

**PÓS-GRADUAÇÃO EM CRIPTOGRAFIA E SEGURANÇA EM REDES  
UNIVERSIDADE FEDERAL FLUMINENSE – UFF E EXÉRCITO BRASILEIRO - EB**

**POLÍTICAS DE SEGURANÇA DE REDES DE COMPUTADORES**

**Marcello Reus Koch**

TEMA: O Paradoxo entre a Segurança da Informação e o Crime Virtual  
Professor Orientador: Luiz Manoel Silva de Figueiredo

**Marcello Reus Koch**

## **POLÍTICAS DE SEGURANÇA DE REDES DE COMPUTADORES**

Monografia apresentada como Trabalho Final do Curso de Especialização em Criptografia e Segurança em Redes, Universidade Federal Fluminense - UFF e Exército Brasileiro – EB/MD, como exigência para a aprovação.

Professor Orientador: Luiz Manoel Silva de Figueiredo

Porto Velho  
2009

# Sumário

## Parte I

### 1 – Prefácio:

1.1 - Dedicatória.....	8
1.2 - Considerações Iniciais.....	9
1.3 - Questões norteadoras.....	10
1.4 – Objetivos.....	10
1.5 – Justificativa.....	11

## Parte II

### 2 – Aspectos Teóricos:

2.1 – Breve histórico.....	12
2.2 - Os panoramas nacional e mundial das Políticas de Segurança de Redes de Computadores.....	13

## Parte III

### 3 – Metodologia:

3.1 – Metodologia aplicada para a realização desta Monografia.....	18
--	----

## Parte IV

### 4 – O Paradoxo entre a Segurança da Informação e o Crime Virtual:

4.1 - O limite de respeito às liberdades individuais e o direito privado no ciberespaço.....	19
4.1.1 A evolução da <i>Internet</i> em um mundo globalizado e suas conseqüências.....	20
4.1.1.1 Conceito de globalização.....	21
4.1.1.2 Histórico da globalização.....	22
4.1.1.3 A Revolução tecno-científica.....	23
4.1.1.4 O ser humano e a tecnologia.....	24
4.1.1.5 Conceito de <i>Internet</i> .....	25
4.1.1.6 O usuário e a <i>Internet</i> .....	26

4.1.1.7 O custo e benefício da <i>Internet</i> .....	26
4.1.1.8 A abrangência e a bi-direcionalidade.....	27
4.1.1.9 A evolução da <i>Internet</i> .....	28
4.1.1.10 O uso da <i>Internet</i> .....	30
4.1.1.11 A <i>Internet</i> e a globalização.....	32
4.1.1.12 A divisão digital.....	34
4.1.1.13 A evolução da <i>Internet</i> no Brasil.....	37
4.1.2 Os Crimes na <i>Internet</i> .....	38
4.1.2.1 Tipos de crimes na <i>Internet</i> .....	38
4.1.2.1-A: Extorsões e Fraudes.....	38
4.1.2.1-B: Pirataria de <i>softwares</i> .....	39
4.1.2.1-C: Pedofilia e pornografia na <i>Internet</i> .....	40
4.1.3 Como evitar “ <i>crimes cibernéticos</i> ”.....	41
4.2 - O limite entre o direito à informação e os ataques à liberdade no ciberespaço em um mundo globalizado.....	41
4.2.1 O Futuro da <i>Internet</i> no contexto jurídico.....	42
4.2.2 A assinatura digital no plano da validade do ato jurídico.....	43
4.2.2.1 A assinatura digital no ato jurídico.....	44
4.2.2.2 O fato jurídico.....	45
4.2.2.3 Conceito de fato jurídico.....	46
4.2.2.4 Ato jurídico.....	47
4.2.2.4.1 Conceito de ato jurídico.....	47
4.2.2.4.2 Elementos do ato jurídico – Uma nova visão.....	48
4.2.2.5 Vontade de manifestação.....	48
4.2.2.6 Vontade do conteúdo do ato.....	50
4.2.2.7 Vinculação da vontade de manifestação com a vontade do conteúdo do ato.....	51
4.2.2.8 A Assinatura Digital.....	52

4.3 – As Mudanças nas legislações americana e européia contra os "crimes virtuais", após o dia 11 de setembro de 2001.....	55
4.3.1 A restrição de direitos fundamentais e o 11/09/2001.....	55
4.3.2 Análise de três disposições do <i>Patriot Act</i> .....	56
4.3.3 Definição de terrorismo doméstico.....	56
4.3.4 detenção compulsória de terroristas suspeitos e os tribunais Militares.....	57
4.3.5 Pós-notificação dos mandados de busca e apreensão.....	59
4.3.6 a convenção do conselho europeu sobre o <i>crime eletrônico</i> .....	62
4.4- A legislação brasileira sobre os crimes de informática.....	63
4.4.1 Conceito e características do crime organizado.....	63
4.4.2 Estrutura e atuação do crime organizado.....	66
4.4.3 Legislação aplicável ao crime organizado.....	67
4.4.4 Questões sobre o crime organizado.....	67
4.4.4.1 Qual a política pública mais adequada para se controlar este tipo de criminalidade?.....	68
4.4.4.2 como se prevenir ao crime organizado, à luz da criminologia moderna?.....	69
4.4.5 Crimes de informática e legislação penal brasileira.....	69
4.4.5.1 O direito penal da informática - a regulamentação penal da informática.....	69
4.4.5.2 Necessidade de implantação de legislação especial.....	69
4.4.5.3 Legislação brasileira.....	71
4.4.5.3.1 o direito penal de informática vigente no Brasil.....	71
4.4.5.3.2 A Lei dos Direitos Autorais.....	71
4.4.5.3.3 O Código Penal e o Direito de Informática.....	72

4.4.5.3.4 A Lei de <i>software</i> .....	72
4.4.5.4 O futuro do Direito Penal de Informática.....	73
4.4.5.4.1 Projetos de Lei.....	73
4.4.5.4.2 O Projeto de Lei n.76 de 2000 (do Senador Renam Calheiros).....	73
4.4.5.4.3 O Projeto de Lei n. 84 de 1999 (do Deputado Luiz Piauhylino).....	74
4.5 O Congresso Nacional, a Polícia Federal, o Poder Judiciário e demais órgãos públicos brasileiros e o " <i>crime virtual</i> ".....	75
4.5.1 O que trata o PLC-89/2003?.....	76
4.5.2 O que trata o PLS-137/2000?.....	76
4.5.3 O que trata o PLS-76/2000?.....	77
4.5.4 Textos de Projetos de Lei do Congresso Nacional.....	77
4.5.5 A atuação da Polícia Federal contra os crimes cibernéticos.....	92
4.5.5.1 Polícia Federal cria endereço específico para denúncia de <i>crimes eletrônicos</i> .....	92
4.5.5.2 A atuação do Poder Judiciário contra os <i>"crimes cibernéticos"</i> .....	94
4.5.5.3 O Sistema de Execução Fiscal Virtual.....	95
4.5.5.4 O anteprojeto de lei apresentado pela associação dos Juízes Federais do Brasil.....	95
4.6 – <i>Hackers, crackers</i> e a sociedade contemporânea.....	100
4.6.1 <i>Hackers</i> .....	101
4.6.2 <i>Crackers</i> .....	103
4.6.3 <i>Phreakers</i> .....	109
4.6.4 <i>Defacers</i> .....	109
4.6.5 Assuntos ou serviços de redes tipicamente negligenciados pelos administradores.....	110
4.6.6 Como pensam os <i>hackers</i> e os <i>crackers</i> ?.....	111

4.6.7 Por que a sociedade teme os <i>hackers</i> e os <i>crackers</i> ?.....	112
4.7– As alternativas tecnológicas e jurídicas para proteger eficazmente a sociedade e as organizações cooperativas dos “crimes virtuais”:	
4.7.1 Por que se preocupar com a segurança da informação?.....	113
4.7.2 Qual são as principais ameaças à segurança da informação em 2009 e como se proteger delas?.....	116
4.7.3 O Direito Objetivo e os “ <i>Crimes Cibernéticos</i> ”.....	120

## **Parte V**

5 – Conclusões.....	125
---------------------	-----

## **Parte VI**

### 6 – Referências:

6.1 – Referências Bibliográficas.....	126
6.2 – Anexos.....	132

## Parte I

### 1 PREFÁCIO

#### 1.1 DEDICATÓRIA

*“Dedico este Trabalho de Conclusão do Curso de Especialização em Criptografia e Segurança em Redes a Jesus Cristo, o Senhor dos Exércitos, meu único Deus, a minha querida esposa Terezinha e a minha filha amada, Sarah Beatriz, as quais foram tantas vezes abdicadas do convívio familiar; a fim de que não somente esta monografia fosse concluída, mas também, para o fiel cumprimento do dever inerente a minha profissão, ao longo da minha carreira”.*

## 1.2 CONSIDERAÇÕES INICIAIS

O presente estudo representa uma análise da política de segurança de redes de computadores a nível cooperativo, das novas tecnologias de combate e prevenção aos “crimes virtuais” e, principalmente, da legislação vigente contra os mesmos.

Com o advento da *Internet*, o ser humano encurtou distâncias, geograficamente impossíveis de serem percorridas em milésimos de segundo. A “World Wide Web” (que significa “rede de alcance mundial”, em inglês; também conhecida como *Web* e *WWW*), sem fronteiras geográficas, permite que saibamos o que se passa no mundo, em tempo real, *on-line*. Ela possibilita a troca de informações, notícias, experiências de todo o tipo com gente de todas as partes. Porém, todas as vantagens virtuais da rede mundial, imprescindíveis para um mundo altamente competitivo, vêm sendo ameaçadas por ataques de *script kiddies*, *hackers*, *crackers*, *cyberpunks*, *insiders*, *coders*, *white hat*, *black hat*, *gray hat*, *trojans*, *spywares* e outros tipos de “criminosos virtuais” e de vírus de computadores, antigos ou novos; que exigem em contrapartida, uma constante preocupação por uma proteção mais eficaz dos dados guardados pelas organizações, por parte dos empresários, administradores de redes de computadores, desenvolvedores de sistemas e analistas em segurança da informação.

De fato, com o surgimento das redes cooperativas conectadas via *Web* ao mundo, não se imaginava que seria tão séria e dispendiosa a guerra contra os “criminosos virtuais”, conhecidos, geralmente, como *hackers* e/ou *crackers*.

Sendo assim, a fim de aplacar os prejuízos com a perda e a violação de dados críticos e valiosos, na proteção contra as invasões e na prevenção aos danos morais e financeiros; há um crescente investimento em novas tecnologias que tornem as redes cooperativas mais seguras e em uma política de segurança de redes de computadores a nível organizacional. Já que no campo jurídico a luta ainda é desigual, e a impunidade prevalece na maioria dos casos, afinal, falta legislação específica sobre “crimes virtuais” e a “jurisprudência”. Assim, a batalha vem sendo travada, na verdade, no campo tecnológico. De um lado, “criminosos virtuais” esmeram-se em invadir os sistemas de segurança e os desenvolvedores empenham-se no desenvolvimento de sistemas de proteção cada vez mais avançados e eficientes. Paradoxalmente, ainda há uma escassez muito grande de legislação contra “*crimes eletrônicos*”.

### 1.3 QUESTÕES NORTEADORAS

- 1 - Qual é o limite de respeito às liberdades individuais e o direito privado no ciberespaço?
- 2 - Qual é o limite entre o direito à informação e os ataques à liberdade no ciberespaço?
- 3 - O que houve de mudança nas legislações americana e européia contra os "crimes virtuais", após o dia 11 de setembro de 2001?
- 4 - Qual é a legislação brasileira sobre os crimes de informática?
- 5 - O que o Congresso Nacional, o Poder Judiciário, a Polícia Federal e demais órgãos públicos brasileiros planejam no combate ao "crime virtual"?
- 6 - Quais são os benefícios do "Direito Objetivado" contra os "crimes virtuais"?
- 7 - Por que a sociedade teme os *hackers* e os *crackers*?

Estas questões levam a questão fundamental, portanto, é:

- 8 - Existem alternativas tecnológicas e jurídicas que protejam eficazmente a sociedade e as organizações cooperativas dos "crimes virtuais"?

### 1.4 OBJETIVOS

O objetivo do estudo é propor alternativas tecnológicas e jurídicas que visem aplacar os prejuízos com a perda e a violação de dados críticos e valiosos, na proteção contra as "invasões eletrônicas" (OLIVEIRA, 2007) e na prevenção aos danos morais e financeiros de usuários da *Internet* e das organizações cooperativas com conexão via *Web*.

Pretende-se, igualmente, mostrar a aplicabilidade de várias tecnologias de segurança de Informação, tais como o *Firewall*, o sistema de detecção de intrusão (*Intrusion Detection System, IDS*), a criptografia, a autenticação de dois fatores, a biometria, a *Single Sign-On (SSO)*, a infra-estrutura de chaves públicas (*Public Key Infrastructure, PKI*), o *IP Security (IPSec)*, a rede privada virtual (*Virtual Private Network, VPN*), assim como a integração de tais ferramentas de Segurança de Informação (NAKAMURA, 2007).

Propoe, também, contribuir para o debate acerca da política de segurança de redes de computadores (BURNETT, 2002), demonstrando a necessidade de segurança e a influência das medidas de segurança nas funcionalidades dos sistemas e na produtividade dos usuários. Afinal, a segurança é necessária, porém sua estratégia de implementação deve ser bem definida, medindo-se custos e benefícios, pois a segurança total não é possível. A análise dos riscos tem um papel fundamental neste contexto. Além do mais, de nada vale implementar sistemas arrojados e de custo elevado na área de segurança de informação; se não houver um investimento considerável na educação dos usuários, por parte das organizações cooperativas (NAKAMURA, 2007). Assim como, apresenta para discussão, também, a falta de uma legislação protecionista e coercitiva contra os "ataques virtuais" de *hackers* e/ou *crackers* no Brasil (HOGLUND, 2006); comparando com a realidade

dos Estados Unidos da América e de países europeus, os quais têm obtido resultados promissores contra os “crimes cibernéticos”, na *Web* (ULBRICH, 2007).

## 1.5 JUSTIFICATIVA

A questão da prática de “crimes virtuais” está em voga. Em função destes “piratas virtuais”, um mercado milionário de produtos e serviços de segurança da informação se encontra em amplo crescimento. Em um ambiente cooperativo, cada vez mais dependente da *Web*, as triangulações, nas quais uma organização A acessa as informações de C, por intermédio de sua comunicação com a organização B, é apenas um dos problemas a serem tratados. A complexidade de conexões e a heterogeneidade do ambiente também devem ser consideradas, para efeito de segurança de dados e de política de segurança de redes de computadores.

Os bens jurídicos situados na *Internet* são alvos de debate, cada vez mais. Algumas correntes de pensamento defendem a criação de diversas leis e de duras penas para regular o “ciberespaço”, através do emprego de novas tecnologias aplicadas às políticas de segurança de redes de computadores. Por outro lado, há quem defenda que a *Web* é um espaço de relações humanas, como outro qualquer. Portanto, a *Internet* não demanda toda uma legislação própria para que haja tutela de bens jurídicos; já que existiria legislação suficiente para tutelar grande parte dos atos cometidos neste ambiente e criar leis específicas, sendo que em alguns casos, seria como “legislar sobre o que já está legislado”.

A realidade brasileira e a mundial são que os riscos em segurança da informação envolvem tanto aspectos humanos, explorados pela engenharia social, quantos os aspectos técnicos também. Ferramentas de *Distributed Denial-of-Service Attack* (DDoS Attack), de *Worms*<sup>1</sup> e de *Sniffers*<sup>2</sup>, usadas constantemente pelos *hackers* e/ou *crackers*, tais como o *Nimda*, o *Code Red*, o *Klez*, o *Sapphire* e o *Deloder*, etc; visam obter informações sobre os sistemas-alvo, através de ataques ativos, ataques coordenados e ataques às aplicações e aos protocolos.

<sup>1</sup>*Worms*: Um Worm (verme, em português) para a computação é um programa auto-replicante, semelhante a um vírus. Entretanto um vírus infecta um programa e necessita deste programa hospedeiro para se propagar, já o Worm é um programa completo e não precisa de outro programa para se propagar.

<sup>2</sup>*Sniffers*: Os *Sniffers* (Analisadores de Rede) podem ser utilizados com propósitos maliciosos por invasores que tentam capturar o tráfego da rede com diversos objetivos, dentre os quais podem ser citados, obter cópias de arquivos importantes durante sua transmissão, e obter senhas que permitam estender o seu raio de penetração em um ambiente invadido ou ver as conversações em tempo real.

## Parte II

## 2 ASPECTOS TEÓRICOS

### 2.1 BREVE HISTÓRICO

No Brasil, em virtude da crescente demanda em aquisição de microcomputadores, tanto a nível corporativo, quanto a nível de usuário em particular; a questão da prática de “crime virtual” vem se intensificando desequilibradamente, em grandes proporções. Conseqüentemente, os investimentos em novas tecnologias de segurança da informação e a adoção de políticas de segurança em redes de computadores (política de senhas, *firewall*, tipos de acesso remoto, etc) mais sérias e pragmáticas, por parte das iniciativas privada e pública, têm crescido extraordinariamente também.

A falta de uma legislação apropriada para lidar com os “crimes eletrônicos” torna o Brasil um verdadeiro paraíso para todo o tipo de invasão e manipulação ilícita de dados. As punições aplicadas são baseadas em leis que se aproximam da situação do “crime eletrônico”. Grande parte dos casos resolvidos pelas autoridades do Poder Público (Tribunais de Justiça, Ministérios Públicos, Polícias Federal e Civil, etc) são relativos a casos de “pirataria” e “pedofilia”; e, raramente, tratam de invasões e “hackeamento” de sistemas em redes de computadores, conectados à *Internet*.

Em contrapartida, após o fatídico dia 11 de setembro de 2001, os Estados Unidos da América implementaram pesadas medidas punitivas e coercitivas contra o “ciberterrorismo”, tais como o “*USA Act of 2001*” (*Uniting and Strengthening America Act of 2001*) e o “*USA PATRIOT Act of 2001*” (*Uniting and Strengthening America by Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*), a fim de combater o “vandalismo cibernético”. A elaboração de um conjunto de novas leis contra os “crimes virtuais”, baseadas na “*Doutrina Bush*” (WIKIPEDIA, 2008), transformou milhares de *hackers* e/ou *crackers* em terroristas por definição.

A maioria dos países da União Européia (UE) adotaram o padrão norte-americano de combate aos “*cibercrimes*”. Em 23 de novembro de 2001, houve a “Convenção sobre o Cibercrime”, celebrada em Budapeste, Hungria, pelo Conselho da Europa e 43 países signatários, europeus na sua maioria, e ainda os Estados Unidos da América, Canadá e Japão. A Convenção recomendou procedimentos processuais penais, a guarda criteriosa das informações trafegadas nos sistemas informatizados e sua liberação para as autoridades de forma a cumprir os objetivos relacionados no preâmbulo. Além disso, tratou da necessária cooperação internacional, das questões de extradição, da assistência mútua entre os Estados, da denúncia espontânea e sugeriu procedimentos na ausência de acordos internacionais específicos, além da definição da confidencialidade e limitações de uso. Definiu também a admissão à Convenção de novos Estados por convite e a aprovação por maioria do Conselho.

## 2.2 OS PANORAMAS NACIONAL E MUNDIAL DAS POLÍTICAS DE SEGURANÇA DE REDES DE COMPUTADORES

O investimento em Tecnologia da Informação (TI) nas empresas brasileiras, de vários segmentos industriais, assim como a nível governamental tem crescido tremendamente, a passos largos.

De acordo com a pesquisa da Fundação Getúlio Vargas – FGV (MEIRELLES, 2002), no começo de 2001, os gastos com tecnologia da informação eram 4,2% da receita líquida das cerca de 1,2 mil médias e grandes empresas analisadas pelo estudo da FGV. Decorrido um ano, a proporção passou para 4,5%. Esta mesma pesquisa da FGV mostra também que os maiores investimentos na área, proporcionalmente à receita, foram feitos pelo setor de serviços. Liderança que, por sua vez, veio da área bancária, um segmento que gastou em informática, em média, 9,7% de sua receita líquida. A mesma pesquisa igualmente informou que enquanto a indústria gastou 3% de sua receita em informática e o comércio destinou 2%, as empresas de serviços empregaram 7%, e que as empresas brasileiras já alcançaram a marca de 1,1 usuários por computador.

Com a regulamentação da Lei de Informática, o ministro da Ciência e Tecnologia, Sérgio Rezende preveu um aumento nos investimentos feitos pelas empresas do setor, que podem chegar a R\$ 1 bilhão a partir de 2007 (PIMENTEL, 2006).

Segundo a pesquisa realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), conforme a “Pesquisa Anual de Serviços – PAS 2005”, em 2005 as telecomunicações geraram 67,1% da receita dos serviços de informação e o conjunto das atividades de informática, 19,9%; perfazendo uma receita operacional líquida de R\$ 25,8 bilhões em atividades de informática. As atividades de informática foram responsáveis por 19,9% do total da receita dos serviços de informação em 2005, contra 19,4% em 2004. Os serviços de desenvolvimento de *softwares* sob encomenda ou específico para o cliente foram os que mais contribuíram na receita (19,1%), os quais somados aos serviços de desenvolvimento, edição e licenciamento de *softwares* prontos para uso, inclusive representação, representaram 36,6% do segmento, em 2005. Os serviços de processamento de dados para terceiros responderam por 13,6% da receita dos serviços de informação, em 2005 (MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, 2005).

<sup>1</sup> George Walker Bush, nascido em New Haven, EUA, no dia 6 de Julho de 1946, é um político dos Estados Unidos da América, 43º e atual presidente de seu país, havendo sucedido Bill Clinton em 2001. O seu segundo mandato termina em 2009.

No Brasil, o cenário do desenvolvimento na área de informática nos setores público e privado é deveras promissor, conforme revelam os dados estatísticos anteriormente apresentados. Naturalmente, os mercados de desenvolvimento de *softwares* e de consultoria para segurança de informação têm vivido um período auspicioso também; pois em 47% dos casos de “crimes virtuais” em ambientes cooperativos, a pessoa jurídica ou seu funcionário contribuiu com o delito por meio de imprudência, negligência ou imperícia (FOINA, 2001). Há a necessidade premente de não somente adotar sistemas de segurança de dados: Os Sistemas de Detecção de Intrusão (*Intrusion Detection System – IDS*) e os Sistemas de Prevenção de Intrusão (*Intrusion Prevention System – IPS*); em empresas e instituições governamentais, mas principalmente, políticas de segurança de redes de computadores (BS 7799, Parte 1, de 1995 e BS 7799, Parte 2, de 1998) mais conscientes e eficazes para com seus funcionários. Faz-se necessário que nos objetivos de uma organização esteja incluída, intrinsecamente, a “cultura de segurança de informação”.

Concomitante ao “boom” vivido pelo crescimento de novas tecnologias em segurança da informação, assim como a adoção de políticas de segurança de redes de computadores nos setores público e privado; o Brasil tem sido um verdadeiro “oásis” para o “vandalismo cibernético”, haja vista a falta de uma legislação punitiva aos *hackers* e/ou *crackers*. As notícias dos jornais relatam centenas de casos onde consumidores procuram as agências bancárias, todas as semanas, para denunciar saques virtuais realizados por *hackers* que invadem contas bancárias depois de conseguir descobrir a senha dos usuários com a ajuda de um programa de computador. Por mais que a mídia alerte para este tipo de crime, chamando a atenção para os e-mails com vírus que chegam aos milhares de computadores todos os dias, os correntistas ainda são vencidos pela curiosidade e acabam abrindo arquivos que contaminam o computador e transformam todos em vítimas fáceis dos “marginais cibernéticos”. Os *sites* de órgãos públicos e de empresas transnacionais de renome são invadidos por estes “criminosos virtuais”, diariamente, sem haver uma legislação específica que os puna.

O Projeto de Lei Substitutiva N° 76/2000, de autoria do Senador Eduardo Azeredo, que trata dos “Crimes Cibernéticos”, em tramitação na comissão de Constituição e Justiça (CCJ) do Congresso Nacional (CN), modifica o Código Penal (CP/1940), o Código Penal Militar (CPM/1969), o Código de Processo Penal (CPP/1941), o Código de Defesa do Consumidor (CDC/1990), visando tipificar condutas mediante o uso de sistema eletrônico, o que hoje não existe em nossa lei. O PLS 76/2000 estabelece penas para:

- Acesso indevido a sistemas;
- Roubo de dados;
- Quebra de confidencialidade (um dos pilares da segurança);
- Criação ou propagação de código malicioso;
- Falsificação de cartão de crédito, débito ou similar;

- Clonagem de telefones celulares ou meio de acesso a redes de computadores.

Além disso, o projeto ainda cria um mecanismo de proteção ao consumidor, obrigando que o mesmo seja informado sobre a necessidade do uso de senhas ou similares, visando protegê-los de diversas ações maliciosas.

Apesar do Brasil ainda não ser signatário da “Convenção sobre o Cibercrime”, o presente Projeto de Lei Substitutiva está em harmonia com vários artigos do Acordo Internacional, celebrado em Budapeste, na Hungria, em 2001, na “Convenção sobre o Cibercrime”.

Outro Projeto de Lei é o de N° 1.713 (ULBRICH, 2007), do Deputado Federal Décio Braga, que dispõe sobre os crimes de informática. Este, também em tramitação no Congresso Nacional, que trata dos seguintes assuntos:

- Dano a dado ou programa de computador;
- Acesso indevido ou não autorizado;
- Alteração de senha ou mecanismo de acesso a programa de computador ou dados;
- Obtenção indevida ou não autorizada de dado ou instrução de computador;
- Violação de segredo armazenado em computador, meio magnético de natureza magnética, óptica ou similar;
- Criação, desenvolvimento ou inserção em computador de dados ou programa de computador com fins nocivos;
- Veiculação de pornografia através de rede de computadores.

Como podemos observar, o Projeto é abrangente também, lidando com assuntos que vão desde invasões até a criação de vírus e programas nocivos a dados alheios. Com certeza, centenas de *hackers* teriam a maioria dos seus atos impedidos caso a Lei entrasse em vigor. Mas, além do burocrático processo de aprovação da Lei, o Governo tem que prover condições aceitáveis para que a Lei em questão seja efetivamente executada.

Algumas unidades federativas brasileiras, conscientes dos danos irreparáveis provocados pelo uso ilícito de computadores conectados à *Internet*, tomaram iniciativas pioneiras, no que se refere a Brasil, e legislaram no combate ao “*e-crime*”. No Mato Grosso do Sul, foi aprovada pela Assembléia Legislativa daquele Estado, a Lei N° 3.103 de 11 de novembro de 2005 (GOVERNO DO ESTADO DO MATO GROSSO DO SUL, 2005), que disciplina as atividades de “*Lan-Houses*”, “*Cybercafes*”, “*Cyber-Offices*” e estabelecimentos congêneres no âmbito daquela unidade federativa, e dá outras providências. De igual forma, a Assembléia Legislativa do Estado de São Paulo sancionou a Lei N° 12.228 de 11 de janeiro de 2006 (GOVERNO DO ESTADO DE SÃO PAULO, 2006), que trata dos

estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à *Internet* e dá outras providências.

Em contrapartida, os Estados Unidos da América e a Europa já possuem uma rígida e forte legislação contra os “crimes virtuais”, colocando os *hackers* e os *crackers* no mesmo patamar que terroristas internacionais.

Nos EUA, através do “*USA Act of 2001*” (*Uniting and Strengthening America Act of 2001*), que traduzindo seria o mesmo que “*Ato de 2001 para Unificação e Fortalecimento da América*”, é uma expansão do “*FISA of 1978*” (*Foreign Intelligence Surveillance Act of 1978*), que traduzindo significa “*Ato de 1978 para Fiscalização da Inteligência Estrangeira*”. A diferença preliminar entre os “*USA Act of 2001*” e o “*FISA of 1978*” é a definição do terrorismo. Em FISA, o terrorismo é limitado aos atos que são suportados pelo poder estrangeiro. Entendendo-se que o “poder estrangeiro” é considerado como o “governo estrangeiro”, geralmente. Em virtude da ação terrorista do “*Al Qaeda*” (WIKIPEDIA, 2008), contra os EUA, após o inesquecível dia 11 de setembro de 2001, criou-se o “*USA Act of 2001*”, cujo texto é ainda mais abrangente que o do “*FISA of 1978*”; pois os “terroristas” que não são suportados por um “governo estrangeiro” e mesmo aqueles que podem atuar completamente sozinhos, estão também contemplados no novo ordenamento jurídico. No “*USA Act of 2001*”, o “terrorismo” foi redefinido como a atividade que realmente parece ser pretendida pelos “terroristas”; intimidando ou forçando o governo ou a população civil, e conseqüentemente, quebrando leis criminais e pondo em perigo a vida humana.

Os Estados Unidos da América, após o trágico dia 11 de setembro de 2001, tem demonstrado levar a sério a sua luta contra o “ciberterrorismo”, através de seu conjunto de leis, dentre as quais, destaca-se a “*USA PATRIOT Act of 2001*” (*Uniting and Strengthening America by Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*), que significa “*Ato de 2001 para Unificação e Fortalecimento da América Provendo Ferramentas Apropriadas Requeridas para Interceptar e Obstruir Terrorismo*” (CONGRESSO NORTE-AMERICANO, 2001), que declara no preâmbulo do texto legislativo:

*“Para intimidar e punir atos de terrorismo nos Estados Unidos e em torno do mundo, para fortalecer ferramentas investigativas a fim de que a Lei seja aplicada e para outras finalidades”.*

<sup>1</sup> Grafada também como Al-Qaida ou Alcaida (“A Fundação” ou “A Base”) é uma organização fundamentalista islâmica internacional, constituída por células colaborativas e independentes que visam, supostamente, reduzir a influência não-islâmica sobre assuntos islâmicos.

Outro ato legislativo norte-americano que envolve os “cibercrimes” é o “*FAT Act of 2001*” (*Financial Anti-Terrorism Act of 2001*), que seria o mesmo que “*Ato de 2001 Financeiro Anti-Terrorismo*” (BIBLIOTECA DO CONGRESSO NORTE-AMERICANO, 2001) dá plenos poderes ao governo federal norte-americano para controlar e monitorar criminosos financeiros e, inclusive, poder para sentenciá-los. O “*Ato financeiro do Anti-Terrorismo de 2001*” estatui que:

- Os criminosos a serem punidos são aqueles que foram autuados na prática ilegal de “*lavagem de dinheiro*”;

- Devem-se seguir diretrizes procedimentais para a realização de intimações federais aos registros dos fundos nas contas bancárias correspondentes;

- Existe uma jurisdição federal sobre criminosos envolvidos em “*lavagem de dinheiro estrangeiro*” e sobre o dinheiro “*lavado*” através de um banco estrangeiro;

- Todas as instituições financeiras participantes de um programa de “*lavagem dinheiro*” deverão ser devidamente punidas.

O Departamento de Justiça Norte-Americano manifestou-se solidário ao Governo daquele país, na guerra contra os crimes cometidos com computadores (DEPARTAMENTO DE JUSTIÇA NORTE-AMERICANO, 2002), através da Lei N° 1.030, que trata da “*Fraude e Atividade Relatada em Conexão com Computadores*”.

Finalizando, como apresentado anteriormente, a União Européia (UE) têm adotado o padrão norte-americano na batalha contra o “ciberterrorismo”; além de 43 países signatários, europeus na sua maioria, e ainda os Estados Unidos da América, Canadá e Japão terem participado da “*Convenção sobre o Cibercrime*”, celebrada em Budapeste, Hungria, em 23 de novembro de 2001.

## Parte III

### 3 METODOLOGIA

#### 3.1 METODOLOGIA APLICADA PARA A REALIZAÇÃO DESTA MONOGRAFIA

A pesquisa a ser apresentada, quanto aos objetivos a que se propõe, será do tipo descritivo, sobre a questão da política de segurança de redes de computadores a nível cooperativo, as novas tecnologias de combate e prevenção aos “crimes virtuais” e a legislação vigente contra os mesmos. Será, também, quanto aos procedimentos, do tipo bibliográfico, a fim de possibilitar a consulta e a análise histórico-evolutiva acerca da legislação vigente contra o “ciberterrorismo”.

As fontes de pesquisa a serem utilizadas serão, entre outros, a Constituição Federal (CF/1988) e as legislações específicas, tais como: o Projeto de Lei Substitutiva N° 76/2000 (PLS 76/2000), o Projeto de Lei N° 1.713 (PL 1713), Lei N° 3.103 de 11 de novembro de 2005 (Governo do Estado do Mato Grosso do Sul), Lei N° 12.228 de 11 de janeiro de 2006 (Governo do Estado de São Paulo), o Código Penal (CP/1940), o Código Penal Militar (CPM/1969), o Código de Processo Penal (CPP/1941), o Código de Defesa do Consumidor (CDC/1990), o “*FISA of 1978*”, o “*USA Act of 2001*”, o “*USA PATRIOT Act of 2001*”, o “*FAT Act of 2001*”, a Lei N° 1.030 do Departamento de Justiça Norte-Americano e o Tratado Internacional da “*Convenção sobre o Cibercrime*”, celebrado em Budapeste, na Hungria, em 2001, assim como artigos de jornais e revistas especializados, e material disponível na *Internet*.

A realização da coleta de dados deverá ocorrer ao longo do terceiro bimestre de 2008, em visitas às bibliotecas da Universidade Federal de Rondônia (UNIR), da Ordem dos Advogados de Rondônia (OAB/RO), do Tribunal Regional Federal da Primeira Região (TRF 1ª Região) e do Tribunal Regional do Trabalho da 14ª Região (TRT 14ª Região).

A análise dos dados ocorrerá a partir do estudo do material apurado, das legislações e metodologias existentes, com o objetivo de descrever e analisar o papel das políticas de segurança de redes de computadores cooperativas, conectadas via *Web* ao mundo; assim como, as novas tecnologias em segurança da informação e da legislação vigente contra o “*ciberterrorismo*”, no Brasil e no exterior.

## Parte IV

### 4 O PARADOXO ENTRE A SEGURANÇA DA INFORMAÇÃO E O CRIME VIRTUAL

#### 4.1 O LIMITE DE RESPEITO ÀS LIBERDADES INDIVIDUAIS E O DIREITO PRIVADO NO CIBERESPAÇO

O ser humano em sua evolução viu a necessidade de obter e repassar certos tipos de informações para uma melhor vida em sociedade. Por causa desta necessidade ele foi aperfeiçoando desde a invenção da escrita até a atual *Internet*. A “*Grande Rede*”, por sua vez, apresentou ao mundo uma nova evolução da sociedade, trazendo a informação imediata a todos.

Segundo FILHO (FILHO, 2000):

*“A explosão da Internet para nós, mesmo os menos atentos aos fatos históricos, a clara visão de que uma nova sociedade estava se formando; uma sociedade em que o poder da informação passou a desempenhar papel muito mais importante do que qualquer outra forma de poder. As diferenças entre os povos não mais se medem pelo arsenal bélico ou domínios territoriais, mas pelo domínio e uso das novas formas de tecnologia da informação”.*

Sabe-se claramente que o ser humano ao criar a *Internet*, tinha em mente que tal ferramenta deveria, única e exclusivamente; fomentar e auxiliar a comunicação na sociedade, assim como dinamizar as relações de comércio entre os povos. Mas, ao nos depararmos com a realidade atual, notamos que não é só isso que esta acontecendo no “mundo cibernético”.

Com o grande avanço da globalização, há um maior número de *internautas* na rede, há também um grande número de transações, compras *on-line*, que despertam o interesse de pessoas de mal-intencionadas; as quais adentram a *Internet* e em alguns sistemas, sem a devida autorização para fazer operações fraudulentas, também conhecidas como “operações piratas”. Pode-se invadir sistemas, furtar informações sigilosas e causar sérios danos irreparáveis.

O grande problema da justiça para desvendar esse crime, é porque os crimes *on-line* são crimes sem suspeitos, um crime com poucas pistas.

Como afirma GUIMARÃES (GUIMARÃES, 2000):

*“Em vez de pistolas automáticas e metralhadoras, os ladrões de banco podem agora usar uma rede de computadores e sofisticados programas para cometer crimes. E o pior, fazem isso impessoalmente, de qualquer continente, sem a necessidade de presença física, pois atuam num “território” sem fronteiras, sem leis, acreditando que , por isso, estão imunes ao poder de policia”.*

Para termos noção com que tipo de informações estamos nos deparando, aproximadamente oito milhões de brasileiros acessam a *World Wide Web (WWW)*. Dentro de dois anos esse número pode chegar a quinze milhões, segundo as pesquisas do Instituto de Peritos em Tecnologias Digitais e Telecomunicações – IPDI. Os dados da pesquisa revelam que os prejuízos causados pelos crimes *on-line*, atingiram uma média de um valor superior a 100 milhões de reais. Os benefícios da modernidade e celeridade alcançados com a rede mundial trazem, na mesma proporção, a prática de ilícitos penais que vêm confundindo não só as vítimas como também os responsáveis pela persecução penal.

