UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
FACULDADE DE ARQUITETURA, ARTES E COMUNICAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM COMUNICAÇÃO

DÉBORA CORRÊA CHAMA

O COMITÊ GESTOR DA INTERNET NO BRASIL:
GESTÃO, SEGURANÇA E COMUNICAÇÃO

Bauru – SP
2008

DÉBORA CORRÊA CHAMA

O COMITÊ GESTOR DA INTERNET NO BRASIL:
GESTÃO, SEGURANÇA E COMUNICAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Comunicação, da Faculdade de Arquitetura, Artes e Comunicação da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de Bauru, como requisito para obtenção do Título de Mestre em Comunicação (Área de Concentração: Comunicação Midiática).

Orientadora: Profª. Drª. Mª. Teresa Miceli Kerbauy

Bauru – SP
2008

DIVISÃO TÉCNICA DE BIBLIOTECA E DOCUMENTAÇÃO
UNESP – BAURU

Chama, Débora Corrêa.
O comitê gestor da internet no Brasil: gestão, segurança e comunicação / Débora Corrêa Chama, 2008.
186 f. : il.

Orientadora: Maria Teresa Micely Kerbauy.

Dissertação (Mestrado) – Universidade Estadual Paulista. Faculdade de Arquitetura, Artes e Comunicação, Bauru, 2008.

1. Comitê gestor. 2. Gestão da internet. 3. Inclusão digital. 4. Comunicação. I. Universidade Estadual Paulista. Faculdade de Arquitetura, Artes e Comunicação. II. Título.

Ficha catalográfica elaborada por Maria Thereza Pillon Ribeiro – CRB 3.869

DÉBORA CORRÊA CHAMA

O COMITÊ GESTOR DA INTERNET NO BRASIL:

GESTÃO, SEGURANÇA E COMUNICAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Comunicação, da Faculdade de Arquitetura, Artes e Comunicação, da Universidade Estadual Paulista, Campus de Bauru, para obtenção do título de Mestre em Comunicação.

Banca Examinadora:

Presidente: Profa. Dra. Maria Teresa Miceli Kerbauy (presidente)

Instituição: UNESP – Universidade Estadual Paulista

Titular: Prof. Dr. Danilo Rothberg

Instituição: USC – Universidade do Sagrado Coração

Titular: Prof. Dr. Juliano Maurício de Carvalho

Instituição: UNESP - Universidade Estadual Paulista

Bauru, 22 de agosto de 2008

Aos meus queridos pais, JOSÉ e NASTA.

AGRADECIMENTOS

Agradeço de modo especial a:

JESUS, fonte inspiradora de toda a minha vida;

PEDRO ULISSES, meu esposo, clareza, inteligência e apoio constantes;

DANILO, meu filho, talento presente e futuro;

MARIA TERESA, minha orientadora, perspicácia e direção ao longo deste caminho;

DEMI GETSCKO, visão e grandeza a serviço do Brasil;

ANTÔNIO TAVARES, exemplo de cidadania e representatividade;

HELDER e SÍLVIO, profissionais corretos e atenciosos;

CLAUDETE, amizade e dedicação no cotidiano e...

a todos que contribuíram para tornar este sonho possível.

LISTA DE ACRÔNIMOS E SIGLAS

ABRANET	Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet
ANATEL	Agência Nacional de Telecomunicações
ASACP	Association of Sites Advocating Child Protection
CEPTRO BR	Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações
CERT BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CETIP BR	Centro de Estudos sobre as Tecnologias da Informação e da Comunicação
CGI BR	Comitê Gestor da Internet no Brasil
FAPESP	Fundação de Amparo à Pesquisa do Estado de São Paulo
IANA	Internet Assigned Numbers Authority
IBGC	Instituto Brasileiro de Governança Corporativa
ICANN	Internet Corporation for Assigned Names and Numbers
MC	Ministério das Comunicações
MCT	Ministério da Ciência e Tecnologia
MINC	Ministério da Cultura
NIC BR	Núcleo de Informação e Coordenação do Ponto Br
NTP BR	Network Time Protocol
ONU	Organização das Nações Unidas
PROCON	Fundação de Proteção e Defesa do Consumidor
PTT BR	Ponto de Troca de Tráfego
REGISTRO BR	Registro de Domínios para a Internet no Brasil
SAFERNET BRASIL	Central Nacional de Denúncias de Crimes Cibernéticos
TELECO	Informação em Telecomunicações
TIC's	Tecnologias da Informação e Comunicação
UFPA	Universidade Estadual do Pará
UNESCO	Organização das Nações Unidas para a Educação, a Ciência e a Cultura
USP	Universidade de São Paulo

LISTA DE FIGURAS

Figura 1 - Presença da Internet por região no mundo em percentagem (2007) 36

Figura 2 - Percentual de usuários de Internet, segundo as regiões do globo (2007) 37

Figura 3 - Presença da Internet por Região no Brasil (2007) 46

Figura 4 - Usuários de Internet por gênero (2006-2007) 47

Figura 5 - Usuários de Internet por graus de instrução em percentual (2006-2007) 48

Figura 6 - Número anual de endereços IP suspeitos de hospedar pornografia infantil (2000 2007) 68

