Crimes da Informática

Remy Gama Silva

Título: Crimes da Informática
Autor: Remy Gama Silva
Editora: CopyMarket.com, 2000

Crimes da Informática
Especialização em Direito Penal

Remy Gama Silva

Sumário

Título: Crimes da Informática
Autor: Remy Gama Silva
Editora: CopyMarket.com, 2000

Crimes da Informática
Especialização em Direito Penal

Remy Gama Silva

Introdução

O espantoso crescimento da informática nas últimas décadas, trouxe grandes benfeitorias para a sociedade como um todo.

Com estes avanços tecnológicos, surgiram novos tipos penais e também a transformação de crimes tradicionais em crimes não mais praticados na sua forma habitual.

Trata-se dos crimes da informática.

A sociedade moderna já não consegue viver sem os computadores, seja no trabalho, na escola, no uso pessoal e nas suas mais variadas utilidades.

Tanto a criminalidade nacional, como a internacional, acompanharam este desenvolvimento ampliando a tecnologia para o proveito criminal.

O direito estrangeiro tenta seguir esta evolução, discutindo e apresentando leis que coíbam os ilícitos, encontrando dificuldades em muitos aspectos legais.

O direito pátrio parece esperar que definições ocorram no exterior para começar a legislar especificamente sobre a matéria.

Este trabalho tem a finalidade de discutir o assunto, apresentando material para estudo e reflexão sobre a necessidade de uma legislação que trate do tema, adequando-se a globalização e a internacionalização decorrente destes crimes.

A pesquisa foi realizada em trabalhos, estudos e artigos, principalmente internacionais, já que nossa literatura é esparsa, começando a se desenvolver.

A Internet aqui foi muito utilizada com o objetivo único de aprimoramento, conhecimento e de poder proporcionar um estudo mais abrangente.

O comércio eletrônico está em pleno desenvolvimento, movimentando muito dinheiro, onde a obrigação de oferecer a máxima segurança, em todos os sentidos, é essencial.

Temos que nos adequar e enfrentar os crimes da informática para podermos sobreviver a um futuro globalizado, que está bem próximo.

1. Conceito de Crime da Informática

Na literatura científica e na imprensa pública, mais especificamente na internacional, desde a década de 60 já se fazia referência aos crimes da informática[1], com denominações outras, sendo, "*criminosos de computador*", "*as infrações cometidas por meio de computador*", "*criminalidade de informática*", "*fraude de informática*", "*infrações ligadas a informática*", "*delinqüência informática*", etc.

Artigos em jornais e revistas especializadas escreviam sobre temas relacionados aos crimes, tais como, a sabotagem de computador, manipulação de computador, espionagem e o uso ilegal de sistemas de computador.

A partir dos anos 80, surgiram casos de "hacker"[2], vírus, pirataria de programas, etc., onde começaram a se discutir também assuntos relacionados a segurança e controle de crimes.

Vários autores conceituaram os crimes da informática.

{©A Prof.ª IVETE SENISE FERREIRA, em artigo intitulado "*Os Crimes da Informática*" [3] , define: *"toda ação típica, antijurídica e culpável contra ou pela utilização de processamento automático de dados ou sua transmissão*". Em estudo introdutório de MANUEL LOPES ROCHA[4], este define a criminalidade informática, como "*aqueles que tem por instrumento ou por objeto sistema de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos".*

CARLOS M. CORREA[5], e outros, cita que "*conforme a definição da Organização para a Cooperação e Desenvolvimento Econômico (OECD), delito informático é qualquer conduta ilegal, não ética e não autorizada que envolva o processamento automático de dados ou a transmissão de dados*". (trad. livre).

O precursor da Organização para a Cooperação e Desenvolvimento Econômico (OECD) era a Organização para Cooperação Econômica Européia (OEEC) que foi formada para a reconstrução da Europa depois da Segunda Guerra Mundial.

O Profº ULRICH SIEBER[6], em trabalho produzido para a União Européia, escreve: "*foram produzidos conceitos mais amplos em relação a dados e crime de informação. Este trabalho está baseado na definição feita pela OECD",* já citada. (trad. livre).

Na década dos anos 70, o principal criminoso era o técnico da informática. Na década seguinte, nos anos 80, tanto os técnicos de informática quanto os funcionários de instituições financeiras eram os principais criminosos. Já na atual década, qualquer pessoa física pode praticar os crimes da informática, pelas inúmeras oportunidades que as novas tecnologias e os novos ambientes organizacionais proporcionam. [7]

A rapidez no desenvolvimento e o refinamento das técnicas na informática, principalmente com o surgimento da grande rede, denominada "Internet", dificultam a formação de um conceito específico, mais numa visão ampla definiria como "toda ação ilícita praticada com a utilização do computador ou por meio dele".

---

[1]Aaron M Kohn. "*Computer Criminals*", The Journal of Criminal Law,Criminology and Police Science, vol.60, nº 1, 1969.
[2]" Hacker" é um especialista em resolver problemas e descobrir furos de segurança em redes, como a Internet, é erroneamente confundido com um "cracker", que é uma espécie de pirata virtual, que penetra remotamente em computadores integrados à rede com o objetivo de causar algum dano ou obter informações ilegalmente.
[3] Estudos jurídicos em homenagem a Manuel Pedro Pimentel – SP: ed. Revista dos Tribunais, 1992, p.139.
[4] Direito da Informática Legislação e Deontologia – Lisboa: ed. Cosmos,1994, p.38.
[5] Derecho Informático – Buenos Aires: ed.Depalma, 1994, p.295.
[6] Legal Aspects of Computer-Related Crime in the International Society – COMCRIME-STUDY- 1998.
[7] Página da Internet: http://www.modulo.com.br/noticia/clip-22.htm , consultada em 11/05/99.

Não há dúvida, entre os autores e peritos, que tentam chegar a uma definição, de que o fenômeno crime de computador ou da informática existe.

Uma definição global ainda não foi alcançada.

Os crimes da informática podem envolver atividades criminais tradicionais, como furto, fraude, falsificação, dano, etc. e específicas, ou sejam o acesso não autorizado, a transmissão de vírus, material ofensivo divulgado na rede, etc. Com o aumento das redes de telecomunicações e o surgimento da Internet, globalizaram-se as atividades criminais. As tradicionais formas de delinqüir, tornaram-se não tradicionais.

Uma distinção deve ser feita entre o que é pouco ético e o que é ilegal. A resposta para o problema deve ser proporcional à atividade que é alegada. Só quando o comportamento é determinado para ser verdadeiramente criminoso é que deveria ser buscada a proibição criminal.

Calcula-se que 90% dos crimes da informática, relacionados aos crimes econômicos, são cometidos por funcionários das próprias empresas.

A impressão de que o criminoso de computador é um indivíduo menos prejudicial, ignora o óbvio. A ameaça atual é real. A ameaça futura será diretamente proporcional aos avanços tecnológicos da informática.

2. Dos Crimes

2.1. Categorias

Os crimes tradicionais relacionados à informática, descritos na legislação penal em vigor, mereceriam ser definidos em lei especial, para melhor interpretação e adequação. Com os recursos que a informática pode oferecer, a conduta delituosa chega quase que a perfeição dificultando, em muito, a sua identificação.

ULRICH SIEBER[8] em seu estudo, dispõe os crimes da informática em "*formas atuais de crime de computador*", sendo estas as infrações de privacidade, as ofensas econômicas, a espionagem, a pirataria de software e outras formas de pirataria de produtos, a sabotagem, a fraude, os conteúdos ilegais, as ofensas, o homicídio, o crime organizado e a guerra eletrônica.

FRANCESCO MUCCIARELLI[9] classifica três categorias como principais:

> a) "*Uma primeira, onde estão substancialmente unidos pela circunstância que o computador constitui a necessária ferramenta de realização pela qual o agente alcança o resultado legal";* (trad. livre)
>
> b) "*A Segunda categoria de crimes do computador, poderia incluir todos aqueles comportamentos ilegítimos que contestam os computadores, ou mais precisamente, seus programas"*; (trad. livre)
>
> c) "*A última categoria deveria juntar todas as possíveis violações da reserva sobre a máquina. Aqui entram em consideração as habilidades de colheita e elaboração de todo tipo de dados*". (trad. livre)

[8] Idem,ibidem.P.38
[9] Digesto delle Discipline Penalistiche – "*Computer (disciplina giuridica dell) nel diritto penale*"- Itália: ed: Utet, vol.II, p.376

Para MUCCIARELLI, os crimes seriam:

1) uso sem autorização ou furto de tempo;

2) subtração de informações, idéias, projetos, etc., contidas na memória do computador;

3) divulgação de segredo;

4) tutela do software;

5) fraude;

6) falsificação e

7) obrigação do empregado em manter segredo sobre as informações a que tem acesso.

DAVID E. THOMPSON e DESMOND R. BERWICK[10] consideram que nos últimos cinco anos, houve uma crescente preocupação da comunidade com o abuso e a apropriação de informações eletrônicas e o uso de computadores para cometer crimes. A tendência do não uso de documentos de papel está tendo um enorme impacto na natureza de crimes tradicionais como, o roubo, a fraude e a falsificação. A introdução do dinheiro eletrônico, compras on-line e acesso a sistemas de computadores privados, trarão formas de crimes eletrônicos que irão requerer regulamentação e controle legislativo. A disponibilidade de computadores e a confiança da comunidade no sistema de informações são um valioso recurso para organizações e indivíduos potencializarem o uso dos computadores nos crimes que envolvem fraude, pornografia, drogas, pedofilia, direitos autorais, e espionagem. (trad. livre)

RICARDO GUIBOURG[11] em seu manual, descreve tipos semelhantes aos já citados, incluindo entre outros, o homicídio por computador e a interceptação de comunicações. (trad. livre)

O Ministro LUIZ VICENTE CERNICCHIARIO, em entrevista à Revista Perícia Federal[12], considera que o estelionato é o crime que mais interessa, atualmente nos crimes por computador, tendo que haver uma definição prévia em lei específica para sua melhor aplicação.