#### **4.1.1 A EVOLUÇÃO DA INTERNET EM UM MUNDO GLOBALIZADO E SUAS CONSEQÜÊNCIAS**

A comunicação exige um meio de comunicação. No caso humano é a linguagem. As línguas favorecem o relacionamento entre as pessoas e servem para estabelecer elos. Ao mesmo tempo a comunicação exige também instrumentos para transmitir a linguagem, sejam por meio de sinais de fumaça, luminosos, com alto falantes, megafones, rádio, TV ou Internet.

Duas barreiras, portanto, limitam a comunicação: a linguagem comum, que permite a compreensão, e um instrumento que permita e facilite a comunicação. A diferença de línguas é assim um obstáculo para a comunicação e, indiretamente, para a globalização. A outra barreira é tecnológica.

O homem primitivo não era globalizado porque não se integrava, e não se integrava porque não se comunicava. Por isso uma língua universal permite a integração. A tecnologia avança a passos largos e as barreiras das distâncias diminuem a uma insuspeitada velocidade. Os limites técnicos de comunicação estão sendo superados a cada dia, o que não ocorre com a barreira da língua.

A revolução nas comunicações promove a globalização e representa um avanço para a integração mundial. Apresenta, entretanto, como contrapartida, um desafio e um risco. Quando o acesso à informação se torna um fim e não um meio, a pessoa pode empobrecer-se tanto em aquisição de conhecimento, ciência, que só é possível adquirir pelo estudo, quanto na procura e conquista da sabedoria, que é um saber em profundidade, essencial, alcançado pela reflexão e muito distante do simples acúmulo de dados.

A globalização é um processo que se inicia com a comunicação. O advento da globalização traz inúmeras vantagens, porém apresenta sofismas e desafios. A análise desse processo exige reflexão. A comunicação é a ponta do iceberg. A comunicação favorece o relacionamento econômico, o diálogo político e tem um papel importante também cultural e em termos de valores. Para ir ao âmago da globalização é preciso analisar não só a comunicação, mas também a economia, a política e os valores.

Dentre esses parâmetros, o trabalho relata a junção globalização x Internet e como essa parceria tem sido fundamental para todas as áreas da nossa vida, tal como para a evolução do homem como sociedade e mundo.

#### **4.1.1.1 CONCEITO DE GLOBALIZAÇÃO**

Globalização é o conjunto de transformações na ordem política e econômica mundial que vem acontecendo nas últimas décadas. O ponto central da mudança é a integração dos mercados numa "aldeia-global", explorada pelas grandes corporações internacionais. Os Estados abandonam gradativamente as barreiras tarifárias para proteger sua produção da concorrência dos produtos estrangeiros e abrem-se ao comércio e ao capital internacional. Esse processo tem sido acompanhado de uma intensa revolução nas tecnologias de informação - telefones, computadores e televisão.

As fontes de informação também se uniformizam devido ao alcance mundial e à crescente popularização dos canais de televisão por assinatura e da Internet. Isso faz com que os desdobramentos da globalização ultrapassem os limites da economia e comecem a provocar uma certa homogeneização cultural entre os países.

A globalização é marcada pela expansão mundial das grandes corporações internacionais. A cadeia de fast food McDonald's, por exemplo, possui 18 mil restaurantes em 91 países. Essas corporações exercem um papel decisivo na economia mundial. Segundo pesquisa do Núcleo de Estudos Estratégicos da Universidade de São Paulo, em 1994 as maiores empresas do mundo (Mitsubishi, Mitsui, Sumitomo, General Motors, Marubeni, Ford, Exxon, Nissho e Shell) obtêm um faturamento de 1,4 trilhão de dólares. Esse valor equivale à soma dos PIBs do Brasil, México, Argentina, Chile, Colômbia, Peru, Uruguai, Venezuela e Nova Zelândia. Outro ponto importante desse processo são as mudanças significativas no modo de produção das mercadorias.

Auxiliadas pelas facilidades na comunicação e nos transportes, as transnacionais instalam suas fábricas sem qualquer lugar do mundo onde existam as melhores vantagens fiscais, mão-de-obra e matérias-primas baratas. Essa tendência leva a uma transferência de empregos dos países ricos - que possuem altos salários e inúmeros benefícios - para as nações industriais emergentes, com os Tigres Asiáticos. O resultado desse processo é que, atualmente, grande parte dos produtos não tem mais uma nacionalidade definida. Um automóvel de marca norte-americana pode conter peças fabricadas no Japão, ter sido projetado na Alemanha, montado no Brasil e vendido no Canadá.

### 4.1.1.2 HISTÓRICO DA GLOBALIZAÇÃO

Fatos históricos marcantes ocorridos entre o final da década de 1980 e o início da de 1990 determinaram um processo de rápidas mudanças políticas e econômicas no mundo. Até mesmo os analistas e cientistas políticos internacionais foram surpreendidos pelos acontecimentos:

- 1) A queda do Muro de Berlim em 1989;
- 2) O fim da Guerra Fria;
- 3) O fim do socialismo real;
- 4) A desintegração da União Soviética, em dezembro de 1991, e seu desdobramento em novos Estados Soberanos (Ucrânia, Rússia, Lituânia etc.);
- 5) A explosão étnica ou das nacionalidades em vários lugares, acompanhada da guerra civil: antiga Iugoslávia, Geórgia, Chechênia etc.;
- 6) O fim da política do Apartheid e a eleição de Nelson Mandela para presidente, na África do Sul;
- 7) O acordo de paz entre Israel, OLP (organização para libertação da Palestina) e Jordânia;
- 8) A formação de blocos econômicos regionais (União Européia, Nafta, Mercosul, etc.);
- 9) O grande crescimento econômico de alguns países asiáticos (Japão, Taiwan, China, Hong-kong, Cingapura), levando a crer que constituirão a região mais rica do Século XXI;
- 10) O fortalecimento do capitalismo em sua atual forma, ou seja, o neoliberalismo;
- 11) O grande desenvolvimento científico e tecnológico ou Terceira Revolução Industrial ou Tecnológica.

Até praticamente 1989, ano da queda do Muro de Berlim, o mundo vivia no clima da Guerra Fria. De um lado, havia o bloco de países capitalistas, comandados pelos Estados Unidos, de outro, o de países socialistas, liderado pela ex-União Soviética, Configurando uma ordem mundial bipolar.

As reformas iniciadas por Gorbachev, na ex-União Soviética, em 1985, através da Perestroika e da Glasnost, foram pouco a pouco minando o socialismo real e, conseqüentemente, essas ordens mundiais bipolares. A queda do Muro de Berlim, com a reunificação da Alemanha, e muitos outros acontecimentos do Leste Europeu alteraram profundamente o sistema de forças, até então existente no mundo.

De um sistema de polaridades definidas passou-se, então, para um

sistema de polaridades indefinidas ou para a multi-polarização econômica do mundo. O confronto ideológico (capitalismo versus socialismo real) passou-se para a disputa econômica entre países e blocos de países. O beneficiário dessa mudança, historicamente rápida, que deixou muitas pessoas assustadas e preocupadas, foi o sistema capitalista, que pôde expandir-se praticamente hegemônico na organização da vida social em todas as suas esferas (política, econômica e cultural). Assim, o capitalismo se “mundializou”, se “globalizou” e universalizou-se, invadiu os espaços geográficos que até então se encontravam sob o regime de economia centralmente planejada ou nos quais ainda se pensava poder viver a experiência socialista.

A globalização não é um acontecimento recente. Ela se iniciou já nos séculos XV e XVI, com a expansão marítimo-comercial européia, conseqüentemente a do próprio capitalismo e continuou nos séculos seguintes. O que diferencia aquela *globalização* ou *mundialização* da atual são a velocidade e abrangência de seu processo, muito maior hoje. Mas o que chama a atenção na atual é, sobretudo, o fato de generalizar-se em vista da falência do socialismo real.

De repente, o mundo tornou-se capitalista e globalizado.

#### **4.1.1.3 A REVOLUÇÃO TECNO-CIENTÍFICA**

A rápida evolução e a popularização das tecnologias da informação (computadores, telefones e televisão) têm sido fundamentais para fomentar o comércio e as transações financeiras entre os países. Em 1960, um cabo de telefone intercontinental conseguia transmitir 138 conversas ao mesmo tempo. Atualmente, com a invenção dos cabos de fibra óptica, esse número sobe para 1,5 milhão. Uma ligação telefônica internacional de 3 minutos, que custava cerca de 200 em 1930, hoje em dia é feita por US\$ 2. O número de usuários da Internet, rede mundial de computadores, é de cerca de 50 milhões e tende a duplicar a cada ano, o que faz dela o meio de comunicação que mais cresce no mundo. E o maior uso dos satélites de comunicação permite que alguns canais de televisão - como as redes de notícias CNN, BBC e MTV - sejam transmitidas instantaneamente para diversos países. Tudo isso permite uma integração mundial sem precedentes.

A crescente concorrência internacional tem obrigado as empresas a cortar custos, com o objetivo de obter preços menores e qualidade alta para os seus produtos. Nessa reestruturação está sendo eliminados vários postos de trabalho, tendência que é chamada de desemprego estrutural. Uma das causas desse desemprego é a automação de vários setores, em substituição à mão de obra humana. Caixas automáticas tomam o lugar dos caixas de bancos, fábricas *robotizadas* dispensam operários, escritórios informatizados prescindem datilógrafos e contadores. Nos países ricos, o desemprego também é causado pelo deslocamento de fábricas para os países com custos de produção mais baixos.

O fim de milhares de empregos, no entanto, é acompanhado pela criação de outros pontos de trabalho. Novas oportunidades surgem, por exemplo, na área de informática, com o surgimento de um novo tipo de empresa, as de “inteligência intensiva”, que se diferenciam das indústrias de capital ou mão-de-obra intensivas. A IBM, por exemplo, empregava 400 mil pessoas em 1990, mas, desse total, somente 20 mil produziam máquinas. O restante estava envolvido em áreas de

desenvolvimento de outros computadores - tanto em hardware como em software - gerenciamento e marketing. Mas a previsão é de que esse novo mercado de trabalho dificilmente absorverá os excluídos, uma vez que os empregos emergentes exigem um alto grau de qualificação profissional. Dessa forma, o desemprego tende a se concentrar nas camadas menos favorecidas, com baixa instrução escolar e pouca qualificação.

#### 4.1.1.4 O SER HUMANO E A TECNOLOGIA

Segundo Sílvio Fróes Abreu (ABREU, 1959):

*"A tecnologia sempre afetou o homem: das primeiras ferramentas, por vezes consideradas como extensões do corpo, à máquina a vapor, que mudou hábitos e instituições, ao computador que trouxe novas e profundas mudanças sociais e culturais, a tecnologia nos ajuda, nos completa, nos amplia... Facilitando nossas ações, nos transportando, ou mesmo nos substituindo em determinadas tarefas, os recursos tecnológicos ora nos fascina, ora nos assustam."*

A tecnologia não causa mudanças apenas no que fazemos, mas também em nosso comportamento, na forma como elaboramos conhecimentos e no nosso relacionamento com o mundo. Vivemos num mundo tecnológico, estruturamos nossa ação através da tecnologia, como relata KERCKHOVE, na Pele da Cultura "os meios eletrônicos são extensões do sistema nervoso, do corpo e também da psicologia humana".

De acordo com Sílvio Fróes Abreu (ABREU, 1959): *"Os recursos atuais da tecnologia, os novos meios digitais: a multimídia, a Internet, a telemática trazem novas formas de ler, de escrever e, portanto, de pensar e agir. O simples uso de um editor de textos mostra como alguém pode registrar seu pensamento de forma distinta daquela do texto manuscrito ou mesmo datilografado, provocando no indivíduo uma forma diferente de ler e interpretar o que escreve, forma esta que se associa, ora como causa, ora como consequência, a um pensar diferente"*.

Já o escritor GALLO (GALLO, 1994), vai um pouco mais além, quando coloca *"seres humanos com mídias"* dizendo que *"os seres humanos são constituídos por técnicas que estendem e modificam o seu raciocínio e, ao mesmo tempo, esses mesmos seres humanos estão constantemente transformando essas técnicas"*.

Dessa forma, devemos entender a Informática. Ela não é uma ferramenta neutra que usamos simplesmente para apresentar um conteúdo. Quando a usamos, estamos sendo modificados por ela.

Vivemos em um mundo tecnológico, onde a Informática é uma das peças principais. Conceber a Informática como apenas uma ferramenta é ignorar sua atuação em nossas vidas. E o que se percebe? Percebe-se que a maioria das escolas ignora essa tendência tecnológica, do qual fazemos parte; e em vez de levarem a Informática para toda a escola, colocam-na circunscrita em uma sala, presa em um horário fixo e sob a responsabilidade de um único professor. Cerceiam

assim, todo o processo de desenvolvimento da escola como um todo e perdem a oportunidade de fortalecer o processo pedagógico.

A globalização impõe exigência de um conhecimento holístico da realidade. E quando colocamos a Informática como disciplina, nós fragmentamos o conhecimento e delimitamos fronteiras, tanto de conteúdo como de prática. Segundo GALLO (1994) – "*A organização curricular das disciplinas coloca-se como realidades estanques, sem interconexão alguma, dificultando para os alunos a compreensão do conhecimento como um todo integrado, a construção de uma cosmovisão abrangente que lhes permita uma percepção totalizante da realidade*".

**Aprender a partir da tecnologia** (*Learning from*), em que a tecnologia apresenta o conhecimento, e o papel do aluno é receber esse conhecimento, como se ele fosse apresentado pelo próprio professor;

**Aprender acerca da tecnologia** (*Learning about*), em que a própria tecnologia é objeto de aprendizagem;

**Aprender através da tecnologia** (*learning by*), em que o aluno aprender ensinando o computador (programando o computador através de linguagens como BASIC ou o LOGO);

**Aprender com a tecnologia** (*Lerning with*), em que o aluno aprende usando as tecnologias como ferramentas que o apóiam no processo de reflexão e de construção do conhecimento (ferramentas cognitivas). Nesse caso a questão determinante não é a tecnologia em si mesma, mas a forma de encarar essa mesma tecnologia, usando-a, sobretudo, como estratégia cognitiva de aprendizagem.

Para finalizar, GALLO (GALLO, 1994) que:

*"O acesso à Informática deve ser visto como um direito e, portanto, nas escolas públicas e particulares o estudante deve poder usufruir de uma educação que no momento atual inclua, no mínimo, uma alfabetização tecnológica. Tal alfabetização deve ser vista não como um curso de Informática, mas sim, como um aprender a ler essa nova mídia. Assim, o computador deve estar inserido em atividades essenciais, tais como aprender a ler, escrever, compreender textos, entender gráficos, contar, desenvolver noções espaciais etc. E, nesse sentido, a Informática na escola passa a ser parte da resposta a questões ligadas à cidadania."*

#### **4.1.1.5 CONCEITO DE INTERNET**

A Internet é uma rede mundial que interliga milhões de computadores em todo o mundo, de vários tipos e tamanhos. Assim, de modo simples, é uma forma fácil e barata de fazer com que computadores distantes possam se comunicar. A partir daí, o uso está nas mãos das pessoas. Apesar de ter uma história relativamente curta, a Internet se revela como um grande fator de comunicação, integração social e globalização de produtos.

É formada por computadores comuns e por outros, especiais, os servidores, máquinas de alta capacidade, com grande poder de processamento e conexões velozes, controladas por universidades, empresas e órgãos do governo.

Esses computadores podem ter sistemas operacionais diferentes, mas compartilham informações de diferentes formas e conteúdos, disponibilizando vários serviços de diferentes mídias (textos, imagens, vídeo e som). Aliás, essa parte multimídia da Internet é chamada *World Wide Web - WWW*.

Essa comunicação entre tantos sistemas é viável devido a um protocolo padrão de comunicação chamado TCP/IP (*Transfer Communication Protocol/Internet Protocol*). O TCP começou a ser projetado nos anos 60, a partir de interesses militares dos Estados Unidos, para garantir a manutenção e a interoperabilidade de rede, mesmo em condições adversas como uma guerra, por exemplo.

Uma maneira de entender a Internet é pensar nela como uma rede de redes. Sendo assim, a Internet não tem um dono ou uma empresa encarregada de administrá-la. Cada rede individual conectada à Internet pode ser administrada por uma entidade governamental, uma empresa ou uma instituição educacional. Mas, a Internet, como um todo, não tem um dono ou um poder central.

A Internet tem aplicações as mais diversas possíveis: a localização de pessoas, empresas e assuntos (Pesquisa); a troca de informações (Comunicação); a ministração de cursos (Educação), a apresentação de produtos e serviços (Marketing); a comercialização de produtos e serviços (Vendas); o uso de jogos, vídeos, sons e diversos passatempos (Entretenimento), entre outros.

#### **4.1.1.6 O USUÁRIO E A INTERNET**

Como a Internet é uma grande teia, integrada por máquinas de todos os tipos e tamanhos, é importante notar que estando conectado à Internet um computador tem seu poder multiplicado milhares de vezes. Enquanto o computador isolado se limita a acessar as informações gravadas no seu disco rígido, a máquina conectada à rede tem o mundo ao seu alcance.

Os serviços propiciados pela rede nos trouxeram a uma nova realidade: navegar na Internet tornou-se a mais moderna forma de aquisição de informações, sobre praticamente qualquer assunto, já que um usuário tem acesso a uma imensa quantidade de dados, espalhados por toda a rede, de forma prática e amigável. Como muitos endereços estão oferecendo diversos serviços gratuitamente a informação está cada vez mais acessível.

Note-se que a qualidade dos dados é impressionante: toda a informação já existente pode ser atualizada e aperfeiçoada continuamente, por pessoas espalhadas pelo mundo inteiro, durante todo o tempo.

#### **4.1.1.7 O CUSTO E BENEFÍCIO DA INTERNET**

Deve-se ressaltar que o acesso aos servidores da Internet pode ser feito por qualquer pessoa, por meio de um computador, através de uma linha telefônica simples ou de uma rede, lhe possibilitando o uso dos serviços já existentes.

Como a Internet é uma complexa malha de computadores interligados, sempre existe um caminho alternativo para o tráfego, ainda que seja mais longo. Se

for necessário acessar um computador localizado do outro lado do mundo, no Japão, por exemplo, não é necessário fazer um interurbano internacional. Basta conectar-se a um computador ligado à Internet na própria cidade. Esse computador local está conectado a uma máquina em outro estado (ou país) e assim por diante, traçando uma rota até chegar ao destino.

Essa forma de funcionamento garante um custo baixo de conexão. Assim, um usuário comum, que acessa a Internet em casa, por meio de linha telefônica, só precisa pagar a ligação local até o seu fornecedor de acesso. Essa empresa (ou instituição) cobra uma taxa mensal de cada usuário para cobrir, entre outros, os custos da conexão com a rede.

#### **4.1.1.8 A ABRANGÊNCIA E A BI-DIRECIONALIDADE**

A Internet tem alcance e abrangência ímpar, que nenhuma outra mídia, eletrônica (TV, rádio) ou impressa (jornais, revistas e correios) contempla: uma informação pode ser acessada de qualquer lugar do mundo, a qualquer hora e por qualquer pessoa que tenha acesso a um computador devidamente equipado. Como atualmente, se podem encontrar computadores ligados à Internet em praticamente todos os lugares (empresas, lares, escolas, universidades, clubes, igrejas, entre outros), milhões de pessoas que já utilizam esse meio de comunicação estão experimentando enormes alterações em seu modo de vida.

Diz-se que a Internet é uma mídia bi-direcional, já que um usuário pode responder a qualquer questionamento, por meio de formulários.

Assim sendo, a Internet é um valioso auxiliar para educadores, qualquer que seja sua área de atuação.

Note-se que muitas universidades mantêm diversos serviços onde disponibilizam informações gerais sobre a Internet, passando por publicação de artigos, manutenção de listas de discussão, ministração de treinamentos e cursos, inclusive de educação à distância (EaD), numa tentativa de realmente disponibilizar os recursos da rede a um grande número de pessoas, pois, para que se tenha um bom uso dos serviços disponíveis é necessário algum conhecimento sobre a maneira de utilizá-los, o que envolve, além de informações gerais, o conhecimento sobre o uso de vários programas, inclusive diversos detalhes de configurações e funcionamento.

Uma faceta importante da Internet - sobretudo para empresas estrangeiras que querem ligar suas redes internas à Internet mundial - é que todos os endereços numéricos dos computadores (conhecidos como endereços IP) são alocados por uma autoridade central. Essa entidade, o *Network Information Center (NIC)*, tem sua sede nos EUA e é financiado pelo governo, possuindo filiais em todo o mundo. Para se conectar à rede uma empresa precisa assegurar-se de que nenhum de seus computadores tenha um número de identificação interno que esteja sendo usado por alguém na Internet. Qualquer empresa que solicitar uma série de números de identificação para seus computadores receberá do NIC um nome de domínio (*domain name*).

O NIC aloca os domínios "com" a empresas comerciais localizadas nos EUA. Em outros países, o identificador como normalmente vem seguido da sigla ISO para o país em questão. Uma firma inglesa, por exemplo, poderia ter "isle-of-wight.com.uk", e uma firma brasileira poderia ter "sybase.com.br". Cada país pode especificar um uso diferente de domínios hierarquicamente superior daquele país. Os outros domínios principais da Internet incluem: ".edu", para *sites* educacionais (faculdades ou universidades); ".gov", para *sites* governamentais e ".org" para organizações.

Três tipos principais de serviços de informação estão disponíveis na Internet: pessoa-pessoa, pessoa-grupo, e publicação. O primeiro talvez seja o mais usado, sendo representado sobretudo pelo e-mail, que corresponde a mais de 25 por cento do tráfego total da Internet. Existem vários pacotes de e-mail disponíveis no mercado. Os melhores têm recursos úteis, como suporte para múltiplos idiomas, Latim ISO e conjuntos de caracteres de 16 bits, além de capacidade de fazer *file attachment*. O usuário pode redigir mensagens com um aplicativo bilíngüe que permita usar ora o francês, ora o japonês; anexar um arquivo e, depois enviar a correspondência inteira a destinatários em qualquer parte do mundo.

Os serviços pessoa-grupo incluem listas de discussão *online* centralizadas numa caixa postal eletrônica. Os usuários escolhem entre mais de 13 mil grupos de assuntos para, em seguida, trocar mensagens nesse fórum com outros participantes em todo o planeta.

Os serviços de publicação fornecidos pela Internet vêm recebendo bastante publicidade nos últimos tempos. O mais conhecido é a *World Wide Web*, um sistema de publicação distribuído em multimídia e hipermídia. Há ainda muitas maneiras de compartilhar documentos, notas técnicas, *updates* de suporte, boletins, informativos de empresas e outras informações, inclusive o acesso a arquivos remotos, através do sistema *File Transfer Protocol (FTP)*, ou a provisão de suporte ao Gopher, um valioso serviço híbrido que oferece o melhor da *World Wide Web* com a simplicidade e os requisitos mínimos de conectividade do FTP.

#### **4.1.1.9 A EVOLUÇÃO DA INTERNET**

Durante sua vida a Internet sofreu muitas mutações, sempre se adaptando a novas realidades. Mudou o perfil de seus usuários, mudaram as características dos computadores a ela ligados, a velocidade das redes, programas aplicativos, enfim, praticamente tudo.

E para infelicidade de todos aqueles que previam o fim da grande rede mundial, a Internet continua cada vez mais firme e passando a invadir (ou ser convidada) à intimidade de cada vez mais empresas, lares, escolas, universidades e muitos outros locais. Hoje, se podem encontrar computadores ligados à Internet em praticamente todos os lugares.

Uma revolução deste porte, que tem em sua essência a comunicação, tem alterado fortemente o nosso estilo de vida. O modo como pensamos, trabalhamos, e vivemos, estão sendo alterados com uma velocidade nunca vista.

Esta alteração se dá pela incrível sinergia de milhões de pessoas utilizando um meio comum de comunicação, a Internet. Novos conhecimentos, novas tecnologias são criadas e postas à disposição de quem delas precisa em uma velocidade nunca vista. A informação já existente é continuamente trabalhada e aperfeiçoada por pessoas espalhadas por todo o mundo, 24 horas por dia, 7 dias por semana.

Originalmente, antes da sua extensa popularização iniciada em 1993 com a criação do primeiro *browser web*, a utilização eficiente da Internet requeria o conhecimento de vários programas diferentes (*ftp*, *gopher*, *telnet* e vários outros). Além de conhecer o funcionamento destes programas, era necessário também conhecer onde a informação se encontrava. Existiam alguns mecanismos de busca de informação, mas nada comparado aos mecanismos de busca hoje existentes. E a informação existente era em sua maioria composta apenas por texto, sem imagens e sons.

O primeiro *browser Web*, o *Mosaic*, veio mudar radicalmente esta situação. O acesso à informação disponível na Internet passou a ficar ao alcance de praticamente todos, mesmo aqueles com pouca cultura em informática.

A informação passou a ficar disponível de uma maneira simples e intuitiva. A transição entre um computador e outro passou a se dar de forma totalmente transparente para o usuário. A Internet deixou de ser um reduto dos iniciados, dos *experts* em informática.

A revolução criada pelo *Mosaic* se deu pela possibilidade, até então inexistente, de se integrar imagens aos documentos e pela implementação do formato hipertexto. Em documentos hipertexto nós temos informações ligadas, ou seja, o documento deixa de ser linear. A leitura não mais necessita ser feita do começo ao fim. O documento se abre lateralmente, permitindo uma leitura por associações. Através de um documento, em tese, tem-se acesso a toda a informação existente na Web. É o documento sem fronteiras.

O *browser Web* na verdade é apenas um componente de um sistema de informações mais amplo organizado segundo o protocolo chamado *HTTP* ou *Hyper Text Transport Protocol*. Este protocolo foi criado, em 1990, por Tim Berners Lee, que trabalhava então no CERN, na Suíça.

Como se vê, o protocolo HTTP já existia há algum tempo e era muito pouco utilizado. Um outro sistema de informações, chamado *Gopher*, era então a estrela da Internet. A informação era estruturada hierarquicamente, de forma semelhante à estrutura de diretórios de microcomputadores.

Qualquer instituição ligada à Internet que não possuísse o seu servidor *Gopher* estava condenada ao esquecimento. Após o surgimento do *Mosaic*, a maioria dos servidores *Gopher* foi gradualmente substituída por servidores Web e a grande teia mundial começou a se formar. Esta popularização imediata da Web se deu principalmente por duas razões. A primeira delas foi a facilidade de integração entre diversos servidores de informação propiciada pelo protocolo HTTP associada à facilidade de uso do programa *Mosaic* e da integração de imagens aos documentos.

O segundo fator, não menos importante, foi a disponibilização gratuita do código fonte, tanto do servidor HTTP quanto do *browser Mosaic*.

Desta forma, apareceram versões de ambos os programas para praticamente qualquer tipo de computador existente. A partir de então, o número de usuários e paralelamente a quantidade de informação disponível na Internet apresentaram taxas de crescimento nunca vistas.

Com este crescimento apareceram alguns problemas, o mais grave deles sendo justamente a questão da organização e acesso à informação. A Internet passou a ser então o equivalente a uma biblioteca, imensa, sem fichas catalográficas. Um perfeito caos. Da mesma forma que o valor de uma biblioteca está diretamente relacionado ao índice que lista seus livros, o valor da Web é estreitamente dependente dos mecanismos de pesquisa que a servem. Algo precisava ser feito urgentemente. E foi. Como em outras ocasiões, a Internet se adaptou. Se o problema é achar a informação, que se criem então ferramentas de busca que colem o conhecimento armazenado na Web e o organizem de forma a ser facilmente consultado.

O primeiro mecanismo de busca, *Yahoo*, apareceu já em 1994. O *site Altavista*, patrocinado pela Digital, surgiu em 1995, juntamente com o *Excite* e *Infoseek*. Em 1996 foram criados os *sites HotBot* e *LookSmart*.

A tarefa de indexação da *Web*, entretanto, não é tarefa das mais simples. Em seguida ao deslumbramento inicial, de ter a informação disponível facilmente, os usuários sofreram alguns desapontamentos. O primeiro deles, a informação chegava em grandes quantidades e nem sempre o que se obtinha era o que se desejava. E os mecanismos de busca tiveram que se adaptar à esta nova realidade. Esta é uma luta que não tem fim. Cresce a quantidade de informação na Internet, cresce o número daqueles que tentam, de forma honesta ou fraudulenta, obter as primeiras posições nas listagens dos mecanismos de busca.

E isto é o que vamos abordar neste espaço. Tentar entender a tarefa gigantesca de se colocar ordem neste mundo anárquico de informação que é a Internet. As peculiaridades de cada mecanismo de busca, as novas tendências em tecnologia de informação, o que está acontecendo de novo nesta área. Como tirar proveito dos mecanismos de busca de forma a conseguir informações relevantes ao exercício competente de sua profissão e mesmo de sua vida.

É um assunto praticamente inesgotável. Espero conseguir trazer estas informações para vocês de uma forma agradável, interessante e principalmente útil.

#### **4.1.1.10 O USO DA INTERNET**

É difícil encontrar uma categoria de empresas que não esteja "ligada" na Internet global atualmente. Em março de 1995, o número de computadores acessíveis via Internet já estava aumentando constantemente em 11 por cento ao mês. Mais de 1 milhão de japoneses estão conectados ao *NiftyServe*, uma rede japonesa de computadores ligada à Internet. Atualmente mais de 90 países estão representados nos mapas de conectividade da Internet.

A Internet serve de anfitriã a milhares de corporações globais todos os dias, para acesso rápido, previsões, informações do censo, buscas nos cadastros de funcionários ou transações entre empresas. As firmas globais não precisam ir além do próprio quadro de funcionários para aproveitar-se da Internet. As comunicações internas e a distribuição de materiais corporativos podem ser realizadas agora através das chamadas redes privadas virtuais (*virtual private networks*, ou *VPNs*) que, ao trafegarem pela Internet, evitam o considerável custo de se construir uma rede privada internacional.

O atendimento e o suporte aos clientes constituem uma área de negócios que pode ser mantida mais facilmente através de fontes de informação e documentação acessíveis via Internet. Em vez de enviar pelo correio milhares de atualizações de software, as empresas podem oferecer aos seus clientes em todo o mundo a opção mais barata de receber as modificações pela Internet.

Uma das facetas mais empolgantes da Internet é a venda on-line de produtos a clientes novos. Durante os últimos anos, a Internet vem deixando de ser uma espécie de seminário para intelectuais e acadêmicos, passando a funcionar também como feira livre de fim de semana. Milhares de firmas estão ampliando as fronteiras da criatividade comercial com vitrines *online*, *shopping* no ciberespaço, arte, fotografia, *softwares*, *hardwares* e até roupas, alimentos, bebidas e móveis - tudo acessível a partir de qualquer ponto do planeta.

Comércio *online* oferece vantagem, entre outras, de apresentar para as microempresas barreiras menores do que as que os meios convencionais de expansão oferecem para mercados que estão além da comunidade local. Por menos de US\$ 10 mil, uma pequena empresa pode criar uma presença na Internet, evitando a necessidade de montar uma força de vendas ou um canal tradicional de distribuição.

Alguns obstáculos:

Os principais obstáculos atuais ao comércio eletrônico global são: o acesso limitado à Internet em alguns países, a ausência de equivalentes de assinatura digital, internacionalmente aceitos, e a falta de uma tecnologia global de criptografia que garanta a segurança das transações.

Entretanto, o acesso à Internet vem aumentando a uma velocidade notável. No ano passado, a única maneira pela qual uma firma francesa podia se ligar era através da *France Telecom*. Hoje, mais de uma dúzia de empresas operam como provedores de acesso. O número de países cadastrados no banco de dados de acesso no NIC aumentou significativamente nos últimos anos.

As tecnologias de criptografia crescem mais devagar. Entre os obstáculos que impedem a expansão mais rápida de comunicações ponto-a-ponto na Internet estão as restrições impostas às exportações pelos Estados Unidos. A criptografia é considerada de interesse estratégico e por isso sofre restrições significativas quanto a sua exportação. Já que grande parte do trabalho de desenvolvimento da criptografia é feita por empresas sediadas nos EUA, seus produtos ainda não podem ser legalmente exportados. Certamente, essa situação deverá melhorar nos

próximos anos ampliando assim os horizontes do comércio global on-line de todo tipo.

À medida que a queda do custo de entrada for permitindo a expansão global das empresas, enquanto a criação de empresas virtuais for sendo viabilizada através de parcerias fundamentadas na conectividade Internet, a indústria global tornar-se-á rapidamente mais competitiva. As firmas que estiverem prontas para aproveitar os recursos oferecidos pela Internet serão provavelmente as mais bem sucedidas no século XXI. Do ponto de vista empresarial, há de fato um maravilhoso mundo novo à nossa espera.

#### **4.1.1.11 A INTERNET E A GLOBALIZAÇÃO**

A gigantesca rede de redes conhecida como Internet vem crescendo constantemente numa velocidade extraordinária (Vide em 6.2 Anexos). Mais de 2 milhões de sistemas estão interligados atualmente, trocando informações através de um amplo leque de serviços com nomes exóticos, como *FTP*, *Gopher*, *World*, *Wide*, *Web* e *MIME encoded e-mail*. Nos dias atuais, nenhuma empresa que opera globalmente ou planeja se expandir para além das fronteiras nacionais pode se dar ao luxo de desprezar a Internet. A Internet oferece um modo relativamente barato de aproximar compradores e vendedores em escala mundial.

A Globalização Econômica e social que estabelece uma integração entre os países e as pessoas do mundo todo. Através deste processo, as pessoas, as transações financeiras e comerciais e espalham aspectos culturais pelos quatro cantos do planeta. O conceito de Aldeia Global se encaixa neste contexto, pois está relacionado com a criação de uma rede de conexões, que deixam as distâncias cada vez mais curtas, facilitando as relações culturais e econômicas de forma rápida e eficiente. Muitos historiadores afirmam que este processo teve início nos séculos XV e XVI com as Grandes Navegações e Descobertas Marítimas. Neste contexto histórico, o homem europeu entrou em contato com povos de outros continentes, estabelecendo relações comerciais e culturais. Porém, a globalização efetivou-se no final do século XX, logo após a queda do socialismo no leste europeu e na União Soviética. Com os mercados internos saturados, muitas empresas multinacionais buscaram conquistar novos mercados consumidores, principalmente dos países recém saídos do socialismo. A concorrência fez com que as empresas utilizassem cada vez mais recursos tecnológicos para baratear os preços e também para estabelecerem contatos comerciais e financeiros de forma rápida e eficiente. Neste contexto, entra a utilização da Internet, das redes de computadores, dos meios de comunicação via satélite, entre outros.

Uma outra característica importante da globalização é a busca pelo barateamento do processo produtivo pelas indústrias. Muitas delas produzem suas mercadorias em vários países com o objetivo de reduzir os custos. Elas optam por países onde a mão-de-obra, a matéria-prima e a energia são mais baratas. Um tênis, por exemplo, pode ser projetado nos Estados Unidos, produzido na China, utilizado matéria-prima do Brasil e comercializado em diversos países do mundo.

Para facilitar as relações econômicas, as instituições financeiras (bancos, casas de câmbio, financeiras) criaram um sistema rápido e eficiente para favorecer a transferência de capital. Investimentos, pagamentos e transferências bancárias

podem ser feitas em questões de segundos através da Internet ou de telefone celular.

A globalização extrapola as relações comerciais e financeiras. As pessoas estão cada vez mais descobrindo na Internet uma maneira rápida e eficiente de entrar em contato com pessoas de outros países ou, até mesmo, de conhecer aspectos culturais e sociais de várias partes do planeta. Junto com a televisão, a rede mundial de computadores quebra barreiras e vai, cada vez mais, ligando as pessoas e espalhando as idéias, formando assim uma grande Aldeia Global. Saber ler, falar e entender a língua inglesa torna-se fundamental dentro deste contexto, pois é o idioma universal e o instrumento pelo qual as pessoas podem se comunicar.

A Internet possui uma série de características impressionantes. Ela é instantânea, imediata, de alcance mundial, descentralizada, interativa, expansível até ao infinito em termos de conteúdo e de alcance, flexível e adaptável a um nível surpreendente. É igualitário, no sentido de que qualquer pessoa que disponha do equipamento necessário e de uma modesta capacidade técnica, pode constituir uma presença ativa no espaço cibernético, transmitir a sua mensagem para o mundo e reivindicar um seu auditório. Ela permite às pessoas o luxo de permanecer no anonimato, de desempenhar uma determinada função, de devanear e também de formar uma comunidade com as outras pessoas e de nela participar. Em conformidade com os gostos do *internauta*, ela presta-se tanto à participação ativa como ao isolamento passivo como num mundo narcisista, que tem a si mesmo como ponto de referência, feito de estímulos cujos efeitos são semelhantes aos dos narcóticos. A ela pode recorrer-se também para interromper o isolamento de indivíduos ou de grupos.