Figura 7 - Páginas do Orkut denunciadas à Safernet contendo pornografia infantil (janeiro de 2006 a junho de 2007) 70

Figura 8 - As leis brasileiras e a Convenção de Budapest 80

Figura 9 - Total de incidentes reportados ao CERT.br no período de 1999 a setembro de 2007 83

Figura 10 - Total de spams reportados ao CERT.br no período de 2003 a outubro de 2007 83

Figura 11 - Domínios genéricos 96

Figura 12 - Valores definidos para aquisição de nomes de domínios 98

Figura 13 - Receitas provenientes do registro de domínios 99

Figura 14 - Despesas relacionadas ao registro de domínios 99

Figura 15 - Saldos apurados por exercício 100

Figura 16 - Saldo acumulado no período de nove anos 101

Figura 17 - Total de nomes de domínios registrados no mundo (2005-2007) 102

Figura 18 - Os dez maiores em registros de nomes de domínio de primeiro nível (ccTLDs) no mundo (jan./abr. 2007) 103

Figura 19 - Domínios registrados no país de 01/01/1996 a 15/06/2008 105

Figura 20 - Grupos de segurança e resposta a incidentes no Brasil 107

Figura 21 - Nomenclaturas padrão - Grupos de resposta a incidentes na Internet 108

Figura 22 - Três etapas de tratamento dos incidentes de segurança 108

Figura 23 - Regiões brasileiras e tempo universal coordenado 118

LISTA DE TABELAS

Tabela 1 - Usuários de Internet e estatísticas populacionais (2000-2007) 35

Tabela 2 - Usuários de Internet e estatísticas populacionais do Brasil (2007) 45

Tabela 3 - Classes sociais e o uso da Internet em percentual (2006-2007) 48

Tabela 4 - Tipo de conexão à Internet no domicílio 90

Tabela 5 - Internet Banda Larga no Brasil: total de conexões (2002-2006) 91

Tabela 6 - Estratos de Região 111

CHAMA, Débora Corrêa. **O Comitê Gestor da Internet no Brasil:** gestão, segurança e comunicação. 2008. 186 f. Dissertação (Mestrado em Comunicação) – Faculdade de Arquitetura, Artes e Comunicação, Universidade Estadual Paulista "Júlio de Mesquita Filho", Bauru, 2008.

RESUMO

O Comitê Gestor da Internet no Brasil é o tema desta pesquisa, que tem por objetivo analisá-lo nas dimensões: gestão, através do modelo de governança eletrônica, adotado no Brasil e segundo os padrões da governança mundial da Internet; comunicação, através da análise das atividades desenvolvidas por este Comitê, no que diz respeito à produção de indicadores de caráter estratégico sobre a Internet brasileira; e segurança quanto à sua utilização, destacando os aspectos de confidencialidade, integridade, ética e disponibilidade da informação, aspecto também destacado no trabalho de gestão empreendido pela entidade aqui analisada. A Internet é um meio de comunicação capaz de sediar modelos de compartilhamento de informações que vêm transformando rapidamente as relações interpessoais de maneira significativa. Neste sentido, é um veículo que traz questões importantes para reflexão de pesquisadores da área de comunicação, no tocante a seus efeitos em diversos aspectos da vida social, cultural e política na sociedade da informação. Há uma expansão constante do número de internautas no mundo e no Brasil. Dados do Comitê Gestor da Internet apontam o total de usuários da rede no país em 2007: são aproximadamente 45 milhões de indivíduos incluídos digitalmente, que representam 34% da população. Os brasileiros em questão estão adentrando no ciberespaço, consumindo e produzindo informações, entretenimento, produtos e serviços. O Brasil é considerado, hoje, a segunda comunidade mundial presente no Orkut. O volume cultural produzido no ciberespaço, além de apresentar transformações em aspectos de sociabilidade e hábitos de consumo, traz também novas dimensões e problemas, como os cibercrimes, por exemplo, que surgem com o crescimento da utilização da Internet. São poucos os estudos acadêmicos brasileiros que analisam e apontam os problemas relativos à gestão, comunicação e segurança na Internet, hoje de responsabilidade formal do Comitê Gestor da Internet no Brasil. É nesta lacuna que se insere este trabalho, cuja metodologia fundamenta-se nas pesquisas bibliográfica e quantitativa, bem como no método qualitativo de investigação, utilizado na realização de entrevistas em profundidade, interpretadas segundo os critérios da análise de conteúdo. O presente estudo possui, portanto, um caráter indutor, pois busca apresentar o Comitê Gestor da Internet no Brasil como importante organismo para a inclusão digital e para o desenvolvimento qualitativo desta mídia no país.

Palavras-chave: Comitê gestor; Gestão da Internet; Segurança; Cibercrimes; Inclusão digital; Comunicação.

CHAMA, Débora Corrêa. **The Internet Charge Comitée in Brazil:** management, security and communication. 2008. 186 f. Dissertation (Master's Degree in Communication) – Faculdade de Arquitetura, Artes e Comunicação, Universidade Estadual Paulista "Júlio de Mesquita Filho", Bauru, 2008.