Podem ser visualizadas três categorias gerais no ambiente de proteção de computador. São elas:

a) *Software, dados e informações.*

> Exigências de proteção para software, dados e informações estão baseadas na necessidade de preservar a confidência, integridade e disponibilidade. A confidência pode ser requerida, porque o sistema contém dados pessoais, informações de uma organização ou até dados relacionados a segurança nacional. A integridade de dados é exigência de todo sistema de computador. Usuários do sistema exigem garantias de que mudanças sem autorização, deliberada ou acidentalmente, não aconteçam. A preocupação da disponibilidade é importante a curto e em longo prazo.

b) *Serviços de processamento de dados.*

> Serviço de processamento pode ser o recurso mais importante para requerer proteção em casos onde a segurança nacional, a segurança ou sustento de cidadãos individuais ou serviços essenciais, são dependentes dos sistemas de computador, p.ex., controle de tráfego aéreo, informações policiais, sistemas de monitoramento médico, fundos eletrônicos de transferência, etc.

[10] National Police Research Unit – "Minimum Provisions for the investigation of computer based offences – October 1997, p.7.
[11] Ricardo Guibourg, Jorge Alende, Elena Campanella. *Manual de Informática Jurídica*. Buenos Aires: ed. Astrea, 1996, p.273
[12] Perícia Federal – Publicação da Associação dos Peritos Criminais Federais – ano I, nº 1, março/99, p.6

c) *Equipamento de processamento de dados eletrônicos e instalação.*

> Esta categoria envolve a propriedade tangível. O próprio computador e materiais, as instalações físicas, bibliotecas de mídia, áreas de preparação de dados e áreas terminais, como também os serviços ambientais.

Assegurar proteção completa envolve outras áreas que devem ser levadas em conta, como pessoal, segurança física e comunicação eletrônica, muitas vezes desprezadas.

Não tratarei aqui de um estudo individualizado, pois, tornaria este trabalho muito extenso e desnecessariamente fatigante.

Descreverei as condutas que trazem maior preocupação.

2.2. Os crimes praticados com a utilização do computador ou por meio dele

Para facilitar a compreensão esta categoria é definida como sendo aquela em que o computador é o instrumento para a execução do crime, podendo também, ser o meio para atingir um propósito ilícito.

Aqui a máquina, sob comandos, executa a tarefa ou transfere comandos para a execução em outra máquina.

Destaco os crimes:

2.2.1. Espionagem informática

A espionagem caracteriza-se pela alteração dos programas do computador que pode ser efetuada pela troca de cartões, discos ou fitas originais, por falsos, modificando-se assim a programação originária, promovendo o acesso ao banco de dados, registros, etc. O acesso intencional e injustificado de uma pessoa não autorizada pelo dono ou operador de um sistema de computador pode constituir um comportamento criminal. Este acesso é freqüentemente realizado de um local remoto, ao longo de uma rede de telecomunicações, dentre outros meios. O intruso pode tirar proveito da falta de segurança, ou encontrar falhas de segurança existentes no sistema utilizando programas específicos para este fim. Quando a informação é subtraída levando-se a parte corpórea (fita, disco, etc), as providências penais tradicionais, como o furto e a apropriação, não criam problemas para o sistema penal. Porém, quando as informações são copiadas rapidamente pelos sistemas de telecomunicações, sem a presença do agente, subtraindo-as, surge a questão sobre a extensão da aplicação da legislação penal. Países como a Áustria, Bélgica, Alemanha, Grécia e Itália, são relutantes em aplicar as providências tradicionais em roubo (denominação utilizada nestes países) e apropriação de informações de dados, porque suas leis geralmente requerem que o bem seja corpóreo e retirado com a intenção de privar permanentemente a vítima. Na França, aplicação da legislação penal tradicional, seria possível dentro de alguns casos específicos. Nos Estados Unidos, alguns tribunais consideram as informações contidas no computador como propriedade, no senso de apropriação tradicional e em muitos Estados americanos as legislações definem os dados de computador ou a informação sigilosa, como propriedade, ou valor, afim de habilitar a aplicação da apropriação. O termo propriedade insinua exclusividade, posse, enquanto que a informação tende a ser concebida como um bem público. Destaque-se as informações pessoais e as confidenciais. No direito pátrio, o furto não requer comentários neste trabalho, já a denominação furto de informações merece algumas observações. Comparando-se analogicamente, a informação e a energia elétrica, temos que a informação pode ser bem móvel, passível de furto. Sendo bem móvel pode-se, usufruir, gozar, modificar, etc, ou seja, é propriedade. Havendo a alteração em

programas de computador, por meio da espionagem, para a transferência ou subtração de informações e dados do computador para uma pessoa não autorizada, conclui-se pela existência do furto de informação. Seguindo esta linha de raciocínio a apropriação pode existir, quando os dados ou informações não forem subtraídos, mas sim, copiadas por meio de artifícios eletrônicos mantendo-as intactas, sem que seu proprietário perceba que estas foram clonadas. Raramente este tipo de delito aparece em estatísticas oficiais, constituindo um perigo se comparado com a espionagem tradicional, pois em sistemas de computador são armazenadas enormes quantidades de dados em um espaço muito pequeno e estes dados podem ser copiados rapidamente e facilmente com a ajuda de tecnologia moderna, inclusive pela rede de telecomunicação. Em estudo realizado com 1.000 empresas pela revista americana "Fortune", foi reportado em 1997 mais prejuízos devido ao vandalismo e a espionagem do que em anos anteriores. Várias empresas informaram que as perdas alcançaram valor superior a US10 milhões de dólares em uma única invasão.[13]

2.2.2. Sabotagem informática

É a danificação ou destruição do material de que é feito o computador ou seus componentes. Os objetivos da sabotagem de computadores são as instalações tangíveis, como também os dados intangíveis que contém os programas de computação e outras valiosas informações, causando danos físicos e lógicos. A sabotagem envolve, tanto o acesso sem autorização como o acesso efetuado por um funcionário, em sistema de computador para a introdução de programas conhecidos como o do vírus. A modificação sem autorização e a supressão de dados do computador ou de suas funções, seja pela Internet ou no próprio sistema, impedindo o seu normal funcionamento, são atividades claramente criminais. A sabotagem de computador pode ser o veículo para garantir vantagem econômica sobre um concorrente, pode promover atividades ilegais de terroristas e pode também ser usada para destruir dados ou programas com o propósito de extorsão. O vírus é uma série de códigos de programas que tem a habilidade de se prender em outro programa e se propagar por outros sistemas de computação. Os propósitos potenciais de um vírus são muitos, podendo variar desde a exibição de mensagens inofensivas, até a destruição total e irreversível de todas as informações e dados de um sistema operacional. A dependência da sociedade em sistemas de computação, faz com que a extorsão de computador seja uma forma perigosa de ataque. Nestes casos a vítima é ameaçada da destruição total ou parcial de seu sistema ou pela divulgação de informações sigilosas e pessoais, caso não pague quantia em espécie, designada pelo agente. Em 1990, comunidades de pesquisas médicas da Europa sofreram sabotagem por meio de ataques de vírus, usados para cometer extorsão, onde quantias significantes de valiosos dados seriam destruídos de forma crescente caso não fosse efetuado determinado pagamento para a solução do problema. A sabotagem informática é um crime a ser especificado em lei própria para enquadramento e justificação adequados. A extorsão é possível desde que demonstrada a grave ameaça, o constrangimento e se considerado como crime material, o recebimento da vantagem indevida. Os vírus muitas vezes estão em um software pirata ou são captados pelo uso da Internet. Apenas neste ano de 1999, dois casos de vírus tornaram-se notórios, pela sua capacidade de proliferação. São eles o "Happy 99" e o "Melissa". Agentes do FBI conseguiram chegar a um suspeito, usando um recurso do Word chamado "Guid", que permite identificar a máquina na qual foi composto um determinado documento para identificar o autor do arquivo[14].Um fenômeno novo é a implementação de software para chocar programas e sistemas de computador.

[13] Página da Internet: http://www.modulo.com.br/noticia/a-mitos.htm – consultada em 14/05/99
[14] Página da Internet: http://www.modulo.com.br/noticia/a-melis.htm – consultada em 14/05/99

2.2.3. Estelionato

A figura do estelionato é caracterizada pelo emprego de meios fraudulentos, induzindo alguém em erro, para obtenção de vantagem ilícita. Consiste no fato de quem, por meio enganoso, causa dolosamente injusto dano patrimonial a outrem. Desta forma, melhor se moldaria o tipo, para se enquadrar na esfera da informática, na figura da fraude informática, onde esta seria a lesão ao patrimônio por meio enganoso, consumando-se, também, com o alcance da vantagem ilícita, em prejuízo alheio.

2.2.4. Fraude informática

É utilizada em muitos casos de crimes econômicos, como manipulação de saldos de contas, balancetes em bancos, etc, alterando, omitindo ou incluindo dados, com o intuito de obter vantagem econômica. A fraude informática é o crime de computador mais comum, mais fácil de ser executado, porém, um dos mais difíceis de ser esclarecido. Não requer conhecimento sofisticado em computação e pode ser cometido por qualquer pessoa que obtenha acesso a um computador. Tradicionalmente a fraude envolve o uso de cartões de bancos roubados ou furtados. Usando software específico, pode-se codificar amplamente as informações eletrônicas contidas nas tarjas magnéticas dos cartões de bancos e nos de crédito. A quebra do Banco Nacional revelou uma fraude eletrônica que estendeu por vários anos, sem que as auditorias ou o Banco Central tomassem conhecimento. Funcionários graduados do banco mantiveram 652 contas fictícias, sob controle de um micro não conectado ao sistema central de processamento. Os balanços eram desta forma fraudados mostrando lucros inexistentes. A fraude informática tem de ser estritamente separada de casos onde a falsa informação é usada para atacar outros interesses legalmente protegidos, p. ex., a vida. Existem leis específicas em fraude da informática em países como a Austrália, Áustria, Dinamarca, Alemanha, Finlândia, Luxemburgo, Japão, Holanda, Noruega, Espanha, Suécia e Estados Unidos. Porém em alguns países é requisito do delito de fraude, que a pessoa seja enganada. Se o computador foi o objeto enganado, não se aplica a legislação referente à fraude. É o caso da Áustria, Bélgica, Alemanha, França, Japão, Itália, Luxemburgo, Suíça, e outros. As conexões de computadores pelas redes de telecomunicações internacionais, abriram a possibilidade de se cometer manipulações, de fora das companhias, bancos e instituições. A Internet é muito usada para esta ação e propicia o surgimento de novos delitos, como, o falso anúncio, a fraude da pirâmide e o jogo ilegal. Em 1997, três sites para apostas foram processados no Estado de Winsconsin, Estados Unidos, por promoverem apostas pela Internet e desrespeitarem a legislação local.[15] Caso interessante aconteceu também nos Estados Unidos, na Califórnia, onde será julgado o primeiro caso dentro do Estatuto de Defesa do Ciberespaço, aprovado recentemente no Estado. O réu é um homem que usou o e-mail para tentar convencer uma mulher a fazer sexo com ele. Diante da recusa da vítima, ele forjou e-mails em nome da mulher convidando homens a irem ao seu apartamento, para satisfazerem sua fantasia sexual de ser estuprada. Alguns homens foram ao apartamento da mulher, que nada sofreu. O autor das mensagens foi preso e é acusado pelos crimes de assédio, preparar armadilha e estabelecer fraude pelo computador.[16] A muralha armada para evitar fraudes eletrônicas, invasões e quebras de sistemas compensa qualquer investimento: as perdas anuais por falha na segurança dos computadores chegam a US 7,5 bilhões de dólares, segundo estimativa do "FBI" e do "Computer Security Institute".[17]