A configuração tecnológica subjacente à Internet tem uma influência considerável sobre os seus aspectos éticos: as pessoas, geralmente, usam-na de acordo com o modo em que ela é projetada, e delineiam-na de forma a adaptá-la a este tipo de uso. Com efeito, este novo sistema remonta ao período da guerra fria nos anos 60, quando se procurava confundir os ataques nucleares, criando uma rede descentralizada de computadores portadores de dados vitais. A descentralização constituía a chave do esquema, pois desta forma — então, era assim que se raciocinava — o extravio de um ou até mesmo de muitos computadores não significava a perda dos dados.

Uma visão idealista do livre intercâmbio de informações e de idéias desempenhou uma parte notável no desenvolvimento da Internet. Contudo, a sua configuração descentralizada e o projeto analogamente descentralizado da *World Wide Web*, no final dos anos 80, também demonstraram que são adequados a uma *forma mentis* oposta a qualquer coisa que saiba a uma regulação legítima da responsabilidade pública. Assim, nasceu um individualismo exagerado em relação à Internet. Dizia-se que nela se encontrava um novo domínio, a maravilhosa terra do espaço cibernético, onde era permitido qualquer tipo de expressão e onde a única lei consistia na liberdade individual total, de fazer o que quiser. Com efeito, isto significava que a única comunidade, cujos direitos e interesses seriam verdadeiramente reconhecidos no espaço cibernético, era a comunidade dos libertários radicais. Este modo de pensar ainda exerce a sua influência em determinados círculos, apoiados por conhecidos argumentos libertários, aos quais se

recorre também para defender a pornografia e a violência nos meios de comunicação em geral.

Embora os individualistas e os empresários radicais sejam, obviamente, dois grupos muito diferentes entre si, existe uma convergência de interesses entre aqueles que querem que a Internet seja um lugar para quase todos os tipos de expressão, independentemente de quão ignóbeis ou destruidores os mesmos sejam, e aqueles que desejam que ela constitua um veículo de atividades comerciais incondicionadas, segundo o modelo neoliberal que considera o lucro e as leis de mercado como parâmetros absolutos, em prejuízo da dignidade e do respeito das pessoas e dos povos.

A explosão das tecnologias de informação multiplicou muitas vezes as capacidades de comunicação de alguns indivíduos e grupos privilegiados. A Internet pode servir as pessoas no seu uso responsável da liberdade e da democracia, aumentar a gama de opções em vários sectores da vida, alargar os horizontes educativos e culturais, erradicar as divisões e promover o desenvolvimento humano de inúmeras formas. Este livre fluxo de imagens e palavras à escala mundial está a transformar não só as relações entre os povos a níveis político e económico, mas até a própria concepção do mundo. Quando se fundamenta sobre valores comuns, radicados na natureza da pessoa, o diálogo inter-cultural, que se torna possível através da Internet e de outros meios de comunicação social, pode constituir um instrumento privilegiado para construir a civilização do amor.

Contudo, esta visão não é completa. Paradoxalmente, as mesmas forças que contribuem para o melhoramento da comunicação podem levar, de igual modo, ao aumento do isolamento e à alienação. A Internet pode unir as pessoas, mas também as pode dividir, tanto a nível individual como em grupos mutuamente suspeitos, separados por ideologias, políticas, posses, raças, etnias, diferenças de geração e até mesmo de religião. Ela já tem sido utilizada de maneiras agressivas, quase como se fosse uma arma de guerra, e já se tem falado do perigo do « terrorismo cibernético. Seria dolorosamente irónico se este instrumento de comunicação, com um potencial tão elevado para unir as pessoas, voltasse às suas origens da guerra fria e se tornasse uma arena para o conflito internacional.

#### **4.1.1.12 A DIVISÃO DIGITAL**

Certo número de preocupações acerca da Internet está implícito naquilo que se disse até aqui.

Uma das mais importantes delas diz respeito àquilo a que hoje se chama divisão digital — uma forma de discriminação que separa os ricos dos pobres (tabela 1, 6.2 - ANEXOS), tanto dentro das nações como entre elas mesmas, com base no acesso, ou na falta de acesso, às novas tecnologias de informação. Neste sentido, trata-se de uma versão atualizada da diferença mais antiga entre as pessoas ricas de informação e as outras pobres de informação.

A expressão divisão digital salienta o fato de que os indivíduos, os grupos e as nações devem ter acesso às novas tecnologias em ordem a participar nos prometidos benefícios da globalização e do desenvolvimento, e não ser privados dos mesmos. É imperativo « que a brecha entre os beneficiários dos novos meios de

informação e expressão, e os que ainda não tiveram acesso aos mesmos, não se converta noutra obstinada fonte de desigualdade e discriminação. Devem-se encontrar formas de tornar a Internet acessível aos grupos menos avantajados, ou diretamente ou pelo menos vinculá-la aos meios de comunicação tradicionais, cujo custo seja inferior. O espaço cibernético deve constituir um recurso de informações e serviços abrangentes, disponíveis gratuitamente para todos, e numa vasta gama de línguas. As instituições públicas têm a particular responsabilidade de criar e de manter *sites* deste gênero.

Na medida em que a economia global adquire a sua forma, a Igreja está preocupada em garantir que neste processo vença a humanidade inteira e não apenas uma elite próspera que controla a ciência, a tecnologia, a comunicação e os recursos do planeta; isto significa que a Igreja deseja uma globalização ao serviço de todo o homem e do homem todo.

Neste caso, deve-se ter em mente que as causas e as conseqüências da divisão não são unicamente econômicas, mas inclusive técnicas, sociais e culturais. Assim, por exemplo, outra divisão da Internet contribui para a desvantagem das mulheres e também ela precisa ser eliminada.

Estamos particularmente preocupados com as dimensões culturais daquilo que hoje se está a realizar. Precisamente como poderosos instrumentos no processo de globalização, as novas tecnologias de informação e a Internet transmitem e contribuem para formar uma série de valores culturais — modos de pensar acerca dos relacionamentos sociais, da família, da religião e das condições humanas — cuja novidade e fascínio podem desafiar e ultrapassar as culturas tradicionais.

Sem dúvida, o diálogo e o enriquecimento inter-culturais são deveras desejáveis. Com efeito, o diálogo entre as culturas é particularmente necessário hoje, quando se pensa no *impacto das novas tecnologias da comunicação* sobre a vida das pessoas e dos povos. Contudo, este caminho deve ser bilateral. As culturas têm muito a aprender umas das outras, e meramente impor a visão, os valores e até mesmo a linguagem mundial de uma determinada cultura sobre as outras não significa diálogo, mas imperialismo cultural.

O domínio cultural é um problema particularmente sério, quando uma cultura predominante transmite valores falsos, contrários ao bem genuíno dos indivíduos e dos grupos. Desta forma a Internet, juntamente com os outros instrumentos de comunicação social, está a transmitir uma mensagem imbuída dos valores da cultura secular ocidental a pessoas e a sociedades que, em muitos casos, não estão adequadamente preparadas para avaliar e para lidar com a mesma. Daqui resultam problemas sérios — por exemplo, no que diz respeito à vida matrimonial e familiar, cuja instituição está a experimentar uma crise generalizada e radical em muitas partes do mundo.

Em tais circunstâncias, a sensibilidade cultural e o respeito pelos valores e credos dos outros povos são fundamentais. Para construir e conservar o sentido da solidariedade internacional é necessário o diálogo inter-cultural, uma vez que as expressões históricas diversas e geniais da unidade originária da família humana, as culturas, encontram no diálogo a salvaguarda das suas peculiaridades e da sua mútua compreensão e comunhão.

Analogamente, o problema da liberdade de expressão na Internet é complexo e dá origem a uma outra série de preocupações.

Deve-se apoiar de forma vigorosa a liberdade de expressão e o livre intercâmbio de idéias. A liberdade de procurar e de conhecer a verdade é um direito humano fundamental, e a liberdade de expressão constitui uma pedra angular da democracia. Salva a lei moral e o bem comum, que o homem possa livremente procurar a verdade, manifestar e divulgar a sua opinião e, por fim, que possa ser informado, com verdade, acerca dos acontecimentos públicos. E a opinião pública, uma expressão fundamental da natureza humana organizada em forma de sociedade, exige absolutamente « a liberdade da expressão das idéias e dos sentimentos.

À luz destas exigências do bem comum, deve-se combater também as tentativas que as autoridades públicas empreendem a fim de impedir o acesso às informações, seja na Internet ou nos outros instrumentos de comunicação social; pois a consideram como uma ameaça ou um obstáculo para manipular o público mediante a propaganda e a desinformação. Destarte, para impedir a legítima liberdade de expressão e de opinião. A este propósito, os regimes autoritários são absolutamente os piores agressores; contudo, o problema existe também nas democracias liberais, onde o acesso aos meios de comunicação para a expressão política geralmente depende da riqueza, enquanto os políticos e os seus conselheiros violam a lealdade e a imparcialidade, apresentando os seus opositores de maneira errônea e reduzindo as questões a uma dimensão fragmentária.

Neste novo ambiente, o jornalismo está a passar por profundas transformações. A combinação das novas tecnologias e da globalização aumentou as capacidades dos meios de comunicação social, mas também cresceu a sua exposição às pressões ideológicas e comerciais, e isto é verdade também no que se refere ao jornalismo.

A Internet é um instrumento muito eficaz para transmitir rapidamente as notícias e as informações às pessoas. Contudo, a concorrência econômica e a natureza de continuidade perene do jornalismo através da Internet também contribuem para o sensacionalismo e a intriga, para a fusão de notícias, publicidades e divertimentos, bem como para o aparente declínio das reportagens e dos comentários sérios. O jornalismo honesto é essencial para o bem comum das nações e da comunidade internacional. Os problemas atualmente visíveis na prática do jornalismo através da Internet exigem uma emenda urgente por parte dos próprios jornalistas.

Além das questões que dizem respeito à liberdade de expressão, a integridade e a exatidão das notícias, e a partilha das idéias e das informações constituem uma ulterior série de preocupações geradas pelo liberalismo. A ideologia do liberalismo radical é tanto errônea quanto prejudicial — não em menor medida, quando visa tornar legítima a livre expressão ao serviço da verdade. O erro encontra-se na exaltação da liberdade *até o ponto de se tornar um absoluto, que seria a fonte dos valores...* Deste modo, porém, a imprescindível exigência de verdade desaparece em prol de um critério de sinceridade, de autenticidade, de "acordo consigo próprio". Neste modo de pensar não há espaço para a comunidade autêntica, o bem comum e a solidariedade.

#### 4.1.1.13 A EVOLUÇÃO DA INTERNET NO BRASIL

A Internet começou a ser utilizada no Brasil, em meados de 1989 e 1990, somente por Instituições de pesquisas e um pouco depois por Universidades, permanecendo, assim, até o final de 1995, quando a exploração comercial teve início com a liberação de um *BackBone* lançado pela EMBRATEL, com um grande incentivo para a sua propagação da mídia, que passou a abordar o assunto, utilizando-se até de novelas.

Há dois anos atrás, o país contava com cerca de 6 milhões de usuários de *Internet*, enquanto em todo mundo existiam aproximadamente de 349 milhões de usuários. Em janeiro de 2003, já existia no Brasil 22,4 milhões de usuários enquanto nos Estados Unidos são 120,5 milhões de *internautas*. De acordo com os dados acima, não é difícil imaginar o atraso que estamos em relação a outros países, apesar de estarmos na 9ª posição em relação à quantidade de usuários (tabela 2, 6.2 - ANEXOS). Nos Estados Unidos, por exemplo, "em 1995, os consumidores americanos preencheram 49,5 bilhões de cheques. Já, em 2000, esse número caiu de 14%, passando para 42,5 bilhões. Isso se deu em razão do aumento da procura pelo pagamento de fatura on-line que vem sendo utilizado atualmente por cerca de 12 milhões de famílias norte-americanas, isto é, um número em franco crescimento em relação aos 10 milhões de lares que utilizam essa forma de pagamento. Esta mentalidade na América Latina, como um todo, é algo ainda bastante atrasado haja vista que a utilização de banda larga está começando só agora a popularizar-se, enquanto nos Estados Unidos a tendência são as conexões sem fio ( *wireless* ou *wi-fi*).

Enquanto este mundo novo cresce a cada dia, o Brasil vem lentamente tentando acompanhá-lo. Em contra partida, o conceito de "dados" se intensifica no contexto globalizado da propriedade intelectual, bem como a discussão sobre o uso justo e a necessidade de conscientização sobre os efeitos marcantes da tecnologia na rotina das pessoas. Um dos maiores desafios continua sendo a compreensão do potencial intangível e da latente virtualidade do ciberespaço.

Sendo assim, concluímos momentaneamente que nos anos 1980, foram os microcomputadores; nos anos 1990, surgiu a rede que lhes permitiu falar entre si, interligando-os por meio do fio telefônico - a nossa hoje conhecida Internet; na primeira década do século 21, espalha-se a comunicação sem fio, via satélite, móvel e esperta como um telefone celular. Em pouco mais de duas décadas, produziu-se uma revolução planetária, que penetrou capilarmente no dia-a-dia de pessoas, estados, corporações, universidades. No mundo dos negócios, da pesquisa, da medicina, da educação, já não se vive sem a rede. No campo da administração pública, ensaiam-se passos que, por meio do *e-government*, levarão à redução da burocracia e a mais respeito aos direitos dos cidadãos.

Para a sociedade civil, a Internet abre horizontes imensos, ainda não inteiramente medidos. Os vários grupos sociais que se reúnem para a defesa de seus interesses, independente dos programas de Estado (e freqüentemente contra eles), organizaram-se e moldaram formas de representação que são alternativas aos canais habituais de representação política. Com a Internet, esses grupos sociais (vale dizer, a sociedade civil) ganharam uma poderosíssima ferramenta, que supera fronteiras instantaneamente. Com um toque de envio no computador, pessoas e

grupos conseguem espalhar abaixo-assinados que alteram, em poucos dias ou horas, decisões de governos ou ofensas aos direitos dos consumidores. A rede potencializa como nunca se viu antigas formas de pressão, muda costumes, cria novos centros de poder. E dissemina conhecimentos.

Alguns argumentam que as novas tecnologias digitais estão tendo um papel tão revolucionário quanto a tecnologia de impressão no final do século 15. Afinal, a tipografia permitiu a divulgação dos princípios que levaram à criação da democracia, como se conhece hoje, e do Estado moderno - portanto, à construção da consciência nacional. As novas tecnologias digitais, por sua vez, fazem emergir uma nova consciência em escala planetária.

Com a trans-nacionalização das instituições, as decisões que afetam a vida das pessoas são tomadas cada vez mais longe delas. Parte da população está integrada nos processos globais, é afluente, viaja e tem acesso a novas formas de informação e comunicação; a vasta maioria está excluída, mas é vulnerável às suas influências. Disparidades de renda, desemprego, pobreza, violência são o outro lado da moeda.

#### **4.1.2 OS CRIMES NA INTERNET**

As inovações da informática propiciaram a área para o aparecimento de novos tipos de crimes ou novas formas de praticar os já conhecidos tipos penais, surgindo os crimes de informática.

Os tipos de ataques são dos mais variados. Disseminação de vírus que coletam *e-mails* (Correio eletrônico) para venda de *mailings* (Dados Cadastrais), distribuição de material pornográfico envolvendo crianças (pedofilia), fraudes bancárias ou mera invasão de *sites* para deixar pichações virtuais em ambientes, em tese, muito bem guardados.

Assim, crime de informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador. Convém inserir neste conceito os delitos praticados através da *Internet*, pois o pressuposto para acessar a rede é a utilização de um computador.

##### **4.1.2.1 TIPOS DE CRIMES NA INTERNET**

A seguir, abordar-se-á sobre alguns crimes informáticos mais conhecidos e combatidos:

###### **4.1.2.1-A: EXTORSÕES E FRAUDES**

A *Internet* atualmente, é um dos maiores veículos de comércio moderno, fazendo parte da vida de muitas pessoas no mundo. A “*WWW*”, se tornando parte do comércio mundial, acabou envolvendo várias relações comerciais como: compras *online*, pagamentos via *Internet Banking*, pagamentos com cartões de crédito e várias outras, que também são os principais casos de fraudes e extorsões no universo digital.

Nos dias de hoje, as fraudes via *Internet* representam um número assustador, pois indivíduos enganam possíveis compradores via *Internet*, que acabam sendo vítimas de golpes. Tais ocorrências ocorrem, em grande parte, através da transferência de grandes valores entre contas correntes, em questão de segundos. Outra forma bem conhecida entre os *internautas* é a propaganda de anúncios de produtos inexistentes, que geralmente são recebidos em forma de *e-mails*, e assim, após o usuário ter depositado o dinheiro na conta do “estelionatário virtual”, este não envia o produto ao comprador. As queixas mais freqüentes, no entanto, são casos de planos de pirâmides e *marketing de multilevel*, ofertas cartões de créditos, oportunidades de negócios mirabolantes, entre outros. Assim, vale o bom senso e a cautela, antes de realizar qualquer negócio via *Internet*.

Isso tudo ocorre, devido aos grandes gênios, que criam esses fantásticos programas de computador, muito sofisticados, e que inibem qualquer tipo de pista dessas ações fraudulentas.

A partir daí começam os abusos de lavagem eletrônica de dinheiro e o crime organizado, possibilitando até mesmo o tráfico de drogas pela “*Grande Rede*”.

#### **4.1.2.1-B: PIRATARIA DE SOFTWARES**

Os *softwares* ou programas de computador foram uma das maiores criações humanas dos últimos tempos. A invenção desses programas impulsionou o desenvolvimento tecnológico mundial.

As grandes empresas existentes trabalham com *softwares* de última geração, que armazenam cada vez mais, um maior número de dados e informações que, na maioria das vezes, são confidenciais. Esses *softwares* são programas caríssimos, roubados e revendidos, fomentando cada vez mais a “*pirataria virtual*”.

A lei do *software* prevê punições cíveis e criminais para os crimes de violação dos direitos autorais de programas de computador. Do ponto de vista civil, quem violar direitos autorais responde por perdas e danos, ou aplicar uma pena pecuniária pela transgressão do preceito.

Na esfera criminal, a pena sobre crimes de violação de direitos autorais de *softwares*, ou programas de computador, pode ser de 6 (seis) meses a 2 anos de detenção, ou até mesmo 4 anos de reclusão, juntamente com o pagamento de uma indenização extremamente absurda.

Comenta GUIMARÃES (GUIMARÃES, 2000):

*"No Brasil e demais países latino-americanos, para termos um parâmetro dessa realidade, a pirataria é responsável por um rombo de mais de 1,1 bilhões de dólares. A taxa de pirataria é superior a 80% dos programas, vendidos, perdendo apenas para os países asiáticos".*

#### 4.1.2.1-C: PEDOFILIA E PORNOGRAFIA NA INTERNET

Dos crimes praticados através da *Internet*, a pedofilia é sem sombra de dúvidas o que causa maior repúdio e revolta na sociedade. É inaceitável o constrangimento que as crianças e adolescentes são submetidos, a fim de saciar o prazer doentio e repugnante de pessoas imorais. A pedofilia tira da criança o que ela tem de mais valioso, sua inocência, sua pureza, sua infância. Uma conduta tão grave como esta merece uma severa reprimenda por parte da sociedade, seja pelo Poder Público, ao processar e julgar os criminosos, seja pela participação individual de todo cidadão, ao denunciar os envolvidos nesta prática e apontar os sites de divulgação.

A pedofilia consiste num distúrbio de conduta sexual, no qual o indivíduo adulto sente desejo compulsivo por crianças ou pré-adolescentes, podendo ter caráter homossexual ou heterossexual. Na maior parte dos casos, se trata de homens, muitos deles casados, que se sentem incapazes de obter satisfação sexual com uma pessoa adulta.

O Estatuto da Criança e do Adolescente - ECA, Lei 8.069/90, cuida dos direitos das crianças e dos adolescentes. Criança, para o estatuto, é a pessoa até doze anos de idade incompleto e adolescente aquela entre doze e dezoito anos (artigo 2º da Lei 8.069/90).

A Lei 8.069/90 possui vários tipos penais, dentre eles encontramos o referente à pedofilia.

Art. 241. Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão de um a quatro anos.

Publicar é tornar público, divulgar. Quem insere fotos de criança ou adolescentes em cena de sexo na *Internet* está publicando e, assim, cometendo a infração. O crime pode ser praticado através de *sites*, *homepages*, muitas delas destinadas à pornografia. É importante salientar que não importa o número de *internautas* que acessem a página, ainda que ninguém conheça o seu conteúdo, as imagens estarão à disposição de todos, configurando a infração. Por outro lado, quem envia um *e-mail* com uma foto anexada não está tornando público e sim enviando a uma determinada pessoa, destarte, a conduta é, infelizmente, atípica.

Como a lei protege o menor, há quem sustente que só existirá crime quando a vítima for conhecida e identificada. Ousamos discordar. Ainda que desconhecida, a criança ou adolescente que teve sua foto divulgada está protegida pelo ECA. Desta forma, a identificação pode facilitar a persecução penal, mas sua ausência não tem o condão de impedir o processo.

Na pedofilia, como nos outros crimes praticados através da *Internet*, não é difícil identificar a máquina, posto que todo computador possui um endereço IP (*Internet Protocol*). O problema é saber quem utilizou o computador para divulgar as fotos de crianças e adolescentes. Em se tratando de empresas, estabelecimentos de ensino, cafés (*LAN Houses*) e outros locais em que o uso é feito por diversas pessoas, a investigação pode ser infrutífera.

Embora a pena abstratamente cominada admita a suspensão condicional do processo, entendemos ser impossível a concessão do benefício (art. 89 da Lei 9.099/95), pelas seguintes razões: A conduta social de quem divulga fotos de crianças e adolescentes em cena de sexo é extremamente reprovável, causando repúdio e revolta na sociedade. Os motivos que levam o agente à prática do crime são imorais e repugnantes. Acrescente-se que as conseqüências deste tipo de infração podem ser gravíssimas. O agente que divulga as fotos de um menor, além de expor sua privacidade, provoca traumas irreparáveis. Observe-se, que muitas vezes tais fotos são divulgadas a outros menores, o que gera um distúrbio em seu amadurecimento sexual. As circunstâncias do fato são desprezíveis, o agente utiliza as crianças para satisfazer sua lascívia. Sendo assim, quem comete tal conduta é indigno, depravado e pervertido.”

#### **4.1.3 COMO EVITAR “CRIMES CIBERNÉTICOS”**

A melhor forma de evitar ser vítima desses crimes é a informação. Todo o *internauta* deve ter o mínimo de segurança no *site* em que vai visitar. Por isso, algumas recomendações são essenciais para segurança na rede, entre elas podemos destacar:

- Desconfiar de qualquer *e-mail* de pessoas desconhecidas ou *e-mails* escritos em língua estrangeira;
- Grandes organizações ou grandes empresas de confiança raramente realizam a solicitação de senhas eletrônicas, números de documentação, entre outras;
- Nunca confie em *links* prontos que aparecem em *e-mail*: Digite sempre você mesmo o endereço de *site* a visitar;
- Tenha um bom antivírus e sempre atualizado em seu computador. Mas cuidado, um antivírus nem sempre resolve a situação.

Hoje os Estados Unidos é o primeiro país em combate a esses crimes devido sua população ser bem informada sobre o assunto, e também, por já existirem agentes especializados responsáveis por investigar esses crimes.

## **4.2 O LIMITE ENTRE O DIREITO À INFORMAÇÃO E OS ATAQUES À LIBERDADE NO CIBERESPAÇO EM UM MUNDO GLOBALIZADO**

Como a idéia de crimes na *Internet* é nova, não existem leis específicas para esse ato. O que temos hoje, que pode condenar, são alguns artigos do código civil, como os Art. 927, 186, 187. Esses códigos falam em possíveis atos criminosos, ou àquele que viola por omissão voluntária cometer um ato ilícito.

Afirma BACELAR (apud CARVALHO, 2001):

*"Internet não cria um espaço livre, alheio ao direito. A legislação vigente se aplica, aonde e quando for cabível às relações jurídicas decorrentes de fatos jurídicos ocorridos na Internet e pela Internet".*

Hoje não existem leis específicas para os crimes na *Internet*, o que há são leis que punem em relação da consequência. Por isso, já estão em fase de elaboração e votação, projetos de lei que buscam punir casos de crimes na Internet, com o objetivo de diminuir o número de “*crimes cibernéticos*”.

Paulo José Tupinambá apresentou um projeto de lei no senado e afirmou:

*“Acredito que a partir da aprovação da lei, a tendência é de que o número de crimes de informática diminua, já que a punição aos crimes será muito mais contundente que a atual. A lei deverá prever situações como a reincidência no crime eletrônico, que atualmente não existe”.* (Apresentação de Projetos de Lei no Senado, 2004).

O Projeto de Lei nº 84/99 e o Projeto de Lei nº 1713/96, são os dois projetos mais importantes que estão em tramite no Congresso Nacional e tem como objetivo a regulamentação dos crimes digitais.

O Projeto de Lei nº 84/99 dispõe sobre crimes cometidos na área da informática e suas penalidades. Esse projeto prevê sete modalidades de delitos com relação à informática, que são chamados de crimes digitais, podendo chegar até 6 (seis) anos de reclusão e multa. O principal objetivo do projeto é o preenchimento das lacunas na legislação brasileira, isto é, retratar atos que não existem na legislação penal em vigor.

O capítulo I do Projeto de Lei nº 84/99 preceitua os princípios que regulam a prestação de serviço por redes de computadores. Os serviços de rede devem fornecer segurança, garantia de acesso às informações e devem respeitar os direitos individuais e coletivos.

O capítulo II regulamenta o uso de informações disponíveis em computadores ou redes de computadores. A informática é alvo de muitas atividades, desde sociais até criminais.

É muito importante que se realize um trabalho de base nas faculdades de direito, para que se tenha um efetivo desenvolvimento da capacidade técnica do judiciário, sobre um assunto que cedo ou tarde vai estar nos tribunais. Por isso é importante que haja um destaque na realização de eventos que proporcionam debates sobre o Direito e *Internet*.

Para que não haja “*crimes virtuais*” é preciso investir na prevenção. Deve haver discussões tanto no âmbito estatal quanto no privado, para encontrar maneiras de aumentar a confiança nas novas tecnologias. Como é algo recente, a “*Grande Rede*” se torna um desafio para o Direito, o qual visa pacificar e acabar com conflitos sociais.

## 4.2.1 O FUTURO DA INTERNET NO CONTEXTO JURÍDICO

Algum dia os negócios *online* serão regra e não exceções. Décadas atrás, a informática era importante e não popular. Com o advento da *Internet*, esta conseguiu se expandir em todos os segmentos e camadas da sociedade. A utilização do computador e da *Internet* é uma realidade inquestionável devido às vantagens que ambos proporcionam a sociedade.

Como o número de *internautas* que passam a usar a *Internet* cada dia é maior, a “*WWW*” acaba se tornando uma sociedade, e como por regra de boa convivência, uma sociedade deve ser regida por leis. Por esse motivo, as perspectivas do futuro da *Internet* deveriam ser de uma sociedade *online* regada por leis específicas.

A inclusão digital é um dos principais objetivos para o futuro da *Internet*, na qual as escolas de 1º e 2º graus serão responsáveis por essa inserção social à informática, com o fomento das relações sociais e comerciais.

É preciso a criação de novas formas de proteção à propriedade intelectual, para resolver os problemas trazidos pela *Internet*. É preciso resgatar a essência original da *Internet*, como o ambiente de comunicação universal, livre de interesses mercantilistas. O uso sem fins lucrativos de obras na rede virtual deve ser considerado lícito, pois não há qualquer prejuízo por parte do autor. Porém, o uso com fins lucrativos é abusivo, desatendendo ao interesses coletivos e aos interesses individuais do autor de determinada obra.

A facilidade de como as informações são armazenadas, distribuídas e transmitidas na *Internet* trouxe a obsolescência das leis de proteção a propriedade intelectual.

Segundo Liliana Paesani (*apud* MARTINI, 2001):

*"Se o jurista se recusar a aceitar o computador, que formula um novo modo de pensar o mundo, que certamente não dispensará a máquina, dispensará o jurista. Será o fim do Estado do Direito e a democracia se transformará facilmente em tecnocracia".*

Após discussões em saber qual a proteção jurídica a conferir nessa obra intelectual, a maioria dos países decidiu por atribuir aos criadores de programas de computador direitos autorais. Mas no Brasil, são protegidos os programas através dos direitos autorais.

Com os direitos autorais, o criador tem direito exclusivo de dispor, usar e fruir de sua obra, por período determinado. A *Internet*, por sua vez, amplia as possibilidades de violação desses direitos.

O direito autoral possui dupla finalidade, proteger o indivíduo e a coletividade, ou ainda, da utilização do mesmo para proveito de outros. Ele possui uma natureza pessoal-patrimonial. O vínculo pessoal é o decorrente da personalidade do autor. Já o outro decorre do tratamento que a lei dispensa, ao mesmo tempo, a obra: o de um bem econômico.

## 4.2.2 A ASSINATURA DIGITAL NO PLANO DA VALIDADE DO ATO JURÍDICO

Atualmente o mundo conhece uma nova realidade: a realidade da era digital ou eletrônica.

O homem admite e reconhece com muita facilidade aquilo que é capitado por um dos seus cinco sentidos, destarte, naquilo que é tangível. Entretanto, os recursos tecnológicos fazem o homem experimentar uma nova forma de existência – a existência virtual. É sobre este palco que se criou a figura da assinatura digital.

A assinatura digital é uma novidade ao ordenamento jurídico brasileiro. Neste momento, há um grande esforço do poder legislativo na aprovação de um projeto de lei que versa sobre este novo conceito.

O Direito sendo um fato social, supõe-se a pré-existência da sociedade. Conclui-se que não é a sociedade que depende do direito, mas ao contrário, o direito que deve se adaptar a sociedade.

Partindo deste pressuposto, optou-se por utilizar princípios já que são eles que dão o sustentáculo ao Direito, reconhecidamente aceitos desde a fundação de Roma e que permanecem íntegros no Direito moderno. Aprenderam-se alguns destes princípios e a partir de então, o Direito foi adaptado a esta invenção, obra da sociedade, a assinatura digital.

### 4.2.2.1 A ASSINATURA DIGITAL NO ATO JURÍDICO

Na tentativa de responder a esta questão, ascendeu-se a relevante conclusão: demonstrou-se a possibilidade de inserir a assinatura digital no plano da validade do ato jurídico, para tanto, devendo preencher alguns requisitos:

O direito antigo era formalista, deu mais importância à forma. Por isso, os atos jurídicos do *Direito Quiritário (Jus Civile)* exigiam formalidades, de cuja observância dependia a validade do ato e conseqüentemente o efeito jurídico<sup>1</sup>.

A evolução posterior acentuou-se cada vez mais ao valor do elemento intencional do ato jurídico. Desta forma, a manifestação da vontade deveria ser feita de maneira clara, porém sem tanta prevalência das formas solenes.

1. MARKY, THOMAS. Curso Elementar de Direito Romano. Editora Saraiva, São Paulo, 1995, P. 47.

Na atualidade, assiste-se ao renascimento do formalismo. O excesso de cultura está produzindo efeitos análogos aos decorrentes da simplicidade e da ignorância dos povos primitivos. A solenidade dos atos jurídicos ressurgiu quando a lei, por exemplo, prescreve a necessidade de autenticação, registro, transcrição, reconhecimento de firma, apresentação de originais, entre outros.

Por outro lado, a sobrevivência do formalismo, em certos casos, tem sido justificada, pela necessidade de garantir maior segurança na vida jurídica. Destarte, faz-se necessário criar uma legislação específica que trate dos temas que a *Internet* tem suscitado, como por exemplo, o comércio eletrônico. E inserido no comércio eletrônico está a assinatura digital, objeto de estudo deste trabalho.

Estamos no início de uma estrada que possui uma trajetória linear e avança até o horizonte, perdendo-se de vista. Lá adiante, onde quase os olhos não alcançam, existe um objeto desconhecido.

Motivados pela curiosidade e pelo desejo do conhecimento, damos o primeiro passo e caminhamos por esta estrada. Na medida em que vamos evoluindo, este objeto obscuro passa a ganhar contornos, uma vez que vamos conhecendo e entendendo o assunto em pauta, em detalhes.

Seguiremos com determinação, até que chegará o momento que alcançaremos este objeto. E assim, poderemos analisá-lo com clareza, e finalmente compreendê-lo.

O objeto desconhecido é o novo conceito que as inovações tecnológicas estão trazendo ao mundo. A estrada é o exercício da pesquisa. O ponto de partida é o fundamento e o princípio jurídico. E primeiro passo é o *fato jurídico*.

#### **4.2.2.2 O FATO JURÍDICO**

A qualidade de ser humano já é suficiente para podermos afirmar que o homem, naturalmente, precisa viver em sociedade. Esta necessidade além de nascer *com* o homem, nasce *do* homem. Não obstante, conclui-se que viver em sociedade é condição para a existência do homem.

Quando surge o ser humano na face da terra, por instinto, começa a se agrupar. Deste grupo, conseqüência do aumento do número de seus integrantes, deriva a sociedade. Na medida em que esta sociedade se desenvolve, as relações sociais assumem formas mais variadas e complexas. Neste contexto, o direito torna-se instrumento indispensável a convivência inter-humana, já que é ele que vai impor regras de comportamento, atingindo a paz e a ordem social. É sobre este alicerce que se erigem a doutrina da sociedade civil.

A vida é uma sucessão de fatos. A norma jurídica atua sobre alguns destes fatos produzindo conseqüências específicas, os chamados efeitos jurídicos. Nesta hipótese, a norma jurídica atribui uma característica ao fato, que o torna distinto dos demais, o de ser fato jurídico.

Dentre os fatos jurídicos, uns são de ordem natural, alheios à vontade humana. Outros são as ações humanas. Entre estes, aqueles que produzem efeitos jurídicos em consonância com a vontade do agente, são os atos jurídicos<sup>1</sup>.

#### 4.2.2.3 CONCEITO DE FATO JURÍDICO

O Direito Romano não conheceu a teoria do fato jurídico, por isso não há expressão latina própria para mencionar a espécie<sup>2</sup>. Porém no fragmento 1, parágrafo 1, D, XLI, 1 diz: "*Omnia Igitur animalia, quae terra, mari, coelo capiuntur, id est ferae bestiae et uolucres et pisces, capientium fiunt*" (Todos os animais que são apreendidos na terra, no mar ou no ar, isto é, as feras, as aves e os peixes passam a ser dos que deles se apoderam). Portanto, os juristas romanos previram, ainda que abstratamente, uma situação de fato (isto é, que alguém cace uma fera) a qual atribuiu um efeito jurídico (o nascimento de uma relação jurídica, com a aquisição do direito de propriedade)<sup>3</sup>.

O jus-filósofo Washington de Barros Monteiro diz que fatos jurídicos são os acontecimentos de que decorrem o nascimento, a subsistência e a perda dos direitos, contemplados em lei.

Muitas outras definições têm sido propostas, apenas como exemplo, citaremos:

*"São fatos jurídicos os que produzem um evento jurídico que pode consistir, em particular, na constituição, modificação ou extinção de uma relação jurídica, ou, também, na substituição duma relação nova a uma relação*

1. MONTEIRO, Washington de Barros. Curso de Direito Civil. Editora Saraiva, São Paulo, 1997, P. 170.

2. MELLO, Marcos Bernardes de. Teoria do Fato Jurídico. Saraiva, São Paulo, 1999, P. 06.

3. ALVES, José Carlos Moreira Alves. Direito Romano. Forense, Rio de Janeiro, 1996, P. 149.

*preexistente, e, ainda, na qualificação duma pessoa, duma coisa ou de um fato<sup>1</sup>".*

*"Fato jurídico é, pois, o fato ou complexo de fatos sobre o qual incidiu a regra jurídica; portanto, o fato de que dimanar, agora, ou mais tarde, talvez condicionalmente, ou talvez não dimanar, eficácia jurídica. Não importa se é singular, ou complexo, desde que, conceptualmente, tenha unidade<sup>2</sup>".*

#### **4.2.2.4 - ATO JURÍDICO**

Foi visto que a diferença fundamental entre fato jurídico e ato jurídico é que o primeiro é acontecimento natural, independe da vontade interna. O segundo é acontecimento voluntário, fruto da inteligência e da vontade do interessado.

Vale salientar que do ato jurídico, nascem muitos direitos e obrigações que não tem fundamento no querer do agente, mas nas imperiosas disposições normativas.

##### **4.2.2.4.1 CONCEITO DE ATO JURÍDICO**

O legislador definiu o ato jurídico no art. 81 do Código Civil, como sendo todo ato lícito, que tenha por fim imediato adquirir, resguardar, transferir, modificar ou extinguir direitos.