ABSTRACT

Internet Charge Comiteé is the theme of this research, which strives to analyze it in the following aspects: management, through the model of e-governancy, adopted in Brazil; communication, analysis of the developed activities by this Comitée, regarding strategic indicators on the brazilian Internet and security when handling its use, highlighting the issues of confidentiality, integrity, ethics and information availability, an aspect that is also highlighted in the management work charged by the entity analyzed here. The Internet is a communication tool able to group information share models that are quickly transforming interpersonal relation in a significant way. It is a tool that brings us important questions for researchers in the communication area, to reflect upon its effects in various aspects in the social, cultural and political life in the age of information. There is a constant expansion in the number of Internet users in Brazil and in the world. Data from the Internet Charge Comiteé show the total of users in the country in 2007: around 45 million of people digitally included, composing 34% of the total population. The brazilians in question are entering the cyberspace, consuming and producing information, entertainment, products and services. Brazil is considered today the world's second biggest community in Orkut. The cultural quantity produced in cyberspace, other than presenting in sociability aspects and consuming habits, also brings new dimensions of problems, like for example e-crimes, which appear with the growth of Internet utilization. There are few brazilian academical studies which analyze and point out the problems related to management, communication and security in the Internet. This project enters this column, and its methodology is based on the following researches: bibliographical, quantitative and in the qualitative investigation method, used in the realization of detailed interviews, interpreted following the conditions of content analysis. This research has, therefore, an inductive character, since it strives to present the Internet Charge Comiteé in Brazil as in important entity to aid the digital inclusion and for the qualitative development of this media in the country.

Keywords: Charge Comitée; Internet management; Security; E-crimes; Digital inclusion; Communication.

SUMÁRIO

1 INTRODUÇÃO 11

2 GOVERNANÇA ELETRÔNICA 21
2.1 Internet e sociedade global 21
2.2 Internet e indivíduo 29
2.3 Gestão da Internet no mundo 35
2.4 Gestão da Internet no Brasil 44

3 SEGURANÇA NA REDE 54
3.1 Internet e controles 54
3.2 Cibercrimes 60
3.3 Combate aos cibercrimes 65
3.4 Crimes financeiros 66
3.5 Pornografia infantil 68
3.6 Direitos do autor 72
3.7 Liberdade versus controle 73
3.8 Legislação Brasileira 76

4 A INTERNET BRASILEIRA E O COMITÊ GESTOR 89
4.1 Registro de nomes de domínio para a Internet no Brasil – registro.br 95
4.2 Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – cert.br 106
4.3 Centro de Estudos sobre as Tecnologias da Informação e da Comunicação – cetic.br 110
4.3.1 Frequência de uso 111
4.3.2 Atividades desenvolvidas na Internet 112
4.3.3 Local de acesso individual à Internet 113
4.3.4 Barreiras de uso 114
4.4 Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações ceptro.br 115
4.4.1 Ponto de Troca de Tráfego – Ptt.br 116
4.4.2 Network Time Protocol – NTP.br 116

5 CONSIDERAÇÕES FINAIS 119

REFERÊNCIAS 128

APÊNDICES 136

ANEXOS 164

1 INTRODUÇÃO

O tema desta pesquisa é o Comitê Gestor de Internet e seu objetivo é analisá-lo, considerando sua gestão, a qual hoje é realizada segundo o modelo denominado como governança eletrônica, adotado nos padrões de administração desta mídia no mundo e no Brasil. Tal processo, a governança eletrônica, foi desenvolvido a partir da experiência de administração das Tecnologias da Informação e Comunicação, que, por apresentarem características distintas das demais áreas de negócios em razão de sua necessidade constante de inovação e expansão, demandaram novos modelos de controle e gestão.

Com isso, os gestores das Tecnologias da Informação e Comunicação, as quais representam um dos principais alicerces da sociedade da informação, se depararam com necessidades sociais também muito novas, como é o caso da comunicação, propiciada e mediada por veículos revolucionários, como a Internet e o telefone celular, que representam grandes desafios para o aperfeiçoamento desses novos modelos de gestão, entre eles a governança eletrônica da Internet.

A presente pesquisa, cujo recorte temático é a gestão da Internet, problematiza e busca respostas para uma importante e recente questão que vem preocupando os gestores e a comunidade envolvida com a Internet: como administrar a comunicação mediada pela rede, conciliando a liberdade que a caracterizou desde o início de seu desenvolvimento, com os controles que vêm se tornando necessários, na medida em que aumentam os incidentes que ameaçam, em graus e circunstâncias distintas, a segurança na comunicação dos internautas? É possível que o atual modelo de gestão da Internet, a governança eletrônica, preserve a confidencialidade, a integridade, a ética e a disponibilidade da informação, sem ferir os princípios de liberdade permitidos pela rede mundial de computadores?

A hipótese deste estudo considera que o já citado modelo de gestão não está suficientemente preparado para esta investidura, até porque o Brasil não possui ainda regulamentados os controles e as políticas necessárias para o avanço da Internet, bem como um plano de comunicação eficaz que possa divulgar e estimular sua utilização consciente.

Controles para a Internet, por sua vez, são aqui entendidos como governança eletrônica responsável, uma vez que a rede Internet e sua arquitetura tecnológica tornam extremamente difíceis e caras as censuras e os controles rígidos.

Quanto a metodologia utilizada, fundamenta-se nas pesquisas: bibliográfica, quantitativa e no método qualitativo de investigação, utilizado na realização de entrevistas em profundidade, cuja interpretação efetivou-se através da análise de conteúdo.