[15] Página da Internet: http://www2.uol.com.br/info/infonews/160997c.html - consultada em 14/05/99
[16] Página da Internet: http://www.dgabc.com.br/internet/2201.htm – consultada em 14/05/99
[17] Revista Internet Business , ano 1, nº6, 1998, p.66

2.2.5. Contra a privacidade

Com a propagação volumosa de computadores, a proteção à privacidade tornou-se fator de preocupação para as pessoas. Como garantir a segurança das informações, para arquivos de dados de bancos, hospitais, empresas, etc. O anteprojeto do nosso Código Penal traz a figura da violação da intimidade.

Antes da invenção dos computadores a proteção legal das pessoas, com respeito ao conteúdo das informações pessoais, estava limitada. Com o surgimento da informática, novas tecnologias ampliaram as possibilidades de acesso a informações, causando novas ameaças à privacidade. Isto provocou muitos sistemas jurídicos estrangeiros a ordenar novos regulamentos civis e penais direcionados a proteção da privacidade. A maioria dos estatutos de privacidade internacionais inclui providências que limitam o direito de acesso em dados pessoais de outra pessoa. A proteção legal destas pessoas está ligada a providencias para o crime de calúnia e proteção de segredo profissional, principalmente no campo médico. A União Européia começou a harmonizar leis de privacidade em 1976. Uma inovação decisiva para a proteção da privacidade na Europa, foi alcançada em 1990, quando a Comissão das Comunidades Européias, submeteu um pacote com seis propostas no campo da proteção de dados pessoais e segurança de informação. O pacote inclui a proteção de dados, aplicável em todos os arquivos de dados pessoais, dentro da extensão da lei na Comunidade Européia. Para a União Européia a proteção da privacidade contra ofensas causada por tecnologia moderna é de grande importância, porém, esta proteção deveria ser resolvida em regulamentos de direito civil. O recurso da lei criminal, só deveria ser utilizado em ultimo caso. As providências criminais necessitam descrever precisamente os atos proibidos, devendo evitar cláusulas vagas e imprecisas.

Em princípio, infrações de privacidade relacionadas aos crimes da informática, só deveriam ser apenadas se o agente as efetuasse com intenção dolosa.

Constituições como a da Espanha (1978), a revisada de Portugal (1982), a dos Países Baixos (1983) e a do Brasil (1988), contém dispositivos de proteção específicos relacionados à privacidade dos cidadãos.

Algumas leis internacionais de proteção de dados definem as infrações de direitos da privacidade em:

- a revelação ilegal, disseminação, obtenção de acesso a dados, que estão cobertos na maioria das leis estrangeiras, para extensões diversas;
- o uso ilegal de dados, que são ofensas criminais, somente em alguns países;
- o acesso ilegal, modificação, falsificação de dados com a intenção de causar dano, criminalizado nas leis de privacidade e nos estatutos gerais de lei criminal de alguns países;
- registro e armazenamento de dados que são ilegais, em algumas leis de privacidade; e
- armazenamento incorreto de dados, coberto na maioria dos países, como ofensas gerais de informação e em outros através de estatutos adicionais das leis de privacidade.

2.2.6. Divulgação de material ofensivo

Nos anos 80 aconteceram casos em que foram distribuídas informações que glorificavam a violência e o racismo, com a ajuda de computadores.

Nos Estados Unidos, a "Ku Klux Klan", a "Resistência Ariana Branca", os "Skinheads" e outras organizações de neonazismo, perceberam que seria muito mais efetivo o trabalho com os meios de comunicação eletrônica do que com os informativos tradicionais.

Nos anos 90, a elevação da Internet, foi acompanhada de material ilegal e prejudicial.

Hoje o centro das atenções é: a pornografia infantil e a pedofilia, na rede internacional de computadores, Internet. A internet é responsável por 95% da pedofilia nos Estados Unidos[18]. No reino da pedofilia virtual, as crianças asiáticas são ouro puro, e estão expostas na Internet como produto da ignorância ou da fome de seus parentes, da mesma forma que meninos e meninas são vendidos ou se prostituem nas ruas da Tailândia para garantir o pão de cada dia. É dificílimo identificar quem produz e divulga a pedofilia na Internet, pois as fotos ou vídeos, mesmo que não exibidas em home pages tradicionais, já que os provedores de acesso estão atentos ao assunto, são espalhados por e-mail ou em qualquer ambiente da Internet onde seja possível o envio ou a troca de arquivos. Em janeiro deste ano (1999) a Unesco promoveu uma reunião em Paris/França com o tema "Exploração sexual de crianças, pornografia e pedofilia na Internet: Um desafio Internacional". O evento reuniu mais de 250 especialistas de 40 países, além de representantes de 75 organizações não governamentais. O tema debatido era, como deter de forma concreta a expansão da pornografia infantil e da pedofilia na Internet sem violar o direito à liberdade de expressão. Os conferencistas disseram que são necessárias novas estruturas legais e jurídicas para combater o problema e pediram a cooperação dos provedores de acesso à rede[19]. A Interpol assumiu um papel de coordenação das polícias de vários países, incluindo o Brasil, no combate do abuso sexual de crianças. A maior ação executada até hoje nessa área ocorreu em setembro passado (1998), quando 96 pessoas foram presas em 12 países. Entre elas estavam grupos que produziam estupros de crianças ao vivo. Em um único computador, de um finlandês, a polícia encontrou 48 gigabites de materiais pornográficos envolvendo crianças, uma quantidade de informação que ocuparia 30 mil disquetes. Nos Estados Unidos uma única pessoa tinha 75 mil fotos de crianças nuas ou envolvidas em atos sexuais. Um site brasileiro na Internet com fotos de crianças nuas e mantendo relações sexuais com adultos, que vinha sendo investigado pela Polícia Federal, foi retirado do ar em janeiro deste ano (1999). Com dezenas de fotos de crianças e adolescentes aparentando ter entre 6 e 17 anos, a "Mad's Sexy Page" era toda apresentada em português e estava hospedada em um provedor internacional gratuito, o Angelfire[20]. A Internet está se tornando rapidamente o fator mais significativo de abuso sexual de crianças e o principal meio de troca de pornografia infantil. Um dos principais desafios enfrentados pela Interpol é a diversidade das legislações. Muitos países nem se quer têm leis sobre a exploração sexual de crianças, menos ainda pela Internet.

A persecução criminal dos agentes de disseminam conteúdos ilegais, seja pela Internet ou não, é extremamente difícil pelo fato deles agirem também no exterior e pelos mecanismos internacionais de cooperação não estarem, ainda preparados para tal.

2.2.7. Acesso sem autorização.

O desejo de ganhar o acesso sem autorização a sistemas de computador pode ser iniciado por vários motivos. Da simples curiosidade em quebrar os códigos de acesso aos sistemas de segurança, até o acesso intencional para causar danos ou cometer outros ilícitos.

A proteção de contra senha é freqüentemente utilizada como um dispositivo protetor contra acesso sem autorização, porém, o hacker moderno pode evitar esta proteção, descobrindo a contra senha que lhe permite o acesso, introduzindo programa específico para este fim que irá capturar outras senhas de usuários legítimos. Se a intenção do agente for a de apenas penetrar no sistema, driblando a segurança, este será denominado hacker, mas se a intenção for a de causar dano ou cometer outro ilícito, a denominação correta será craker, como já definido no início deste trabalho.

Com o desenvolvimento dos sistemas de telecomunicações foram criados novos campos para a infiltração sem autorização. Estes sistemas de telecomunicações são igualmente vulneráveis a atividade criminal. Sistemas de

[18] Página da Internet: http://www.noticias.com/1999/9905/11/n99051104.htm - consultada em 10/06/99
[19] Página da Internet: http://www.uol.com.br/aprendiz/especial/pedofilia_Online/id010299.html - consultada em 10/06/99.
[20] Página da Internet: http://www.agestado.com.br/especial/noticias/internet/htm/128.htm - consultada em 10/06/99.

automatização de escritórios, com trocas de caixas de correio de voz, sistemas de computação projetados para a conveniência de seus usuários, etc., proporcionam o acesso de criminosos do computador.

O agente que maliciosamente usa ou entra em um sistema de computadores, na rede informática ou em qualquer parte do mesmo, sem autorização com o propósito de alterar, destruir, fraudar, obter vantagem, conseguir informações, interceptar, interferir, usar, provocar dano, danificar sistemas ou rede de computadores, comete o acesso não autorizado antes de qualquer outro crime.

São determinantes para o uso sem autorização de computador os seguintes elementos:

- a obtenção de qualquer serviço de computador seja direta ou indiretamente;
- a interceptação de qualquer comunicação, ou função do sistema de computador;
- a intenção de prejudicar o sistema ou o seu funcionamento;
- o uso do sistema de computação; e
- possuir, copiar, distribuir ou usar qualquer instrumento ou dispositivo do computador.

O acesso sem autorização a sistemas de computação, é a grande chave para a prática dos crimes da informática.

3. Internet

A estrutura que deu base à criação da Internet tem sua origem num sistema de interligação de redes de computadores nos Estados Unidos, para fins de proteção militar, no final dos anos 60.

Com a guerra fria no auge e a possibilidade sempre presente de um conflito nuclear em escala global, havia nos Estados Unidos a preocupação em montar um sistema logístico auxiliado por computadores que concentrasse toda a informação estratégica, mas que não fosse vulnerável a um único ataque nuclear.