Seu conceito é completado pela doutrina, afirmando que o ato jurídico é o fato jurídico cujo suporte fático tenha como cerne uma exteriorização consciente de vontade, dirigida a obter um resultado juridicamente protegido ou não proibido e possível<sup>3</sup>. Silvio Rodrigues diz que o ato jurídico é aquele ato lícito, da vontade humana, capaz de gerar efeito na órbita do direito<sup>4</sup>.

Do seu conceito, é possível extrair os elementos que compõe o ato jurídico. Destarte, partindo de seus elementos iremos propor uma nova visão da constituição do ato jurídico.

1. PASSARELLI, Santoro. Teoria Geral do Direito Civil. Atlantida, Coimbra, 1967, P. 77.

2. PONTOS DE MIRANDA, Francisco Cavalcante. Tratado de Direito Privado. Bosch, Rio de Janeiro, 1972, P. 77.

3. MELLO, Marcos Bernardes de. Teoria do Fato Jurídico (Plano da Existência). Editora Saraiva, São Paulo, 1999, P. 119.

4. RODRIGUES, Silvio. Direito Civil. Editora Saraiva, São Paulo, 1996, P. 169.

#### 4.2.2.4.2 ELEMENTOS DO ATO JURÍDICO – UMA NOVA VISÃO

Amparado pela legislação brasileira e por conceitos doutrinários, demonstraremos ser possível a realização da seguinte operação:

*Vontade de manifestação + Vontade do conteúdo do ato = Ato jurídico perfeito*

Este modelo sugere que o ato jurídico, é formado por duas vontades: de manifestação e do conteúdo do ato. São vontades distintas e autônomas entre si, porém, quando unidas, produzem efeitos jurídicos suficientes para alcançar a qualidade de ser ato jurídico perfeito.

Esta nova visão do ato jurídico tem o escopo analisar a função desempenhada por seus elementos. A partir desta análise, verificar a exata localização da assinatura e conseqüentemente a assinatura digital, enquanto estiverem compondo um ato jurídico.

#### 4.2.2.5 VONTADE DE MANIFESTAÇÃO

A vontade é uma faculdade que o homem tem de querer, espontaneamente, alguma coisa. É uma energia que domina e dirige suas idéias.

Entretanto, suscita a seguinte questão: Como exteriorizar esta vontade? Como manifestar a vontade?

Em regra, a vontade de se manifestar é livre. Este princípio liberal é consagrado pelo art. 129 do Código Civil, que assim reza: "A validade das declarações de vontade não dependerá de forma especial, senão quando a lei expressamente exigir".

É indiscutível que tudo que acontece no mundo deve se apresentar revestido de alguma forma. Para algo se tornar realidade concreta importa, necessariamente, ter uma forma. A vontade também, ao exteriorizar-se toma alguma forma. Assim a vontade se revela da forma tácita ou expressa, conforme art. 1.079 do Código Civil que diz: "A manifestação da vontade, nos contratos, pode ser tácita, quando a lei não exigir que seja expressa".

A manifestação da vontade é expressa quando se revela da deliberação de externar o pensamento em determinado sentido. Pode ser através da *palavra escrita* ou oral<sup>1</sup>. Igualmente Vicente Rao diz que a manifestação expressa é a *palavra escrita* ou falada<sup>2</sup>.

1. RODRIGUES, Silvio. Direito Civil. Editora Saraiva, São Paulo, 1997, P. 56.

2. VICENTE, Rao. Ato Jurídico. Revista dos Tribunais, São Paulo, 1997, P. 120.

O *Dicionário Houaiss* diz que a assinatura é o nome escrito. Logo, podemos afirmar que a assinatura, sendo uma palavra escrita, pode ser uma forma expressa de manifestação de vontade.

A assinatura por sua vez, tem três funções: (i) a função declarativa: individuar o autor do documento; (ii) a função declaratória: afirmação da autoria do conteúdo do documento pela pessoa e (iii) a função probatória: garante a autenticidade do documento .

Resumidamente, podemos afirmar que as funções da assinatura são: (i) revelar a identidade; (ii) manifestar a vontade e (iii) garantir a integridade.

Não obstante, se fizermos uma análise do efeito pode-se concluir que qualquer meio empregado, independente da forma utilizada, mas que desempenhe as mesmas funções da assinatura, pode ser equiparada a esta e, por conseguinte, adquirir a mesma validade.

Neste contexto, a assinatura digital, uma vez desempenhando as mesmas funções da assinatura tradicional (autográfica) encontra sua validade.

Observe o art. 371 do Código de Processo Civil: "Reputa-se autor do documento particular: I. Aquele que o fez e o assinou."

Da mesma forma, o art. 131 *caput* do Código Civil afirma: "As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários".

Note-se que ordenamento jurídico brasileiro, em suas diversas disposições, pressupõe que a assinatura esteja vinculada a um documento. Contudo, a assinatura pode ter existência própria, como será demonstrado a seguir:

Imagine o seguinte: Um fã de determinado artista, consegue que seu ídolo deposite sua assinatura em um pedaço de papel. Assim temos o autógrafo, isto é, um simples escrito feito pelo punho do autor. Porém, para este fã, a assinatura adquire inestimável valor sentimental, e eventualmente até um valor financeiro. É como se um pedaço daquele que assina, aderisse ao papel, ganhando vida e existência própria.

<sup>1</sup>Segundo Carnelutti, "Studi sulla sottoscrizione", in Riv. Dir. Comm. 1929, I, pág. 523, apud Paolo Piccoli e Giovanna Zanolini. "Il Documento Elettronico e la Firma Digitale", P. 67.

Imagine outra situação: É indiscutível a qualidade da obra de *Picasso*. Porém, por vezes, poderá ocorrer que entre as inúmeras de suas obras, uma não tenha atingido boa qualidade. Contudo, a assinatura *Picasso*, prevalece sobre o conteúdo, valorizando-se. Perceba que nesta hipótese, a assinatura mostrou-se mais relevante que a própria obra.

Diante das situações apresentadas, a assinatura pode adquirir autonomia ou prevalecer sobre o conteúdo a que esteja vinculada.

#### **4.2.2.6 VONTADE DO CONTEÚDO DO ATO**

O próximo elemento que compõe o ato jurídico é a vontade do conteúdo do ato. O conteúdo do ato guarda o objeto. Dispõe o art. 82 do Código Civil que o objeto lícito é uma das condições para validade do ato. Desta forma, será inexistente o conteúdo que abrigar um objeto ilícito.

O Código Civil dispõe no art. 147, o seguinte: "É anulável o ato jurídico: II. por vício resultante de erro, dolo, coação, simulação ou fraude"

O mesmo código, no artigo seguinte (148), diz: "O ato anulável pode ser ratificado pelas partes, salvo direito de terceiro. A ratificação retroage a data do ato".

1. Recentemente foi divulgado pela imprensa radiofônica, que fora arrematado por um valor expressivo, um guardanapo autografado pelos integrantes da banda inglesa "*The Beatles*". Uma peculiaridade é que tal guardanapo estava manchado com molho de tomate.

Desta forma, podemos verificar que os vícios atuam somente sobre o conteúdo do ato. Pois se as partes deliberarem ratificar o conteúdo, poderão fazer. Note-se, portanto, que os vícios não conseguem atingir a vontade de manifestação.

Única objeção se faz quanto a coação absoluta. Pois a coação absoluta é a pressão física exercida sobre alguém para induzi-lo a prática de um ato. A coação é o vício que atinge a própria base, isto é, a vontade livre do agente. Contudo, o legislador equiparou a coação aos outros vícios, quando os colocou no mesmo artigo de lei.

Conclui-se que a partir do instante que se manifesta a vontade, o conteúdo do ato adquire autonomia. Por exemplo, após a assinatura, os efeitos decorrem do conteúdo, e não mais da manifestação. Tanto é assim que mesmo quando uma das partes, em um contrato, muda de idéia e persistem os efeitos do contrato. Neste momento, o conteúdo do ato obriga as partes, e a vontade de manifestação já não mais existe. Assim, o conteúdo do ato é autônomo.

#### 4.2.2.7 VINCULAÇÃO DA VONTADE DE MANIFESTAÇÃO COM A VONTADE DO CONTEÚDO DO ATO

Temos demonstrado até o momento que a existência da vontade de manifestação independe do conteúdo. Em outro caminho, também, a existência do conteúdo independe da vontade de manifestação. São elementos autônomos, distintos, cada um com vida própria.

Far-se-á necessário para concretização do ato jurídico, a união ou vinculação destes dois elementos. Note que o resultado desta união é o ato jurídico perfeito. A partir do momento que o ato adquire a qualidade de ser perfeito, ganha estabilidade, garantida constitucionalmente pelo art. 5º, inciso XXXVI:

*"A lei não prejudicará o direito adquirido, o ato jurídico perfeito e a coisa julgada". José Abreu diz que o ato jurídico reputa-se perfeito quando reúna todas as condições necessárias para torná-lo existente, isto é, dotado de força e conteúdo<sup>1</sup>.*

A vinculação deve ser consciente. A inconsciência implica a inexistência do ato. Em um contrato, a vinculação ocorre quando se registra a assinatura abaixo do conteúdo. Em um leilão, onde a vontade de manifestar faz por simples gesto, a vinculação ocorre quando o leiloeiro ao fazer o lance percebe o gesto.

Em um contrato eletrônico, a vinculação faz-se por intermédio de uma Autoridade Certificadora. Sobre a Autoridade Certificadora, analisaremos com maiores detalhes, no capítulo seguinte.

<sup>1</sup>ABREU, José. O Negócio Jurídico e sua Teoria Geral. Editora Saraiva, São Paulo, 1988, P. 311

#### 4.2.2.8 – A ASSINATURA DIGITAL

Encontra-se em tramitação o projeto de lei Nº 1.483/99 (apensado ao projeto Nº 1.589/99) que trata da assinatura digital e dos documentos eletrônicos.

A assinatura digital é a assinatura tradicional (autográfica), incrementada por recursos tecnológicos. Portanto, ambas buscam produzir os mesmos efeitos. Segundo QUEIROZ (QUEIROZ, 2000) a assinatura digital se apresenta de forma eletrônica, foi desenvolvida a partir da tecnologia da criptografia assimétrica.

A criptografia (escrita oculta, em grego) consiste na técnica de “*embaralhamento*” de dados que somente poderão ser identificados por alguém habilitado, garantindo o sigilo das informações..

Da mesma forma, Davi Monteiro Diniz (DINIZ, 1999) afirma que a criptografia consiste em uma escrita que se baseia em um conjunto de símbolos, cujos significados são conhecidos por poucos. Isto permite que se criem textos que serão incompreensíveis para os que não saibam o padrão de conversão necessário para sua leitura<sup>2</sup>.

Na “criptografia assimétrica”, também conhecida como de “chave pública”, o programa codificador serve-se de uma chave privada para *criptografar* e de uma chave pública para *descriptografar*.

O sistema de chaves funciona da seguinte forma: ao se cadastrar no sistema, o usuário recebe um par de chaves, uma privada e outra pública. A primeira deve ser mantida em sigilo absoluto. A segunda é tornada pública.

Por exemplo, ao expedir um documento eletrônico, insere-se a chave privada, que se incumbe de *criptografar* o documento, convertendo-o em símbolos e sinais inteligíveis, que somente poderão ser decifrados pelo destinatário com a utilização da chave pública.

Em vez de *criptografar* o documento, o usuário pode preferir inserir a sua assinatura digital. O destinatário, de posse da chave pública do remetente, pode conferir a autenticidade da assinatura digital, obtendo a certeza de sua procedência e integridade.

Além disso, a validade do documento eletrônico depende de uma certificação. É preciso que alguma entidade certifique a autenticidade da chave pública, atestando a identidade do seu titular.

O Governo Federal editou no dia 28 de Junho de 2001 a medida provisória 2.200 que instituiu a ICP-Brasil (Infra-Estrutura de Chaves Públicas Brasileiras), esta medida provisória disciplina a arquitetura da infra-estrutura de chaves públicas e o seu funcionamento com o comitê gestor e a cadeia de *autoridades certificadoras (AC)*.

A autoridade certificadora é um agente, público ou privado, que procura atender a necessidade de serviços confiáveis de terceiros no comércio eletrônico,

emitindo certificados digitais que atestam para o mesmo fato sobre o assunto de certificado<sup>1</sup>.

A legislação brasileira admite o documento eletrônico como meio de prova através do art. 332 do Código de Processo Civil: "Todos os meios legais, bem como os normalmente legítimos, ainda que não especificados neste código, são hábeis para provar a verdade dos fatos em que se funda ação ou a defesa".

Pelo princípio da liberdade de negócio, sempre que não houver exigência legal de alguma forma especial, os contratos estabelecidos e assinados digitalmente cumprem os requisitos para terem validade jurídica. Por isso, devem ser reconhecidos como qualquer outro documento particular assinado manualmente.

É comum nos livros de Direito, o emprego de vocábulos existência, validade e eficácia dos fatos jurídicos, como se tivessem a mesma denotação, até mesmo como se fossem sinônimos. Há uma corrente doutrinária (pertence a esta, Pontes de Miranda) que propõe se considerar distintos, dividindo-os em três planos:

#### a) Plano da existência

Para o fato ingressar no plano da existência, basta que sofra a incidência da norma jurídica. Assim será transportado para o mundo jurídico. Por exemplo, o casamento realizado perante a quem não tenha autoridade para casar, não configura fato jurídico, simplesmente, não existe. Já o simples nascimento com vida, implica a existência de um ato jurídico. Portanto pertencente ao plano da existência.

#### b) Plano da eficácia

O plano da eficácia é a parte do mundo jurídico onde os fatos jurídicos produzem seus efeitos, criando as situações jurídicas, direitos e deveres, pretensões e obrigações, ações e exceções, ou os extinguindo<sup>2</sup>.

#### c) Plano da validade

Entre existir e produzir efeitos, a questão de valer se interpõe. O plano de validade reside entre estes dois pólos.

O ato passa pelo plano da validade, onde o direito fará uma triagem e manterá somente aquilo que for perfeito.

1. ALBERTIN, Alberto Luiz. Comércio Eletrônico. Editora Atlas, São Paulo, 1999, P. 163.

<sup>2</sup>MELLO, Marcos Bernardes de. Teoria do Fato Jurídico (Plano da Existência). Editora Saraiva, São Paulo, 1999, P. 82.

O art. 82 do Código Civil, assim diz: "A validade do ato jurídico requer agente capaz (art. 145, N.I), objeto lícito e forma prescrita ou não defesa em lei (Arts. 129, 130 e 145).

Do texto legal, extraímos os pressupostos de validade do ato jurídico, como sendo: a) a capacidade do agente; b) o objeto lícito; c) a forma.

A doutrina, entretanto, distingue os pressupostos de validade dos elementos essenciais. Entre os elementos essenciais figura: a) a vontade humana; b) idoneidade do objeto; c) a forma<sup>1</sup>. Perceba que os pressupostos de validade se confundem com os elementos essenciais. Os pressupostos devem estar presentes no momento da formação do ato, e os elementos formam a estrutura do ato.

Assim, já temos condições de responder a seguinte questão: Qual o pressuposto de validade do ato jurídico que fora constituído por uma assinatura digital?

Sua validade dependerá de alguns requisitos atribuídos aos elementos essenciais do ato, como segue:

a) A vontade humana

A vontade humana pode, como foi demonstrado, ser manifestada por uma assinatura. Porém, a assinatura tradicional (autográfica) não é adequada aos documentos eletrônicos. Assim, a assinatura digital foi criada para solucionar o problema da identificação e da integridade.

b) A idoneidade do objeto

O objeto decorre da vontade negocial, pertence ao conteúdo do ato. E o requisito de validade é a licitude.

c) A forma

A forma diz respeito ao modo pelo qual a vontade humana se vinculará ao objeto. O Poder Legislativo está empenhado em criar regras para determinar como isto irá ocorrer. Baseado na lei modelo para comércio eletrônico da UNCITRAL (Comissão das Nações Unidas para o Direito Comercial Internacional) a vinculação será intermediada por uma Autoridade Certificadora.

Desde o início deste trabalho, procurou-se extrair dos fundamentos jurídicos, material que pudesse sustentar a validade jurídica da assinatura digital. Por conseguinte, foi demonstrado que é válida a assinatura digital para constituir um ato jurídico.

<sup>1</sup>RODRIGUES, Silvío. Direito Civil. Editora Saraiva, São Paulo, 1997, P. 82.

Em um futuro próximo, a aptidão natural do homem em buscar inovações, trará ao mundo concreto, novos instrumentos. Estes instrumentos serão mais eficazes, mais seguros, mais ágeis, enfim, mais modernos.

Caberá ao operador do direito, buscar a validade jurídica a estas inovações.

### **4.3 AS MUDANÇAS NAS LEGISLAÇÕES AMERICANA E EUROPEIA CONTRA OS "CRIMES VIRTUAIS", APÓS O DIA 11 DE SETEMBRO DE 2001**

#### **4.3.1 A RESTRIÇÃO DE DIREITOS FUNDAMENTAIS E O 11/09/2001**

O *Patriot Act*<sup>1</sup>, sem dúvida, foi a reação mais visível e imediata tomada pelo governo americano para combater os atos de terrorismo perpetrados no fatídico dia 11 de setembro de 2001. Assinada pelo presidente George Bush em 26 de outubro de 2001, após rápida e quase unânime aprovação do Senado americano<sup>2</sup>, a citada lei expande o nível de atuação de agências nacionais de segurança, como o *Federal Bureau of Intelligence - FBI*, bem como das internacionais de inteligência - *Central Intelligence Agency (CIA)*, conferindo-lhes poderes até então inéditos. Seu objetivo principal era o de prender os responsáveis pelo ataque; atualmente, visa evitar ocorrências de igual natureza no território norte-americano.

O texto integral, composto por 342 páginas, aborda mais de quinze estatutos, e, além de autorizar agentes federais a rastrear e interceptar comunicações de eventuais terroristas, esta lei traz as seguintes inovações, referidas por *Charles Doyle*: a) torna mais rigorosas leis federais contra lavagem de dinheiro; b) faz com que leis de imigração sejam mais exigentes; c) cria novos crimes federais; d) aumenta a pena de outros crimes anteriormente tipificados, e também, e) institui algumas mudanças de procedimento, principalmente para autores de crimes de terrorismo (DOYLE, 2002).

<sup>1</sup> Também conhecido como USAPA (*United States Patriot Act*, acrônimo para *Uniting and Strengthening America by providing Appropriate Tools Required to intercept and Obstruct Terrorism* e Lei Pública nº 107-56.

<sup>2</sup> A única exceção, de um universo de 88 senadores, foi a de Russell Feingold, um democrata do Estado do Wisconsin, que votou contra a lei. Uma das maiores críticas ao *Patriot Act* foi o fato de, apesar das polêmicas disposições contidas em seu bojo, não terem ocorrido discussões e debates mais aprofundados sobre o seu teor.

Pode-se visualizar, até mesmo pelo contexto desta lei e da atual política norte-americana, a existência de choque entre direitos fundamentais: de um lado, o direito fundamental à segurança nacional, inerente à comunidade americana, e, do outro, as liberdades civis dos cidadãos americanos. A discussão sobre o tema vem ocasionando um grande número de palestras, colóquios e conferências.

Para que possamos visualizar um choque de direitos, importante é a observação de *Canotilho* (CANOTILHO, 1999), o qual esclarece que *"haverá colisão ou conflito sempre que se deva entender que a Constituição protege simultaneamente dois valores ou bens em contradição concreta"* (ANDRADE, 1998). Ainda segundo o doutrinador português, *"uma colisão autêntica de direito fundamentais ocorre quando o exercício de um direito fundamental por parte do seu titular colide com o exercício do direito fundamental por parte de outro titular"* (CANOTILHO, 1999).

Evidente que a análise profunda das inúmeras seções do *Patriot Act* ensejaria trabalho mais minucioso e detalhado. Todavia, o que se busca é, partindo-se daquelas disposições que tem causado mais controvérsia, proceder a um teste de proporcionalidade, a fim de constatar, por fim, se algumas restrições de direitos fundamentais levadas a cabo pela citada lei ferem o núcleo essencial de direitos fundamentais da população norte-americana.

Logo, *"a questão do conflito de direitos ou de valores depende, pois, de um juízo de ponderação, no qual se procura, em face de situações, formas ou modos de exercício específicos (especiais) dos direitos, encontrar e justificar a solução mais conforme ao conjunto de valores constitucionais"* (ANDRADE, 1998).

#### **4.3.2 ANÁLISE DE TRÊS DISPOSIÇÕES DO PATRIOT ACT**

Passemos, agora, à análise de três pontos que se configuram como problemáticos na lei, quais sejam, a) a definição do crime de terrorismo doméstico; b) a detenção compulsória de terroristas suspeitos e os tribunais militares, e também, c) a pós-notificação dos mandados de busca e apreensão.

#### **4.3.3 DEFINIÇÃO DE TERRORISMO DOMÉSTICO**

Uma das mais polêmicas disposições do *Patriot Act* é aquela contida no parágrafo 802 do citado documento legal, o qual proclama a definição de novo crime, denominado de terrorismo doméstico, conceituado da seguinte forma:

Seção 802. Definição de Terrorismo Doméstico (...)

*omissis*

(...)

(5) o termo terrorismo doméstico significa atividades que (A) configurem atos perigosos à vida humana que são uma violação de leis criminais dos Estados Unidos ou de qualquer Estado; (B) que pareçam pretender (i) intimidar ou coagir uma

população civil; (ii) influenciar a política de um governo por intimidação ou coação; ou (iii) visem modificar a conduta de um governo utilizando-se de destruição em massa, assassinatos ou seqüestro; (...)

*omissis*"

Após leitura rápida constata-se que a definição do que seja terrorismo doméstico é ampla em demasia; as expressões utilizadas, tais como "*atos perigosos*", "*pareçam pretender*", "*influenciar a política de um governo por intimidação ou coação*", podem ser utilizadas ao bel-prazer das autoridades americanas. Se mal utilizadas, podem, inclusive, incriminar pessoas que simplesmente estão colocando em exercício seus direitos de expressão, de reunião, de dissenso e de protesto.

Tal atitude atingiria, certamente, condutas que estariam protegidas pela 1ª emenda da Constituição dos Estados Unidos, que concede, dentre outros direitos, a liberdade de expressão, o de reunião pacífica e o de peticionar o governo para reparação de injustiças.

Destarte, na mesma linha de pensamento referente a evolução jurisprudencial americana ocorrida com as "*loitering laws*" (leis de vadiagem), os verbos nucleares dos tipos penais deveriam ser mais detalhados, a fim de que o choque de direitos existentes no caso em tela não fulminasse o núcleo duro de um ou mais direitos fundamentais.

Outras disposições que, em princípio, ferem a 1ª emenda: seção 215 do Patriot Act; decreto do procurador-geral dos Estados Unidos que aumenta a vigilância de organizações políticas e religiosas; decreto do procurador-geral dos Estados Unidos minando requerimentos e petições protegidos pela Lei de Liberdade de Informação (*Freedom of Information Act*).

#### **4.3.4 DETENÇÃO COMPULSÓRIA DE TERRORISTAS SUSPEITOS E OS TRIBUNAIS MILITARES**

A frase, cuja autoria é de *Georges Clemenceau*, chefe de estado Francês na 1ª Guerra Mundial e um dos formuladores do Tratado de Versalhes: "*A justiça militar está para a justiça assim como a música militar está para a música*".

O *Patriot Act* concedeu uma gama de poderes inédita ao Procurador-geral dos Estados Unidos, atualmente, *John Aschcroft*. Uma delas refere-se a prerrogativa de deter, de modo compulsório, pessoas suspeitas de serem terroristas. Para colocar tais suspeitos sob custódia, o procurador-geral tem a capacidade de certificar/atestar que um estrangeiro esteja descrito em uma das seções abaixo citadas, ou esteja empenhado em qualquer outra atividade que ponha em perigo a segurança nacional dos Estados Unidos.

A seção modificada é a de nº 412, da Lei de Imigração e Nacionalidade, que passa a vigor com a seguinte inserção:

"Seção 412. Detenção Compulsória de Suspeitos Terroristas; *Habeas Corpus*; Revisão Judicial

(...)

‘Seção 236A. (a) Detenção de terroristas estrangeiros. –

‘(1) Custódia. – O Procurador-Geral pode colocar sob custódia qualquer estrangeiro que esteja certificado sob as disposições do parágrafo (3).

(...)

‘(3) Certificação. – O procurador-geral pode certificar/atestar um estrangeiro sob este parágrafo se o mesmo tenha razoáveis fundamentos para acreditar que o estrangeiro -

(a) esteja descrito na seção 212(a)(3)(A)(i), 212(a)(3)(A)(iii), 212(a)(3)(B), 237(a)(4)(A)(i), 237(a)(4)(A)(iii), or 237(a)(4)(B); ou

(b) está empenhado em qualquer outra atividade que ponha em perigo a segurança nacional dos Estados Unidos.

Juntamente com a detenção compulsória de suspeitos terroristas, a questão da implantação de tribunais militares é outro fato que acende discussões sobre a política norte-americana. Tais tribunais aplicam-se apenas para não-americanos.

A relação entre a seção 412 e a ordem militar do presidente Bush, que instituiu tais tribunais, como diz *Charles Doyle*, é incerta. Essa ordem, de 13 de novembro de 2001, permite o Secretário de Defesa deter estrangeiros suspeitos como terroristas, nos Estados Unidos ou em qualquer lugar, sem condições ou limitações expressas, exceto no que se refere a comida, água, abrigo, roupas, tratamento médico, e exercício religioso (DOYLE, 2002). Apesar de duvidosa a relação entre os dispositivos, ambos ferem a 5ª emenda.

A quinta emenda à constituição americana diz que:

*“... ninguém será obrigado a responder por crime capital, ou por outro crime infamante, a não ser perante denúncia ou acusação de um grande júri (...) nem será obrigado a servir de testemunha contra si próprio em qualquer processo criminal, nem ser privado da vida liberdade ou propriedade sem um devido processo legal (...)”.* (ALVAREZ, 2001).

Logo, nenhuma pessoa pode ter sua liberdade tolhida sem um devido processo legal, não importa o tipo de crime que tenha praticado. Nesse caso, a igualdade formal perante a lei deve ser mantida a todo custo, uma vez que, apesar de nacionais e estrangeiros pertencerem a categorias diferentes, todos estão abarcados pela garantia fundamental do devido processo legal.

O que se pretende com o exposto é a não-criação, na esfera pública, de uma *Lynch Law*<sup>1</sup>, o que, certamente, fulminaria com o devido processo legal, levando, junto com ele, todos os demais princípios basilares do Estado Democrático de Direito.

#### 4.3.5 PÓS-NOTIFICAÇÃO DOS MANDADOS DE BUSCA E APREENSÃO

Outra disposição que tem causado controvérsia é aquela referente aos mandados de busca e apreensão, localizada na seção 213 do *Patriot Act*, que acrescenta nova disposição ao título 18, seção 3103a do Código dos Estados Unidos, *verbis*:

"Seção 213. Autoridade para retardar a notificação da execução de um mandado.

*omissis (...)*

(2) acrescenta-se no fim o seguinte:

(b) Dilação de Prazo – Com respeito a emissão de qualquer mandado ou ordem judicial sob essa seção, ou qualquer outro preceito legal, a procurar e confiscar qualquer propriedade ou material que constitua prova de ofensa criminal que viole as leis dos Estados Unidos, qualquer notificação requerida, ou que possa ser requerida, pode ser retardada se -

(1) a corte julgar que há causa razoável de que, procedendo à imediata notificação da execução do mandado, possa ocorrer um resultado adverso (...);

(...)

*omissis*

(3) o mandado proporciona para o fornecimento de tal notificação um período razoável para sua execução, cujo período pode, após tal ato, ser estendido pela corte se for demonstrado um bom motivo”.

<sup>1</sup>Termo que significa criminosos pegos em flagrante.

Os mandados de busca e apreensão, na expressão americana *sneak and peek warrants* são protegidos pela 4ª emenda à carta constitucional daquele país, que também garante o direito à privacidade. Segundo a emenda, o povo americano tem direito "*à inviolabilidade de suas pessoas, casas, documentos e haveres, contra buscas e apreensões arbitrárias (...) e nenhum mandado será emitido senão com base em indício de culpabilidade, confirmado por juramento ou declaração solene, e particularmente com a descrição do local de busca e das pessoas ou coisas a serem apreendidas*" (ALVAREZ, 2001).

Mais uma vez, a disposição restritiva de direito possui expressões dúbias e "abertas" em demasia. O lapso temporal para a pós-notificação não é determinado; assim, podem os mandados de busca e apreensão ser cumpridos e a respectiva notificação ser procrastinada *ad eternum*. Procedendo deste modo, as pessoas podem ter suas casas invadidas, e ter seus bens confiscados, sem saberem o objeto do mandado.

No caso da pós-notificação, nas palavras de *Nancy Talanian*, membro do Comitê de Defesa da *Bill of Rights* "*... uma pessoa cuja casa está para ser inspecionada não pode ver o mandado para certificar-se que o endereço é correto ou que o agente adere estritamente à descrição do que deve ser procurado*" (TALANIAN, 2003).

É tão polêmica a disposição acima exposta que, em 23 de julho de 2003, a Câmara dos Deputados aprovou uma emenda tanto republicana como democrata, oferecida pelos deputados *C. L. "Butch" Otter, Dennis J. Kucinich e Ron Paul*, dos Estados americanos de Idaho, Ohio e Texas, impedindo a implementação das buscas e apreensões efetuadas sob a égide do *Patriot Act*. A passagem desta emenda marca a primeira vez em que tanto deputados republicanos como democratas agiram para revogar qualquer provisão da lei. Importante notar, todavia, que tal emenda começará a vigor apenas após a aprovação do Senado e do presidente *George Bush*.

Outras disposições do *Patriot Act* que eventualmente ferem a 4ª emenda: seção nº 213, que concede autoridade para compartilhar informações de investigações criminais entre agências, inclusive estrangeiras; seções números 206, 215, 218 e 411.

Após a breve análise feita acerca das disposições do *Patriot Act*, importante sublinhar que a mesma apóia-se no art. 6º, nº 2 da Constituição Americana, baseada na supremacia hierárquica daquela lei perante todas as outras, *verbis*,

Esta Constituição e as leis dos Estados Unidos feitas em sua conformidade, e todos os tratados celebrados ou por celebrar sob a autoridade dos Estados Unidos, constituirão a lei suprema da nação; e os juízes de todos os Estados a ela estarão sujeitos, ficando sem efeito qualquer disposição contrária na Constituição ou lei de quaisquer dos Estados (ALVAREZ, 2001).

Comunga-se, também, do posicionamento de Cançado Trindade a respeito das restrições de direitos fundamentais:

*“...as eventuais limitações ou restrições permissíveis ao exercício de direitos consagrados, ademais de deverem ser interpretadas restritivamente e em favor deste últimos, deverão necessariamente ser previstas em lei (...) Qualquer limitação deve ser justificada, e o ônus de tal justificação recai sobre o estado. (...) As limitações, além disso, não de ser aplicadas no interesse geral da coletividade, coadunando-se com os requisitos de uma "sociedade democrática", e respeitando o princípio da proporcionalidade; as limitações não podem ser aplicadas de modo arbitrário ou discriminatório, devendo sujeitar-se a controle por órgãos independentes (com a previsão de recursos para os casos de abusos), e ser compatíveis com o objeto e o propósito dos tratados sobre proteção dos direitos humanos” (TRINDADE, 1991).*

Sobre perigo de leis que atinjam direitos individuais referiu Sérgio Moccia (MOCCIA, 1999):

*“O risco, portanto, concerne sobretudo às garantias individuais que, como limites postos para a defesa do homem contra os abusos estatais, representam a expressão mais significativa daquele longo e atormentado processo evolutivo que caracterizou o desenvolvimento da civilização jurídica contemporânea. Não é admissível, portanto, que numa estrutura ordenamental de democracia avançada se adotem, ainda que com a finalidade de remediar gravíssimas perturbações do complexo sócio estatal, remédios normativos e práticas jurisprudenciais que acabem por fazer com que a estrutura ordenamental deslize na direção de preocupantes formas de arbítrio que têm sempre caracterizado os momentos mais difíceis para os direitos do indivíduo”.*

Além disso, a atual "paisagem jurídica" vivenciada pelos norte-americanos, em que se pode vislumbrar restrição em demasia a certos direitos fundamentais, sob a alegação de segurança nacional, possui um precedente em contrário: é o que constatou *Marcelo Caetano* quando do episódio *Watergate*, que gerou "a crise constitucional de 1974", a afirmação do predomínio dos valores da liberdade e da democracia sobre o da segurança nacional (CAETANO, 1977).

E é neste sentido que a sociedade civil deve estar alerta quanto à restrição de direitos fundamentais, a qual poderá ser acirrada e aumentada, se o atual nível de tensões se mantiver. Neste panorama, o princípio da proporcionalidade se materializa como peça chave, instrumento delineador dos limites de leis restritivas de direitos fundamentais.

Como disse o saudoso diplomata brasileiro, Sérgio Vieira de Mello, em discurso proferido por ocasião do *Third Committee of the UN General Assembly*, em 04 de novembro de 2002:

*“Nenhuma causa pode justificar o terrorismo (...). tal fenômeno deve ser universalmente e inequivocadamente condenado. O combate exitoso contra o terrorismo, contudo, requer mais do que um rigoroso reforço das disposições legais,*

*mesmo sendo estas vitais. Também requer uma aproximação a longo prazo, e mais holística, assim como a determinação de assegurar de que todos os direitos são realmente usufruíveis por todos: particularmente quando é um dos objetivos dos terroristas forçar-nos a negar tais direitos”* (MELLO, 2002).

Seguindo as palavras do renomado diplomata brasileiro, parece que os legisladores americanos, ao contrário de seu Poder Executivo, após o choque dos acontecimentos catastróficos de 11 de setembro, estão novamente legiferando de modo a proteger os cidadãos americanos e imigrantes inocentes de lesões mortais a direitos fundamentais assegurados pela carta magna daquela nação e por tratados internacionais.

#### **4.3.6 A CONVENÇÃO DO CONSELHO EUROPEU SOBRE O CRIME ELETRÔNICO**

Em 23 de novembro de 2001, foi firmada na cidade de Budapeste, Hungria, a Convenção do Conselho Europeu sobre o *crime eletrônico*, sem a participação do Brasil.

De acordo com o Secretário-Geral do Ministério das Relações Exteriores, Samuel Pinheiro Guimarães, o país só pode se tornar signatário do tratado se for convidado pelo Comitê de Ministros do Conselho Europeu.

A resposta foi dada ao requerimento do senador Eduardo Azeredo (PSDB-MG), que considera o instrumento peça fundamental na cooperação internacional para o combate aos crimes cibernéticos.

O acordo entrou em vigor no dia 1 de julho de 2004, depois que cinco países o ratificaram, sendo três, integrantes do Conselho Europeu, composto por 46 membros. Até o dia 14 de março, 19 países haviam ratificados o tratado. Os Estados Unidos são o único país de fora do Conselho Europeu que o ratificou, em 29 de setembro de 2006.

Samuel Pinheiro Guimarães lembra que o Brasil, se obrigado pelo Congresso Nacional, a aderir ao tratado, terá de legislar sobre os crimes tipificados na Convenção. Disse ainda que o Ministério da Justiça, através do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional; o Gabinete de Segurança Institucional da Presidência da República; Departamento de Polícia Federal; o Ministério de Ciência e Tecnologia, e o Ministério das Relações Exteriores, analisam a Convenção à luz do ordenamento jurídico brasileiro.

Para tanto, também estão sendo avaliados os resultados de seminários e congressos realizados no âmbito da *Organização dos Estados Americanos (OEA)*, em foros como o *Comitê Interamericano contra o Terrorismo (CICTE)*.

Pinheiro Guimarães diz ainda que, segundo estudo preliminar realizado pelo Grupo de *Segurança da Informação - GSI*, as diferentes normas brasileiras contemplariam uma pequena parte da Convenção.

Por outro lado, o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, do Ministério da Justiça, estaria levantando os aspectos da

convenção sobre os quais proporia reservas, como na questão da interceptação de comunicações.

Na avaliação do *Itamaraty*, Ministério das Relações Exteriores – MRE, o acordo é de difícil aplicabilidade, embora seja o único tratado internacional de combate aos crimes cibernéticos. No Congresso tramitam quatro projetos de lei que tratam do assunto.

## **4.4 A LEGISLAÇÃO BRASILEIRA SOBRE OS CRIMES DE INFORMÁTICA**

Antes de se abordar sobre os “crimes de informática”, se faz necessário comentar sobre a origem do “crime organizado”, suas características e sua evolução ao longo da história da humanidade e, concomitantemente, os aspectos jurídicos que envolvem esta questão.