A pesquisa bibliográfica apóia-se em livros, periódicos e artigos científicos, bem como na obtenção de propostas, documentos e acompanhamento eletrônico de matérias legislativas junto ao Senado Federal; na utilização da Internet, através do acesso a portais e *sites* de entidades referenciais para o estudo; e na análise do material produzido no Segundo Fórum Internacional de Governança da Internet realizado no Rio de Janeiro em dezembro de 2007. A pesquisa quantitativa referencia-se na análise de pesquisas científicas publicadas sobre o uso da Internet no Brasil e no mundo, publicadas por entidades e institutos especializados na área.

As entrevistas em profundidade foram realizadas com o Diretor Presidente do Nic.br (Núcleo de Informação e Coordenação do Ponto br), representante de notório saber sobre Internet, Demi Getschko (Apêndice A) e com Antônio Alberto Valente Tavares (Apêndice B), presidente da ABRANET (Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet) e representante dos provedores junto ao Comitê Gestor da Internet no Brasil, pessoas, cuja percepção, informação e experiência com o tema permitiram um aprofundamento da compreensão do fenômeno Internet.

A literatura científica a respeito de Internet permite perceber que se trata de um campo de estudos bastante amplo, uma vez que envolve um veículo de múltiplas dimensões: comunicação, tecnologia, sociedade, política, economia, entre outras. Porém, a literatura brasileira em comunicação, na área de gestão de Internet, ainda se encontra em estágio incipiente.

Neste sentido, esta é uma pesquisa que investiga a gestão da comunicação na Internet e as atividades desenvolvidas pelo CGI.br (Comitê Gestor da Internet no Brasil), constituído por um núcleo principal, o Nic.br (Núcleo de Informação e Coordenação do Ponto Br), que coordena e administra quatro áreas essenciais: administração, infra-estrutura, pesquisa e segurança. A análise da gestão da comunicação na Internet, realizada através da estrutura de seu

administrador máximo, o Comitê Gestor da Internet no Brasil, traz à discussão questões importantes para o futuro desse veículo no país, justificando, assim, este estudo.

O referencial para a presente análise é, portanto, o Comitê Gestor da Internet no Brasil, uma vez que é esta a entidade responsável por gerir o processo de governança eletrônica da rede mundial de computadores em território brasileiro. Esta entidade foi criada através da Portaria Interministerial n° 147 (1995), expedida em conjunto pelos Ministérios das Comunicações e Ciência e Tecnologia. Tal portaria foi alterada posteriormente através do Decreto presidencial n° 4829, em 2003, que estabeleceu as normas de funcionamento e as atribuições do Comitê Gestor.

Sua composição total é de vinte e um membros, sendo que nove são pertencentes ao governo federal, representando os ministérios: Ciência e Tecnologia; Casa Civil; Comunicações; Defesa; Desenvolvimento, Indústria e Comércio Exterior; Planejamento, Orçamento e Gestão; Agência Nacional de Telecomunicações e os Conselhos Nacional de Desenvolvimento Científico e Tecnológico e Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia.

O setor empresarial se faz representar por quatro provedores: Provedores de Acesso e Conteúdo da Internet; Provedores de Infra-estrutura de Telecomunicações; Indústria de Bens de Informática, de Bens de Telecomunicação e de Software e do Setor Empresarial Usuário.

O terceiro setor (organizações não-governamentais e outras entidades sem fins lucrativos) está representado por quatro pessoas de expressão neste segmento. Pela comunidade acadêmica e tecnológica participam três membros, sendo o representante de notório saber em assunto da Internet, o engenheiro Demi Getschko.

Já os núcleos que compõem a estrutura do Comitê Gestor da Internet no Brasil, cujas ações são implementadas pelo braço executivo deste Comitê, o Nic.br (Núcleo de Informação e Coordenação do Ponto.br) estão contemplados neste estudo como:

- **Registro.br** (Registro de nomes de domínio para a Internet no Brasil): administra e atribui nomes de domínio para acesso à Rede, distribui

endereços válidos e zela pela manutenção dos mesmos dentro das normas estabelecidas pelo Comitê Gestor para o adequado funcionamento da rede (REGISTRO, 2007a);

- **Cert.br** (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil): produz documentos e estatísticas a respeito de ataques de vírus e outras questões relacionadas à segurança, coordenando e apoiando os processos que envolvem análise e resposta a ataques a computadores e sistemas, além de treinar equipes para atuar em empresas e entidades interessadas em montar grupos de resposta próprios (CERT.BR, 2008a);
- **Cetic.br** (Centro de Estudos sobre as Tecnologias da Informação e da Comunicação): tem a responsabilidade de produzir indicadores sobre a Internet brasileira, divulgando-os à sociedade de forma sistemática e transparente (CETIC.BR, 2008);
- **Ceptro.br** (Centro de Estudos e Pesquisas em Tecnologias de Rede e Operações): gerencia e viabiliza a infra-estrutura para que as áreas metropolitanas estejam interconectadas com qualidade, além de desenvolver estudos que permitam a expansão da Internet brasileira com qualidade. Subdivide-se em duas áreas: o PTT.br (Ponto de Troca de Tráfego) e o NTP.br (*Network Time Protocol*) (CEPTRO, 2008).