A solução encontrada foi distribuir os recursos de computação por todo o país, mantendo-os interligados na forma de uma grande rede, mas de tal modo que a destruição de alguns não impedisse o funcionamento dos restantes. Uma rede de computadores em que nenhum, fosse isoladamente vital para todo o sistema.

Em 1993, surge a Internet comercial. Removeu-se as restrições que tornavam a Internet um privilégio de instituições de órgãos governamentais e permitiu-se a comercialização de acesso. Surgiu a figura do provedor comercial de acesso.

Em maio de 1995, começa a Internet comercial no Brasil. Forma-se o Comitê Gestor Internet/Brasil com a finalidade de coordenar e disciplinar a implantação da Internet comercial brasileira.

A Internet é hoje o resultado de uma experiência técnica bem sucedida cuja utilidade extrapolou seu objetivo original. É gigantesco o universo que a Internet alcança. Pode-se consultar bancos de dados em todos os países do mundo, visitar museus, faculdades e universidades, efetuar transações de compra e venda, bancárias, enfim, uma gama infindável de serviços.

O avanço tecnológico que provoca mudança nos hábitos sociais, tem como conseqüência gerar mudanças nas regras jurídicas.

O crescente uso da rede seja para consultar um saldo bancário, seja para comprar um livro, envolve envio ou recepção de informações, que devem ser protegidas. A rede é aberta a todos que se conectarem a ela, visita-se uma página, de qualquer assunto, quem quiser e a hora que quiser, porém, como ferramenta de comunicação fabulosa que é, não deve sofrer censura. O que não podemos aceitar é que criminosos usem a ferramenta.

Soluções e problemas navegam sem restrições no mundo dos computadores.

O princípio de rege a Web, parte do pressuposto de que todos os sites são invioláveis, até que um hacker ou craker prove o contrário.

A Internet de um modo geral surgiu com um conceito de uso, onde a preservação da autonomia e liberdade dos indivíduos que a utilizam, são fundamentais para o seu funcionamento. Daí surgem alguns problemas, com a tal liberdade de expressão utilizada e tão preservada pela rede, que chega a oferecer para consulta artigos e matérias completas não muito convencionais, divulgando fotos de crianças nuas ou praticando sexo, páginas com o modo de fabricação de bombas, racismo, etc. É certo que o acesso a estas páginas são efetuados de livre e espontânea vontade por qualquer pessoa, seja por curiosidade, para consulta ou por erro. Bombas relógio encontradas em escolas do Distrito Federal, foram fabricadas conforme indicações contidas em páginas da Internet[21]. Uma das bombas tinha alto teor explosivo e poderia, se detonada, causar mortes.

Difícil é encontrar uma maneira de conter estas inserções na rede. Empresas especializadas têm desenvolvido softwares que permitem a seleção do material disponível na Internet, assim estariam protegidas tanto as crianças, quanto o direito de expressão dos adultos. É o caso do bloqueador de acesso da empresa de software "Net Nanny"[22]. O Net Nanny permite monitoramento, seleção e bloqueio do acesso a tudo que está dentro do computador, inclusive alguns programas, esteja o usuário conectado ou não à Internet.

Senadores americanos propuseram a criação de leis de incentivo para que os sites da Internet possuam uma classificação, assim haveria a passagem da censura das mãos dos órgãos oficias para as mãos dos pais ou responsáveis pela educação das crianças e dos adolescentes, por meio de um software de filtragem, que depende desta classificação. No Japão já se experimentam os filtros contra obscenidades na Internet[23]. O Ministério da Indústria e Comércio Internacional do Japão e o Conselho de Redes Eletrônicas, presidido pela NEC Corp., estão trabalhando juntos para desenvolver sistemas de filtragem que negarão acesso a sites relacionados ao crime, sexo e violência.

As empresas brasileiras estão extremamente vulneráveis a ataques e invasões via Internet[24]. E o mais alarmante é que a grande maioria não possui uma política de uso e somente 22% possuem algum plano de ação formalizado em caso de ataques ou invasões. Um grande perigo, p. ex., é o acesso à Internet via modem utilizado em 42% das empresas pesquisadas, sem quaisquer medidas de proteção e controle. A preocupação maior é quanto ao vazamento de informações sigilosas e fraudes em mensagens utilizadas para operações e transações de negócios. Nos Estados Unidos, estima-se que as companhias americanas tenham prejuízos de mais de 300 bilhões de dólares com crimes por computador. Segundo relatório do FBI/CSI 1998, o valor médio das perdas anuais é de 568 mil dólares por empresa. Os principais fatores considerados para estes cálculos são decorrentes de prejuízos diretos como, perda de contratos, roubo de segredos industriais, fraudes financeiras, danos à imagem e custos com investigações, parada de serviços e reposição.

É difícil a prevenção dos crimes por computadores. A prevenção somente é possível através de uma combinação de medidas, tais como, o limite do acesso às informações e ao uso do sistema aliado a uma política de alerta, prevenção e controle, dirigida aos usuários finais. A Polícia Federal do Brasil dispõe de um setor que apura os crimes da informática, baseado no Instituto Nacional de Criminalística em Brasília, aonde vem com êxito, apesar das dificuldades encontradas, conseguido desvendar alguns casos, culminando inclusive com prisões em flagrante, como aconteceu em outubro de 1998 no interior de São Paulo, de um cidadão que divulgava e distribuía fotos de crianças praticando sexo pela Internet[25]. "*O material da Internet é muito volátil. É preciso agir depressa. Caso contrário, quando a gente chega não encontra mais nada"*, afirma o Perito Criminal Federal André Caricatti.

Em Belo Horizonte/MG, existe uma Delegacia especializada em crimes eletrônicos criada recentemente, pela Secretaria de Segurança do Estado[26].

---

[21] Página da Internet: http://www.jt.com.br/noticias/98/06/20/ge12htm - consultada em 07/04/99
[22] Página da Internet: http://www.8415.com.br - consultada em 05/06/99
[23] Página da Internet: http://infojur.ccj.ufsc.br.../Japao_experimenta_filtros_contra_obscenidades_na_internet.htm – consultada em 31/05/99
[24] Página da Internet: http://www.modulo.com.br/noticia/pesquisa.htm - consultada em 26/01/99
[25] Revista Sin-DPF, Sindicato dos Delegados de Polícia Federal/SP – ano 2, nº 7, nov/dez/98, p.27/32
[26] Página da Internet: http://www2.bhnet.com.br/lista-internet/msg00252.html – consultada em 10/03/99

França e Reino Unido dispõem de um serviço denominado "*linha quente*", em que os usuários da Internet podem denunciar páginas julgadas ofensivas ou que contenha material considerado ilegal.

A tentativa de regulamentação da Internet esbarra no problema da sua internacionalidade, que apresenta aspectos até o momento incompatíveis com o potencial existente. A idéia de uma regulamentação internacional, com a inclusão de países signatários, seria o começo para que a grande rede atingisse suas funções básicas, ou seja, a divulgação de informações de conteúdo legal, o comércio eletrônico global e o desenvolvimento científico e humano.

Na Europa se discute um código de condutas para os provedores, que começam a se antecipar aos legisladores e já estão fechando acordos com a Polícia Civil de São Paulo e a Polícia Federal do Brasil para liberar informações dos internautas brasileiros que mantém páginas incentivando ou divulgando crimes[27].

O Brasil ocupa o 1º lugar na América do Sul em número de computadores centrais que controlam redes (ver apêndice nº9.1) e o 17º lugar no mundo (ver apêndice nº9.2).

4. Software

Hoje o conceito de propriedade intelectual é baseado no reconhecimento de direitos naturais e na razão pragmática de estipular a criação de trabalhos, concedendo um prêmio ao seu criador.

No campo da informática este conceito é especialmente importante para a proteção de programas de computação.

Depois que programas de computação foram excluídos de proteção patente ao longo do mundo nos anos setenta, alguns países aprovaram novas leis para assegurarem a proteção por direitos autorais para estes programas.

Vários países promoveram a proteção por direitos autorais, explicitamente para programas de computação desde 1980. Foi o caso, p.ex., da Austrália, Áustria, Brasil, Canadá, Dinamarca, Alemanha, Finlândia, França, Hungria, Israel, Japão, Luxemburgo, Malásia, México, Filipinas, China Cingapura, Espanha, Suécia, Inglaterra e Estados Unidos.

Software é um conjunto de instruções lógicas desenvolvidas em linguagem específica, que permite ao computador realizar as mais variadas tarefas do dia a dia para empresas, profissionais de diversas áreas e usuários em geral.

O Brasil possui uma legislação específica de proteção a indústria do software.

É a Lei sobre Propriedade Intelectual de Programa de Computador (Lei 9.609, de 19/02/98), que disciplina a proteção da propriedade intelectual de programa de computador, sua comercialização no país e dá outras providências.

A pirataria de software é a reprodução, distribuição ou utilização de software sem a devida licença. Isto gera um problema mundial.

Existem também os produtos falsificados, consistindo na duplicação ilegal do software e embalado de forma que se pareça com o produto original.

Com a Internet a pirataria eletrônica ficou muito rápida, permitindo aos distribuidores de software ilegal chegarem a um mercado mundial, aumentando em muito seus lucros.

Dados da ABES (Associação Brasileira das Empresas de Software)[28], indicam que o índice de pirataria após a nova lei, chamada lei do software, caiu de 68% em 1997, para 61% em 1998, mas ainda continua muito elevado.

[27] Revista Veja, ed. 1596, ano 32, nº18, p.110, 05/05/99

Se comparado a dados estatísticos de outros países, estamos entre os grandes da pirataria. Nos Estados Unidos o índice é de 40%; na Alemanha sobe para 76%; no Japão vai a 86% e na Tailândia aos 98%.

As perdas são gigantescas, segundo relatório da "*Business Software Alliance*"[29], organização mundial das empresas que mais sofrem com esta pratica ilegal, o prejuízo chega a 11 bilhões de dólares anualmente.

Além do prejuízo financeiro das empresas de software, há o prejuízo do governo que perde sem a arrecadação dos impostos e traz consigo o desemprego.

A pirataria de software precisa ser tratada com seriedade pelas grandes empresas, pois, os danos à imagem e as penalidades previstas na legislação não justificam o uso irregular de programas de computador.