### **4.4.1 CONCEITO E CARACTERÍSTICAS DO CRIME ORGANIZADO**

Não existe um consenso sobre a conceituação de crime organizado; surge aí, já, a primeira dificuldade no trato da questão. A Lei n.º 9.034/95 dispõe sobre a "utilização de meios operacionais para a prevenção e repressão de ações praticadas por organizações criminosas". Porém, não estabelece o que seja crime organizado; daí, juridicamente falando, não determina do que se trata. O artigo 1º da Lei, em sua redação original, mencionava "crime resultante de ações de quadrilha ou bando", surgindo daí o entendimento errôneo de crime organizado como crimes que resultam de ações cometidas por quadrilha ou bando.

Com a nova redação dada pela Lei n.º 10.217, de 11 de abril de 2001, o artigo 1º da Lei 9.034 passou a definir e regular os "meios de prova e procedimentos investigatórios que versem sobre ilícitos decorrentes de ações praticadas por quadrilha ou bando ou organizações ou associações criminosas de qualquer tipo". Com essa redação, ficou determinado o alcance da lei sobre os ilícitos decorrentes de: (a) quadrilha ou bando; (b) organização criminosa; e, (c) associação criminosa.

Embora criticada por alguns, a ausência de conceituação também tem seus defensores que acreditam, desta forma, não estabelecer limitação para a abrangência que a lei pode estabelecer, nem tornar por demais elástica a conceituação.

No entanto, podemos, então, utilizar definições oferecidas por inúmeros estudiosos do assunto, para, assim, tentar compreender melhor o que é crime organizado.

Segundo *Winfried Hassemer*, a criminalidade organizada

*não é apenas uma organização bem feita, não é somente uma organização internacional, mas é, em última análise, a corrupção da legislatura, da*

*Magistratura, do Ministério Público, da polícia, ou seja, a paralisação estatal no combate à criminalidade. [...] é uma criminalidade difusa que se caracteriza pela ausência de vítimas individuais, pela pouca visibilidade dos danos causados bem como por um novo modus operandi (profissionalidade, divisão de tarefas, participação de 'gente insuspeita', métodos sofisticados etc.). Ainda mais preocupante, para muitos, é fruto de uma escolha individual e integra certas culturas.*

Para Alberto Silva Franco, o crime organizado "*possui uma textura diversa: tem caráter transnacional na medida em que não respeita as fronteiras de cada país e apresenta características assemelhadas em várias nações*". Detém, também, um grande poder baseado em uma estratégia global e em uma estrutura organizativa capaz de utilizar as fraquezas estruturais do sistema penal. Além disso, "*provoca danosidade social de alto vulto; tem grande força de expansão, compreendendo uma gama de condutas infracionais sem vítimas ou com vítimas difusas; dispõe de meios instrumentais de moderna tecnologia; apresenta um intrincado esquema de conexões com outros grupos delinquentiais e uma rede subterrânea de ligações com os quadros oficiais da vida social, econômica e política da comunidade; origina atos de extrema violência; exibe um poder de corrupção de difícil visibilidade; urde mil disfarces e simulações e, em resumo, é capaz de inerciar ou fragilizar os poderes do próprio Estado*".

Dessa forma, vimos que a construção do conceito do que é crime organizado não é fácil, e diante das opiniões citadas, é possível afirmar que a definição de crime organizado pode variar de acordo com o ponto de vista daquele que o estuda. São mantidas, contudo, as principais características e a identidade quanto aos aspectos criminológicos dessas organizações.

Aspectos econômicos e institucionais devem ser levados em consideração para tentar construir um conceito de crime organizado. Inicialmente, é de vital importância tentar descobrir quais são as características – que estão no âmbito econômico e institucional – que permitem que um grupo de indivíduos que pratica atos ilícitos possa ser classificado como organização criminosa. Dentre essas características, devem ser observados o *modus operandi* dos atores na operacionalização dos atos criminosos, as estruturas de sustentação e ramificações do grupo, as divisões de funções no interior do grupo e o seu tempo de existência.

As características do crime organizado são constituídas por aspectos que lhe permitem atuar com grande mobilidade, alto poder de ação e intimidação, além de lograr resultados impressionantes em termos financeiros.

A Academia Nacional de Polícia Federal do Brasil enumera 10 características do crime organizado:

- 1) Planejamento empresarial;
- 2) Antijuridicidade;
- 3) Diversificação de área de atuação;
- 4) Estabilidade dos seus integrantes;

- 5) Cadeia de comando;
- 6) Pluralidade de agentes;
- 7) Compartimentação;
- 8) Códigos de honra;
- 9) Controle territorial;
- 10) Fins lucrativos.

Já Mingardi aponta quinze características do crime organizado. São elas:

- 1) Práticas de atividades ilícitas;
- 2) Atividade clandestina;
- 3) Hierarquia organizacional;
- 4) Previsão de lucros;
- 5) Divisão do trabalho;
- 6) Uso da violência;
- 7) Simbiose com o Estado;
- 8) Mercadorias ilícitas;
- 9) Planejamento empresarial;
- 10) Uso da intimidação;
- 11) Venda de serviços ilícitos;
- 12) Relações clientelistas;
- 13) Presença da lei do silêncio;
- 14) Monopólio da violência;
- 15) Controle territorial.

Cabe serem citadas, ainda, as seguintes características:

- 1) Participação de agentes estatais, em função do alto poder de corrupção do crime organizado;
- 2) Criminalidade difusa, decorrente da ausência de vítimas diretas, individuais;

3) Pouca visibilidade dos danos que, embora muito elevados, permanecem invisíveis durante algum tempo;

4) Alto grau de operacionalidade, já que os grupos são formados por pessoas com excelente qualificação em diversas áreas onde precisam atuar, bem remuneradas e que quase nunca recebem informações sobre o restante da organização, evitando, assim, o vazamento de informações;

5) Mutação constante, que dificulta o trabalho de investigação por causa da dificuldade em mapear as ações do grupo.

#### **4.4.2 ESTRUTURA E ATUAÇÃO DO CRIME ORGANIZADO**

Para que qualquer crime logre êxito, é necessário que haja um mínimo de organização, pois não há como fazer qualquer coisa sem uma organização mínima.

Então, partindo-se desta premissa, deveremos entender por Crime Organizado as "*grandes empresas do crime*", organizações altamente sofisticadas, com utilização de tecnologia de ponta e profissionais qualificados, com infiltrações em diversos ramos de atividades comerciais e governamentais, inclusive.

As estruturas do crime organizado são o poder institucional (Estado) e o econômico. O *modus operandi* das organizações precisam dos poderes citados para sobreviver, e por conseqüência, ser lucrativo. Além disso, as organizações criminosas podem dominar uma parcela do mercado econômico ou um território geográfico – onde nestes exercem os seus poderes político e econômico.

Dessa forma, comprovamos que a relação entre Estado e crime organizado está presente. Portanto, uma das características do crime organizado é buscar apoio para a sua atuação no âmbito institucional – instituições do Estado. Um outro ponto importante é que as ações do crime organizado têm como engrenagem o sistema capitalista. Por meio dos benefícios do capitalismo, como, por exemplo, a interação dos mercados financeiros, é possível tornar as atividades das organizações criminosas bastante lucrativas. A interação dos mercados financeiros proporciona, é importante ressaltar, a lavagem de dinheiro.

As divisões de funções e a presença da hierarquia são outras características apontadas. Neste sentido, as organizações criminosas têm o seu funcionamento parecido com uma empresa capitalista, onde funções são estabelecidas para cada um de seus integrantes – funções estas, obedecendo ao princípio da hierarquia. A atuação à margem dos poderes do Estado, através de atos que contrariam a ordem jurídica, é uma característica apontada. As atividades do crime organizado se contradizem com o ordenamento jurídico oficial. Neste sentido, apesar da contradição, temos, conforme anteriormente citado, que as atividades das organizações criminosas precisam dos atores estatais para serem lucrativas e terem uma vida durável.

Além disso, as organizações criminosas devem ser analisadas também por meio de suas dimensões de atuação. Ou seja: existem organizações que atuam apenas em nível local, sem conexão com outros grupos no âmbito nacional ou internacional. Por outro lado, existem organizações que são nacionais ou

transnacionais, as quais criam uma cadeia de interação nas esferas local, nacional e internacional. Os poderes econômico e político devem ser analisados também por meio das dimensões.

Sendo assim, temos que o crime organizado dispõe de uma estrutura organizacional bastante complexa e hierarquizada, possuindo divisão sistematizada de funções, infiltrações em órgãos dos poderes administrativo, legislativo e judiciário, sistemas informatizados e interligados transnacionalmente, tecnologia de ponta e mão de obra altamente qualificada, dentre muitos outros atributos.

As atividades do crime organizado vão desde o tráfico de drogas, tráfico de armas, tráfico de seres humanos, a fraudes fiscais, lavagem de dinheiro e a interferência em licitações públicas, dentre tantas outras esferas de ação.

Outros campos de atuação das associações criminosas são: furto e roubo de veículos, roubo de cargas, o jogo do bicho, falsificação de medicamentos, contrabando, fraudes financeiras, corrupção, sonegação fiscal e crimes contra a ordem econômica, roubo a bancos, seqüestros, grupos de extermínio.

#### **4.4.3 LEGISLAÇÃO APLICÁVEL AO CRIME ORGANIZADO**

A Lei nº. 9.034, de 03 de março de 1995, conhecida como a "Lei do Crime Organizado", foi editada tendo como escopo disciplinar, segundo a sua ementa, *"a utilização de meios operacionais para a prevenção e repressão de ações praticadas por organizações criminosas"*.

A referida Lei, que está disposta em três Capítulos (CAPÍTULO I - Da Definição de Ação Praticada por Organizações Criminosas e dos Meios Operacionais de Investigação e Prova; CAPÍTULO II - Da Preservação do Sigilo Constitucional; e CAPÍTULO III - Das Disposições Gerais) e que contém em 13 artigos, vem tentar disciplinar eficazmente o crime organizado.

Demonstra-se, com a referida Lei, a preocupação político-criminal com a repressão à macro criminalidade, tendo em mira propiciar mecanismo mais eficaz no combate aos delitos resultantes de organizações criminosas, mas se deixa transparecer, com a redação do art. 1º, que a proposição legislativa não se volta apenas para a facilitação da ação policial na investigação de delitos provenientes de organizações criminosas, mas também para regular o procedimento a ser adotado nesses casos.

Registre-se, também, que ao legislador infraconstitucional não restaram alternativas maiores, pois os mecanismos disponíveis à investigação desses crimes, em rigor, não diferem daqueles admissíveis quanto aos ilícitos menores, haja vista que a Constituição da República (C.F./88), no impor dos direitos e garantias individuais e coletivos, os limites ao direito de punir, não fez qualquer ressalva quanto à amplitude de ação na repressão do crime organizado.

#### **4.4.4 QUESTÕES SOBRE O CRIME ORGANIZADO**

##### **4.4.4.1 QUAL A POLÍTICA PÚBLICA MAIS ADEQUADA PARA SE CONTROLAR ESTE TIPO DE CRIMINALIDADE?**

Como é de senso comum, a infiltração das organizações criminosas na máquina estatal compromete a finalidade do Estado, que é servir à sociedade, promovendo o bem comum. Além disso, incentiva a utilização de práticas ilícitas que violam o princípio do interesse público. Os custos políticos e sociais do crime organizado são, portanto, terríveis para qualquer país e, em especial, para aqueles em desenvolvimento, por serem mais vulneráveis ao poderio econômico e financeiro das organizações criminosas, sejam elas locais ou transnacionais. A prática habitual e profunda da corrupção e a conseqüente penetração do crime organizado no processo político esmagam as chances de elaboração de novas leis necessárias a desenvolvimento das bases para uma economia de mercado livre e democrática.

Diante dessa realidade, o Estado, através dos atores públicos, passou a ser parceiro no desenvolvimento das atividades ilícitas, perdendo a sua transparência, e acima de tudo, passando a funcionar guiado pelos interesses dos senhores do crime, deixando de lado o agir em prol dos interesses da sociedade.

Torna-se necessário, como tentativa de combater e controlar o crime organizado, o Estado reavaliar seu papel, sua função, a começar por readquirir a transparência em suas ações, que devem ser voltadas a servir à sociedade, ao bem comum, tentando se esquivar de participar da estrutura do crime organizado, através da elaboração de leis que se demonstrem mais eficazes que a atual Lei do Crime Organizado, e através de ações e políticas públicas que visem cada vez mais retirar os agentes públicos dessa teia, e fazer com que o Estado não mais participe do crime organizado, sendo também mais afetivo através das punições dispensadas aos autores de crimes organizados e através de uma atuação policial também mais efetiva.

Sintetizando, cremos ser possível tentar controlar o crime organizado através de uma maior fiscalização estatal, bem como através da reavaliação pelo Estado, através de seus agentes, do seu verdadeiro papel dentro da sociedade, que é visar ao bem comum, servir à sociedade, e não contribuir para sua degradação, participando, sustentando, estruturando e dando suporte ao crime organizado.

Contudo, cremos que essa luta não poderá ser vencida apenas pela ação das instituições policiais e estatais. É uma luta que deve envolver toda a sociedade, mesmo porque com fatos, situações e comportamentos desviantes aceitos no âmbito das camadas sociais mais elevadas, sob o escudo da proclamada moral dos negócios, as práticas delituosas vão contaminando todas as camadas sociais, mesmo as mais humildes, e acabam por ser institucionalizadas como crimes.

#### **4.4.4.2 COMO SE PREVENIR AO CRIME ORGANIZADO, À LUZ DA CRIMINOLOGIA MODERNA?**

Falar em prevenção diante do quadro em que nos encontramos torna-se complicado. O mais correto, diante da atual situação, é falarmos primeiramente em tentar combater e controlar o crime organizado.

Temos que o combate às atividades criminosas torna-se cada vez mais difícil, pois a sofisticação e o aparelhamento das organizações criminosas alcançam níveis tão elevados, que os órgãos de segurança pública, especialmente as polícias brasileiras, estão longe de alcançar. No entanto, apesar de não se poder deter a globalização e o avanço tecnológico, e de ser difícil impedir o acesso desses agentes criminosos a tais avanços, a Criminologia moderna busca as causas da delinquência, sugere modelos para impedir a conduta delituosa e, por fim, evitar a reincidência.

#### **4.4.5 CRIMES DE INFORMÁTICA E LEGISLAÇÃO PENAL BRASILEIRA**

##### **4.4.5.1 O DIREITO PENAL DA INFORMÁTICA - A REGULAMENTAÇÃO PENAL DA INFORMÁTICA**

O que denominamos de Direito da Informática seria o conjunto de normas destinadas a regular a prevenção, a repressão e a punição relativamente aos fatos que atentem contra o uso, exploração, segurança, transmissão e sigilo de dados armazenados e de sistemas manipulados por estes equipamentos - os computadores.

Para se ter uma idéia de quanto é importante que exista a regulação penal da informática, na Suíça as seguradoras perdem anualmente cerca de 6 milhões de francos, somente através de crimes de informática. Em 1998, na França, 700 milhões de francos foram perdidos em delitos de informática, valor este superior aos prejuízos com assaltos bancários no mesmo ano.

Tais perdas não se apuram apenas em países desenvolvidos. Os mesmos delitos são perpetrados no Brasil.

Por outra, já é uma instituição mundial a inoculação, em todos os tipos de computadores, por vírus, principalmente nos sistemas bancários, que geram incalculáveis prejuízos e, no Brasil, mais especificamente, estes destruidores de dados, arquivos e informações, vicejam impunes, por falta de legislação própria.

##### **4.4.5.2 NECESSIDADE DE IMPLANTAÇÃO DE LEGISLAÇÃO ESPECIAL**

Para buscar uma fórmula jurídico-penal, é necessário implantar uma legislação para coibir os delitos de informática, cujos autores se utilizam de extremo conhecimento técnico para praticarem atos lesivos ao patrimônio de pessoas físicas e jurídicas.

No Brasil existem algumas tímidas iniciativas através de projetos de lei que ora tramitam no Senado e na Câmara Federal. Todavia, não atendem os anseios dos usuários de computadores, que esperam uma legislação forte e efetiva à prevenção, repressão e punição dos atos lesivos praticados por delinqüentes de informática.

Muitas condutas delitivas de natureza informatizada são difíceis de ser tipificadas, e até de serem criminalizadas, seja ao prisma das normas existentes ou vislumbrando-se um novo direito. Assim, muitas propostas de criminalização são deficientes ou carecedoras de conhecimento da própria informática, ou ainda, são propostas de normas que se sobrepõem às existentes.

Os crimes de Informática devem ser classificados adequadamente para que o legislador pátrio possa elaborar normas eficientes, e, se necessário, indicar as normas vigentes que podem ser aplicadas.

Além da classificação, é necessário que se busque individualizar as espécies de delitos de informática, assim instrumentalizaria o aprofundamento do objeto jurídico a ser protegido, bem como a aplicação da norma adequada, e a pena adequada ao delito.

O Direito Penal da Informática deve ser desenvolvido com extrema rapidez e segurança, de modo a serem sistematizadas normas que atinjam os crimes empiricamente tipificados, que são cometidos com o emprego de computadores e sistemas, desenvolvendo proteção à privacidade, instrumentalização da produção de provas, inclusive reciclando os conceitos de provas, principalmente aquelas provas técnicas.

Já que existe, no mundo dos fatos, sobejos elementos indicadores de crimes de informática, devem o legislativo nacional redigir o Direito Penal Brasileiro de Informática.

Em relação ao bem jurídico protegido, o Direito Penal de Informática é concebido para proteger os sistemas de computadores e das comunicações, além da informação.

A preocupação do Direito penal de Informática com os sistemas de computadores e de comunicação deve-se, fundamentalmente, à proteção dos seus componentes imateriais ou intangíveis, ou seja, o software e dados, e os dados que ainda não contam com a mesma proteção do outro componente, o hardware.

O Direito ainda caminha lentamente para a implementação de um sistema jurídico que proteja os bens incorpóreos e imateriais tão bem como os bens materiais.

O computador é usado para a prática de um delito, do mesmo modo que outros artefatos. Discute-se, então, a criminalização de tais meios de cometimento, visto que certos crimes se tornam quase impossíveis de tipificar, provar e processar quando praticados no ambiente informático.

Discutem-se, agora, a proteção a bens jurídicos redefinidos em sua importância, como o dado, a informação e as redes de computadores.

### **4.4.5.3 LEGISLAÇÃO BRASILEIRA**

#### **4.4.5.3.1 O DIREITO PENAL DE INFORMÁTICA VIGENTE NO BRASIL**

O Direito Penal de Informática no Brasil caracteriza-se pela sua absoluta pobreza. A Parte Especial do Código Penal de 1940 (CP/1940) e as normas incriminadoras são de um tempo em que sequer existia o computador, de modo que as normas vigentes somente podem ser aplicadas aos crimes de informática de forma incidental a tais hipóteses.

#### **4.4.5.3.2 A LEI DOS DIREITOS AUTORAIS**

Uma questão controvertida aos doutrinadores e estudiosos do direito no campo dos direitos autorais é a proteção legal a todo e qualquer tipo de criação intelectual veiculada através da rede mundial de computadores - *Internet*.

A facilidade em disponibilizar, pela Internet, conteúdos, informações, bases de dados ou qualquer outro tipo de criação intelectual se entrelaça, igualmente, com a simplicidade na produção e edição de cópias de tais criações, em detrimento ao direito de seus autores.

A lei 9.610/98 veio dar proteção legal a toda e qualquer criação intelectual, ensejando indenizações aos seus autores e titulares, seja no campo moral, seja no campo patrimonial, independentemente do meio que a suporta (eletrônico ou tangível), quando dispõe, em seu artigo 7º, inciso XIII, que *"são obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como as coletâneas ou compilações, antologias, enciclopédias, dicionários, bases de dados e outras obras, que, por sua seleção, organização ou disposição de conteúdo, constituem uma criação intelectual."*

Assim, o meio eletrônico está inserido na proteção legal vigente, sendo perfeitamente cabível a reivindicação dos direitos autorais violados através desse meio.

A proteção conferida pela legislação vigente abrange aquelas obras explicitamente referidas no texto do artigo 7º, da Lei 9.610/98, porém a estas não se limita, podendo ser ampliada a qualquer tipo de criação de espírito humano, que constitua uma obra intelectual.

#### **4.4.5.3.3 O CÓDIGO PENAL E O DIREITO DE INFORMÁTICA**

O Código Penal Brasileiro tutela a matéria relacionada ao direito do autor no Título III, que trata "Dos Crimes contra a Propriedade Imaterial", mais especificamente no Capítulo I, que diz respeito aos "crimes contra a propriedade intelectual", a saber:

Violação de direito autoral:

*"Art. 184 – Violar direito autoral:*

*Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.*

*1º Se a violação consistir em reprodução, por qualquer meio, com intuito de lucro, de obra intelectual, no todo ou, em parte, sem autorização expressa do autor ou de quem o represente, ou consistir na reprodução de fonograma ou videofonograma, sem a autorização do produtor ou de quem o represente:*

*Pena - reclusão, de 1(um) a 4(quatro) anos, e multa de Cr\$ 10.000,00 (dez mil cruzeiros) a Cr\$ 50.000,00(cinquenta mil cruzeiros).*

*2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, aluga, introduz no País, adquire, oculta, empresta, troca ou tem em propósito, com intuito de lucro, original ou cópia de obra intelectual, fonograma ou videofonograma, produzidos ou reproduzidos com violação de direito autoral.*

*3º Em caso de condenação, ao prolatar a sentença, o juiz determinará a destruição da produção ou reprodução criminosa."*

No que se refere a estes dispositivos, há muitas críticas a respeito, entendendo que não existe uma previsão específica de cada tipo penal, deixando o crime de violação ao direito autoral bastante genérico (diz-se que é uma norma penal em branco). Desta forma, o que se tem de fazer é dar uma interpretação extensiva a estes artigos, tentando, com isso, aplicar a sanção penal disposta.

#### **4.4.5.3.4 A LEI DE SOFTWARE**

A Lei 9.609/98 dispõe sobre a proteção da propriedade intelectual dos softwares (programas de computador) e sua comercialização no país.

Conforme a supracitada lei, o uso regular do software dar-se-á através do contrato de licença. Não existindo referido contrato, sua regularização fiscal dar-se-á através do documento fiscal relativo à aquisição ou licenciamento da cópia.

Outra novidade introduzida pela nova lei foi a possibilidade do titular do software autorizar ou proibir o aluguel comercial, não sendo este direito exaurível pela venda, licença ou outra forma de transferência da cópia, exceção feita ao software cujo objeto em si não seja essencialmente o aluguel.

Relativamente à questão da pirataria, podemos dizer que a nova lei considera crime de sonegação fiscal todo aquele que piratear ou usar cópia não autorizada. Dessa forma, a lei confere poderes à Receita Federal para investigar a origem das cópias de programas utilizados nos microcomputadores.

Em relação à tutela penal, a lei do software trata dos crimes e das penalidades em seu Capítulo V, artigo 12, ao prever a *"pena de detenção de seis meses a dois anos ou multa a quem violar direitos de autor de programa de computador, reproduzindo para fins de comércio, sem autorização expressa do autor ou de quem o represente; e pena de reclusão de um a quatro anos e multa a quem tem o intuito de vender, expor à venda ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral."*

Devem-se aplicar com rigor as normas existentes a coibir a violação dos direitos dos autores de software, bem como, incentivar a edição de legislação que possa acompanhar a evolução dos programas e das técnicas de vilipêndio dos direitos intelectuais.

O sistema legal ainda contempla proteção aos crimes contra a ordem econômica e contra as relações de consumo. No âmbito da ordem tributária, a Lei n.8.137 de 27 de dezembro de 1990, define uma nova forma de mau uso do computador, qual seja, ação de utilizar ou divulgar programas de processamento de dados que permita ao contribuinte possuir informação contábil diversa que é, por lei, fornecida à Fazenda Pública, sendo apenado com detenção de seis meses a dois anos e multa. É, pois, um programa de computador destinado a permitir a fraude fiscal.

#### **4.4.5.4 O FUTURO DO DIREITO PENAL DE INFORMÁTICA**

##### **4.4.5.4.1 PROJETOS DE LEI**

Devido à incerteza quanto ao Direito Criminal de Informática, tramitam no Congresso Legislativo, por sua vez, milhares de projetos de lei pertinentes aos crimes virtuais e, no entanto, é perceptível o desinteresse do governo perante a matéria.

Dois destes vem ganhando a atenção nacional. Um pertencente ao Deputado Luiz Piauhyllino e outro do Senador Renam Calheiros. Ambos tratam da tipificação e definição dos crimes de informática.

##### **4.4.5.4.2 O PROJETO DE LEI N.76 DE 2000**

##### **(DO SENADOR RENAM CALHEIROS)**

O projeto 76/00, em seu artigo primeiro, define e tipifica os crimes de uso indevido da informática. Dentre estes crimes destacam-se a destruição de dados e de sistemas (artigo 1º, 1º, I), apropriação de dados alheios (artigo 1º, 1º, II), a supressão de dados (artigo 1º, 1º, IV), a divulgação de informações sobre a

intimidade das pessoas sem que haja consentimento prévio (art. 1º, 3º, II). Para tais crimes, a pena prevista é detenção de um a seis meses, acrescida de multa.

Destacam-se, ainda, os crimes praticados contra a moral pública e a opção sexual (art. 1º, 6º). Dentre estes crimes estão a corrupção de menores e a divulgação de material pornográfico. Em relação a esta divulgação o legislador deveria restringi-la somente se tratar de pornografia infantil, de ofensa à privacidade, ou se não houver aviso prévio sobre a inadequação do conteúdo para crianças e adolescentes.

Conforme o artigo 1º da supracitada lei, os crimes de uso indevido da informática podem ser: 1) contra a inviolabilidade de dados; 2) contra a propriedade e o patrimônio; 3) contra a honra e a vida privada; 4) contra a vida e a integridade física das pessoas; 5) contra o patrimônio fiscal; 6) contra a moral pública e a opção sexual; e 7) contra a segurança nacional.

As normas do projeto de lei 76/00, devido ao fato de serem muito específicas, podem se tornar obsoletas em um curto período de tempo, uma vez que as mudanças no campo da informática ocorrem com extrema rapidez.

#### **4.4.5.4.3 O PROJETO DE LEI N. 84 DE 1999**

##### **(DO DEPUTADO LUIZ PIAUHYLINO)**

O projeto trata dos crimes de informática em geral, definindo-os e prevendo as respectivas penas. Dentre os crimes destacados no projeto estão a destruição, o apagamento e a modificação de dados sem que haja devida autorização, a obtenção de acesso indevido a computadores, a criação ou introdução de programa em computador, de forma indevida, com o objetivo de destruir, apagar ou modificar outro programa de computador.

Quanto aos direitos individuais, o referido Projeto inova ao prever punição para a veiculação de pornografia em redes de computadores, sem prévio aviso aos usuários sobre a natureza da informação disponibilizada.

Os projetos supracitados têm características mais próximas do que almejam os doutrinadores brasileiros, embora, ainda esteja distante, não da perfeição jurídica, do mínimo que atenda ao presente tecnológico, de modo a proteger o sistema, o computador, seus periféricos, e também o uso adequado.

Apesar de não preencher totalmente as necessidades da área de informática, são os mais completos, e tem nos especialistas, tanto da informática como do Direito, ferrenhos defensores da sua aprovação. Todavia, a normatização dos crimes de informática deve ser mais ampla, abrangendo um maior leque de condutas.

Vê-se, pois, que os projetos são abrangentes e inovadores. Apesar dos avanços, em termos de projeto, já que a legislação brasileira é pobre sobre o tema, é importante que os crimes de informática sejam normatizados ao abrigo do conhecimento técnico de condutas ilícitas, evitando-se, assim, as lacunas ocasionadas pela generalidade dos seus núcleos.

#### 4.5 O CONGRESSO NACIONAL, A POLÍCIA FEDERAL, O PODER JUDICIÁRIO E DEMAIS ÓRGÃOS PÚBLICOS BRASILEIROS E O "CRIME VIRTUAL"

Os *hackers* brasileiros têm muita sorte, pois a falta de uma legislação apropriada contra os crimes eletrônicos é o seu grande trunfo. A ausência de leis específicas torna o Brasil um verdadeiro "paraíso" para todo o tipo de invasão e manipulação de ilícita de dados. As punições aplicadas são baseadas em leis que se aproximam da situação do crime eletrônico. O enfoque das autoridades nacionais está nos crimes de pirataria e pedofilia, enquanto que os crimes de invasão e "*hackeamento*" de Sistemas Computacionais estão renegados a segundo plano, não se dando a devida atenção e importância.

Diante deste cenário tão preocupante, Governo e grandes empresários gastam vultosas quantias em *softwares* e equipamentos de segurança, pois a informação é o seu maior ativo. Porém, apesar de todo o investimento, não conseguem evitar a ação dos "vândalos digitais".

Preocupados com a situação, alguns senadores e deputados federais do Congresso Nacional (CN), como os Senadores Eduardo Azeredo (PL-84/1999), Leomar Quintanilha (PLS-137/2000), e Renan Calheiros (PLS-76/2000); assim com os Deputados Federais Décio Braga (PL-1.713/1996) e Luiz Piauhyllino (PLC-89/2003); os quais elaboraram projetos de lei para deter a ação dos "invasores cibernéticos". Porém, devido ao lento e vagaroso processo de votação no CN, aliados à total insipiência dos parlamentares sobre o importante assunto e as diversas alterações e correções pelas Comissões do CN (CAE - Comissão de Assuntos Econômicos, CCJ - Comissão de Constituição, Justiça e Cidadania, CE - Comissão de Educação, Cultura e Esporte, CCT - Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática, dentre outras); fazem com que a impunidade contra o crime organizado na *Web* continue impunemente, por falta de uma legislação punitiva e eficaz contra os crimes de informática. Enquanto isso, órgãos públicos dos Poderes Executivo, Legislativo e Judiciário, assim como grandes empresas; onde se tramitam um vasto volume de documentos digitais, são "alvos" de *cybercrimes*. Diariamente, a *Internet*, a televisão digital, o *e-commerce*, o Imposto de Renda de Pessoa Física (IRPF), os bancos, *e-mails* particulares e corporativos, os celulares, etc; tudo isso se tornou um "meio", um "caminho", um "canal", uma "via" para toda a ordem e tipo de "crimes virtuais".

O Projeto de Lei Substitutivo ao Projeto de Lei (PL) da Câmara nº 89, de 2003, e Projetos de Lei do Senado nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática, apresentam a seguinte situação:

- Apresentação: O Substitutivo apresentado pelo Senador Eduardo Azeredo aglutinou três projetos de lei que já tramitavam no Senado, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital e similar, de rede de computadores ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.
- Ementa: Altera o Decreto-Lei nº 2848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal

Militar), a Lei nº 9.296, de 24 de julho de 1996, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor); para tipificar condutas realizadas mediante uso de sistema eletrônico, digital e similar, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

- Relator: Senador Eduardo Azeredo (PSDB-MG)
- Projeto(s) Apensado(s): **PLC-89/2003; PLS-137/2000; PLS-76/2000.**
- Tramitação: A primeira versão do Substitutivo foi aprovada na Comissão de Educação do Senado em 20/06/2006. O Substitutivo está agora na Comissão de Constituição, Justiça e Cidadania do Senado (CCJ) e uma vez aprovado será apreciado em Plenário do Senado, daí seguindo à Câmara dos Deputados, para tramitação nas comissões de Ciência e Tecnologia, Constituição e Justiça e votação em plenário.
- Situação atual: Aguardando leitura e votação do relatório e substitutivo na Comissão de Constituição, Justiça e Cidadania do Senado.

#### **4.5.1 O QUE TRATA O PLC-89/2003?**

O Projeto de Lei da Câmara N° 89, de 2003 (PLC-89/2003), cuja autoria é do Deputado Federal Luiz Piauhyllino; altera o Código Penal (CP/1940), Decreto-Lei N° 2.848, de 7 de dezembro de 1940.

O mesmo dispositivo também altera a Lei N° 9.296, de 24 de julho de 1996, a qual cuida da interceptação de ligações telefônicas, de qualquer natureza, para prova e investigação criminal e instrução processual penal.

Sendo assim, o presente PLC dispõe sobre os crimes cometidos na área da informática e trata das suas penalidades. O mesmo Projeto dispõe também que o acesso de terceiros, não devidamente autorizados pelos interessados, a informações privadas mantidas em redes de computadores, dependerá de autorização judicial.

#### **4.5.2 O QUE TRATA O PLS-137/2000?**

O Projeto de Lei do Senado N° 137, de 2000 (PLS-137/2000), cuja autoria é do Senador Leomar Quintanilha; altera também o Código Penal (CP/1940), Decreto-Lei N° 2.848, de 7 de dezembro de 1940.

O mesmo dispositivo atribui o triplo das penas dos crimes já tipificados no CP/1940, se forem cometidos usando ferramentas de Tecnologias da Informação e Comunicação (TIC).

### **4.5.3 O QUE TRATA O PLS-76/2000?**

O Projeto de Lei do Senado N° 76, de 2000 (PLS-76/2000), cuja autoria é do Senador Renan Calheiros; altera também o Código Penal (CP/1940), Decreto-Lei N° 2.848, de 7 de dezembro de 1940.

O mesmo dispositivo apresenta a tipificação dos delitos cometidos com o uso de TIC e atribuem-lhes as respectivas penas em sete categorias:

- 1) Contra a violência de dados e sua comunicação;
- 2) Contra a propriedade e patrimônio;
- 3) Contra a honra e a vida privada;
- 4) Contra a vida e a integridade física das pessoas;
- 5) Contra o patrimônio fiscal;
- 6) Contra a moral pública e a opção sexual; e
- 7) Contra a segurança nacional.

### **4.5.4 TEXTOS DE PROJETOS DE LEI DO CONGRESSO NACIONAL**

Segue abaixo, na íntegra, o texto do Projeto de Lei N° 1.713/1996 (PL-1.713/1996), do Deputado Federal Décio Braga, cujo Projeto de Lei dispõe sobre os crimes de informática e dá outras providências:

#### **CAPÍTULO I**

#### **DOS PRINCÍPIOS QUE REGULAM A PRESTAÇÃO DE SERVIÇO POR REDES DE COMPUTADORES**

Art. 1º. 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 da rede.

Art. 2º. É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

#### **CAPÍTULO II**

#### **DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES OU REDES DE COMPUTADORES**

Art. 3º. Para fins desta lei, entende-se por informações privadas aquelas relativas a pessoa física ou jurídica identificada ou identificável.

Parágrafo Único: É identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.

Art. 4º. Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.

Art. 5º. 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.

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

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

§ 3º. Salvo por 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 validade.

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

Art. 6º. Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a origem racial, opinião política, filosófica, religiosa ou de orientação sexual, e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.

Art. 7º. O acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

### CAPÍTULO III

#### DOS CRIMES DE INFORMÁTICA

##### 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.

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 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

Acesso indevido ou não autorizado

Art. 9o. 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 considerável prejuízo para a 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 um a dois anos e multa.

Alteração de senha ou mecanismo de acesso a programa de computador ou dados

Art. 10o. 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.

Obtenção indevida ou não autorizada de dado ou instrução de computador

Art. 11o. 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 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

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

Art. 12o. Obter segredos, de indústria 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.

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

Art. 13o. 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 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.

Parágrafo único. Se o crime é cometido:

I - contra a 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 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.

Veiculação de pornografia através de rede de computadores

Art. 14o. Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exhibir, previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes.

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

## CAPÍTULO IV

### DAS DISPOSIÇÕES FINAIS

Art. 15o. 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.

Art. 16o. 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.

Art. 17o. Esta lei regula os crimes relativos à informática sem prejuízo das demais cominações previstas em outros diplomas legais.

Art. 18o. Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

Art. 19o. Revogam-se todas as disposições em contrário.

Segue abaixo também, na íntegra, o texto do Projeto de Lei N° 84, de 1999 (PL-84/1999), renomeado para PLC-89/2003:

REDAÇÃO FINAL DO PROJETO DE LEI N° 84, de 1999.

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e a Lei nº 9.296, de 24 de julho de 1996, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1º Esta Lei dispõe sobre os crimes de informática, e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar acrescido da seguinte Seção V do Capítulo VI do Título I:

" Seção V

Dos crimes contra a inviolabilidade  
Dos sistemas informatizados Acesso indevido a meio eletrônico

Art. 154A. Acessar, indevidamente ou sem autorização, meio eletrônico ou sistema informatizado:

Pena - detenção, de três meses a um ano, e multa.

§ 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a meio eletrônico ou sistema informatizado.

§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista.

Manipulação indevida de informação eletrônica

Art. 154B. Manter ou fornecer, indevidamente ou sem autorização, dado ou informação obtida em meio eletrônico ou sistema informatizado:

Pena - detenção, de seis meses a um ano, e multa.

§ 1º Nas mesmas penas incorre quem transporta, por qualquer meio, indevidamente ou sem autorização, dado ou informação obtida em meio eletrônico ou sistema informatizado.

§ 2º Somente se procede mediante representação, salvo se o crime é cometido

contra a União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista.