Além desses núcleos principais, também fazem parte da estrutura do Comitê Gestor grupos e comissões de trabalho que se debruçam sobre temas específicos, com o objetivo de subsidiar decisões ou desenvolver projetos em áreas estratégicas. Engenharia e Operação de Redes, Grupo de Segurança de Redes e Formação de Recursos Humanos são os grupos de trabalho. Já as comissões são *Spam*, Indicadores e Conteúdos.

O Comitê Gestor da Internet, organização responsável pela governança eletrônica no Brasil, têm, no contexto tecnológico e político das Tecnologias da Informação e Comunicação, uma oportunidade histórica de impulsionar com qualidade a expansão da Internet, um veículo poderoso e cada vez mais fundamental na vida econômica de países e pessoas.

O estudo da rede mundial de computadores – Internet - traz, além de sua crescente importância econômica, questões importantes para reflexão de

pesquisadores de todas as áreas da ciência, relacionadas às novas práticas sociais originadas deste novo meio, cuja essência é constituída de processos tecnológicos e midiáticos extremamente mutáveis. Com isto, surgem problemas nesta nova dimensão sócio-comunicacional - sob diversos aspectos e condições culturais e econômicas - que estão a demandar análises e encaminhamentos científicos.

A comunicação, mediada pela Internet, ganhou novos contornos, incluindo inovações que se materializaram nas máquinas de comunicar eletrônicas (computadores, celulares, *palm-tops*, entre outras). Tais dispositivos possibilitaram que a referência de proximidade na comunicação fosse profundamente alterada, instaurando a desterritorialização que se tornou uma realidade que abrange cada vez mais pessoas e processos.

No Brasil, dados do CGI (Comitê Gestor da Internet) apontam uma expansão do contingente de pessoas em nosso país que acessou a rede em 2007: os índices passaram de 32% do total da população em 2005, para 33% em 2006 e 41% em 2007. São, portanto, mais de 50 milhões de brasileiros que acessaram a Internet pelo menos uma vez no ano de 2007.

Em 2007, 34% da população brasileira, representando 45 milhões de pessoas[1], já utilizavam a Internet como meio de comunicação e, portanto, eram considerados usuários[2], demonstrando uma evolução de 6% sobre os números apurados pela Pesquisa de 2006, uma vez que neste ano, indivíduos considerados como usuários somaram 35 milhões, ou seja, 28% da população[3] conheciam e utilizavam este meio naquele período. Quanto ao perfil revelado dos usuários em 2007 é de 60% jovens (idade entre 16 e 24 anos), sendo que 37% estão empregados e 78% possuem curso superior.

Por outro lado, há uma grande desigualdade digital, pois em 2006, 54% da população do país, totalizando 68 milhões de pessoas, nunca usaram um computador e 67%, ou seja, mais de 84 milhões de brasileiros, nunca utilizaram a Internet. Este percentual de exclusão digital diminuiu um pouco em 2007, uma vez que a pesquisa registrou as seguintes quedas: 54 para 47% no indicador de número

[1] Considerados 131,1 milhões de habitantes – Base População PNAD 2006 (total de indivíduos com 10 anos ou mais residentes em zonas urbanas).
[2] Usuários, de acordo com a metodologia TIC 2006, são pessoas que acessaram a Internet nos últimos três meses da data da pesquisa.
[3] Considerados 126,1 milhões de habitantes – Base População PNAD 2005 (total de indivíduos com 10 anos ou mais residentes em zonas urbanas).

de pessoas que nunca utilizaram o computador e 67 para 59% no índice de pessoas que nunca utilizaram a Internet.

Esses números fazem parte das Pesquisas sobre o Uso das Tecnologias da Informação e Comunicação no Brasil em 2005, 2006 e 2007 (SANTOS, 2006; BALBONI, 2007; 2008) , que revelaram, entre outras informações, a freqüência de acesso individual à Internet, o local de acesso, o tempo gasto na Internet por semana, bem como o propósito das atividades realizadas.

Com relação à segurança na rede, em 2006, 26% dos usuários revelaram ter tido problemas, que foram originados principalmente por: 28% de ataque de vírus, seguidos por 1,85% referentes a abuso de informações pessoais, 0,86% devidos a fraudes bancárias e com cartões de crédito e 1,14% gerados por outros problemas. Em 2007, o percentual total de usuários que revelaram ter tido problemas de segurança elevou-se para 29%.

Os brasileiros em questão adentraram no ciberespaço, passando a consumir e produzir informações, entretenimento, produtos e serviços. O Brasil é considerado hoje, um dos líderes em comunidades presentes no Orkut, segundo Demi Getschko, em entrevista pessoal concedida em 04/01/2008 na sede do Comitê Gestor da Internet, São Paulo (SP).

Este volume cultural, originário da Internet brasileira, tem provocado no meio acadêmico da área de comunicação, intensos debates a respeito de conceitos como ciberespaço, identidade cibernética, territórios informacionais, cibercultura, entre outros.

Por outro lado, nos campos jurídico e político, a Internet tem levantado, no mundo e no Brasil, problemas[4] difíceis de serem equacionados sem ferir a liberdade de expressão permitida pela rede. A ocorrência de atos ilícitos veiculados na Internet e ali concretizados levou o Congresso brasileiro a colocar em pauta projetos de lei que pretendem disciplinar a conduta dos internautas.