Uma importante inovação em nossa legislação é a caracterização da pirataria também como um crime de sonegação fiscal, o que torna a Receita Federal um dos agentes de fiscalização das empresas na investigação da procedência de programas utilizados em computadores.

5. Panorama Geral da Legislação Nacional e Internacional Relacionada aos Crimes da Informática

Algumas das atividades em ciberespaço podem precisar de nova legislação penal específica ou de fortalecer a já existente.

O acesso sem autorização a dados ou informações, como já foi dito, é o predicado fundamental para qualquer ofensa realizada com um computador. É a base de muitos crimes da informática.

Vejamos como estão as legislações de alguns países relacionadas aos crimes da informática em geral.

1) ARGENTINA - Projeto de Lei sobre Delitos Informáticos, tratando do acesso ilegítimo a dados, dano informático e fraude informática, entre outros tipos.

- arts. 183 e 184 do Código Penal.
- Decreto 165/94, relacionado ao software.
- Lei 11.723, Direito Intelectual.

2) ALEMANHA - Código Penal, Seção 202 a, Seção 263 a, Seção 269, Seção 270 a 273, Seção 303 a, Seção 303b;

- Lei contra Criminalidade Econômica de 15/05/86.

3) AUSTRÁLIA - possui Legislação Federal e os Estados têm independência para legislarem sobre o assunto.

4) ÁUSTRIA - Lei de reforma do Código Penal de 22/12/87, que contempla os delitos de destruição de dados (art. 126) e fraude informática (art. 148).

5) BELGICA - nenhuma legislação penal específica.

[28] Página da Internet: http://www.abes.org.br - consultada em 12/06/99.
[29] Página da Internet: http://www.uol.com.br/idgnow/pc/pc1703g.sh1 - consultada em 12/06/99.

6) BRASIL - nenhuma legislação penal específica. - Projeto de Lei 84/99, da Câmara dos Deputados, Dispõe sobre os crimes cometidos na área de informática, suas penalidades e outras providências. Deputado Federal Luiz Piuahylino.

- Lei 9.609, de 19/02/98 - Lei sobre Propriedade Intelectual de Programa de Computador.
- Lei 9.610, de 19/02/98 - Lei de Direitos Autorais.
- Lei 9.800, de 26/05/99 – Sistema de Transmissão de Dados e Imagens via fax ou similar.
- Código Penal.
- Estatuto da Criança e do Adolescente.

7) CANADA - Código Criminal, Seção 183, Seção 242.2, Seção 326, Seção 342, Seção 342.1, Seção 430.(1.1), Seção 487;

8) CINGAPURA - Ato de Abuso do Computador, Seção 3;

9) CHILE - Lei 19.223 de 07/06/93, sobre Delitos Informáticos.

10) CHINA - possui regulamentos para proteção da segurança de informações de computadores. Dec. 147 do Conselho Estatal da República Popular da China;

11) CUBA - Regulamento de Segurança da Informática em vigor desde novembro de 1996, emitido pelo Ministério do Interior.

- Regulamento sobre a Proteção e Segurança Técnica dos Sistemas Informáticos, de novembro de 1996, emitido pelo Ministério da Indústria Mecânica e Eletrônica.
- O vigente Código Penal – Lei nº 62 de 29/12/87, em vigor desde 30/04/88, modificado pelo Decreto Lei 150 de junho de 1994, traz um conjunto de figuras aplicáveis aos delitos cometidos contra sistemas informáticos.

12) DINAMARCA - Código Penal, Seção 263;

13) EGITO - nenhuma legislação penal específica;

14) ESPANHA - Novo Código Penal, aprovado pela Lei Orgânica 10/1995 de 23/11/95, traz vários artigos intimamente relacionados com os crimes da informática. Ex. arts. 197 a 201, arts. 211/ 212, art. 248, arts. 255/256, art. 279, art.278, art. 400, art. 536.

15) ESTADOS UNIDOS - Ato Federal de Abuso do Computador (18 USC. Sec. 1030), que modificou o Ato de Fraude e Abuso do Computador de 1986.

- Ato de Decência de Comunicações de 1995.
- Ato de Espionagem Econômico de 1996.
- Seção 502 do Código Penal relativo aos crimes da informática.
- Os Estados têm independência para legislar sobre o assunto.

16) FINLANDIA - Código Penal, Capítulo III, art. 323.1, art. 323.2, art.323.3, art. 323.4;

17) FRANÇA - Novo Código Penal, Seção 202 a, Seção 303 a, Seçã0 303 b;

- Projeto de Lei relativo a criminalidade informática.
- Lei 88-19 de 05/01/88 sobre Fraude Informática.

18) GRÉCIA - Código Criminal, art. 370 c, par. 2;

19) HONG KONG - Ordenação de Telecomunicação, Seção 27 a, Seção 161;

20) HUNGRIA - nenhuma legislação penal específica;

21) IRLANDA - Ato de Dano Criminal de 1991, Seção 5;

22) ISLÂNDIA - nenhuma legislação penal específica;

23) ISRAEL - possui Lei de 1979 relacionada a crimes informáticos.

24) ITÁLIA - Código Penal, art.491 bis, art. 615, art.616, art.617, art. 621, art. 623 bis, art.635 bis. Lei 547 de 23/12/93 - modifica e integra norma ao Código Penal e ao Código de Processo Penal em tema de criminalidade informática.

- Lei 675 de 31/12/96, sobre a Tutela da Privacidade.

25) JAPÃO - Tem legislação penal relacionada a crime de computadores;

26) LUXEMBURGO - Ato de 15/07/93, art. 509.1;

27) MALASIA - Ato de Crimes do Computador de 1997.

- Ato de Assinatura Digital de 1997.

28) NOVA ZELANDIA - nenhuma legislação penal específica;

29) NORUEGA - Código Penal, par. 145, par.151 b, par.261, par.291;

30) PAÍSES BAIXOS - Código Criminal, art. 138 a;

31) PERU - nenhuma legislação penal específica;

32) POLÔNIA - nenhuma legislação penal específica;

33) PORTUGAL - Lei de Informação Criminal nº 109 de 17/08/91. Lei de Proteção de Dados Pessoais, 67/98 de 26/10/98;

- Constituição Portuguesa, art. 35.
- Código Penal, arts. 193 e 221.

34) REINO UNIDO - Ato de Abuso do Computador de 1990, Cap. 18;

35) REP. DOMINICANA - Existe a proteção jurídica do autor e da propriedade intelectual. A Lei 32 de 1986 é considerada incompleta e necessita de atualização.

36) SUÉCIA - Lei de Dados de 1973, com emendas em 1986 e 1990, par. 21;

37) SUIÇA - Código Penal, art. 143 bis;

6. Competência para Processo e Julgamento

Grande dificuldade é a de definir a competência para o processo e julgamento dos crimes da informática, principalmente aqueles envolvendo vários países.

Juristas brasileiros já descreviam, na década de 80, a dificuldade em se estabelecer a competência para os crimes da informática, "*Essas condutas delitivas vão causar um problema grande que é o que se refere à competência – justamente por serem crimes cometidos a distancias ....*" [30]

Nos países em que existem leis específicas para o caso, temas como o da extraterritorialidade, jurisdição e competência são amplamente discutidos.

O que é considerado crime em um lugar pode não ser em outro, o que por si só já dificulta a forma de disciplinar a matéria.

O ideal seria a criação de um Estatuto Internacional definindo crimes de informática, impondo regras para a Internet e para o uso das redes de telecomunicações internacionais, com poder de questionar os países signatários e de punir os que contrariassem as regras impostas.

Seria um Estatuto com tipos penais internacionais, que poderiam também complementar as legislações penais específicas dos países membros.

O ciberespaço é um ambiente criativo informativo, muito lucrativo, porém, não harmonioso.

Com o uso da Internet pode-se obter acesso a um sistema num determinando país, manipular dados em outro e obter resultados em um terceiro país.

A elevação do crime organizado transnacional é um subproduto infeliz da globalização, por seus avanços tecnológicos e pelas baixas barreiras que o comércio eletrônico impõe.

Organizações terroristas também se beneficiam de operações transnacionais pelo acesso a tecnologia avançada, proporcionando maior facilidade de movimentação, encobrimento e de meios para esparramar suas mensagens, globalmente. O mesmo acontece com o tráfico de drogas, a lavagem de dinheiro, tráfico de órgãos, pedofilia, crimes financeiros, etc.

Crimes internacionais foram nutridos pelo desenvolvimento nas comunicações internacionais.

Mais do que qualquer outro crime transnacional, a velocidade, mobilidade, significação e valor das transações eletrônicas produzem profundos desafios às regras existentes em Estatutos Criminais.

[30] Valdir Sznick – "*Crimes Cometidos com o Computador*" in Justitia , vol.124, 1984, jan/mar, p.70.

Como determinar qual país está comprometido? De quem é a jurisdição para descrever as condutas e aplicar a lei?

Buscando soluções, a comunidade internacional deveria se esforçar para[31]: (trad. Livre)

- cooperação máxima entre as nações para ordenar e dirigir, primeiramente o grande potencial para perdas econômicas e secundariamente a ameaça da privacidade e outros valores fundamentais;
- proteção mundial para evitar paraísos de crimes da informática, onde os criminosos possam achar refúgio e lançar seus ataques; e
- um esquema de cooperação legalmente estruturado, levando-se em conta, por um lado o equilíbrio e as necessidades de relações comerciais internacionais e por outro lado os direitos e liberdades individuais.

Em todo crime de computador a determinação do lugar do crime dependerá da habilidade do país em descrever o crime.

Dependendo dos elementos ou fases do crime que determinarão a prioridade sobre a jurisdição o país dentro da sua soberania, poderá declarar o incidente como tendo acontecido em seu território, assim utilizando a sua legislação para processar os criminosos.

Os conflitos de jurisdição possuem riscos. O principal deles é quando o acusado é submetido a várias persecuções pelo mesmo ato.

Um mecanismo entre os países interessados poderia determinar a prioridade sobre a jurisdição, relacionados à ofensa exercida, com a divisão desta em atos separados.

Na sociedade global esforços técnicos e legais devem ser realizados em conjunto.

Nossos dispositivos legais mandam aplicar a lei brasileira aos crimes cometidos no território nacional, ou seja, no âmbito da validade espacial do ordenamento jurídico do Brasil.

