este artigo prevê um crime comum, visto que consta no Estatuto da Criança e Adolescente.

> CAPÍTULO IV: DAS DISPOSIÇÕES FINAIS
>
> Art. 16. Se qualquer dos crimes previstos nesta lei é praticado no exercício de atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

No Artigo 16 é punido quem está praticando o crime, no exercício de atividade profissional ou funcional, ou seja: em seu trabalho.

3. Conclusões

A segurança da informação é um tema muito complexo e difícil de ser compreendido, pois envolve diversas áreas. Para que haja uma melhor compreensão da segurança da informação é necessário a união de todos para se construir um sistema com menos falhas e mais seguro, pois assim todos ganharão com a segurança.

A criação de leis que auxiliem e que ajudem na detenção das pessoas que cometem os crimes de informática deve ser mais criteriosa, pois somente assim haverá um melhor controle sobre estes crimes. Decretos, programas de computador e manuais de conduta não trarão grandes resultados no combate aos crimes de informática. É necessário uma mudança cultural em toda a sociedade.

4. REFERÊNCIAS

ADVOGADO. Disponível em <http://www.advogado.com/internet/84-99.htm>. Acessado em 11/09/2005.

LUCCA, Newton de. *Direito e Internet: aspectos jurídicos relevantes.* 1.ed. Bauru-SP: Edipro, 2000.

MODULO. *Modulo Security.* Disponível em <http://www.modulo.com.br/pt/page_i>. Acessado em 13/09/2005.

MODULO. *Modulo Security*. Disponível em <http://www.modulo.com.br>. Acessado em 13/09/2005.

MODULO. *Modulo Security.* Disponível em <http://www.modulo.com.br/pt/page_i>. Acessado em 17/09/2005.

POLÍCIA CIVIL *Polícia Civil do Rio de Janeiro*. Disponível em <http://www.policiacivil.rj.gov.br/artigos/ARTIGOS/drci.htm>. Acessado em 17/09/2005.

TERRA. Disponível em <http://www.terra.com.br/istoe/digital/seguranca.htm>. Acessado em 12/09/2005.

UNIV. Universal Telecom S.A. Disponível em <http://www.univ.com.br/acmm/Public/Livro_SI/BIBLIOGRAFIA/HackersFamosos/hackers_famosos.htm>. Acessado em 13/09/2005.

MODULO. *Modulo Security.* Disponível em <www.modulo.com.br/pdf/lucena-segcorp.pdf>. Acessado em 11/09/2005.

CERT. BR**.** *Cartilha de Segurança para Internet*. Disponível em <http://cartilha.cert.br/fraudes/>. Acessado em 09/09/2005.

ESTADÃO. CONSULTOR JURÍDICO. Disponível em <http://conjur.estadao.com.br/ static/text/ 11500,1>. Acessado em 11/09/2005.

INVASÃO. Disponível em: <http://www.invasao.com.br>. Acessado em em 12/09/2005.

NTI. Disponível em <http://www.faimi.edu.br/nti/artigo.asp?id=1>. Acessado em 02/08/2005.

WAVE COMPANY. Disponível em <http://www.wavecompany.com.br/br/crimes.htm>. Acessado em 14/08/2005.