No Senado Federal foram elaborados dois projetos de lei que tratam dos crimes informáticos: o Projeto de Lei n° 76/2000, de autoria do Senador Renan Calheiros, PMDB/AL, e o Projeto de Lei n° 137, elaborado pelo Senador Leomar

[4] Os crimes digitais são um destes problemas, cuja expansão e repercussão acabaram resultando na Convenção sobre Cibercriminalidade, proposta pelo Conselho da Europa em 2001. Esta Convenção reúne assinaturas de vários países, incluindo não-membros do Conselho, como Estados Unidos da América, Canadá, Japão e África do Sul. O texto da Convenção tipifica os cibercrimes e deixa aos países a responsabilidade pela elaboração de leis e penalidades aplicáveis.

Quintanilha, PMDB/TO. O PLS n° 76 define e tipifica os delitos informáticos, enquanto o PLS n° 137 estabelece nova pena aos crimes cometidos com a utilização de meios de tecnologia de informação e telecomunicações.

O projeto de lei n° 84, de 1999, oriundo da Câmara dos Deputados, e que foi posteriormente acolhido no Senado Federal, cuja autoria é do Deputado Federal Luiz Piauhylino, PDT/PE, dispõe:

> (...) sobre os crimes cometidos na área de informática, e suas penalidades, dispondo que o acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores, dependerá de prévia autorização judicial (BRASIL, 1999, *online*).

Estes três Projetos de Lei que já tramitavam no Senado foram aglutinados ao Substitutivo proposto pelo Senador Eduardo Azeredo, com a finalidade de:

> Tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares, e dar outras providências (AZEREDO, 2007, *online*).

Além do Senado Federal, outras instituições precisaram direcionar esforços nesta área, como é o caso da Polícia Federal, que tem diversas operações em andamento no país, com a finalidade de controlar e punir os criminosos virtuais que vêm sofisticando sua atuação na rede mundial de computadores.

Entidades que atuam em defesa do consumidor, como os PROCON´s (Fundação de Proteção e Defesa do Consumidor), também já acumulam experiências nesta área, uma vez que o comércio eletrônico vem apresentando constante evolução.

Estatísticas coletadas pelo *site E-Commerce*, mostram que no Brasil foram transacionados via Internet em vendas *on line*, números da ordem de R$ 4,4 bilhões de reais em 2006, projetando para 2007 o valor de R$ 6,4 bilhões (exceto automóveis, venda de passagens aéreas e leilões *on line*). São cerca de 7 milhões de e-consumidores registrados no ano de 2006, adquirindo principalmente os produtos CD´s/DVD´s, livros e revistas, eletrônicos, saúde e beleza, e informática.

Esses consumidores estão situados majoritariamente nas classes C (32%), B (22%) e A (13%), sendo que 58% pertencem ao sexo masculino (E-COMMERCE, 2008).

Com a expansão do e-commerce, crescem também as fraudes contra o e-consumidor. Relatório da Fundação Procon SP revela:

> A Fundação Procon registrou, no período de 01/05/2006 a 31/05/2007, 1054 atendimentos referentes ao comércio eletrônico. A maioria dos problemas está ligada a não entrega ou à demora na entrega do produto; à dificuldade de troca do produto ou cancelamento da compra, publicidade enganosa (muitas vezes em relação a preços) e a métodos desleais de venda, através de inserções de “pop-up” ou “banners” em *sites* conhecidos, induzindo o consumidor à compra de produtos que, na realidade, não pretendia adquirir (produtos para obesidade, impotência sexual, sintomas da TPM, etc.). Sem falar no fato desses produtos estarem em desacordo com a legislação sanitária vigente (PROCON, 2007, p.9).

Além de tais fatos, existem problemas políticos, que em diversos países restringem o acesso da população à Internet, como é o caso específico de Cuba, país no qual, embora em março de 2008, tenha sido autorizada a venda de computadores para os cubanos - medida de abertura econômica tomada pelo Presidente Raul Castro - o acesso à Internet continua permitido somente a estrangeiros, funcionários do governo e professores universitários (CUBA..., 2008).

Todos estes problemas relacionados ao acesso, ao controle e à segurança na Internet, além de se constituírem em novos fatos sociais, econômicos e jurídicos, remetem também à gestão desse veículo, que até o momento tem se caracterizado pelo formato denominado como governança eletrônica.

A governança eletrônica é uma forma de gestão compartilhada e descentralizada, tendo como órgão coordenador das atividades relacionadas à Internet no mundo, a ICANN (*Internet Corporation for Assigned Names and Numbers*), entidade sediada nos Estados Unidos da América. Este tipo de gestão compartilhada foi desenvolvido a partir da experiência de administração das Tecnologias da Informação e Comunicação, que se expande da gestão tecnológica para a gestão política:

> É neste contexto que surge uma abordagem reformulada sobre o tema da governança (...) governar torna-se um processo interativo porque nenhum ator detém sozinho o conhecimento e a capacidade de recursos para resolver problemas unilateralmente (FREY, 2002, p. 143).