Meio eletrônico e sistema informatizado

Art. 154C. Para os efeitos penais, considera-se:

I - meio eletrônico: o computador, o processador de dados, o disquete, o CD-ROM ou qualquer outro meio capaz de armazenar ou transmitir dados magnética, óptica ou eletronicamente;

II - sistema informatizado: a rede de computadores, a base de dados, o programa de computador ou qualquer outro sistema capaz de armazenar ou transmitir dados eletronicamente."

Art. 3º O art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar com as seguintes alterações, renumerando-se o parágrafo único para § 1º:

"Art. 163. ....

§ 1º .....

(Pena - Detenção de 1 a 6 meses, ou multa)

Dano eletrônico

§ 2º Equipara-se à coisa:

I - o dado, a informação ou a base de dados presente em meio eletrônico ou sistema informatizado;

II - a senha ou qualquer meio de identificação que permita o acesso a meio eletrônico ou sistema informatizado.

Difusão de vírus eletrônico

§ 3º Nas mesmas penas do § 1º incorre quem cria, insere ou difunde dado ou informação em meio eletrônico ou sistema informatizado, indevidamente ou sem autorização, com a finalidade de destruí-lo, inutilizá-lo, modificá-lo ou dificultar-lhe o funcionamento."(NR)

(Pena - Detenção de 6 meses a 3 anos, e multa)

Art. 4º O art. 167 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar com a seguinte redação:

"Art. 167. Nos casos do art. 163, § 1º, inciso IV, quando o dado ou informação não tiver potencial de propagação ou alastramento, e do art. 164, somente se procede mediante queixa."(NR)

Art. 5º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar acrescido do seguinte artigo:

"Pornografia infantil

Art. 218A. Fotografar, publicar ou divulgar, por qualquer meio, cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:  
Pena - reclusão, de um a quatro anos, e multa.

§ 1º As penas são aumentadas de metade até dois terços se o crime é cometido por meio de rede de computadores ou outro meio de alta propagação.

§ 2º A ação penal é pública incondicionada."

Art. 6º Os arts. 265 e 266, ambos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com as seguintes alterações:  
"Atentado contra a segurança de serviço de utilidade pública

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor ou telecomunicação, ou qualquer outro de utilidade pública:  
"(NR)

(Pena - Reclusão de 1 a 5 anos, e multa)

"Interrupção ou perturbação de serviço telegráfico ou telefônico

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento:  
"(NR)

(Pena - Detenção de 1 a 3 anos, e multa)

Art. 7º O art. 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar acrescido do seguinte parágrafo único:

"Art. 298.....

Falsificação de cartão de crédito

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito."(NR)

(Pena - Reclusão de 1 a 5 anos, e multa)

Art. 8º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar acrescido do seguinte artigo:

"Falsificação de telefone celular ou meio de acesso a sistema eletrônico

Art. 298A. Criar ou copiar, indevidamente ou sem autorização, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de radiofreqüência ou de telefonia celular ou qualquer instrumento que permita o acesso

a meio eletrônico ou sistema informatizado:

Pena - reclusão, de um a cinco anos, e multa."

Art. 9º O art. 2º da Lei nº 9.296, de 24 de julho de 1996, passa a vigorar acrescido do § 2º, renumerando-se o parágrafo único para § 1º:

"Art. 2º.....

§ 1º.....

§ 2º O disposto no inciso III do caput não se aplica quando se tratar de interceptação do fluxo de comunicações em sistema de informática ou telemática."(NR)

Art. 10. Os crimes previstos nesta Lei quando praticados nas condições do inciso II, art. 9º, do Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, serão de competência da Justiça Militar.

Art. 11. As entidades que coletam, armazenam, processam, distribuem ou comercializam informações privadas, ou utilizam tais informações para fins comerciais ou para prestação de serviço de qualquer natureza, não poderão divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, a origem racial, opinião política, filosófica ou religiosa, crenças, ideologia, saúde física ou mental, vida sexual, registros policiais, assuntos familiares ou profissionais, e outras que a lei definir como sigilosas, salvo por ordem judicial ou com anuência expressa da pessoa a que se referem ou do seu representante legal.

Art. 12. Fica revogado o art. 241 da Lei nº 8.069, de 13 de julho de 1990. (Estatuto da Criança e do Adolescente, ver art. 218-A do CP)

Art. 13. Esta Lei entra em vigor na data de sua publicação.

Sala das Sessões, em 5 de novembro 2003.

Finalizando este tópico, segue abaixo também, na íntegra, o texto do Substitutivo aos PLS-76/2000, PLS-137/2000 e PLC-89/2003:

“SUBSTITUTIVO  
(ao PLS 76/2000, PLS 137/2000 e PLC 89/2003)

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.”

O CONGRESSO NACIONAL decreta:

Art.1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Art. 2º O Título VIII da Parte Especial do Código Penal fica acrescido do Capítulo IV, assim redigido:

“Capítulo IV  
DOS CRIMES CONTRA A SEGURANÇA  
DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.  
Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.  
Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Ação Penal

Art. 285-C. Nos crimes definidos neste Capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias.”

Art. 3º O Título I da Parte Especial do Código Penal fica acrescido do seguinte artigo, assim redigido:

“Divulgação ou utilização indevida de informações e dados pessoais  
154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.  
Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte.”

Art. 4º O caput do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

“Dano

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:  
.....”(NR)

Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

“Inserção ou difusão de código malicioso  
Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.  
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano  
§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:  
Pena – reclusão, de 2(dois) a 4 (quatro) anos, e multa.  
§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.”

Art. 6º O art. 171 do Código Penal passa a vigorar acrescido dos seguintes dispositivos:

“Art. 171 .....  
§ 2º Nas mesmas penas incorre quem:  
.....

Estelionato Eletrônico  
VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado:

§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime do inciso VII do § 2º deste artigo, a pena é aumentada de sexta parte.”

Art. 7º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

“Atentado contra a segurança de serviço de utilidade pública  
Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:  
.....”(NR)

“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado  
Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:

..... “(NR)

Art. 8º O caput do art. 297 do Código Penal passa a vigorar com a seguinte redação:  
“Falsificação de dado eletrônico ou documento público  
Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento publico verdadeiro:  
.....”(NR)

Art. 9º O caput do art. 298 do Código Penal passa a vigorar com a seguinte redação:  
“Falsificação de dado eletrônico ou documento particular  
Art. 298. Falsificar, no todo ou em parte, dado eletrônico ou documento particular ou alterar documento particular verdadeiro:  
.....”(NR)

Art. 10. O art. 251 do Capítulo IV do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar acrescido do inciso VI ao seu § 1º, e do § 4º, com a seguinte redação:

“Art. 251. ....

§ 1º - Nas mesmas penas incorre quem:  
.....

Estelionato Eletrônico  
VI - Difunde, por qualquer meio, código malicioso com o intuito de facilitar ou permitir o acesso indevido a rede de computadores, dispositivo de comunicação ou a sistema informatizado, em prejuízo da administração militar  
.....

§ 4º - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte.”

Art. 11. O caput do art. 259 e o caput do art. 262 do Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

“Dano Simples  
Art. 259. Destruir, inutilizar, deteriorar ou faze desaparecer coisa alheia ou dado eletrônico alheio, desde que este esteja sob administração militar:”(NR)  
.....  
.....

“Dano em material ou aparelhamento de guerra ou dado eletrônico  
Art. 262. Praticar dano em material ou aparelhamento de guerra ou dado eletrônico

de utilidade militar, ainda que em construção ou fabricação, ou em efeitos recolhidos a depósito, pertencentes ou não às forças armadas:”(NR)

Art. 12. O Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 262-A, assim redigido:

“Inserção ou difusão de código malicioso  
Art. 262-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado, desde que o fato atente contra a administração militar:  
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão código malicioso seguido de dano  
§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade do funcionamento, ou funcionamento não autorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:  
Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.  
§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte.”

Art. 13. O Título VII da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do Capítulo VII-A, assim redigido:

“Capítulo VII-A  
DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado  
Art. 339-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, desde que o fato atente contra a administração militar:  
Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.  
Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação  
Art. 339-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível, desde que o fato atente contra a administração militar:  
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.  
Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

“Divulgação ou utilização indevida de informações e dados pessoais  
Art. 339-C. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

Pena – detenção, de um a dois anos, e multa.  
Parágrafo único - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de crime, a pena é aumentada da sexta parte.”

Art. 14. O caput do art. 311 do Capítulo V do Título VII do Livro I da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar com a seguinte redação:  
“Falsificação de documento

Art. 311. Falsificar, no todo ou em parte, documento público ou particular, ou dado eletrônico ou alterar documento verdadeiro, desde que o fato atente contra a administração ou o serviço militar:”(NR)

Art. 15. Os incisos II e III do art. 356 do Capítulo I do Título I do Livro II da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar com a seguinte redação:

## “CAPÍTULO I

### DA TRAIÇÃO

#### Favor ao inimigo

Art. 356. ....:

II - entregando ao inimigo ou expondo a perigo dessa conseqüência navio, aeronave, fôrça ou posição, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar;

III - perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração, navio, aeronave, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar.”(NR)

Art. 16. Para os efeitos penais considera-se, dentre outros:

I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;

IV – código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;

V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;

VI – dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Art. 17. Para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado.

Art. 18. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 19. O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

“Art. 20 .....  
.....  
§ 3º.....  
II – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas,  
ou da publicação por qualquer meio.  
..... “(NR)

Art. 20. O caput do art. 241 da Lei nº 8.069, de 13 de julho de 1990, passa a vigorar com a seguinte redação:

“Art. 241. Apresentar, produzir, vender, receptor, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:  
..... “(NR)

Art. 21. O art. 1º da Lei nº 10.446, de 8 de maio de 2002 passa a vigorar com a seguinte redação:

“Art. 1º .....  
.....  
V – os delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado.  
.....”(NR)

Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:

I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;  
II – preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua

absoluta                      confidencialidade                      e                      inviolabilidade;  
III – informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores                      sob                      sua                      responsabilidade.

§ 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento.

§ 2º O responsável citado no caput deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R\$ 2.000,00 (dois mil reais) a R\$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.

§ 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.

Art. 23. Esta Lei entrará em vigor cento e vinte dias após a data de sua publicação.”

## **4.5.5 A ATUAÇÃO DA POLÍCIA FEDERAL CONTRA OS CRIMES CIBERNÉTICOS**

### **4.5.5.1 POLÍCIA FEDERAL CRIA ENDEREÇO ESPECÍFICO PARA DENÚNCIA DE CRIMES ELETRÔNICOS**

Estima-se que a indústria de *crime cibernético* - fraude com cartões de crédito e outras transações bancárias *online* - movimenta US\$ 100 bilhões ao ano em todo o mundo e é o setor do crime organizado que cresce mais rapidamente, cerca de 40% ao ano.

Acredita-se que o Brasil seja um dos países com o maior número de criminosos cibernéticos.

Sendo assim, em março de 2005, durante as festividades da comemoração dos 61 anos da Polícia Federal, o Serviço de Perícia em Informática do Instituto Nacional de Criminalística (INC) anunciou a criação de e-mail para encaminhamento de denúncias de crimes praticados na *Internet*.

Segundo a PF, o *e-mail* crime.internet@dpf.gov.br é a nova arma dos peritos para descobrir as ações de criminosos na *Web*. Qualquer pessoa que for vítima de um crime na internet, como invasão para descoberta de senhas pessoais ou sites falsos, pode usar a nova ferramenta.

O objetivo é centralizar e canalizar as denúncias para o setor apropriado. Depois de feita a perícia, os laudos serão encaminhados às delegacias competentes. Em 2004, o Serviço de Perícia do INC produziu 1.150 laudos periciais só na área de informática, o que representou um aumento de 40% no número de casos periciados.

Diariamente, manchetes sobre “crimes eletrônicos” são disponibilizadas nos diversos meios de comunicação. Notícias como essa: “*Novo vírus já infectou quase 9 milhões de computadores*”, disponibilizada no endereço <http://tecnologia.terra.com.br/interna/0,,OI3452986-EI4805,00-Novo+virus+ja+infectou+quase+milhoes+de+computadores.html>, no dia 16 de janeiro de 2009:

*“Uma nova estimativa da F-Secure, publicada hoje, aponta a descoberta de novos domínios infectados pelo vírus Conficker, também conhecido como Downadup. Ontem os números ultrapassaram 3,5 milhões de infecções. Hoje, o número quase triplicou, e já são 8.976.308 vítimas ao redor do mundo”.*

A Polícia Federal tem atuado juntamente com os Bancos da rede financeira, a fim de erradicar os crimes eletrônicos realizados nas contas de milhões de “inocentes” clientes. A notícia publicada no endereço <http://ultimosegundo.ig.com.br/economia/2009/01/06/em+2008+houve+48+mil+crimes+na+internet+contra+a+caixa+economica+federal+3238605.html>, em 6 de janeiro de 2009, relata o seguinte:

*“De acordo com a Polícia Federal (PF), foram registrados 48 mil ataques virtuais contra a Caixa Econômica Federal em 2008. Foram abertos cerca de 4 mil inquéritos por mês para investigar o uso da internet como ferramenta para invadir sistemas e desviar dinheiro de contas correntes. O número de fraudes seria ainda mais alarmante caso a Polícia Civil centralizasse informações sobre crimes contra os demais Bancos em operação no País”. E mais adiante, há também a informação de que:*

*“Somente de fraude bancária contra a Caixa nós abrimos mais de quatro mil inquéritos por mês”, disse o responsável pela repressão de crimes eletrônicos da Polícia Federal (PF), delegado Carlos Eduardo Sobral.*

Sendo assim, a fim de combater de forma profícua e eficaz o “crime eletrônico”, o Governo Federal, através do Ministério da Defesa (MD), investiu **R\$70.315.300,00 para a implantação de sistema de informática e telecomunicações da Polícia Federal**, assim como **R\$46.000,00 para a integração dos sistemas da PF com o SIPAM/SIVAM**; conforme notificou o site [http://www.defesanet.com.br/zz/md\\_budget\\_07.htm](http://www.defesanet.com.br/zz/md_budget_07.htm), em 27 de fevereiro de 2007:

POLÍCIA FEDERAL:

*“Para a modernização da Polícia Federal, foram aprovados R\$315.173.480,00. Desse total, R\$40.000.000,00 para a construção e ampliação de bases operacionais e unidades da Polícia Federal; R\$70.315.300,00 para a implantação de sistema de informática e telecomunicações da Polícia Federal;*

R\$45.238.700 para o re-aparelhamento das unidades operacionais da PF e do segmento técnico-científico; R\$99.623.480,00 para a emissão de passaportes e controle do tráfego internacional; R\$46.000,00 para a integração dos sistemas da PF com o SIPAM/SIVAM; e R\$36.000.000,00 para a reforma e modernização das bases operacionais do Departamento de Polícia Federal”.

#### **4.5.5.2 A ATUAÇÃO DO PODER JUDICIÁRIO CONTRA OS “CRIMES CIBERNÉTICOS”**

O Judiciário brasileiro, buscando resolver a questão do crescente número de processos aguardando julgamento em suas várias instâncias, tem investido em modernização e em segurança da informação, apelando para os recursos da Informática Jurídica. O Poder Judiciário (PJ), como um todo, a nível Federal, Estadual e Municipal tem procurado se reequipar e se *informatizar*, a fim de dinamizar o julgamento dos processos jurídicos.

De modo geral, a grande maioria das Cortes de Justiça brasileiras tem seu site na *Internet* onde estão disponíveis ao público informações gerais, andamento dos processos e textos das sentenças.

É muito comum a oferta de um serviço gratuito, via e-mail, de informação sobre o andamento dos processos. O usuário, após o cadastro, passa a receber uma mensagem automática toda vez que o processo de seu interesse é movimentado. Essa ferramenta, denominada *Sistema Push* tem sido muito útil aos advogados e às próprias partes.

No entanto, a informatização da Justiça brasileira tem se concentrado nas áreas de informação e documentação, processos em meio eletrônico são projetos pioneiros cuja regulamentação não é ampla. A digitalização do processo propriamente dito é matéria de discussão do projeto de lei federal transcrito ao final deste trabalho. Os órgãos jurídicos têm suas secretarias de informática e poucos serviços especializados são terceirizados.

Para exemplificar, indica-se a consulta aos sites dos Tribunais Superiores:

- Supremo Tribunal Federal - STF <http://www.stf.gov.br/>
- Superior Tribunal de Justiça - STJ <http://www.stj.gov.br/>
- Superior Tribunal Militar - STM <http://www.stm.gov.br/>
- Tribunal Superior Eleitoral - TSE <http://www.tse.gov.br/>
- Tribunal Superior do Trabalho - TST <http://www.tst.gov.br/>

O Poder Judiciário tem os seguintes projetos na área de Tecnologia e Informação:

#### **4.5.5.3 O SISTEMA DE EXECUÇÃO FISCAL VIRTUAL**

Devido ao grande número de processos de execução fiscal tramitando na Justiça Federal brasileira, foi criado o projeto "Execução Fiscal Virtual" a partir de um convênio realizado entre a Justiça Federal, o Serviço Federal de Processamento de Dados (SERPRO), a Receita Federal e a Empresa de Tecnologia e Informações da Previdência Social (DATAPREV). Com a implantação desse sistema piloto nas 12 Varas de Execução Fiscal da Seção Judiciária de São Paulo prevê-se uma agilização considerável das mesmas. Esse projeto, já em andamento, conta com a tecnologia de Gerenciamento Eletrônico de Documentos, WorkFlow (define o fluxo dos documentos), Cold (meio ótico), e assinatura eletrônica através de Smart Card. O Smart Card armazena o certificado eletrônico com a impressão digital do usuário e só é reconhecido com a concomitante leitura ótica da impressão digital "in vivo". Todo o acesso ao sistema e assinatura das peças será por identidade digital. Autorizadas pela Lei 10.259/2001 (Art. 8º § 2º Os tribunais poderão organizar serviço de intimação das partes e de recepção de petições por meio eletrônico.), as varas poderão receber, de advogados cadastrados, petições por meio eletrônico, além das petições padrão em papel. Para se cadastrar nesse serviço, o advogado deverá adquirir uma identidade digital em empresa oficialmente reconhecida.

Todas as peças processuais serão originalmente digitais, salvo as petições recebidas em papel cuja digitalização, através de scanner, será considerada cópia autêntica. Os documentos impressos terão uma marca d'água como certificado e, provavelmente, também o número do original no sistema, para evitar falsificações.

A tramitação dos documentos dentro do sistema seguirá uma engenharia de fluxos procedimentais pré-determinados em função da classificação das peças, com disponibilização de modelos de documentos, diminuindo, assim, o trabalho meramente manual, otimizando o tempo do juiz e do servidor judiciário para o trabalho intelectual. Além disso, acelera o tempo da tramitação do documento, que passa a ser automática, dentro da administração judiciária, com as partes e advogados e Imprensa Oficial.

Naturalmente, o arquivamento dos documentos será em meio digital, alimentando um banco de dados em meio portátil, disponibilizado, também na Internet, com informações sobre a tramitação dos processos e sentenças. Da mesma forma, estarão acessíveis ao público as estatísticas geradas pelo sistema.

#### **4.5.5.4 O ANTEPROJETO DE LEI APRESENTADO PELA ASSOCIAÇÃO DOS JUÍZES FEDERAIS DO BRASIL**

(originalmente, PL nº 5.828/01, na Câmara dos Deputados)

Esse projeto de lei, atualmente tramitando pelo Senado Federal, já tem recebido críticas, especialmente no que concerne ao parágrafo 2º do artigo 1º ao dispensar a apresentação dos "originais". Alguns crêem ser um mero erro de redação, já que o original seria o próprio formato digital, e não o documento em

papel. Sua principal função é trazer agilidade à prestação jurisdicional, tentativa feita pela Lei nº 9.800/00, que permitiu o envio de petições por fax ou e-mail com a posterior apresentação dos originais no prazo de 05 dias. Essa lei foi considerada um fracasso, pois resultou, de fato, em uma mera ampliação dos prazos processuais.

Texto completo do Anteprojeto:

Dispõe sobre a informatização do processo judicial e dá outras providências.

O Congresso Nacional decreta:

Art. 1º O uso de meio eletrônico na comunicação de atos e a transmissão de peças processuais serão admitidos nos termos da presente lei.

§ 1º O disposto nesta lei aplicar-se-á, indistintamente, aos processos civil, penal e trabalhista em todos os graus de jurisdição.

§ 2º O uso do meio eletrônico dispensa a apresentação dos documentos originais.

Art. 2º O envio de petições, de recursos e demais peças processuais por meio eletrônico será admitido àqueles que se credenciarem junto aos órgãos do Poder Judiciário.

§ 1º O credenciamento far-se-á mediante procedimento no qual esteja assegurada a adequada identificação do interessado.

§ 2º Ao credenciado será atribuído registro e meio de acesso ao sistema, de modo a preservar o sigilo, a identificação e a autenticidade de suas comunicações.

§ 3º Os órgãos respectivos de Segunda Instância poderão criar um cadastro único para as Justiças respectivas.

Art. 3º O envio de petições, de recursos e demais peças processuais por meio eletrônico considerar-se-á realizado no dia e hora de seu recebimento pelo provedor do Judiciário.

Art. 4º A publicação de atos e de comunicações processuais poderá ser efetuada por meio eletrônico e considerada como data da publicação a da disponibilização dos dados no sistema eletrônico para consulta externa.

Parágrafo único. Os prazos processuais terão início no primeiro dia útil seguinte ao da publicação feita na forma deste artigo.

Art. 5º Nos casos em que a lei processual exigir a intimação pessoal, as partes e seus procuradores, desde que previamente cadastrados de acordo com o art. 2º, serão intimados por correio eletrônico com aviso de recebimento eletrônico.

§ 1º Os prazos processuais terão início no primeiro dia útil seguinte ao retorno do aviso de recebimento de que trata o "caput" deste artigo.

§ 2º Decorridos cinco dias do envio de que trata o "caput" deste artigo sem confirmação de recebimento, a publicação far-se-á na forma prevista no art. 4º.

Art. 6º As cartas precatórias, de ordem e, de um modo geral, todas as comunicações oficiais que transitem entre órgãos do Poder Judiciário, bem assim entre os deste e dos demais poderes, far-se-ão preferencialmente por meio eletrônico.

Art. 7º As pessoas de Direito Público, os órgãos da administração direta e indireta e suas representações judiciais, deverão disponibilizar, em cento e vinte dias da publicação desta lei, serviço de recebimento e envio de comunicações de atos judiciais por meio eletrônico.

Parágrafo único. As regras da presente lei não se aplicam aos Municípios, enquanto não possuírem condições técnicas de implementação de sistemas eletrônicos.

Art. 8º Os órgãos do Poder Judiciário poderão desenvolver sistemas de comunicação de dados, com distribuição de programa de acesso aos cadastrados nos termos do art. 2º, que será de uso obrigatório nas comunicações eletrônicas de que cuida esta lei.

Parágrafo único. O sistema será dotado dos seguintes requisitos:

- I aviso automático de recebimento e abertura das mensagens;
- II numeração automática ou outro mecanismo que assegure a integridade do texto;
- III protocolo eletrônico das mensagens transmitidas, especificando data e horário;
- IV visualização do arquivo para confirmação de seu teor e forma antes do envio;
- V proteção dos textos transmitidos, obstando alterações dos arquivos recebidos;
- VI armazenamento por meio eletrônico dos atos praticados, bem como dos acessos efetuados na forma da presente lei.

Art. 9º A redução a termo de atos processuais poderá ser efetuada com o emprego de tecnologia de gravação de som, imagem ou reconhecimento de voz, a critério do juízo.

Art. 10. A conservação dos autos do processo poderá ser efetuada total ou parcialmente por meio eletrônico.

Art. 11. Será assegurada a requisição, por via eletrônica, por parte dos Juízes e Tribunais, mediante despacho nos autos, a dados constantes de cadastros públicos, essenciais ao desempenho de suas atividades.

§ 1º Consideram-se cadastros públicos essenciais, para os efeitos deste artigo, dentre outros existentes e que venham a ser criados, ainda que mantidos por concessionárias de serviço público ou empresas privadas, os que contenham informações necessárias a alguma decisão judicial.

§ 2º O acesso de que trata este artigo se dará por meio de conexão direta informatizada, telemática, via cabo, acesso discado ou qualquer meio tecnológico disponível.

§ 3º Os órgãos que mantêm os registros de que trata este artigo, no prazo de noventa dias, contados a partir do recebimento da solicitação, disponibilizarão os meios necessários para o cumprimento desta disposição.

Art. 12. Esta lei entra em vigor sessenta dias depois de sua publicação, revogadas as disposições em contrário.

Sendo assim, o Judiciário brasileiro tem se adaptado rapidamente à evolução das tecnologias de informática e informação, não de maneira uniforme, pois cada instituição possui auto-gerência, mas as diferenças não chegam a ser dissonantes. A aprovação do projeto de lei sobre a informatização do processo judicial obviamente representará um ganho de agilidade e, conseqüentemente, de desempenho na prestação jurisdicional, bem como de avaliação do próprio desempenho. No entanto, é importante ressaltar que, de acordo com a pesquisa "Estrutura Legal e Eficiência Judiciária: o Projeto Lex Mundi", as variáveis administração judiciária e equipamentos foram pouquíssimos significativos na avaliação dos índices de desempenho judiciário, que flutuaram principalmente em função dos sistemas judiciais, especificamente, das normas processuais de caráter mais ou menos complexos.

O Poder Judiciário tem atuado contra os "crimes de informática" ativamente, enquanto aguarda uma fórmula jurídico-penal eficiente. Faz-se necessário implantar uma legislação para coibir os delitos de informática, cujos autores se utilizam de extremo conhecimento técnico para praticarem atos lesivos ao patrimônio de pessoas físicas e jurídicas.

Notícias como esta, são comuns no dia a dia:

*"O Grupo de Combate a Crimes Cibernéticos do Ministério Público Federal em São Paulo recomendou que os provedores Uol, Ig, Terra, Bol e Yahoo façam em 90 dias alterações em seus serviços de bate-papo que ajudem a inibir a atuação de pedófilos que buscam aliciar crianças e adolescentes nesses sites", publicado no dia 13 de junho de 2008, no site [http://www.jornalbaixadasantista.com.br/conteudo/mp\\_recomenda\\_monitoramento\\_chats2008.asp](http://www.jornalbaixadasantista.com.br/conteudo/mp_recomenda_monitoramento_chats2008.asp).*

Outrossim, uma manchete não menos importante, intitulada como: "Hackers controlam PCs sem que usuários percebam", disponibilizada no endereço

<http://tecnologia.terra.com.br/interna/0,,OI1927458-EI4805,00.html>, também ajuda a caracterizar os constantes “crimes virtuais” na *Web*:

*“Os especialistas em segurança estimam que dezenas de milhões de computadores pessoais estejam infectados com programas nocivos. Esses programas, em geral conhecidos como malware, atacam tanto empresas quanto consumidores. Alguns deles registram as ações do teclado, gravando tudo que os usuários digitam e enviando informações valiosas sobre contas bancárias, senhas e números de cartão de crédito a hackers. Em julho, hackers usaram esse tipo de software para obter senhas de bancos de dados usados pelo Departamento de Transportes do governo norte-americano e por empresas como a Booz Allen, Hewlett-Packard e a produtora de equipamentos para redes de satélites Hughes Network Systems, segundo a Prevx, uma produtora britânica de software de segurança para a Internet”.*

No Brasil, a realidade dos “*crimes cibernéticos*” não é diferente e, conseqüentemente, é necessário que o Código Penal (CP/1940) — pensado conforme a doutrina da década de trinta — não se presta *in totum* a regular relações da era digital, em um país que almeja inserir-se na cena global da sociedade da informação. Essa sociedade que é produto da revolução tecnológica, advinda com o desenvolvimento e a popularização do computador.

É preciso, pois, adequar institutos, rever conceitos — a exemplo do de “resultado”, como entendido na atual redação do art. 13, *caput*, do Código Penal —, especificar novos tipos, interpretar adequadamente os elementos normativos dos tipos existentes; e definir, eficazmente, regras de competência e de cooperação jurisdicional em matéria penal, a fim de permitir o combate à criminalidade informática.

Em torno do tema, a professora Ivette Senise Ferreira (FERREIRA, 2000), titular de Direito Penal na USP, pontifica que “A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução”.

A toda nova realidade, uma nova disciplina. Daí cuidar-se do Direito Penal da Informática, ramo do direito público, voltado para a proteção de bens jurídicos computacionais inseridos em bancos de dados, em redes de computadores, ou em máquinas isoladas, incluindo a tutela penal do *software*, da liberdade individual, da ordem econômica, do patrimônio, do direito de autor, da propriedade industrial, etc. Vale dizer: tanto merecem proteção do Direito Penal da Informática o computador em

si, com seus periféricos, dados, registros, programas e informações, quanto aos outros bens jurídicos, já protegidos noutros termos, mas que possam (também) ser atingidos, ameaçados ou lesados por meio do computador.

Nesse novíssimo contexto, certamente serão necessárias redefinições de institutos, principalmente no tocante à proteção penal de bens imateriais e da informação, seja ela sensível<sup>1</sup> ou não, tendo em conta que na sociedade tecnológica a informação passa a ser tida como verdadeira *commodity* e, em alguns casos, tal "valor" pode ser vital para uma empresa ou para uma organização pública ou privada. Sem esquecer que, no plano constitucional dos direitos fundamentais e no plano civil dos direitos de personalidade, as ameaças, por meio de computadores, a bens indispensáveis à realização da personalidade humana também devem ser evitadas e combatidas, partam elas do Estado ou de indivíduos. A isso se propõe o Direito Penal da Informática.

#### **4.6 HACKERS, CRACKERS, PHREAKERS, DEFACERS, SCRIPT-KIDDIES E A SOCIEDADE CONTEMPORÂNEA**

Do ponto de vista prático, e em primeira análise, *hackers*, *crackers*, *phreakers*, *defacers*, *Script-kiddies* ou qualquer outra denominação empregada para definir os "inimigos externos" com potencial de fraudar um Sistema Informatizado são a mesma coisa. Porém, isto está certo em parte, pois um *defacer* não é necessariamente um *hacker*; assim como um *hacker* não é necessariamente um *cracker*, e conseqüentemente, cada uma das classificações aplicadas erroneamente a qualquer um destes indivíduos é capaz, ironicamente, de provocar uma ira imaginável se realizada pessoalmente. Embora a definição de cada uma dessas "categorias" de inimigos pareça desnecessária, ela é particularmente interessante para o delineamento comportamental de suas respectivas ações, e isso, em várias ocasiões; pode permitir linhas adequadas de ação, evitando a utilização desnecessária de ferramentas de segurança, as quais podem fazer com que o corpo de direção de uma empresa ou instituição tenha desconfiança, ante aos custos onerosos com a Segurança de Informação.

Faz-se necessária uma adequada aplicação das linhas de aplicações cabíveis para cada tipo de dano, invasão ou ameaça de ataque aos dados de uma rede de computadores, sendo mais lógica a aplicação de todos os tipos possíveis e imagináveis de equipamentos de segurança. Porém, só há um problema: Não existe a possibilidade de aplicação de todos os recursos por motivos óbvios – A dinamização de todo o contexto de segurança e a impossibilidade gerada por fatores como custo operacional, viabilidade e praticidade. Em termos sucintos e diretos: exterminar um rato com um tiro de bazuca é perfeitamente eficaz, porém desnecessário.

<sup>1</sup> A expressão "informação sensível", como gênero e no sentido empregado, engloba dados relativos à segurança nacional, à intimidade, à vida privada, etc; elementos que, por sua própria natureza, merecem maior proteção contra acesso ou devassa indevidos ou não autorizados.

Sendo assim, é conveniente iniciar o reconhecimento dos “inimigos” em potencial, principalmente para situações nas quais as análises dos procedimentos de segurança são relevantes ao tipo de atividade empregada pela rede de trabalho; classificando-os em “categorias”, a fim de que sejam verificados quem é ameaça ou não, no “mundo virtual”.

#### 4.6.1 HACKERS

*Hacker* não é um termo de fácil definição.

Segundo o pesquisador ULBRICH (2007):

*“São especialistas que já dominam diversas técnicas de invasão e conhecem com profundidade pelo menos um Sistema Operacional. São excelentes programadores (também passaram pela fase larval<sup>1</sup>) e administradores de sistemas. Mas, diferentemente do que popularmente se acreditam, possuem um **rígido código de ética e nunca usam os seus conhecimentos para o mal**, mesmo que sua noção de bem seja contra a lei”.*

De acordo com OLIVEIRA (2007):

*“Hacker: pessoa que possui grande capacidade de análise, simulação e compreensão, aplicadas ao trabalho com um computador. Ele sabe perfeitamente (como todos nós sabemos) que nenhum sistema é completamente livre de falhas, e sabe onde procurá-las utilizando técnicas das mais variadas”.*

Surpreendentemente, o termo original distancia-se enormemente da primeira impressão atual, considerado por profissionais e usuários de computadores contemporâneos. No jargão da informática, o termo foi primeiramente empregado pelo renomado Instituto Tecnológico de Massachusetts (Massachusetts Institute of Technology – MIT), nos anos de 1950, para os indivíduos interessados por uma nova e estimulante ciência: o processamento eletrônico de dados. A de definição aplicada pelo MIT servia, e ainda é aceita até hoje, para caracterizar pessoas engajadas na alteração de algo pronto ou em desenvolvimento, no intuito de aperfeiçoá-lo. A atribuição, defendida fortemente por especialistas no segmento geral da Informática, aponta os *hackers* como pessoas diretamente responsáveis pelo desenvolvimento da *Internet*, como a conhecemos atualmente. Linguagens de programação para *Web* (HTML, PHP, Java, JavaScript, etc), Sistemas Operacionais como o *Unix* e *Linux* (<http://www.linux.org/>) e a “maturação” de serviços públicos eficazes disponíveis na “*WWW*” atualmente, também devem o seu potencial aos *hackers*.

<sup>1</sup> Fase larval: Segundo o escritor ULBRICH (2007), esta fase também é conhecida como *spawn*. É o período de isolamento total pelo qual o candidato a *hacker* tem de passar para, no final do processo, “nascer de novo” como programador. Note que possuir habilidade em programação é condição fundamental para ser considerado *hacker*, mesmo no sentido popular da palavra. O estágio larval restringe-se à programação e pode durar de seis meses a dois anos.

Culturalmente, porém, o *hacker* não é visto na sociedade leiga, e até mesmo na imprensa dita especializada, como um indivíduo “*bom*” e “*ético*”. Ataques a redes de computadores e a endereços de *sites* na *Web*, alteração e perda de dados e toda sorte de “*danos cibernéticos*” são atribuídos *hackers*, e estes, contando com o suporte da definição empregada pelo MIT e outras renomadas instituições do ramo; bem como por especialistas da área de TI (Tecnologia da Informação), se defendem ativamente, propagando as suas diretivas e, obviamente, divulgando com extremo esforço a classificação exata dos indivíduos com intenções marginais, totalmente distante e diferente do termo *hacker*, constituído como um indivíduo **ético e responsável**.

A princípio, de acordo com os termos de defesa destas pessoas, os *hackers* devem ser categorizados como profissionais que têm por objetivo a utilização de seus conhecimentos na exploração e detecção legal de erros sistêmicos. A atitude típica de um *hacker* ao encontrar falha de segurança em um Sistema Informatizado, é contatar os responsáveis pelo mesmo, comunicando o fato e trazer soluções tecnológicas para resolver o problema. Na vida prática dos administradores de redes de computadores, um *hacker*, tal qual o termo definido pelo MIT, não se apresenta com muita frequência. Porém, não são raros os casos de *hackers* que, inadvertida ou intencionalmente, burlam um Sistema Informatizado, na maioria das vezes por constatá-lo tão seguro quanto um carro estacionado no centro de uma grande cidade com vidros abertos e a chave na ignição, a mercê de ladrões e pessoas mal-intencionadas. Neste caso, os *hackers* deixam mensagens para os administradores alertando-os sobre um outro aspecto a ser observado. Neste tipo de ação, evidentemente, o *hacker* quase sempre não se identifica.

A metodologia de trabalho de um *hacker* constitui-se, geralmente, em exaustivas tentativas de burlarem seus próprios Sistemas Informatizados. Também não são nada raros os casos de auditorias de segurança que se utilizam dos serviços de um *hacker* profissional sob contrato para detecção de falhas, sugestão e implantação de medidas de segurança.

Um *hacker* ético é, comumente, denominado *hacker white hat* (*hacker* de “chapéu branco”) e, evidentemente, existem variações deste tipo de indivíduo, como por exemplo, um *hacker gray hat* (*hacker* de “chapéu cinza”). Este, por sua vez, possui habilidades e intenções de um *hacker* ético; porém, pode e geralmente usa seu conhecimento para propósitos pessoais, devido ao fato de sua conduta ética ser diferenciada. Um *hacker* de “chapéu cinza” considera totalmente aceitável a penetração em Sistemas Informatizados, desde que não sejam cometidos furtos, vandalismos ou infrações de aspectos confidenciais. A discussão quanto a esse tipo de conduta é encabeçada pelo fato de os *hackers white hat* não concordarem com atitudes de penetração não autorizada a Sistemas Informatizados fechados, mesmos sem atos de destruição e vandalismo.