O crime como unidade se entende praticado onde quer que ocorra, tanto na prática dos atos executórios, quanto na fase da sua consumação.

Pelos princípios da Territorialidade e da Ubiqüidade, a lei penal de um Estado só impera dentro dos seus limites territoriais e o lugar do crime é tanto aquele em que se inicia a execução, quanto aquele em que houver o resultado.

Mas os crimes da informática, em sua maioria, trazem aspectos divergentes pela sua natureza e pela globalização dos computadores.

A necessidade de uma legislação internacional que defina e de diretrizes para se firmar jurisdição e competência no caso dos crimes da informática é imprescindível.

Regras mínimas para atividades e conteúdos ilegais deveriam ser a base para todas as outras atividades de persecução internacional de crimes da informática. Estas poderiam ser:

a) regras mínimas criando providências de leis criminais com respeito aos crimes da informática.

b) poderes coercitivos adequados com respeito à investigação dos crimes informáticos em redes de computadores internacionais.

[31] "International Review of Criminal Policy – United Nations Manual on the Prevention and Control of Computer Related Crime". Página da Internet: http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html - consultada em 20/05/99.

c) investigações em redes de computadores internacionais.

d) definir a gama de jurisdições em redes de computadores internacionais, especialmente envolvendo conflitos de jurisdição internacional com respeito a conteúdo ilegal.

e) criar regras comuns para a harmonização das polícias especializadas em crimes da informática.

Para os crimes iniciados no Brasil, temos a prerrogativa sobre estes: "*os crimes cometidos em território nacional, embora tenham sido descobertos no estrangeiro, tem determinada a sua competência pelo lugar da infração*"[32].

Nacionalmente a competência para o processo e julgamento dos crimes da informática depende de cada caso especificamente. Na sua grande maioria é a Justiça Estadual competente para julgar os crimes informáticos, não afastando a Justiça Federal de ser competente dependendo do caso em concreto.

Em enquete realizada pelo "Canal Web", cerca de 67% dos internautas acreditam que a Justiça comum deve julgar os crimes na Internet.[33]

No entanto o professor Damásio alerta: "*Enquanto não houver polícia, juízes e promotores com o conhecimento necessário, o crime de informática será a melhor maneira de cometer delitos*".

Para o ex-juiz Luiz Flávio Gomes a prevenção dos crimes é o melhor recurso para evitar ataques.

Os crimes da informática, apesar de alguns ainda serem atípicos ao nosso ordenamento jurídico, são muitas vezes interestaduais, quando não transnacionais. Seus efeitos se estendem por vários países.

Casos de invasão ou acesso não autorizado a sistemas de informática acontecem diariamente, porém, poucos destes são divulgados. No mês de junho/99 foram invadidos sites do governo federal por um grupo que protestava contra o Presidente da República. Essas invasões alteraram dados das páginas provocando a sua retirada do ar para correção.

Apesar da atipicidade da conduta (invasão de sistemas informáticos), teria a Justiça Federal a competência para processar e julgar os infratores, pois, foram atingidos bens e serviços da União[34].

Uma pesquisa da "Transactional Records Access Clearinghouse" mostra que, apesar do crescimento dos crimes informáticos, são poucas as condenações nesses casos. O estudo mostra que, em 1998, apesar do aumento de 43% dos crimes em relação ao ano anterior, apenas 1 em cada 5 casos levados a julgamento recebem condenação, índice bem abaixo de outras categorias de crimes.

Um porta voz do FBI afirma que esse tipo de delito é muito mais difícil de se provar que os demais, o que leva ha um baixo índice de condenação[35].

Estima-se que as transações comerciais pela Internet irão movimentar em 2003 valores superiores a 1 trilhão de dólares. A importância é tanta, que a Organização Mundial do Comércio, em um Acordo Internacional com 132 países, incluindo o Brasil, determinou que o comércio eletrônico permanecerá até 1999 sem regulamentação, para que amadureça e conquiste seu espaço sem as amarras da regulamentação[36].

A importância e a necessidade de proteger as transações comerciais realizadas pela Internet serão cruciais para o desenvolvimento comercial e tecnológico do país.

[32] CC 4.002-2 - Rel. Flaquer Scartezzini – DJU, de 21/06/93, p. 12.228
[33] Página da Internet: http://www.canalweb.com.br/destaque/destaque310599.asp - consultada em 05/07/99.
[34] Página da Internet: http://users.sti.com.br/cdaniel/3pj/invasao.htm - consultada em 06/07/99.
[35] Fonte: ZDNet, 06/08/99
[36] Página da Internet: http://www.gpsnet.com.br/sembra.htm - consultada em 06/07/99.

7. Da Responsabilidade Penal dos Provedores

O provedor é classificado como pessoa jurídica de direito privado com direitos e deveres inerentes a esta condição.

Considera-se o provedor de acesso à Internet um serviço de valor adicionado, portanto, este não se caracteriza como serviço de telecomunicações.

A distinção legal entre serviço de valor adicionado e serviço de telecomunicações é que aquele afasta a incidência do sigilo constitucional, previsto no artigo 5º da Constituição Federal em seu inciso XII, que se refere à comunicação de dados feita por serviço de telecomunicações[37].

O produto mais comercializável e mais imediato relacionado com a Internet é o acesso a ela.

A responsabilidade ou a co-responsabilidade dos provedores é assunto discutido em alguns países, sendo assunto também controverso.

Uma posição que está se tornando a tendência sobre a responsabilidade penal dos provedores é a da responsabilidade limitada, onde, p.ex., sendo de conhecimento do provedor, conteúdo ilegal, seria de se esperar que este não divulgasse tal conteúdo ou o bloqueasse (tendo meios técnicos para isto). Não o fazendo, assumiria a co-responsabilidade pelo fato.

É o que propõe a Lei alemã que responsabiliza os provedores por divulgação de material ilegal, quando estes forem avisados oficialmente do conteúdo questionável e não tomarem providências para bloquear o acesso às informações ilegais.

Os provedores da Internet têm um argumento muito sólido e realista, afirmando que o volume de dados dentro da Internet, como dentro das listas de discussões, é tão grande que o processo de checar e verificar a decência dos mesmos é humanamente impossível.

A Comissão Federal de Comércio dos Estados Unidos (FTC) irá criar um laboratório dedicado à Internet 24 horas por dia, monitorando anúncios on-line para identificar fraudes. Com isso, a FTC espera inibir os golpes via Web e acionar o FBI se algum crime for caracterizado.

Atualmente existem cerca de 170 mil reclamações no banco de dados da FTC. A instituição já detectou 80 fraudes na Internet, envolvendo pirâmides da fortuna e compra de mercadorias pela rede que nunca foram entregues[38].

Hoje temos programas para controle de acesso a páginas eróticas, p.ex., tornando-as inacessíveis a crianças e adolescentes. Desta forma transfere-se a responsabilidade pelo acesso, aos pais.

Mas quanto a divulgação de outros conteúdos ilegais, de negócios fraudulentos, sites que ensinam a produzir bombas, a conduzir campanhas terroristas e racistas? "*O ciberespaço não é uma zona sem lei. Ninguém pode pensar que tecnologias especiais têm o poder de colocar as pessoas fora do alcance da lei*", palavras do Ministro da Educação e Pesquisa da Alemanha, Juergem Ruettgers, em 1996[39].

O que se discute não é a imputação de conduta delituosa a empresa provedora de Internet, mas sim a sua responsabilidade pela divulgação do material considerado ilegal ou ofensivo, desde que conhecedora do fato.

O Estados Unidos é um grande defensor da privacidade e da liberdade de expressão, tendo como filosofia no que diz respeito à Internet, de que esta por ser o maior veículo de expressão já desenvolvido até o momento, merece a maior proteção possível contra a intromissão governamental.

No Japão, o parlamento aprovou em agosto deste ano uma lei polêmica que dá direito aos policiais de interceptarem e-mails e chamadas telefônicas. O governo insiste que a medida só será utilizada com o objetivo de

[37] Página da Internet: http://users.sti.com.br/cdaniel/3pj/sigilo.htm - consultada em 29/04/99.
[38] Fonte: IDGNews Service, 28/06/99.
[39] Página da Internet: http://www.uol.com.br/bol/tec/te11123.htm - consultada em 29/09/99.

combater o crime organizado. Mas os japoneses temem que ela seja usada para quebra de privacidade, já que os criminosos usam criptografia forte, fora do alcance do governo.

Na Europa o Conselho da União Européia aprovou em dezembro de 1998 um plano de ação descrevendo iniciativas para promover o uso mais seguro da Internet, chamando em particular à colaboração dos profissionais da rede. O plano articula quatro ações principais:

- criar um ambiente eletrônico mais seguro. Dê um lado o surgimento de "*disque denúncias*", onde os usuários poderiam denunciar, conteúdos que julgassem ilegais, como já acontece na Inglaterra e França. Por outro lado, seriam convidados os provedores de acesso e serviços para desenvolverem um código de conduta com direito a selo de qualidade aos que aderissem ao referido código;
- desenvolver e unificar os sistemas de segurança e filtrar as informações da rede. Este efeito é previsto para encorajar a cooperação internacional, de forma que os sistemas futuros possam ser unificados;
- fortalecer ações de sensibilização e informação ao público, em particular aos pais e profissionais da educação, sobre os perigos potenciais do uso da Internet; e
- discutir a cooperação européia e mundial sobre questões legais, como lei aplicável, liberdade de expressão, etc.

Tal iniciativa se dá no momento, como prioridade a auto regulação da rede, que é o modo provável mais eficiente de conter a propagação de conteúdo ilegal e prejudicial.

Certos países regulam a Internet de maneira restritiva. Vejamos alguns exemplos:

CHINA - a pouco a China Continental eliminou para os seus cidadãos o acesso a mais de cem sites da Internet. Na China, as pessoas com acesso à Internet têm de apresentar-se as autoridades para a inscrição num registro especial. Além disso, todos os servidores Internet devem passar pelo Ministério de Telecomunicações.

ALEMANHA - A Alemanha procurou controlar o acesso, proibindo-o, ao site da Organização Neo-nazista Zundel. Os americanos, defensores sempre da liberdade de expressão, copiaram o site Zundel nos computadores de universidades como a MIT, Stanford e Carnegie Mellon, sites que as autoridades alemãs não quiseram eliminar. Tudo isso deu publicidade ao site Zundel, resultado contrário ao esperado.