Portanto, considerando a multiplicidade de conhecimentos e atores sociais envolvidos na governança da Internet, os capítulos seguintes procurarão abordar sua gestão, segurança e a comunicação, a partir da experiência do Comitê Gestor da Internet no Brasil.

O capítulo inicial aborda o surgimento do fenômeno Internet, em uma trajetória extremamente veloz, de contexto global e de características únicas, enquanto veículo de comunicação, capaz de alterar hábitos individuais e dar novos rumos à economia de países inteiros. A comunicação, no contexto da Internet, não é apenas por ela mediada, como também pode-se afirmar que, em certo sentido, há uma ampliação na esfera comunicativa, proporcionada pela rede mundial de computadores, uma vez que, a todo momento, pessoas e empresas descobrem novos usos dentro deste ambiente. Conforme Vinton Cerf: “(...) Acredito (...) que a Internet se transforma de acordo com um modelo de coevolução. Interage com tudo que a cerca e, então, se adapta. As novas aplicações levam a rede aos seus limites e forçam a criação de novas soluções técnicas” (A SAGRAÇÃO..., 2008, p. 4). Este primeiro capítulo trata também de situar o tipo de gestão que se fez necessária no mundo e no Brasil, desde o momento histórico de sua criação até chegarmos ao tipo de governança que temos agora, bem como as perspectivas desta administração para o futuro.

No capítulo “Segurança na Rede”, coloca-se o panorama de segurança e confiabilidade da informação na Internet em seus aspectos jurídicos, sociais, penais e políticos, descrevendo fatos e números que poderão ser úteis à reflexão sobre a necessidade de aprofundamento da comunicação dos gestores de rede e do governo como um todo, com a população que se utiliza da Internet, para que se minimizem os efeitos dos crimes virtuais que vêm crescendo no país. Os denominados cibercrimes representam um fenômeno tão expressivo, que extrapolam os limites jurídicos e penais a que estariam restritos, se ocorressem na realidade física, para se constituírem em preocupação na esfera da comunicação, já que podem se tornar obstáculos à livre expressão praticada na Internet.

O capítulo “A Internet Brasileira e o Comitê Gestor” analisa os núcleos que constituem o Comitê Gestor da Internet no Brasil, de maneira a possibilitar uma visão geral e uma análise acurada do processo de gestão empreendido pela entidade. Nesta análise, procurou-se, ainda, verificar o nível de participação da

sociedade nas decisões do Comitê Gestor, bem como o grau de influência da ICANN na condução e na gestão da Internet empreendida no Brasil.

Nas considerações finais, buscou-se responder às seguintes questões:

a. A governança eletrônica nos padrões atuais é a mais adequada para a expansão da rede brasileira com qualidade?
b. Que tecnologias esperam os novos usuários?
c. Que tipo de conexão teremos disponível?
d. É preciso investir em segurança da Internet?
e. É preciso conscientizar os usuários a respeito das boas práticas na rede mundial de computadores?

Dessa maneira, este estudo situa a Internet brasileira no contexto global da governança da rede, considerando os aspectos específicos do país e das práticas de seus gestores para tratar das questões que a crescente inclusão digital vem apresentando.

2 GOVERNANÇA ELETRÔNICA

2.1 Internet e sociedade global

Inicialmente, este estudo descreve a evolução das tecnologias de comunicação e informação e seu papel nas transformações globais ocorridas em todo o mundo. São transformações tão fundamentais do ponto de vista de remodelamento da comunicação, que tornou-se necessário aos pensadores das ciências da comunicação e das ciências sociais elaborarem conceitos e valores para análise das relações sociais mediadas por essas tecnologias e seus desdobramentos nas várias dimensões humanas.

Assim, mais do que descrevê-las, procurou-se também explicá-las à luz dos mais recentes conceitos desenvolvidos a partir da década de 80 por estudiosos como Mattelart, Bell, Morin, entre outros, que se dispuseram a entrar neste novo e desconhecido cenário que mescla realidade com virtualidade. Por isso, optou-se como fio condutor desta pesquisa, pela visão de cientistas que ainda estão descobrindo o que há por vir em um palco que se encontra em constante mutação. Pesquisadores como Derrick de Kerckhove (1995), Pierre Lévy (apud VERAS, 2000), Steven Johnson (2001), Manuel Castells (2003), Rogério Haesbaert (2006) e outros, têm idéias apresentadas neste texto, que busca entender este fenômeno tão revolucionário chamado Internet.

Delinear a conexão de tal fenômeno, a rede mundial de computadores, representada pela Internet, com a sociedade global, marca, por conseguinte, o início desta reflexão.

Desde suas origens, no final da década de 60, a Internet tem possibilitado as mais diversas manifestações individuais e coletivas. Há, portanto, uma revolução de aproximadamente 50 anos e um impacto transformacional equivalente a um século.