Uma das maiores e possivelmente mais completas compilações de termos e definições quanto ao termo *hacker*, incluindo considerações sobre a cultura e vocabulário empregado, tanto escrito quanto falado, é mantida pela coleção de documentos denominada “*Jargon File*”, disponível no endereço <http://www.catb.org/jargon/html/index.html>. De acordo com os conteúdos descritos a partir de *links* da coleção de documentos, *hackers* utilizam como emblema a figura denominada “*Glide*” (figura 1), que alude ao jogo de simulação de dinâmica celular chamado “*Game of Life*”, desenvolvido pelo matemático John Horton Conway, da Universidade de Cambridge, Inglaterra.

Finalizando este tópico, há ainda o *hacker* do tipo *black hat* (“chapéu negro”), também conhecido como *dirk sider* (“lado escuro”) ou, simplesmente, *cracker*.

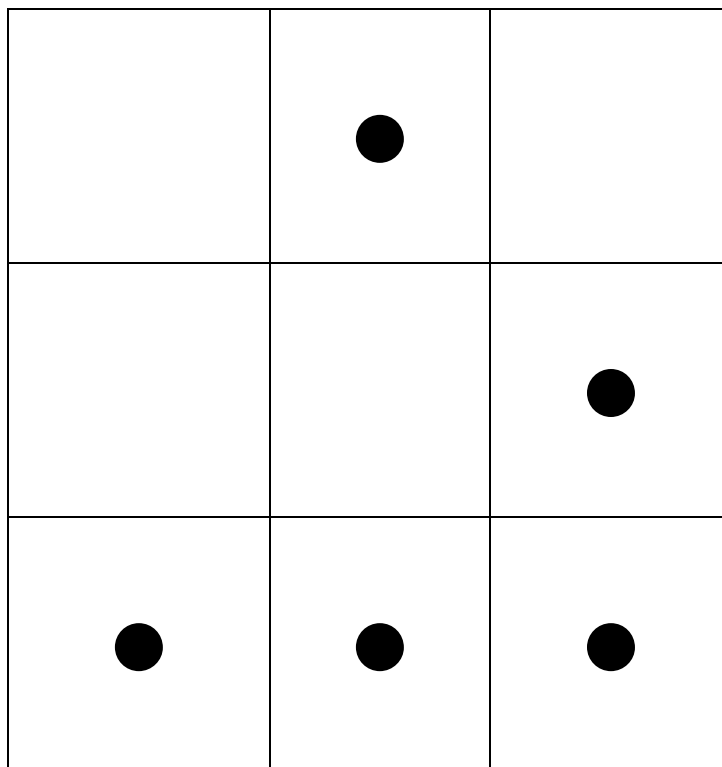


Figura 1 – Emblema dos *hackers*: *Glade*

#### 4.6.2 CRACKERS

O *hacker* às avessas é o *cracker*, indivíduo, muitas vezes com um vasto conhecimento no campo da informática, persistente e paciente quanto aos seus objetivos e dono de uma elaborada metodologia de ação, incluindo, não raro, dois ou mais elementos de confiança. É provável ser esta a única ética de um *cracker* experiente: a de confiar uma de suas táticas e objetivos àqueles que, em uma espécie de equipe, (muitas vezes, uma verdadeira “quadrilha”, caracterizando “crime organizado”) implicam seus esforços para ações verdadeiramente criminosas.

Segundo o pesquisador ULBRICH (2007):

**“Cracker** - Chamado ‘hacker do mal’ ou ‘hacker sem ética’, normalmente é especializado em quebrar as travas de softwares comerciais para poder pirateá-los (chamados de **warez-d00dz**), mas também usa os seus conhecimentos para invadir sites e computadores com objetivos ilícitos, como vandalismo ou roubo. Muitas vezes

os crackers são excelentes programadores e podem criar programas que infectem e destruam completamente sistemas alheios sem deixar vestígios – os **lamers**<sup>1</sup> normalmente usam programas criados pelos crackers”.

De acordo com OLIVEIRA (2007):

*“Cracker: possui tanto conhecimento quanto os hackers, mas com a diferença que, para eles, não basta entrar em sistemas, quebrar senhas e descobrir falhas: precisam deixar um aviso de que estiveram lá. Geralmente são recados malcriados, mas algumas vezes, podem destruir parte do sistema, ou aniquilar tudo o que vêem pela frente. Também são atribuídos aos crackers programas que retiram travas em software, bem como os que alteram as suas características, adicionando, ou modificando, opções muitas vezes relacionadas à pirataria”.*

Crimes virtuais são praticados em uma assustadora e progressiva razão número-quantitativa, a qual nem mesmo os melhores especialistas são capazes de quantificar com total exatidão. Os problemas começam na classificação de tais infrações. Neste exato momento, ao abrir o programa cliente de *e-mail* (correio-eletrônico), qualquer usuário pode se deparar com mensagens falsas contendo *links* para *downloads* de códigos maliciosos e nocivos, os quais tentam providenciar senhas, nomes de *login* e qualquer outro dado válido para um *cracker*. Os “alvos primários” de *cracker* avançados e experientes, na maioria das vezes, são informações pessoais, nas quais há esperança de obtenção de senhas bancárias, de serviços de cartões de crédito ou qualquer outro elemento considerado por esses criminosos como “proveitosos”.

<sup>1</sup> *Lamers*: Segundo ULBRICH (2007) - um usuário comum (*newbie* ou *luser*), o qual aprende a usar alguns programas criados, geralmente, por *crackers*. Não sabe ou não tem condição de saber como as coisas funcionam, mas já sabe pelo menos como operar os aplicativos existentes do computador. *Newbie*: Iniciante interessado em aprender tudo sobre Informática, enquanto que o *Luser* é o iniciante desinteressado.

Por outro lado, algumas ações executadas por *crackers* são consideradas extremamente benéficas para a maioria dos usuários domésticos – e até mesmo para algumas empresas – o que pode ser exemplificado a partir de uma prática bastante comum: ao realizar o *download* de um programa do tipo *shareware*, o caminho correto para a utilização do *software* sem limite estabelecido por uma data de expiração ou para a habilitação de todos os seus recursos; seria o pagamento de uma taxa, referente aos custos de desenvolvimento de tal programa, geralmente cobrada via cartão de crédito. Ao invés de efetuar o pagamento via cartão de crédito, o usuário tem a alternativa, a qual quase sempre não acarretará em nenhum problema para o mesmo; visitar um *site* contendo *cracks* no formato de programas geradores de códigos de licenças compostos por conjuntos de caracteres alfa-numéricos (números de seriais) ou, até mesmo, os próprios números *crackeados*, prontos para o uso, bastando copiar e colar o conteúdo em um campo específico. Assim, o programa passa a ser disponibilizado sem restrição de recursos e sem uma data de expiração, como se fosse legitimamente adquirido. Eis uma prática utilizada por um determinado tipo de *cracker*, que o grande público usuário de computadores domésticos tem medo de perder. Porém, é certo que apesar de todo o benefício aparente, as empresas desenvolvedoras desses programas, a cada ano, perdem cifras astronomicamente altas e, conseqüentemente, uma série complexa de fatores evita a aplicação de medidas preventivas. Afinal de contas, ao se ganhar uma batalha judicial para que determinado *site* contendo *cracks*, números de seriais e outros assuntos relacionados seja fechado, provavelmente mais de um novo *site* estará sendo aberto ao mesmo tempo, para a felicidade da maioria dos usuários. Evidentemente, para deixar o quadro mais complexo, a área jurídica ainda não dispõe de códigos e legislações devidamente elaboradas para a classificação, definição e punição de tais crimes cibernéticos. Os especialistas da área de TI ainda consideram os avanços em estágio embrionário. Apenas um fator é verdadeiramente certo: ao se usar algo de graça, alguém estará efetivamente pagando pelo que está sendo usado.

Concluindo este tópico, vários documentos sugerem o emprego do termo *cracker* pela primeira vez por volta de 1985, para a diferenciação de definição de *hacker*, empregada pela imprensa para definir os responsáveis por qualquer atitude ilegal envolvendo computadores. Assim como os *hackers*, os *crackers* possuem suas classificações em um sumário simples: os *crackers de sistemas* e os *crackers de programas*. Os primeiros são invasores de Sistemas Informatizados interligados em redes, enquanto que o segundo são sabotadores de programas, os quais são ativados ilicitamente. As senhas (*cracks*) destes programas são disponibilizadas na *Web*, para a alegria e deleite dos usuários domésticos. Dentre vários *sites* que disponibilizam *cracks* na *Web*, este endereço é um dos mais acessados: <http://www.westcoastphreakers.com/serve.php?lg=pt&dn=westcoastphreakers.com&ps=03d43a86c626d99fb5c8fe0b5b84b4ff&tk=Q7vLqQ4xu5kKEwji4Ybw5JaYAhUFFrMKHfJMK8AYACAAMlvwoAM4FVCL8KADUOfPowNQoJStDIDLuosPUNa3tRE&le=2009011718000220718&aq=password+cracking>.

Segue uma lista dos *links* para execução de *malwares*<sup>1</sup>, fornecida pelo Governo Brasileiro:

- 1) Amores On-line - cartão virtual - Equipe Carteiro Romântico - Uma pessoa que lhe admira enviou um cartão;
- 2) As fotos que eu tinha prometido. Álbum pessoal de fotos;
- 3) AVG Antivírus - Detectamos que seu *e-mail* está enviando mensagens contaminadas com o vírus w32. bugbear;
- 4) Aviso - você está sendo traído - veja as fotos;
- 5) Aviso - você está sendo traído - veja as imagens do motel;
- 6) Banco do Brasil informa - Sua chave e senha de acesso foram bloqueados - Contrato Pendente - Clique para fazer atualização;
- 7) Big Brother Brasil - ao vivo - quer ver tudo ao vivo e ainda concorrer a promoções exclusivas? Clique na fechadura;
- 8) Câmara dos Dirigentes Lojistas - SPC - Serviço de Proteção ao Crédito - Notificação - Pendências Financeiras - Baixar o arquivo de relatório de pendências;
- 9) Carnaval de 2----- veja o que rolou nos bastidores do carnaval de São Paulo;
- 10) Cartão Terra - eu te amo - webcard enviado através do site Cartões Terra;
- 11) Cartão UOL - I love you - você recebeu um cartão musical - Para visualizar e ouvir escolha uma das imagens;
- 12) Cartões BOL - Você recebeu um cartão BOL;
- 13) Cartõesnico.com - cartõesnico.com - Seu amor criou um cartão para você; Checkline - Consultas de crédito on-line - Consultas no Serasa/SPC;
- 14) Claro Idéias - Grande chance de ganhar meio milhão de reais em ouro e 18 carros;
- 15) Colaneri e Campos Ltda - Ao Gerente de Vendas - orçamento de material e equipamentos em urgência;
- 16) Correio Virtual - hi5 - Seu Amor te enviou este cartão;
- 17) CPF cancelado ou pendente de regularização -verifique; seu CPF está cancelado;

<sup>1</sup> O termo *malware* é proveniente do inglês *malicious software*; é um software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não). Vírus de computador, worms, trojan horses (cavalos de tróia) e spywares são considerados *malware*. Também pode ser considerada *malware* uma aplicação legal que por uma falha de programação (intencional ou não) execute funções que se enquadrem na definição supra citada.

- 18) Declaração de Imposto de Renda de \_\_\_\_\_ 200---- - Ministério da Fazenda - CPF Cancelado ou Pendente de Regularização;
- 19) Ebay - your account could be suspended - Billing Department;
- 20) Embratel - Comunicado de Cobrança - Aviso de Bloqueio;
- 21) Embratel - Notificação Confidencial - Fatura de serviços prestados Clique para detalhamento da fatura;
- 22) Emotion Cards - UOL - Parabéns você recebeu um Presente Virtual;
- 23) Febraban - Guia de Segurança - Febrasoft Security;
- 24) Finasa - Nossa Caixa - Fraudes Bancárias – Febraban;
- 25) Fininvest - débito em atraso - pendências financeiras em seu CPF /CNPJ Ganhe uma viagem a Paris - Guia Paris Lumière;
- 26) Gmail - Gmail Amigo Oculto - Baixar Formulário - E-mail de 1 Giga;
- 27) Humortadela - Piada animada sempre amigos;
- 28) Humortadela - você é 10 - acesse o link e sacaneie;
- 29) Humortadela - você recebeu uma piada animada - Ver Piada Animada;
- 30) Ibest - acesso grátis e fácil - discador ibest - 0800 conexão sem pulso telefônico. Grátis – Download;
- 31) Larissa 22 aninhos - www. mclass. com. br - clique aqui e veja o vídeo;
- 32) Leiam esta informação IMPORTANTE;
- 33) Martins Com Ltda - Setor de Compras – Orçamento;
- 34) Mercado Livre - Aviso - Saldo devedor em aberto na sua conta - e pagamento não for quitado acionaremos departamento jurídico;
- 35) Microsoft - Ferramenta de remoção de softwares Mal-Intencionados do Microsoft Windows - Windows XP fica a cara de quem recebe um cartão Voxcards;
- 36) Microsoft Software - Este conteúdo foi testado e é fornecido a você pela Microsoft Corporation - Veja as novidades;
- 37) Music Cards – Confirmação;
- 38) Necktsun Comércio Ltda - Palmas - Departamento de Vendas – Orçamento;
- 39) Netcard Cartões Virtuais - Emoções de verdade;
- 40) Norton Antivírus - Alerta de Segurança - download do antídoto para o Ms. Bruner;

- 41) Notificação Confidencial - Pendências Financeiras em seu CPF;
- 42) O carteiro - você recebeu um cartão de quem te admira;
- 43) O carteiro. com - tenho uma novidade para você - veja o cartão que preparei;
- 44) O Fuxico - Últimas Notícias - Bomba na TV Brasileira - vídeos de fulano de tal;
- 45) O carteiro.com - seja bem vindo - para visualizar clique aqui;
- 46) Olá, há quanto tempo! Eu me mudei para os Estados Unidos, e perdemos contato... essa! é para bobos!;
- 47) Olha o que a Globo preparou para você neste ano de 2005 ----- Big Brother Brasil nº tal ... - Baixe o vídeo;
- 48) Overture - Promoção para novos assinantes - Tem cliente procurando, tem você oferecendo, vamos juntar os dois. Seja encontrado por quem quer comprar;
- 49) Paparazzo - globo. com - se você gostou de uma espiada no vídeo;
- 50) Parperfeito - Você foi adicionado aos prediletos - Associado do Par Perfeito;
- 51) Passé Livre de 7 dias no Globo Media Center - tem gente que acredita!;
- 52) Promoção Fotolog.net e UBB! - sorteio de 10 Gold Cam por dia - Crie seu fotolog e concorra;
- 53) Radio Terra - dedique uma música;
- 54) Receita Federal - CPF cancelado ou pendente de regularização;
- 55) Saudades de você - Sou alguém que te conheceu há muito tempo, e tive que fazer uma viagem - Espero que goste das fotos;
- 56) SERASA - pendências referentes a seu nome - Extrato de débito;
- 57) SERASA - Regularize seu CPF ou CNPJ - clique para extrato de débitos;
- 58) Sexy Clube - Thaty Rio - Direto do Big Brother - Veja as fotos em primeira mão;
- 59) Sou um amigo seu - você está sendo traído - veja as fotos;
- 60) Symantec - Faça sua atualização do Norton 2005 aqui - Gratuita - Licença para 1 ano grátis;
- 61) Terra Cartões - O meu melhor presente é você;
- 62) Tim pós pago - pendências no SPC - Sistema de Proteção ao Crédito - Serial do Celular;

- 63) [UOL - Promoção Cultural](#) - Cara cadê meu carro;
- 64) [UOL Cartões](#) - Estou com saudades - clique para visualizar;
- 65) [UOL Cartões](#) - Seu amor lhe enviou um cartão - clique para baixar;
- 66) [UOL Cartões](#) - Você recebeu um lindo cartão virtual e 1 vírus também! ;
- 67) [Veja as fotos proibidas](#) das musas do bbb5;
- 68) [Viagens contaminadas com o w32. bugbear](#);
- 69) [Virtual Cards](#) - Um grande abraço da equipe virtual cards - ler cartão;
- 70) [VIVO](#) - Torpedos Web Gratuito - Torpedo Fácil Vivo;
- 71) [Você recebeu um cartão virtual TIM](#);
- 72) [Voxcards](#) - cartão voxcards - para quem você vai mandar um cartão hoje?;
- 73) [Voxcards](#) - mensageiro - você está recebendo um cartão virtual voxcards.

### 4.6.3 PHREAKERS

O objetivo do *phreaker* atual é, na maioria das vezes, a quebra de sistemas de segurança envolvendo a telefonia móvel. Sua intenção é utilizar os serviços de telefonia fixa, pública e celular sem gastar um único centavo. As técnicas geralmente não envolvem ataques excessivamente agressivos a servidores ou redes de operadoras, mas sim um enorme esforço na determinação de falhas de segurança; permitindo a efetiva utilização de programas especiais nos aparelhos e uso de números ilegítimos para a efetuação das ligações (técnica de colanagem).

De acordo com ULBRICH (2007):

*“Phreaker é o cracker dos sistemas telefônicos. Possui conhecimentos avançados de eletrônica e telefonia (principalmente sobre sinalização eletrônica) e pode fazer chamadas de qualquer local sem pagar por elas. Os métodos de fraude incluem transferir as faturas para outros números (válidos ou não), modificar telefones públicos para conseguir crédito ilimitado ou mesmo enganar a central telefônica para que ela não faça o billing”.*

### 4.6.4 DEFACERS

Eles são os “pixadores digitais”, a versão contemporânea dos pixadores de muros tradicionais. Uma ação *defacing* constitui-se basicamente na modificação da página inicial de um *site*, ou qualquer parte dele, pelos mais variados motivos e aspirações. Os *defacers* considerados sérios normalmente apresentam mensagens de protesto e sobre páginas e instituições consideradas danosas ao público ou que tenham praticado qualquer ação considerada repugnante ao bem-comum da comunidade.

Não são raras as vezes que um ataque constituído por *defacers* tenha como único e exclusivo objetivo uma espécie de demonstração de força por parte dos atacantes. De qualquer forma, constitui-se de uma “brincadeira” séria e de conseqüências imprevisíveis.

Um dos sites mais famosos sobre episódios, técnicas, relatos e até mesmo com promoções de competições de *defacing* é o site “Zone-H”, cujo endereço é o <http://www.zone-h.org/>.

#### 4.6.5 ASSUNTOS OU SERVIÇOS DE REDES TÍPICAMENTE NEGLIGENCIADOS PELOS ADMINISTRADORES

Segundo OLIVEIRA (2007), assuntos ou serviços de redes tipicamente negligenciados pelos administrados e que, com certeza, são também “alvos primários” de *crackers* avançados e experientes:

- 1 - *DNS Spoofing*;
- 2 - Direitos de acesso/execução de terceiros;
- 3 - *Trojan Horses* (Vírus conhecido como “Cavalo de Tróia);
- 4 - *Database* (Banco de Dados);
- 5 - *Routing Infrastructure* (Infra-estrutura de rede de computadores);
- 6 - Testes de *IDS*;
- 7 - *WWW Server Side*;
- 8 - *TCP Hijacking*;
- 9 - Teste de *Firewall*;
- 10 - *ISDN* Linhas telefônicas.

- 1- ***Spoofing (falsificação)***: Meio de esconder a verdadeira identidade na rede. Para criar uma identidade enganosa, um invasor usa um falso endereço de fonte que não representa o verdadeiro endereço do pacote. Sendo assim, o *DNS Spoofing* é o desvio da sessão HTTP para o servidor forjado.
- 2- **Direitos de acesso/execução de terceiros**: Deve-se bloquear programas e pastas aos quais usuários não devem ter acesso, aumentando assim, a proteção do Sistema Computacional.
- 3- ***Trojan Horses***: É um programa em que o usuário descuidadamente instala em seu microcomputador e que, aparentemente; não tem problemas, como um programa contendo um pequeno jogo, por exemplo. Ele é instalado e utilizado normalmente, sem nenhum problema, mas ao mesmo tempo que é jogado, o mesmo “abre portas” para que o computador possa ser acessado pelo atacante. Assim, o “Cavalo de Tróia” é um programa que executa as funções normais, para que o usuário não desconfie de nada, mas, em segundo plano;

altera, consideravelmente, as configurações e abre as portas para que o computador do usuário possa ser invadido.

- 4- **Database (Banco de Dados):** O acesso às informações da Base de Dados de uma empresa ou instituição deve ser disponibilizado somente para pessoas credenciadas e autorizadas, pois as informações de uma empresa ou instituição são o seu principal ativo.
- 5- **Routing Infrastructure (Infra-estrutura de rede de computadores):** É a infra-estrutura utilizada para o roteamento de informações, normalmente utilizando um roteador.
- 6- **Testes de IDS (Intrusion Detection System):** O Sistema de Detecção de Intrusos (IDS) é uma ferramenta de *software* utilizada para detectar o acesso não-autorizado de um sistema de computação ou uma rede de computadores. Ele tem a capacidade de alertar em tempo real, ou seja, o administrador é avisado de uma invasão ao mesmo tempo em que efetivamente ocorre a invasão em questão.
- 7- **WWW Server Side:** São páginas desenvolvidas em linguagens para a *Internet*, tais como ASP e PHP. Funcionam ao “lado” do servidor (*Server Side*), porém; por problemas de configuração ou da não-atualização de versões, os Servidores *Web* (*IIS* ou *Apache*, por exemplo), podem tornar acessíveis nossos programas para todos os que estejam navegando na *WWW*. Programas esses que eram para funcionar apenas nos Servidores, o que provoca um grande transtorno de segurança.
- 8- **TCP Hijacking:** Tentativa de “seqüestrar” dados TCP/IP do computador, injetando pacotes que fingem vir de um computador envolvido na sessão em que o usuário efetivamente está.
- 9- **Teste de Firewall:** As regras de segurança do *Firewall* devem ser constantemente testadas, a fim de se evitar a impressão de uma falsa segurança, tornando os dados de uma empresa ou corporação ainda mais vulneráveis.
- 10- **ISDN Linhas telefônicas:** *ISDN (Integrated Service Digital Network)* ou *RDSL (Rate adaptative Digital Subscriber Line)* usa o sistema telefônico comum, ou seja, usa uma linha telefônica convencional; com um computador ligado à *Internet* mediante *modem* comum. É uma séria brecha de segurança, tendo em vista que o usuário não consegue barrar os acessos do usuário invasor por meio de *Firewall* corporativo, então, deve-se ter cuidado de desabilitar todos os *modems* de computadores, limitando ao máximo seu uso, deixando-o somente disponível para casos de extrema necessidade, em prol da segurança de dados.

#### 4.6.6 COMO PENSAM OS HACKERS E OS CRACKERS?

Os *hackers* e *crackers* são especialistas que usam os seus conhecimentos para invadir e conseguir informações (com motivos lícitos ou não). Eles são tão profissionais quantos os *hackers* tradicionais, trancados em laboratórios no MIT ou

em qualquer outra universidade de renome. Os *hackers* associados a qualquer definição da palavra compartilham os mesmos ideais e crenças, com variações locais, mas com um núcleo comum bem definido.

Os *hackers* têm uma característica comum: são aficionados em tudo que envolve computadores, programação, conectividade e tecnologia da informação.

Os *hackers* de qualquer espécie, sejam os do MIT ou sejam até mesmo os *Crime Boyz*, têm em comum também a necessidade de compartilhar o conhecimento e recursos. Isso inclui escrever *software* de código aberto e livre acesso, de divulgar 100% do conhecimento que possui para a comunidade da *Web*, facilitar o acesso a essas informações a qualquer interessado e disponibilizar, sempre que possível, os recursos de computação e de rede de computadores.

Os *hackers* tradicionais, ou seja, segundo o correto significado da palavra; pregam o compartilhamento universal do conhecimento. Há milhares de bons exemplos de compartilhamento *globalizado* e irrestrito de informações na *WWW*, como a própria *Internet* em si; assim como o projeto *Gutenberg* (<http://www.gutenberg.org/>) o projeto *GNU* (<http://www.gnu.org/>) e o *Linux* (<http://www.linux.org/>).

#### 4.6.7 POR QUE A SOCIEDADE TEME OS HACKERS E OS CRACKERS?

Neste tópico, se faz necessário responder a seguinte indagação: Por que a sociedade teme os *hackers* e os *crackers*?

Para a sociedade, a imagem dos *hackers* e/ou *crackers* está intimamente ligada ao crime organizado. Este esteriótipo vem da falta de compreensão do universo digital em que estão inseridos. Eles são vistos como destruidores e ladrões de dados, que se utilizam de meios ilícitos para roubo, vandalismo ou lavagem de dinheiro.

Muito desta imagem é fruto da visão míope promovida pelos meios de comunicação. Nunca o outro lado, o lado do *underground*, o lado da guerrilha, olado da resistência, é levado em conta. Apenas as empresas e os governos, alguns deles autoritários (embora trevestidos de democráticos), têm espaço na mídia quando um evento desses acontece.

De acordo com o estudo acima, conclui-se primeiramente que a sociedade teme os *hackers* e os *crackers* simplesmente porque lhe falta a informação, o conhecimento de quem eles são, suas características, seus objetivos, seus métodos de invasão, etc. Outro fator contribuinte, seria a informação espúria e distorcida sobre os *hackers* (profissionais com ética) que a mídia e os meios de comunicação em massa disponibilizam à sociedade. E também, outro motivo, não menos importante, é por que a sociedade como um todo (Governos, administradores de sistemas computacionais, gerentes de redes, empresas, instituições públicas e/ou privadas, usuários comuns, etc; não dão o devido valor às regras de segurança da informação (conforme item 4.7.3 acima). Assuntos ou serviços de redes os quais são tipicamente negligenciados pelos administrados e que, com certeza, tornam-se “alvos primários” de *crackers* avançados e experientes.

## 4.7 AS ALTERNATIVAS TECNOLÓGICAS E JURÍDICAS PARA PROTEGER EFICAZMENTE A SOCIEDADE E AS ORGANIZAÇÕES COOPERATIVAS DOS “CRIMES VIRTUAIS”

A necessidade de segurança é um fato que vem transcendendo o limite da produtividade e da funcionalidade. Enquanto a velocidade e a eficiência em todos os processos de negócios significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos e falta de novas oportunidades de negócios.

O mundo da segurança, seja pensando em violência urbana ou em *hackers*, é peculiar. Ele é marcado pela evolução contínua, no qual novos ataques têm como resposta novas formas de proteção, que levam ao desenvolvimento de novas técnicas de ataques, de maneira que um ciclo é formado. Não é por acaso que é no elo mais fraco da corrente que os ataques acontecem. De tempos em tempos os noticiários são compostos por alguns crimes ‘da moda’, que vêm e vão. Como resposta, o policiamento é incrementado, o que resulta na inibição daquele tipo de delito.

Os criminosos passam então a praticar um novo tipo de crime, que acaba virando notícia. E o ciclo assim continua. Já foi comprovada uma forte ligação entre seqüestradores e ladrões de banco, por exemplo, na qual existe uma constante migração entre as modalidades de crimes, onde o policiamento é geralmente mais falho.

Esse mesmo comportamento pode ser observado no mundo da informação, de modo que também se deve ter em mente que a segurança deve ser contínua e evolutiva.

Isso ocorre porque o arsenal de defesa usado pela organização pode funcionar contra determinados tipos de ataques; porém, pode ser falho contra novas técnicas desenvolvidas para driblar esse arsenal de defesa.

### 4.7.1 POR QUE SE PREOCUPAR COM A SEGURANÇA DA INFORMAÇÃO?

Alguns fatores podem ser considerados para que a preocupação com a segurança contínua seja justificada:

**a) Entender a natureza dos ataques é fundamental:** é preciso entender que muitos ataques são resultado da exploração de vulnerabilidades, as quais passam a existir devido a uma falha no projeto ou na implementação de um protocolo, aplicação, serviço ou sistema, ou ainda devido a erros de configuração e administração de recursos computacionais. Isso significa que uma falha pode ser corrigida, porém novos *bugs* sempre existirão.

**b) Novas tecnologias trazem consigo novas vulnerabilidades:** é preciso ter em mente que novas vulnerabilidades surgem diariamente. Como novas tecnologias e novos sistemas são sempre criados, é razoável considerar que novas vulnerabilidades sempre existirão e, portanto, novos ataques também serão sempre criados. As redes sem fio (*wireless*), por exemplo, trazem grandes benefícios para as organizações e os usuários, porém trazem também novas vulnerabilidades que podem colocar em risco os negócios da organização.

**c) Novas formas de ataques são criadas:** a própria história mostra uma evolução constante das técnicas usadas para ataques, que estão cada vez mais sofisticadas. A mistura de diferentes técnicas, o uso de tecnologia para cobrir vestígios a cooperação entre atacantes e a criatividade são fatores que tornam a defesa mais difícil do que o habitual.

**d) Aumento da conectividade resulta em novas possibilidades de ataques:** a facilidade de acesso traz como consequência o aumento de novos curiosos e também da possibilidade de disfarce que podem ser usados nos ataques. Além disso, novas tecnologias, principalmente os novos protocolos de comunicação móvel, alteram o paradigma de segurança. Um cenário onde os usuários de telefones celulares são alvos de ataques e usados como porta de entrada para ataques a uma rede corporativa, por exemplo, é completamente plausível.

**e) Existência tanto de ataques direcionados quanto de ataques oportunistas:** apesar de a maioria dos ataques registrados ser oportunística, os ataques direcionados também existem em grande número. Esses ataques direcionados podem ser considerados mais perigosos, pois, existindo a intenção de atacar, a estratégia pode ser cuidadosamente pensada e estudada, e executada de modo a explorar o elo mais fraco da organização. Esses são, geralmente, os ataques que resultam em maiores prejuízos, pois não são feitos de maneira aleatória, como ocorre com os ataques oportunistas. Isso pode ser observado também pelo nível de agressividade dos ataques. Quanto mais agressivo é o ataque, maior é o nível de esforço dispensado em um ataque a um alvo específico. É interessante notar também que a agressividade de um ataque está relacionada com a severidade, ou seja, maiores perdas.

**f) A defesa é mais complexa do que o ataque:** para o *hacker*, basta que ele consiga explorar apenas um ponto de falha da organização. Caso uma determinada técnica não funcione, ele pode tentar explorar outras, até que seus objetivos sejam atingidos. Já para as organizações, a defesa é muito mais complexa, pois exige que todos os pontos sejam defendidos. O esquecimento de um único ponto faz com que os esforços dispensados na segurança dos outros pontos sejam em vão. Isso acaba se relacionando com uma das principais falácias do mundo corporativo: a falsa sensação de segurança. É interessante notar que, quando o profissional não conhece os riscos, ele tende a achar que tudo está seguro com o ambiente. Com isso, a organização passa, na realidade, a correr riscos ainda maiores, que é o resultado da negligência. Isso acontece com os *firewalls* ou com os antivírus, por exemplo, que não podem proteger a organização contra determinados tipos de ataques.

**g) Aumento dos crimes digitais:** o que não pode ser subestimado são os indícios de que os crimes digitais estão se tornando cada vez mais organizados.

As comunidades criminosas contam, atualmente, com o respaldo da própria *Internet*, que permite que limites geográficos sejam transpostos, oferecendo possibilidades de novos tipos de ataques. Além disso, a legislação para crimes digitais ainda está na fase da infância em muitos países, o que acaba dificultando uma ação mais severa para a inibição dos crimes.

Dentre os fatos que demonstram o aumento da importância da segurança, pode-se destacar a rápida disseminação de vírus e *worms*, que são cada vez mais sofisticados. Utilizando técnicas que incluem a engenharia social, canais seguros de

comunicação, exploração de vulnerabilidades e arquitetura distribuída, os ataques visam a contaminação e a disseminação rápida, além do uso das vítimas como origem de novos ataques. A evolução dos ataques aponta para o uso de técnicas ainda mais sofisticadas, como o uso de códigos polimórficos para a criação de vírus, *worms*, *backdoor* ou *exploits*, para dificultar sua detecção. Além disso, ferramentas que implementam mecanismos que dificultam a adoção da forense computacional também já estão sendo desenvolvidos. Os canais ocultos ou cobertos (*covert channels*) tendem a ser usados para os ataques, nos quais os controles são enviados por túneis criados com o uso de HTTPS ou o SSH, por exemplo. O uso de ‘pontes’ de ataques e mecanismos do TCP/IP para dificultar a detecção e investigação igualmente tende a ser cada vez mais utilizado. Ataques a infra-estruturas envolvendo roteamento ou DNS, por exemplo, também podem ser realizados.

Alguns incidentes mostram que os prejuízos com a falta de segurança podem ser grandes. Em 19 de fevereiro de 2003, na manchete do “Jornal da Tarde” intitulada: “*Hacker põe em mão milhões de cartões MasterCard e Visa*”, relatando o roubo de 5,6 milhões de números de cartões de crédito da *Visa* e da *MasterCard* de uma administradora de cartões americana, por exemplo, pode sugerir grandes problemas e inconvenientes para as vítimas.

De acordo com a revista “Época”, edição 252, em 17 de março de 2003, intitulada “*A volta de Melzinha*”, o roubo no Brasil de mais de 152 mil senhas de acesso de grandes provedores de acesso, em março de 2003; resultou em quebra de privacidade e, em muitos casos, perdas bem maiores. No âmbito mundial, variações de *worms* como o *Klez* ainda continuam na ativa, mesmo passado mais de um ano desde seu surgimento.

A primeira versão do *Klez* surgiu em novembro de 2001 e a versão mais perigosa, em maio de 2002. Segundo o site <http://www.message-labs.com>, em março de 2003, o *Klez* era o *worm* mais ativo do mês. Já site <http://tecnologia.terra.com.br/>, em 4 de julho de 2002 foi disponibilizada a manchete: “*Golpe de hacker de Campo Grande atinge cinco bancos*”. Em junho de 2002, um incidente de segurança envolvendo usuários de cinco dos maiores bancos e administradores de cartões de crédito do Brasil resultou em prejuízos calculados em R\$ 100 mil, mostrando que incidentes envolvendo instituições financeiras estão se tornando cada vez mais comuns, seja no Brasil ou em outros países.

Outros incidentes notórios podem ser lembrados, como o que envolveu o *worm Nimda*, em setembro de 2001. Um alto grau de evolução pôde ser observado no *Nimda*, que foi capaz de atacar tanto sistemas *web* quanto sistemas de e-mail. Antes do aparecimento do *Nimda*, um outro *worm*, o *Code Red* (e sua variação *Code Red II*), vinha, e ainda vem, causando grandes prejuízos, não somente às organizações que sofreram o ataque, mas à internet como um todo. Causando lentidão na rede, o *Code Red* resultou em prejuízos estimados em 2,6 bilhões de dólares nos Estados Unidos, em julho e agosto de 2001. Outro notório evento foi a exploração em larga escala de ferramentas para ataques coordenados e distribuídos, que afetaram e causaram grandes prejuízos, durante 2000, a sites como *Amazon Books*, *Yahoo*, *CNN*, *eBay*, *UOL* e *ZipMail*. Somaram-se ainda ataques a sites de comércio eletrônico, notadamente o roubo de informações sobre clientes da *CDNow*, até mesmo dos números de cartões de crédito. Casos de ‘pichações’ de sites *Web* também são um fato corriqueiro, demonstrando a rápida popularização dos ataques a sistemas de computadores.

Porém, os ataques que vêm causando os maiores problemas para as organizações são aqueles que acontecem a partir da sua própria rede, ou seja, os ataques internos.

Somado a isso, está o fato de as conexões entre as redes das organizações alcançarem níveis de integração cada vez maiores. Os ambientes cooperativos, formados a partir de conexões entre organizações e filiais, fornecedores, parceiros comerciais, distribuidores, vendedores ou usuários móveis, resultam na necessidade de um novo tipo de abordagem quanto à segurança. Em oposição à idéia inicial, quando o objetivo era proteger a rede da organização isolando-a das redes públicas, nos ambientes cooperativos o objetivo é justamente o contrário: disponibilizar cada vez mais serviços e permitir a comunicação entre sistemas de diferentes organizações, de forma segura. A complexidade aumenta, pois agora a proteção deve ocorrer não somente contra os ataques vindos da rede pública, mas também contra aqueles que podem ser considerados internos, originados a partir de qualquer ponto do ambiente cooperativo. É interessante observar que o crescimento da importância e até mesmo da dependência do papel da tecnologia nos negócios, somado ao aumento da facilidade de acesso e ao avanço das técnicas usadas para ataques e fraudes eletrônicos, resultam no aumento do número de incidentes de segurança, o que faz com que as organizações devam ser protegidas da melhor maneira possível. Afinal de contas, é o próprio negócio, em forma de bits e bytes, que está em jogo.