ESTADOS UNIDOS - Com a Lei da Decência nas Comunicações (CDA) procurou a legislação dos Estados Unidos proibir entre outros atos a utilização de um serviço interativo de computadores para difundir, de maneira a fazê-la disponível a pessoas menores de 18 anos, matéria sexualmente explícita que segundo os princípios contemporâneos da ética da comunidade são claramente ofensivas. Na medida em que esta lei proíbe a transmissão de matéria indecente a pessoas menores, foi declarada inconstitucional pela Corte Federal do Estado da Pennsylvania. O Ministério Público apelou à Corte Suprema.

CINGAPURA - Este país publicou uma regulamentação limitando o acesso a sua população.

ARABIA SAUDITA - Este país também censura parte da informação disponível na Internet.

FRANÇA - O Conselho Constitucional declarou inconstitucional a Emenda "Fillon" à Lei Francesa de Telecomunicações, afirmando que a regulamentação da Internet ficou deficiente por falta de precisão. Tratava-se de competência que se desejava atribuir ao Conselho do Audiovisual de propor princípios e diretrizes para a Internet. Também reconhece a jurisprudência francesa que os provedores de acesso a Internet não são responsáveis pelo conteúdo da matéria publicada nos seus servidores.

Título: Crimes da Informática
Autor: Remy Gama Silva
Editora: CopyMarket.com, 2000

Crimes da Informática
Especialização em Direito Penal

Remy Gama Silva

Conclusão

As dificuldades encontradas para a realização deste trabalho foram muitas, a começar pelo titulo. Optei por "*Crimes da Informática*", entendendo ser a nomenclatura mais adequada para expressar os delitos praticados. Informática compreende os computadores, os programas e a técnica. Os crimes são praticados pela técnica na informática. O computador é o meio para a pratica ou é utilizado como instrumento para a pratica delituosa.

O volume de material pesquisado em idioma estrangeiro despendeu meses para interpretação e compreensão.

O tema é relativamente novo, bastante discutido e com regulamentação e legislação no exterior.

O Brasil está atrasado no aspecto jurídico, mas em progresso na criminalidade informática.

Os assuntos debatidos na Europa, Ásia e Américas, envolvem os mesmos problemas com soluções nem sempre fáceis e harmoniosas.

Com o advento da Internet a criminalidade e os crimes tornaram-se sem fronteiras. E este é o fator mais preocupante, pois enquanto não houver ações internacionais especialmente combinadas, a resposta para o problema estará distante.

O combate aos crimes da informática depende de medidas futuras de todos os países. Depende de conceitos amplos. Depende de definições sobre competência e jurisdição. De policiais e agentes políticos especializados, jurídica e tecnicamente, para a persecução criminal. Da responsabilidade de provedores para a não proliferação de conteúdos ilegais que alimentam indústrias do crime.

Enfim, da cooperação internacional.

Com relação ao Brasil, precisamos nos igualar aos países que possuem legislação específica para os crimes informáticos, para que não sejamos um paraíso aos criminosos deste setor.

Estamos entre os dez países que mais utilizam a Internet, num mercado promissor e crescente, sem uma legislação que defina e classifique quantos e quais são os crimes da informática, para amparar o mercado nacional.

A necessidade se torna imperiosa. O progresso tecnológico sem controle, exige o aperfeiçoamento técnico jurídico sensato.

A barreira da fronteira, de fato acabou.

Estamos na era do "*ciberespaço*".

Título: Crimes da Informática
Autor: Remy Gama Silva
Editora: CopyMarket.com, Brasília 2000

Apêndices

Remy Gama Silva

Apêndice Nº 1

Host – computador principal que controla uma rede.

Posição do Brasil na América do Sul

Posição dos Países por Número de Hosts fonte: Network Wizards - janeiro 99		
1º	**Brasil**	**215.086**
2º	Argentina	66.454
3º	Chile	30.103
4º	Colômbia	16.200
5º	Uruguai	15.394
6º	Venezuela	7.912
7º	Peru	4.794
8º	Equador	1.548
9º	Paraguai	1.147
10º	Bolívia	626
11º	Guiana Francesa	113
12º	Guiana	69
13º	Suriname	0

Apêndice Nº 2

Posição do Brasil no Mundo

Posição dos Países por Número de Hosts
fonte: Network Wizards - janeiro 99

1º	Estados Unidos	30.488.565
2º	Japão	1.687.534
3º	Reino Unido	1.423.804
4º	Alemanha	1.316.893
5º	Canadá	1.119.172
6º	Austrália	792.351
7º	Países Baixos	564.129
8º	Finlândia	546.244
9º	França	488.043
10º	Suécia	431.809
11º	Itália	338.822
12º	Noruega	318.631
13º	Taiwan	308.676
14º	Dinamarca	279.790

15º	Espanha	264.245
16º	Suíca	224.350
17º	**Brasil**	**215.086**
18º	Korea	186.414
19º	Bélgica	165.873
20º	Rússia	147.352
21º	África do Sul	144.445
22º	Áustria	143.153
23º	Nova Zelândia	137.247
24º	México	112.620
25º	Polônia	108.588
26º	Israel	97.765
27º	Hungria	83.530
28º	Hong Kong	82.773
29º	República Tcheca	73.770
30º	Singapura	67.060

Apêndice Nº 3

Projeto de Lei nº 84, de 1999

CÂMARA DOS DEPUTADOS

(Deputado Luiz Piauhylino)

Dispõe sobre os crimes cometidos na área de informática, sua penalidades e outras providências.

18/05/99 - (As comissões de Ciência e Tecnologia, Comunicação e Informática; e de Constituição e Justiça e de Redação)

O Congresso Nacional decreta:

CAPÍTULO 1
Dos princípios que regulam a prestação de serviço por redes de computadores.

Artigo Primeiro- O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços de rede.

Artigo Segundo- É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas disposições específicas reguladas em lei.

CAPÍTULO 2
Do uso de informações disponíveis em computadores ou redes de computadores.

Artigo Terceiro- Para fins desta lei, entende-se por informações privadas aquelas relativas à pessoa física ou jurídica identificada ou identificável.

Parágrafo Único - É identificável a pessoa cuja individualização não envolva custos ou prazos desproporcionados.

Artigo Quarto- Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.

Artigo Quinto- A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá ser tornada sem efeito a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.

§1. A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas e das retrospectivas fontes.

§ 2. Fica assegurado o direito à retificação de qualquer informação privada incorreta.

§ 3. Salvo a disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua vaidade.

§ 4. Qualquer pessoa, física ou jurídica, tem o direito de interpelar o proprietário de rede de computadores ou o provedor de serviço para saber se mantém as informações a seu respeito, e o respectivo teor.

Artigo Sexto- Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a origem racial, opinião pública, filosófica, religiosa ou de orientação sexual, e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.

Artigo Sétimo- O acesso de terceiros, não autorizados pelos respectivos interessados, à informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

CAPÍTULO 3
Dos crimes de informática.

Seção I – Dano a dado ou programa de computador.

Artigo Oitavo- 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.

Parágrafo único = Se o crime é cometido:

I – contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo da vítima;

III- com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro; ou

VII – com a utilização de qualquer outro meio fraudulento.

PENA: detenção, de dois a quatro anos e multa.

Seção II – Acesso indevido ou não autorizado

Artigo Nono- Obter acesso, indevido ou não autorizado, a computador ou rede de computadores.

PENA: detenção, de seis meses a um ano e multa.

Parágrafo Primeiro: Na mesma pena incorre quem, sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.

Parágrafo Segundo - Se o crime é cometido;

I – com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com o considerável prejuízo para a vítima;

III – com o intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – por motivo fútil;

VI – com o uso indevido de senha ou processo de identificação de terceiro; ou

VII – com a utilização de qualquer outro meio fraudulento.

PENA: detenção, de um a dois anos e multa.

Seção III – Alteração de senha ou mecanismo de acesso a programa de computador ou dados.

Artigo Décimo- Apagar, destruir, alterar, ou de qualquer forma inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

PENA: detenção, de um a dois anos e multa.

Seção IV - Obtenção indevida ou não autorizada de dado ou instrução de computador.

Artigo Décimo Primeiro- Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.

PENA: detenção, de três meses a um ano e multa.

Parágrafo Único - Se o crime é cometido:

I – com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo para a vítima;

III – com o intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – por motivo fútil;

VI – com o uso indevido de senha ou processo de identificação de terceiro; ou

VII – com a utilização de qualquer outro meio fraudulento.

PENA: detenção, de um a dois anos e multa.

Seção V – Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar

Artigo Décimo Segundo- Obter segredos, de industria, ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

PENA: detenção, de um a três anos e multa.

Seção VI – Criação, desenvolvimento ou inserção em computador de dados ou programa de computador com fins nocivos

Artigo Décimo terceiro- Criar, desenvolver ou inserir, dado ou programa 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 rede de computadores, dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.

PENA: reclusão, de um a três anos e multa.

Parágrafo Único - Se o crime é cometido:

I – contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo para a vítima;

III – com o intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – por motivo fútil;

VI – com o uso indevido de senha ou processo de identificação de terceiro; ou

VII – com a utilização de qualquer outro meio fraudulento.

PENA: reclusão, de dois a seis anos e multa.

Seção VII - Veiculação de pornografia através de rede de computadores.

Artigo Décimo Quarto- Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir, previamente, de forma facilmente visível e destacada, aviso sobre a natureza, indicando o seu conteúdo e a inadequação para a criança ou adolescentes.

PENA: detenção, de um a três anos e multa.

CAPÍTULO 4
Das disposições finais.

Artigo Décimo Quinto- 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.

{©***Artigo Décimo Sexto***- Nos crimes definidos nesta lei somente se procede mediante representação do ofendido, salvo se cometidos contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.

Artigo Décimo Sétimo- Esta lei regula os crimes relativos à informática sem prejuízo das demais cominações previstas em outros diplomas legais.

Artigo Décimo Oitavo- Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

Apêndice Nº 4

Páginas Nacionais e Internacionais Consultadas na Internet

http://alumni.dee.uc.pt/~aseco/cris/indice.html
http://bradley.edu/~simonp/atg383/chapter15.html
http://catalaw.com/logic/docs/ds-srch.htm
http://cf3.uol.com.br:8000/consultor/chama1.cfm?numero=1347
http://dgl/dglinfo/1997/dg971108.html
http://inews.tecnet.it/articoli/luglio96/diritto9607b.html
http://info.in2p3.fr/secur/legal/188-19-home.html
http://infojur.ccj.ufsc.br
http://mailer.fsu.edu/~btf1553/ccrr/welcome.htm
http://netgain.co.nz/library/fraud_melchizedek.htm
http://pr.gov.br/celepar/celepar/batebyte/bb74/colunado.htm
http://publicaciones.derecho.org/redp/index.cgi?/N%Famero%203%20-%20Junio.../herrer
http://rampages.onramp.net/~dgmccown/a-fedcc.htm
http://tiny.uasnet.mx/prof/cln/der/silvia/leynac.htm
http://users.sti.com.br/cdaniel/3pj/94272.htm
http://web.nwe.ufl.edu/writing/handbook/33.ad.crimes.html
http://wings.buffalo.edu/Complaw/CompLawPapers/devine.html
http://www.abanet.org/crimjust/fedreport.html
http://www.abes.org.br/antipira/vocesaap.htm
http://www.accusa.com/security/comcrime.htm
http://www.aclu.org/news/1999/n030899ahtml
http://www.amcham.com.br/arko/djalma4p.html
http://www.asnoticias.com/1999/9905/11/n99051104.htm
http://www.auscert.org.au/
http://www.austlii.edu.au/other/crime/12.html
http://www.bakerinfo.com/apec/thaiapec.htm

http://www.canalweb.com.br/destaque/destaque310599.asp
http://www.cefetsc.rct-sc.br/servicos/internet/ftp/virus.html
http://www.cg.org.br
http://www.cg.org.br/debates/debate1.html
http://www.cnpd.pt/Leis/leis_indice.htm
http://www.crystalnet.com.br/inter4.html
http://www.ctv.es/USERS/mpq/delitos.html
http://www.damasio.com.br/artigos/
http://www.datacontrol.com.br/internet.htm
http://www.derechos.org/nizkor/impu/tpi
http://www.digitalcentury.com/encyclo/update/crime.html
http://www.epoca.com.br/edic/ed280699/ciencia5.htm
http://www.fa.utl.pt/cifa/legislacao.html
http://www.fbi.gov/leb/july976.htm
http://www.galeon.com/bolsa/eco2410049811/
http://www.geocities.com/Athens/Rhoders/7959/
http://www.geocities.com/Paris/2009/crime.htm
http://www.gpsnet.com.br/sembra.htm
http://www.ibccrim.com.br
http://www.ifea.net/
http://www.infowar.com/law/law_110498b_1.shtml
http://www.intergov.org/publi_administration/information/latest_web_stats.html
http://www.isc.meiji.ac.jp/~sumwel_h/links/link07.htm
http://www.jei.it/manuale/parte_5/1547-93.htm
http://www.jfrn.gov.br/doutrina1.htm
http://www.jmls.edu/cyber/index/crime1.html
http://www.jurinforma.com.br/artigos/0417.htm
http://www.jus.com.br/doutrina/netbrasil.html
http://www.jus.com.br/infojur/casos.html
http://www.ksg.harvard.edu/iip/stp307/group3/juanca/tsld009.htm
http://www.law.indiana.edu/glsj/vol5/no2/10tract.html
http://www.law.vill.edu/chron/articles/intct.htm
http://www.lexadin.nl/wlg/legis/nofr/legis.htm
http://www.mct.gov.br/conjur/port_int/PORT147.htm
http://www.modulo.com.br
http://www.modulo.com.br/noticia/clip-22.htm
http://www.mossbyrett.of.no/info/legal.html
http://www.ncis.co.uk/ncis/web/Press%20Releases/euro_crime.htm
http://www.novell.com.br/programa/ap-avoidn.html
http://www.ora.com/catalog/crime/desc.html
http://www.rcmp-grc.gc.ca/html/cfraud.htm
http://www.rcmp-grc.gc.ca/html/cpu-cri.htm
Http://www.rrz.uni-hamburg.de/kr-p1/intersem.htm
http://www.scit.wlv.ac.uk/~c9727436/page2.html
http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm
http://www.ufrgs.br/HCPA/gppg/privacid.htm
http://www.unesco.org/webworld/child_screen/com_index.html
http://www.uol.com.br/aprendiz/especial/pedofilia_Online/id010299.html
http://www.uol.com.br/computerworld/computerworld/247/soft_03.htm
http://www.uol.com.br/idgnow/pc/pc1703g.shl
http://www.usdoj.gov/criminal/cybercrime/docs.html
http://www.vogon-international.com/portuguese-oo.htm
http://www.web-police.org/
http://www.zdnet.com/zdnn/stories/news/0,4586,262195,00.html
http://www2.echo.lu/legal/en/comcrime/sieber.html
http://www2.uol.com.br/info/infonews/190298d.html
http://www2.uol.com.br/veja/261197/p_076.html
http://wwwlib.umi.com/dissertations/fullcit?293265
http://www-swiss.ai.mit.edu/6095/student-papers/fall97-papers/kim-crime.html

Bibliografia

Remy Gama Silva

ARDIZZONE, Salvatore. A legislação penal italiana em matéria de computers Crimes Entre direito e política criminal. *Revista da Faculdade de Direito das Faculdades Metropolitanas Unidas de São Paulo.* São Paulo: FMU, n.15: 103-125, 1996.

BARBOSA, Luciano Pestana. O sexo na Internet e as Leis. *Sin-DPF* .São Paulo: SPM, n.7, p.34-35, nov. dez. 1998.

BARRA, Rubens Prestes (Coord). *Estudos Jurídicos em Homenagem a Manoel Pedro Pimentel.* São Paulo: Revista dos Tribunais, 1992.

CAMASSA, Manoel. A Tecnologia Mudando o Perfil da Criminalidade. *Revista Brasileira de Ciências Criminais.* São Paulo: Revista dos Tribunais, n.25: 227-239, 1996.

CARICATTI, André Machado. A Experiência da Polícia Federal nos Crimes por Computadores. *Instituto Nacional de Criminalística.* 1998.

CERNICCHIARO, Luiz Vicente. Reforma do Código Penal. *Perícia Federal.* Brasília: Ipiranga, n.1: 6-10, 1999.

CORREA, Carlos M., BATTO, Hilda N., ZALDUENDO, Susana Czar et al. *Derecho Informático.* Buenos Aires: Depalma, 1994.

DELMANTO, Celso. *Código Penal Comentado.* 3.ed. Rio de Janeiro: Renovar, 1991.

ECO, Umberto. *Como se faz uma tese.* 12.ed. São Paulo: Perspectiva,1995.

FRANCO, Alberto Silva, SILVA JUNIOR, José, BETANHO, Luiz Carlos. *Código Penal e sua Interpretação Jurisprudencial.* 5.ed. São Paulo: Revista dos Tribunais, 1995.

GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com o uso do computador.* Tese de Doutorado. São Paulo: Universidade de São Paulo, 1994, 137 p.

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

GUIBOURG, Ricardo A . *Informática Jurídica Decisória.* Buenos Aires: Astrea, 1993.

GUIBOURG, Ricardo A, ALENDE, Jorge O , CAMPANELLA, Elena M. *Manual de Informática Jurídica.* Buenos Aires: Astrea, 1996.

JUNQUEIRA, Miriam. *Contratos Eletrônicos.* Rio de Janeiro: Mauad,1997.

KARAM, Maria Lúcia. *Competência no Processo Penal.* 2. ed. São Paulo: Revista dos Tribunais, 1998.

KOHN, Aaron M. Computer Criminals. *The Journal of Criminal Law, Criminology and Police Science.* Chicago: Police Science, v.60: p. 1-2.

LIMA JUNIOR, Carlos Daniel Vaz. Persecução Criminal na Internet. *Revista da Associação Paulista do Ministério Público.* São Paulo: Salesianas, n.24, p. 63-64, dez. jan. 1999.

MIRABETE, Júlio Fabbrini. *Processo Pe*

MIRANDA, Gilson Delgado. Responsabilidade Civil na Informática. *Justiça e Democracia.* São Paulo: Associação Juízes para Democracia, n.2: 240-261, 1996.

NUNES, Luiz Antonio Rizzatto. *Manual da Monografia Jurídica.* São Paulo: Saraiva, 1997.

PAESANI, Liliana Minardi. *Direito de informática: comercialização e desenvolvimento internacional do Software.* São Paulo: Atlas, 1998.

PAZIENZA, Francesco. In Tema Di Criminalità Informatica: L'Art. 4 Della Legge 23 Dicembre 1993, N 547. *Rivista Italiana di Diritto e Procedura Penale.* Milano: Giuffrè, fasc.3 : 750-757, 1995.

REALE JUNIOR, Miguel. Crime Organizado e Crime Econômico. *Revista Brasileira de Ciências Criminais.* São Paulo: Revista dos Tribunais, n13: 182-190, 1996.

REIS, Maria Helena Junqueira. Crime Informático. *Revista dos Tribunais.* São Paulo: Revista dos Tribunais, v.670: p.180-181, 1991.

ROCHA, Fernando A . N. Galvão . Criminalidade do Computador. *Revista dos Tribunais.* São Paulo: Revista dos Tribunais, v.718: p.522-535, 1995.

ROTONDA, Tavola. *L'Informatica Giuridica al Servizio del Legislatore.* Genova: Cedam, 1994.

SERGENT, Randolph S. A Fourth Amendment for Computer Networks and Data Privacy. *Virginia Law Riview.* Virginia: Virginia Law Riview Association, v. 81: 1181- 1228, 1995.

SIEBER, Ulrich. *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME – Study.* Alemanha: University of Würzburg, 1998.

SILVA, Reis Silva, MONIZ, Luís Bettencourt, ROCHA, Manuel Lopes et al. *Direito da Informática Legislação e Deontologia. Lisboa*: Cosmos, 1994.

SZNICK, Valdir. Crimes Cometidos com o Computador. *Justitia.* São Paulo: Ministério Público de São Paulo, v. 124: 66-70, 1984.

THOMPSON, David E, BERWICK, Desmond R. *Minimum Provisions for the Investigation of Computer Based Offenses.* Austrália: National Police Research Unit, 1997.

TOURINHO FILHO, Fernando da Costa. *Processo Penal.* 13.ed. São Paulo: Saraiva, 1992.