Assim, entender os problemas e as formas de resolvê-los torna-se imprescindível, principalmente porque não se pode proteger contra riscos que não se conhece.

#### **4.7.2 QUAL SÃO AS PRINCIPAIS AMEAÇAS À SEGURANÇA DA INFORMAÇÃO EM 2009 E COMO SE PROTEGER DELAS?**

Em 2008, vimos o fortalecimento de novas estratégias de infecção, a criação de *malware* (*software* que se infiltra em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações) tornando-se um negócio lucrativo; e também, o aumento do *scareware* (*software* que ameaça e assusta o usuário para que ele pense que deve baixar atualizações de segurança ou visitar determinados *sites* para estar protegido), entre outras ameaças à segurança digital. Fazer previsões é tarefa difícil, mas com base no que foi observado em 2008, empresas como *Symantec*, *Websense* e *Protagon* apontam tendências e fornecem um cenário do que pode ocorrer em 2009. Automatização de ataques, crescimento dos falsos programas de segurança, do *spam* (mensagens eletrônicas não solicitadas) e das *botnets* (redes *spammers*) são algumas destas tendências. O usuário, seja doméstico ou corporativo, precisa estar atento e bem informado.

Segundo o coordenador de TI da *Protagon* Segurança de Dados, Robson de Roma: "O surgimento e a utilização cada vez maior de serviços oferecidos através da Internet, aliado ao crescimento do uso de dispositivos móveis, deverá ser um dos principais focos das ameaças para 2009. Os Sites com scripts maliciosos deverão ter uma disseminação mais elevada usando o método *drive-by-download*, que automatiza os ataques já que o usuário é infectado ao visitar sites com códigos maliciosos embutidos".

A explosão de variantes de *malware* e o aumento do número de novas ameaças baseadas na *Web* também são apontados pela *Symantec* como tendências fortes em 2009. A *Websense* prevê que a "nuvem" da internet será cada vez mais usada para fins maliciosos. "A 'nuvem' pode ser usada para enviar um simples spam ou lançar ataques mais sofisticados, incluindo hospedagem de códigos maliciosos e testes destes códigos", afirma um relatório recente da companhia.

Os especialistas apontam também o crescimento das *botnets* (redes de PCs zumbis, máquinas infectadas que, sem o conhecimento do usuário, são utilizadas para diversos fins, de hospedagem de sites ilegais e depósito de material pornográfico a ataques DDoS<sup>1</sup>) como uma forte tendência, principalmente devido ao retorno financeiro que elas representam. Esperam, ainda, um aumento significativo de ameaças a dispositivos móveis como *smartphones*, graças à popularização destas novas tecnologias.

<sup>1</sup> DDoS: Um ataque distribuído de negação de serviço (também conhecido como DDoS, um acrônimo em inglês para Distributed Denial of Service).

Sendo assim, o usuário, doméstico ou corporativo, deve ficar atento. Além da recomendação habitual de manter programas e sistemas operacionais sempre atualizados, é salutar que o mesmo proceda da seguinte maneira:

1 - Ter ferramentas de segurança com alto poder de detecção pró-ativa, capazes de identificar qualquer variante de *malware* a qualquer momento sem esperar pela atualização de *software* ou criação de vacina;

2 - Atuar na prevenção pela educação: o usuário deve procurar manter-se informado, buscando conhecimento sobre o assunto em fontes confiáveis;

3 - Invista em software de segurança confiável, multifacetado. Busque um software de segurança para PC abrangente e multifacetado que proteja contra vírus, *spyware*<sup>1</sup>, *adware*<sup>2</sup>, *hackers*, e-mails indesejáveis, *phishing scams* e roubo de identidade. Escolha uma marca em que você possa confiar, como *McAfee* (<http://www.mcafee.com/br/>), *Norton Antivírus* (<http://www.symantec.com/pt/br/index.jsp>), *Panda* ([www.pandasoftware.com](http://www.pandasoftware.com)), *AVG Antivírus* ([www.avgbrasil.com](http://www.avgbrasil.com)), dentre outros.

4 - Sempre acesse a *Internet* protegido por um *firewall*. Um *firewall* oferece uma camada de segurança entre o PC e a *Internet*, e ajuda a impedir que *hackers* roubem sua identidade, destrua seus arquivos ou use seu PC para atacar outras pessoas;

5 - Use um PC que você saiba que é seguro. Os *hackers* podem facilmente recuperar dados importantes enviados em uma conexão com a *Internet* não segura. Se precisar enviar informações importantes ou fazer uma transação on-line, use um PC que saiba que é seguro e lembre-se de que há muitos aspectos de segurança. Alguns computadores têm apenas o mínimo, enquanto outros, como o *McAfee Total Protection*, possuem segurança abrangente;

<sup>1</sup> Spyware: consiste num programa automático de computador, que recolhe informações sobre o usuário, sobre os seus costumes na *Internet* e transmite essa informação a uma entidade externa na *Internet*, sem o seu conhecimento nem o seu consentimento.

<sup>2</sup> Adware: é qualquer programa que automaticamente executa, mostra ou baixa publicidade para o computador depois de instalado ou enquanto a aplicação é executada.

6 - Preste atenção aos *phishing scams*. Os *Phishing scams* usam *e-mails* e *Web sites* fraudulentos, mascarados como negócios legítimos, para atrair consumidores desatentos a revelarem informações particulares da conta ou de *login*. Mesmo que você tenha segurança para o PC, pode ser que visite um *Web site* mal-intencionado, sem saber. Negócios legítimos nunca solicitarão que você atualize suas informações pessoais por e-mail. Sempre verifique os endereços da *Web* antes de enviar suas informações pessoais;

7 - Proteja sua conexão sem fio. Seu computador está em risco se você acessa a *Internet* em uma rede *Wi-Fi*. Como as ondas de rádio de sua conexão sem fio passam pelas paredes, um *hacker* com uma simples antena pode atacar seu computador, a milhas de distância, para roubar suas informações e usar sua conexão sem fio para sua própria comunicação. Sempre use uma proteção adicional para uma conexão *Wi-Fi*;

8 - Nunca instale programas potencialmente indesejáveis (PUPs), como *spyware* ou *adware*, em seu PC. Muitos programas gratuitos que você baixa pela *Internet* podem parecer inofensivo, porém são desenvolvidos especificamente para serem maliciosos e monitorar seus pressionamentos de tecla, rastrear seus *logins* na *Internet*, transmitir suas informações confidenciais ou redirecionar o navegador para *Web sites* simulados. Alguns desses programas também podem ser instalados em sua máquina quando você clica no *link* de propaganda na *Internet*. Com o software de segurança, você pode fazer com que esses programas não sejam instalados. Nunca instale programas prontamente, a menos que esteja familiarizado com o *Web site* e tenha lido todo o contrato de licença do usuário final;

9 - Não responda a cadeias de e-mails. Mesmo com a segurança para PC, algumas cadeias encaminhadas por seus amigos podem solicitar informações pessoais. Não baixe arquivos de amigos e familiares, a menos que saiba que o conteúdo do arquivo é seguro;

10 - Monitore seus extratos de crédito e fique atento. Pelo menos uma vez por ano, verifique seu histórico de crédito. Esta é uma das melhores formas de descobrir se alguém está usando suas informações financeiras pessoais sem seu conhecimento. Visite o site de suporte do *Gateway*, para saber as últimas dicas

para manter seu computador em segurança, ou o *site* da *Federal Trade Commission* (<http://www.ftc.gov/>), para se manter atualizado sobre as últimas tendências de roubo de identidade;

11 - Monitore a atividade on-line de seus filhos. Limite o tempo que seus filhos gastam *on-line*. Instale e use um *software* de controle dos pais que lhe permita monitorar a atividade *on-line* de seus filhos, além de impedir que acessem *Web sites* indesejáveis e que compartilhem informações pessoais por comunicação *on-line*; e

12 - Faça *backups* regulares dos dados críticos. Mantenha uma cópia dos arquivos importantes em mídia removível, como discos *Zip* ou *CDs* regraváveis (*CD-R* ou *CD-RW*). Use ferramentas de *backup* do *software*, se disponíveis, e armazene os discos de *backup*, em caso de emergência.

#### **4.7.3 O DIREITO OBJETIVO E OS “CRIMES CIBERNÉTICOS”**

O “Direito Objetivo” é o conjunto de normas que o Estado mantém em vigor. É aquele proclamado como ordenamento jurídico e, portanto, *fora* do sujeito de direitos. Essas normas vêm através de sua fonte formal: a Lei. O direito objetivo constitui uma entidade objetiva frente aos sujeitos de direitos, que se regem segundo ele.

É muito antiga a noção de que Direito e Sociedade são elementos inseparáveis. “Onde estiver o homem, aí deve estar o Direito”, diziam os romanos. A cada dia a Ciência Jurídica se torna mais presente na vida dos indivíduos, porque sempre as relações sociais vão-se tornando mais complexas.

A *Internet*, a grande rede de computadores, tornou essa percepção ainda mais clara. Embora, nos primeiros anos da rede tenham surgido mitos sobre sua “imunidade” ao Direito, esse tempo passou e já se percebe a necessidade de mecanismos de auto-regulação e hetero-regulação, principalmente por causa do caráter ambivalente da *Internet*.

O jus-filósofo Celso Ribeiro Bastos, nos seus *Comentários à Constituição do Brasil*, percebeu essa questão, ao asseverar que:

*“A evolução tecnológica torna possível uma devassa na vida íntima das pessoas, insuspeitada por ocasião das primeiras declarações de direitos”* (BASTOS,1989). Força é convir que não se pode prescindir do Direito, para efeito da prevenção, da reparação civil e da resposta penal, quando necessária.

Tendo em vista as origens da *Internet*, é quase um contra-senso defender a idéia de que o ciberespaço co-existe com o "mundo real" como uma sociedade libertária ou anárquica. Isto porque a cibernética — que se aplica inteiramente ao estudo da interação entre homens e computadores — é a ciência do controle. A própria rede mundial de computadores, como um sub-produto da Guerra Fria, foi pensada, ainda com o nome de Arpanet (*Advanced Research Projects Agency*), para propiciar uma vantagem estratégica para os Estados Unidos, em caso de uma conflagração nuclear global contra a hoje extinta União Soviética.

A *WWW – World Wide Web*, que popularizou a *Internet*, propiciando interatividade e o uso de sons e imagens na rede, foi desenvolvida em 1990 no CERN — *Organisation Européenne pour la Recherche Nucléaire/European Organization for Nuclear Research*, pelo cientista Tim Berners-Lee. O CERN, cujo site é <http://public.web.cern.ch/public/>, é uma organização internacional de pesquisas nucleares em física de partículas, situada nas proximidades de Genebra, na Suíça, e fundada em 1954. Atualmente a sua convenção-constituente tem a ratificação de vinte Estados-partes.

Além dessa origem pouco vinculada à idéia de liberdade, a grande rede não tem existência autônoma. As relações que se desenvolvem nela têm repercussões no "mundo real". O virtual e o real são apenas figuras de linguagem (um falso dilema), não definindo, de fato, dois mundos diferentes, não dependentes. Em verdade, tudo o que se passa no ciberespaço acontece na dimensão humana e depende dela.

Por conseguinte, a vida *online* nada mais é do que, em alguns casos, uma reprodução da vida "real" somada a uma nova forma de interagir. Ou seja, representa diferente modo de vida ou de atuação social que está sujeito às mesmas restrições e limitações ético-jurídicas e morais aplicáveis à vida comum (não eletrônica), e que são imprescindíveis à convivência. Tudo tendo em mira que não existem direitos absolutos e que os sujeitos ou atores desse palco virtual e os objetos desejados, protegidos ou ofendidos são elementos da cultura ou do interesse humano.

Mas a *Internet* não é só isso. No que nos interessa, a revolução tecnológica propiciada pelos computadores e a interconexão dessas máquinas em grandes redes mundiais, extremamente capilarizadas, é algo sem precedentes na história humana, acarretado uma revolução jurídica de vastas proporções, que atinge institutos do direito tributário, comercial, do consumidor, temas de direitos autorais e traz implicações à administração da Justiça, à cidadania e à privacidade.

Não é por outra razão que, do ponto de vista cartorial (direito registrário), a *Internet* já conta com uma estrutura legal no País, representada pelo Comitê Gestor da *Internet* no Brasil, que delegou suas atribuições à FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo, e tem regulamentado principalmente a adoção, o registro e a manutenção de nomes de domínio na rede brasileira.

Assim, verifica-se que não passam mesmo de mitos as proposições de que a *Internet* é um espaço sem leis ou terra de ninguém, em que haveria liberdade

absoluta e onde não seria possível fazer atuar o Direito Penal ou qualquer outra norma jurídica. É conveniente ressaltar que não se defende uma intervenção desnecessária ou máxima do Direito, no ciberespaço, ou em parte alguma. O que se preconiza é a atuação razoável do Direito para assegurar proteção a bens jurídicos valiosos, quando não seja possível conferir essa proteção por outros meios igualmente eficazes.

Estabelecido que a incidência do Direito é uma necessidade inafastável para a harmonização das relações jurídicas *ciberespaciais*, é preciso rebater outra falsa idéia a respeito da Internet: a de que seriam necessárias muitas leis novas para a proteção dos bens jurídicos a serem tutelados pelo Direito Penal da *Internet*. Isto é uma falácia. Afinal, conforme o Ministro Sepúlveda Pertence, do Supremo Tribunal Federal (STF), a invenção da pólvora não mudou a forma de punir o homicídio.

O *Habeas Corpus* 76689/PB, Relator Ministro Sepúlveda Pertence, 1ª Turma, STF:

*"Crime de Computador: publicação de cena de sexo infanto-juvenil (ECA, art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte. 1. O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" — ao contrário do que sucede, por exemplo, aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar [preencher] lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial".*

Destarte, a legislação aplicável aos conflitos cibernéticos será a já vigente, com algumas adequações na esfera infraconstitucional. Como norma-base, teremos a Constituição Federal (CF/1988), servindo as demais leis para a proteção dos bens jurídicos atingidos por meio do computador, sendo plenamente aplicáveis o Código Civil, o Código de Defesa do Consumidor, a Lei dos Direitos Autorais, a Lei do *Software* e o próprio Código Penal (CP/1940), sem olvidar a Lei do *Habeas Data*.

Os bens jurídicos ameaçados ou lesados por crimes informáticos merecerão proteção por meio de tutela reparatória e de tutela inibitória. Quando isso seja insuficiente, deve incidir a tutela penal, fundada em leis vigentes e em tratados internacionais, sempre tendo em mira o princípio da inafastabilidade da jurisdição, previsto no art. 5º, inciso XXXV, da Constituição Federal.

A atuação do Direito Penal será imprescindível em alguns casos, por conta da natureza dos bens jurídicos em jogo. Pois, pela *web* e no ciberespaço circulam valores, informações sensíveis, dados confidenciais, elementos que são objeto de delitos ou que propiciam a prática de crimes de variadas espécies. Nas vias telemáticas, transitam nomes próprios, endereços e números de telefone, números de cartões de crédito, números de cédulas de identidade, informações bancárias, placas de veículos, fotografias, arquivos de voz, preferências sexuais e gostos pessoais, opiniões e idéias sensíveis, dados escolares, registros médicos e informes policiais, dados sobre o local de trabalho, os nomes dos amigos e familiares, o número do *IP* — *Internet Protocol*<sup>1</sup>, o nome do provedor de acesso, a versão do navegador de Internet (*browser*), o tipo e versão do sistema operacional instalado no computador.

A interceptação de tais informações e dados ou a sua devassa não autorizada devem ser, de algum modo, tipificadas, a fim de proteger esses bens que são relevantes à segurança das relações cibernéticas e à realização da personalidade humana no espaço eletrônico.

Como escreveu o ilustre literário Fernando Pessoa: "*Navegar é preciso*". E no mar digital, tanto quanto nos oceanos desbravados pelas naus portuguesas, há muitas "feras" a ameaçar os *internautas* incautos, a exemplo do Estado e de suas agências (vorazes e ameaçadores como tubarões); dos *ciberdelinqüentes* (elétricos e rápidos como enguias); de algumas empresas (sedutoras e enganosas como sereias); dos bancos de dados centralizados (pegajosos e envolventes como polvos); e de certos provedores (oportunistas comensais como as rêmoras).

<sup>1</sup> *Internet Protocol (IP)*: Número que segue padrão universal e que identifica um computador quando conectado à *Internet*.

O maior especialista norte-americano em Direito da *Internet*, Lawrence Lessig, adverte que a própria arquitetura dos programas de computador que permitem o funcionamento da *Internet* como ela é pode se prestar à regulação da vida dos cidadãos *online* tanto quanto qualquer norma jurídica (LESSIG, 1999).

Uma nova sociedade, a sociedade do ciberespaço (LESSIG, 1999) surgiu nos anos noventa, tornando-se o novo foco de utopias. "*Here freedom from the state would reign. If not in Moscow or Tblisi, then here in cyberspace would we find the ideal libertarian society*". Traduzindo-se para o português: "*Aqui a liberdade do estado teria reinado. Se não, em Moscow ou Tblisi, então aqui no ciberespaço iríamos encontrar o ideal libertário da sociedade*".

A idéia anárquica de *Internet* tem nítida relação — que ora apontamos — com o movimento abolicionista, do qual Louk Hulsman (HULSMAN, 1997), o qual prega o fim do sistema penal, é um dos maiores defensores. No entanto, segundo Lawrence Lessig, a etimologia da palavra "ciberespaço" remete à cibernética, que é a ciência do controle à distância. "*Thus, it was doubly odd to see this celebration of non-control over architectures born from the very ideal of control*" (LESSIG, 1999). Traduzindo-se para o português, também: "*Assim, foi duplamente curioso ver essa festa de não-controle sobre arquiteturas, nascido a partir da própria idéia de controle*".

Posicionando-se, *Lawrence Lessig* pontua que não há liberdade absoluta na *Internet* e que não se pode falar no afastamento total do Estado. O ideal seria haver uma "constituição" para a *Internet*, não no sentido de documento jurídico escrito — como entenderia um publicista —, mas com o significado de "arquitetura" ou "moldura", que estruture, comporte, coordene e harmonize os poderes jurídicos e sociais, a fim de proteger os valores fundamentais da sociedade e da *cibercultura*.

## PARTE V

### 5 CONCLUSÕES

Assim como não há ambiente de informática 100% seguro, também não há fraude ou crime em TI que não deixe, em plataformas tecnológicas razoavelmente estruturadas, rastros suficientes para que se chegue a seus autores com relativa facilidade. É só questão de persistência e competência técnica, recursos esses abundantes nas principais instituições financeiras que sempre trabalham em parceria com as Polícias Estaduais e Federal, embora nosso aparato policial ainda careça de maior capacitação na área.

Esperamos que o futuro da “*segurança virtual*” na *Internet* seja promissor, assim que como a inserção digital seja uma realidade, em todos os seguimentos da sociedade, possibilitando que uma grande camada da população mundial possa ter acesso a essa nova tecnologia. Segundo a tendência atual é provável que isso venha a acontecer nas próximas décadas, onde os *internautas* poderão dominar e desfrutar de todos os recursos e benefícios da informática. Mas, para que isso efetivamente ocorra de forma acelerada e pragmática, é necessário que nossas lideranças governamentais tomem atitudes para que a *Internet* seja protegida contra toda e qualquer tipo de “*crime cibernético*”, a fim de erradicar da “*Grande Rede*” as extorsões e fraudes, a pirataria de softwares, a pedofilia e a pornografia, dentre outros.

## Parte VI

### 6 REFERÊNCIAS

#### 6.1 Referências Bibliográficas

NAKAMURA, E., GEUS, P. **SEGURANÇA DE REDES EM AMBIENTES COOPERATIVOS**. São Paulo: Novatec Editora, 2007, 482p.

ULBRICH, H., VALLE, D. **UNIVERSIDADE HACKER**. São Paulo: Digerati Books, 2007, 352p.

OLIVEIRA, W. **DOSSIÊ HACKER: Técnicas profissionais para conhecer e proteger-se de ataques!** São Paulo: São Paulo: Digerati Books, 2007, 288p.

BURNETT, S., PAINE, S. **CRIPTOGRAFIA E SEGURANÇA: O guia oficial RSA**. Rio de Janeiro: Elsevier, 2002, 367p.

HOGLUND, G., MCGRAW, G. **COMO QUEBRAR CÓDIGOS: A arte de explorar (e proteger) software**. São Paulo: Pearson Makron Books, 2006, 424p.

BASTOS, Celso Ribeiro. **COMENTÁRIOS À CONSTITUIÇÃO DO BRASIL: São Paulo: Saraiva, 1989, vol. 2, p. 62.**

GUIMARÃES, A. **SEGURANÇA EM REDES PRIVADAS VIRTUAIS – VPNS: São Paulo: Brasport, 2000.**

CARVALHO, Gustavo de. **TECNOLOGIAS DE ACESSO À INTERNET: São Paulo: Novatec, 2001.**

FILHO, João Rocha Braga. **OS DADOS DE SUA EMPRESA ESTÃO ESGUROS? DUVIDO!** São Paulo: Brasport, 2000.

GALLO, M.A. **COMUNICAÇÃO ENTRE COMPUTADORES E TECNOLOGIAS DE REDE**. New York, EUA: Thomson, 1994.

MARTINI, Renato. **CRIPTOGRAFIA E CIDADANIA DIGITAL**. São Paulo, Cidade Moderna, 2001.

QUEIROZ, Regis Magalhães Soares de. **DIREITO E INTERNET – ASPECTOS JURÍDICOS RELEVANTES**. Edipro – Edições Profissionais Ltda, São Paulo, 2000, P. 398.

DINIZ, Davi Monteiro. **DOCUMENTOS ELETRÔNICOS, ASSINATURAS DIGITAIS – DA QUALIFICAÇÃO JURÍDICA DOS ARQUIVOS DIGITAIS COMO DOCUMENTOS**. LTR, São Paulo, 1999, P. 28.

LESSIG, Laurence. **CODE AND OTHER LAWS OF CYBERSPACE**: New York, EUA, 1999, p.4.

HULSMAN, L. H. C; BERNAT DE CELIS, Jacqueline. **PENAS PERDIDAS** : o sistema penal em questão. 2. ed. Niterói: Rio de Janeiro, 1997. 180p.

FERREIRA, Ivete Senise. **A CRIMINALIDADE INFORMÁTICA - IN DIREITO & INTERNET**: aspectos jurídicos relevantes. Bauru: Edipro, 2000, p. 207.

DOYLE, Charles. **THE USA PATRIOT ACT: A LEGAL ANALYSIS**: 15 de abril de 2002. *Congressional Research Service. The Library of the Congress*. p. 02, 54.

CANOTILHO, José Joaquim Gomes. **DIREITO CONSTITUCIONAL E TEORIA DA CONSTITUIÇÃO**: 3.ed. Coimbra: Livraria Almedina, 1999. p. 1191.

ANDRADE, JOSÉ CARLOS VIEIRA DE. **OS DIREITOS FUNDAMENTAIS NA CONSTITUIÇÃO PORTUGUESA DE 1976**: COIMBRA: COIMBRA EDITORA, 1998. P 220, 224.

ALVAREZ, Anselmo Prieto e FILHO, Wladimir Novaes. **A CONSTITUIÇÃO DOS EUA ANOTADA**: São Paulo: LTR, 2001. p. 65, 70 e 71.

TRINDADE, Antônio Augusto Cançado. **A PROTEÇÃO INTERNACIONAL DOS DIREITOS HUMANOS**: São Paulo: Ed. Saraiva, 1991,p. 16-17.

MOCCIA, Sérgio. **EMERGÊNCIA E DEFESA DOS DIREITOS FUNDAMENTAIS. IN REVISTA DE CIÊNCIAS CRIMINAIS**: Ano 07, nº 25. Janeiro – Março de 1999, São Paulo, p. 58.

CAETANO, Marcelo. **DIREITO CONSTITUCIONAL**: 1ª edição. Volume I, Rio de Janeiro: Forense, 1977 p.123.

FOINA, A. **PUBLICAÇÃO DO CIBERPESQUISA. CENTRO DE ESTUDOS E PESQUISAS EM CIBERCULTURA**. Disponível em [http://www.facom.ufba.br/ciberpesquisa/404nOtF0und/404\\_26.htm](http://www.facom.ufba.br/ciberpesquisa/404nOtF0und/404_26.htm). Acessado em: 15 de julho de 2008.

GOVERNO DO ESTADO DO MATO GROSSO DO SUL. **PORTAL BRASIL CONTRA A PEDOFILIA**. Disponível em <http://brasilcontraapedofilia.wordpress.com/2007/07/01/leis-estaduais-em-vigor-sobre-as-lan-houses-e-cyber-cafes-do-estado-do-mato-grosso-do-sul/>. Acessado em: 19 de julho de 2008.

GOVERNO DO ESTADO DE SÃO PAULO. **PORTAL BRASIL CONTRA A PEDOFILIA**. Disponível em <http://brasilcontraapedofilia.wordpress.com/0000/00/00/leis-estaduais-em-vigor-sobre-as-lan-houses-e-cyber-cafes-do-estado-de-sao-paulo/>. Acessado em: 19 de julho de 2008.

CONGRESSO NORTE-AMERICANO. **PORTAL PUBLICAÇÕES DO CONGRESSO NORTE-AMERICANO.** Disponível em [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107\\_cong\\_public\\_laws&docid=f:publ056.107](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107). Acessado em: 16 de julho de 2008.

BIBLIOTECA DO CONGRESSO NORTE-AMERICANO. **PORTAL LIVRARIA DO CONGRESSO NORTE-AMERICANO.** Disponível em <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:H.R.3004>. Acessado em: 16 de julho de 2008.

DEPARTAMENTO DE JUSTIÇA NORTE-AMERICANO. **PORTAL PUBLICAÇÕES LEGISLAÇÕES DO DEPARTAMENTO DE JUSTIÇA DOS EUA.** Disponível em [http://www.usdoj.gov/criminal/cybercrime/1030\\_new.html](http://www.usdoj.gov/criminal/cybercrime/1030_new.html). Acessado em: 16 de julho de 2008.

WIKIPEDIA. **PORTAL DA ENCICLOPÉDIA LIVRE.** Disponível em <http://pt.wikipedia.org/>. Acessado em: 19 de julho de 2008.

MEIRELLES, F. **PORTAL DE PERIÓDICOS VALOR ONLINE.** Disponível em <http://www.economiabr.net/2002/03/03/Internet.html>. Acessado em: 15 de julho de 2008.

PIMENTEL, C. **PORTAL DE NOTÍCIAS SERPRO.** Disponível em [http://www.serpro.gov.br/noticias-antigas/noticias-2006/20060927\\_01](http://www.serpro.gov.br/noticias-antigas/noticias-2006/20060927_01). Acessado em: 15 de julho de 2008.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. **PORTAL NOTÍCIAS IBGE. PORTAL BRASILEIRO DA PESQUISA ANUAL DE SERVIÇOS – PAS.** Disponível em [http://www.ibge.gov.br/home/presidencia/noticias/noticia\\_visualiza.php?id\\_noticia=933&id\\_pagina=1](http://www.ibge.gov.br/home/presidencia/noticias/noticia_visualiza.php?id_noticia=933&id_pagina=1). Acessado em: 15 de julho de 2008.

TERMOS E DEFINIÇÕES DO TERMO *HACKER*. **SITE QUE TRATA TERMOS E DEFINIÇÕES DO TERMO HACKER.** Disponível em <http://www.catb.org/jargon/html/index.htm>. Acessado em: 17 de janeiro de 2009.

PORTAIS DE INFORMAÇÃO. **PORTAIS DE INFORMAÇÕES DIVERSAS.** Disponíveis em <http://www.ig.com.br/>, <http://www.ibest.com.br/>, <http://www.uol.com.br/>, <http://www.pop.com.br/>, <http://www.terra.com.br/portal/>, <http://www.cnn.com/espanol/>, <http://www.estadao.com.br/home/index.shtm>, e <http://www.folha.uol.com.br/>. Acessados no período de: 1º de junho de 2008 a 21 de janeiro de 2009.

PORTAL SOBRE TECNOLOGIA DA INFORMAÇÃO. **PORTAIS SOBRE TECNOLOGIA DA INFORMAÇÃO.** Disponível em <http://www.uol.com.br/computerworld/news/>, <http://tecnologia.ig.com.br/>, <http://tecnologia.terra.com.br/ultimas/galerias/0,,E14795,00.html>,

<http://poptecnologia.pop.com.br/>, <http://www.estadao.com.br/tecnologia/>,  
<http://www1.folha.uol.com.br/folha/informatica/> e <http://tecnologia.uol.com.br/>.  
Acessados no período de: 1º de junho de 2008 a 21 de janeiro de 2009.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **PORTAL DO INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA – IBGE**. Disponível em <http://www.ibge.gov.br>. Acessado em 20 de dezembro de 2008.

REDE NACIONAL DE ENSINO E PESQUISA. **PORTAL DA REDE NACIONAL DE ENSINO E PESQUISA – RNP**. Disponível em <http://www.rnp.br/rnp2>. Acessado em 25 de dezembro de 2008.

FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO. **PORTAL DA FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO – FEE / UNICAMP**. Disponível em <http://www.fee.unicamp.br/>. Acessado em 1º de janeiro de 2009.

DISPONIBILIZAÇÃO DE SENHAS (CRACKS) VIA INTERNET. **PORTAL DA WEST COAST PHREAKERS**. Disponível em <http://www.westcoastphreakers.com/serve.php?lg=pt&dn=westcoastphreakers.com&ps=03d43a86c626d99fb5c8fe0b5b84b4ff&tk=Q7vLqQ4xu5kKEwji4Ybw5JaYAhUFFrMKHfJMK8AYACAAMlvwoAM4FVCL8KADUOfPowNQoJStDIDLuosPUNa3tRE&le=2009011718000220718&aq=password+cracking>. Acessado em 17 de janeiro de 2009.

COMPARTILHAMENTO UNIVERSAL E IRRESTRITO DE INFORMAÇÕES. **COMPARTILHAMENTO UNIVERSAL E IRRESTRITO DE INFORMAÇÕES – PORTAL PROJETO GNU**. Disponível em <http://www.gnu.org/>. Acessado em 17 de janeiro de 2009.

COMPARTILHAMENTO UNIVERSAL E IRRESTRITO DE INFORMAÇÕES. **COMPARTILHAMENTO UNIVERSAL E IRRESTRITO DE INFORMAÇÕES – PORTAL LINUX**. Disponível em <http://www.linux.org/>. Acessado em 17 de janeiro de 2009.

COMPARTILHAMENTO UNIVERSAL E IRRESTRITO DE INFORMAÇÕES. **COMPARTILHAMENTO UNIVERSAL E IRRESTRITO DE INFORMAÇÕES – PORTAL GUTENBERG**. Disponível em [http://www.gutenberg.org/wiki/Main\\_Page](http://www.gutenberg.org/wiki/Main_Page). Acessado em 17 de janeiro de 2009.

PORTAL SOBRE DEFACING. **PORTAL SOBRE DEFACING – ZONE-H**. Disponível em <http://www.zone-h.org/>. Acessado em 18 de janeiro de 2009.

JORNAL BAIXADA SANTISTA. **JORNAL BAIXADA SANTISTA**. Disponível em [http://www.jornalbaixadasantista.com.br/conteudo/mp\\_recomenda\\_monitoramento\\_chats2008.asp](http://www.jornalbaixadasantista.com.br/conteudo/mp_recomenda_monitoramento_chats2008.asp). Acessado em 19 de janeiro de 2009.

MCAFEE. **MCAFEE ANTIVÍRUS**. Disponível em <http://www.mcafee.com/br/>. Acessado em 20 de janeiro de 2009.

NORTON. **NORTON ANTIVÍRUS**. Disponível em <http://www.symantec.com/pt/br/index.jsp>. Acessado em 20 de janeiro de 2009.

PANDA. **PANDA ANTIVÍRUS**. Disponível em [www.pandasoftware.com](http://www.pandasoftware.com). Acessado em 20 de janeiro de 2009.

AVG. **AVG ANTIVÍRUS**. Disponível em [www.avgbrasil.com](http://www.avgbrasil.com). Acessado em 20 de janeiro de 2009.

FEDERAL TRADE COMMISSION. **FEDERAL TRADE COMMISSION**. Disponível em <http://www.ftc.gov/>. Acessado em 20 de janeiro de 2009.

EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH. **PORTAL DA ORGANIZAÇÃO EUROPÉIA PARA PESQUISAS NUCLEARES**. Disponível em <http://public.web.cern.ch/public/>. Acessado em 20 de janeiro de 2009.

PORTAL TERRA. **PORTAL TERRA – TECNOLOGIA**. Disponível em <http://tecnologia.terra.com.br/interna/0,,OI3452986-EI4805,00-Novo+virus+ja+infectou+quase+milhoes+de+computadores.html>. Acessado em 21 de janeiro de 2009.

PORTAL TERRA. **PORTAL TERRA – TECNOLOGIA**. Disponível em <http://tecnologia.terra.com.br/interna/0,,OI1927458-EI4805,00.html>. Acessado em 21 de janeiro de 2009.

TALANYAN, Nancy. **THE HOMELAND SECURITY ACT: THE DECLINE OF PRIVACY; THE RISE OF GOVERNMENT SECRECY**. Disponível em <http://www.bordc.org/HSAsummary.pdf>. Acessado em 21 de Janeiro de 2009.

MELLO, Sérgio Vieira de. **DISCURSO DE SÉRGIO VIEIRA DE MELLO, ALTO COMISSÁRIO PARA DIREITOS HUMANOS EM RAZÃO DO TERCEIRO COMITÊ DA ASSEMBLÉIA GERAL DA ONU, EM 04/11/2002**. Disponível em <http://www.iccnw.org/documents/statements/unbodies/deMelloICCjudges4Nov02.pdf>. Acessado em 21 de janeiro de 2009.

FOLHA DE SÃO PAULO. **FOLHA DE SÃO PAULO - CADERNO DE DOMINGO**. Ed. 5 de março de 2000.

REVISTA INFORMÁTICA HOJE. **REVISTA INFORMÁTICA HOJE**. Ano 15, Nº 484, Ed. 1º de novembro de 1999.

REVISTA ÉPOCA. **REVISTA ÉPOCA**. Ano II, Nº 91, Editora Globo, Ed. 14 de fevereiro de 2000.

REVISTA LINK. **REVISTA LINK**. Ano 5, Nº 50, 1º de março 2000.

REVISTA OBSERVADOR ECONÔMICO E FINANCEIRO. **REVISTA OBSERVADOR ECONÔMICO E FINANCEIRO**: Abreu, Sílvio Fróes, "Os Velhos e os Novos Institutos de Tecnologia", 24 de novembro de 1959.

REVISTA VEJA. **REVISTA VEJA - VIDA DIGITAL**. Ano 32, Editora Abril, Nº 51.

REVISTA VEJA. **REVISTA VEJA.** Ed. 1.632, Ano 33, Nº 3, Editora Abril, 19 de janeiro de 2000.

REVISTA VEJA. **REVISTA VEJA.** Ed. 1.637, Ano 33, Nº 8, Editora Abril, 23 de fevereiro de 2000.

## 6.2 ANEXOS

**Tabela 1: População e número de usuários Internet no mundo (2003)**

Países e regiões	População dos países e regiões (% da população mundial)	Número de usuários Internet (% da população dos países e regiões)
EUA	4,7	26,3
OECD (exceto EUA)	14,1	6,9
América Latina e Caribe	6,8	0,8
Sudeste Asiático e Pacífico	8,6	0,5
Leste da Ásia	22,2	0,4
Europa do Leste e CIS	5,8	0,4
Estados Árabes	4,5	0,2
Sub-Saara Africano	9,7	0,1
Sul da Ásia	23,5	0,04
Mundo	100	2,4

Fonte: Relatório "Globalization with a human face" - PNUD.

**Tabela 2: Posição dos Países por Números de Hosts:**

Posição dos Países por Número de Hosts (fonte: Network Wizards 2005)				
	País	Julho/05	Jan/05	Class. Jan/05
1º	Estados Unidos	235.047.923	210.817.656	1º
2º	Japão (.jp)	21.304.292	19.543.040	2º
3º	Itália (.it)	9.965.942	9.343.663	3º
4º	Alemanha (.de)	7.657.162	6.127.262	5º
5º	Holanda (.nl)	6.781.729	6.443.558	4º
6º	França (.fr)	5.473.719	4.999.770	6º
7º	Austrália (.au)	5.351.622	4.820.646	7º
8º	Reino Unido (.uk)	4.688.286	4.449.190	8º
9º	Brasil (.br)	4.392.693	3.934.577	9º
10º	Taiwan (.tw)	3.838.383	3.516.215	11º
11º	Canadá (.ca)	3.525.392	3.839.173	10º
12º	Polônia (.pl)	3.055.075	2.482.546	12º