Mattelart (2000) faz a historiografia dos debates que originaram o conceito de sociedade da informação, na qual referencia o sociólogo americano Daniel Bell como o precursor do conceito “sociedade pós-industrial”, bem como das demais definições que a pudessem explicar com clareza. Em 1979, esse pensador já se

preocupava com o novo tipo de sociedade que surgia na década de 70, baseada na tecnologia, sociedade esta que, posteriormente, foi denominada por alguns autores como “sociedade de informação”. Bell (1999 apud MATTELART, 2000, p. 105), no prólogo da reedição de sua obra de 1973, “O advento da sociedade pós-industrial", aderiu a esta nova nomenclatura e assim caracterizou o que seria para ele esta sociedade: “(...) cada sociedade é uma sociedade de informação e cada organização é um organismo de informação. A informação é necessária para organizar e fazer funcionar qualquer coisa, da célula à General Motors”. Informação, para Bell (1999 apud MATTELART, 2000, p. 88), significa a “estocagem, transmissão e o tratamento dos dados enquanto base de todas as trocas econômicas e sociais”.

A partir desta conceituação, percebe-se a importância da informação nesta nova configuração da sociedade. Informação, que ao ser tratada, gera demandas que alteram e movimentam capitais de países e empresas de forma instantânea. Esta volatilidade de capitais é facilitada pela velocidade tecnológica com a qual a informação é processada. Informação que pode ser tratada de múltiplas maneiras, conforme a proposta de Bell, quanto ao fracionamento da informação em três categorias. Na categoria “registro”, encontram-se os seguros sociais, as operações bancárias e os créditos. “Programas” incluem reserva de passagens aéreas, planos de produção e elaboração de inventários, enquanto a categoria “biblioteca/ demografia” abriga recenseamentos, pesquisas de opinião, estudos de mercado, boletins eleitorais, entre outros.

Uma vez desmaterializada a economia, o trabalho também sofre o mesmo processo, uma vez que nas sociedades de informação, o valor do conhecimento (presente no mundo desenvolvido) tende a preceder em importância os valores dos produtos primários e manufaturas (que são vitais para a economia de países em desenvolvimento).

Nesta mesma linha de pensamento, na qual o conhecimento e a informação crescem em importância sócio-econômica, Matellart (2000) cita dois estudiosos que anteciparam o crescimento vertiginoso da sociedade baseada na informação: Alvin Tofler, escritor norte-americano, especialista em previsões e cenários e Zbigniew Brzezinski, cientista político polonês-americano. Tofler (1980 apud MATTELART, 2000, p. 97-98) antecipava em 1980, na obra “O Choque do Futuro”, “uma sociedade completa, de cadência muito rápida, que repousa sobre uma tecnologia extremamente avançada e um sistema de valores pós-materialista”.

Brzezinski (1969 apud MATTELART, 2000, p. 100-101, no estudo "*Between two ages: america's role in the technotronic"*, de 1969, previu uma unificação acelerada do mundo, uma expansão das redes de informação e comunicação, tendo como país-farol (no sentido de iluminar este novo mundo) os Estados Unidos da América, pelo fato deste país comunicar-se mais do que qualquer outro[5].

Hoje, passados vinte e oito anos, estes cenários descritos na década de 80 são reais e remodelaram em pouco tempo a face da sociedade que passa então a ser fundamentada no processamento da informação e em seus efeitos.

Castells (1999, p. 497) é um dos primeiros autores a conceituar esta sociedade que processa rapidamente a informação, denominando-a "sociedade em rede". Para ele, vivemos em uma sociedade em rede, que se tornou a atual forma de organização humana, tendo como principal ingrediente de sua estrutura social a informação, cujo encadeamento básico é realizado pelas redes, interconectadas através de um fluxo de imagens e de mensagens. De acordo com sua teoria, redes são sistemas abertos, dinâmicos, incorporam inovações desde que não sejam ameaças a seu equilíbrio e são capazes de suplantar o espaço e invalidar o tempo.

As possibilidades para que as redes possam existir e funcionar com essas características foram criadas a partir da transformação concentrada nas tecnologias da informação e comunicação, cujo desenvolvimento acelerou-se no final do século XX.

Como conseqüência, a economia como um todo ganhou forte impulso. As empresas, inicialmente as maiores, puderam investir em regiões completamente distintas de sua base territorial. Isto fez com que as economias se tornassem interdependentes globalmente e, em vista disso, criaram-se novas relações econômicas. Esta economia fundamentada na informação conseguiu instalar-se mesmo em países culturalmente muito diferentes, acentuando seu caráter global.

O comércio globalizado alterou inicialmente as relações econômicas entre empresas e países, para logo em seguida atingir as relações entre Economia, Estado e Sociedade, ocasionando drásticas mudanças sociais, tais como: sistemas políticos em crise de legitimidade, declínio da influência dos movimentos sociais, fim do emprego estável e aumento do emprego temporário, novo sistema de comunicação com linguagem digital/universal, novos fluxos de riquezas, imagens e

[5] Segundo Brzezinski, os EUA concentram 65% das comunicações mundiais.

de poder, inclusão das mulheres na força de trabalho e diminuição do Estado do Bem Estar Social.

O salto tecnológico de peso para o cenário de transformações globais em curso até então, acabou ocorrendo na década de 60, nos Estados Unidos, com a emergência da Internet, a partir da ARPANET.

> As origens da Internet podem ser encontradas na ARPANET, uma rede de computadores montada pela Advanced Research Projects Agency (ARPA) em setembro de 1969. A ARPA foi formada em 1958 pelo Departamento de Defesa dos Estados Unidos com a missão de mobilizar recursos da pesquisa, particularmente do mundo universitário, com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética na esteira do lançamento do primeiro Sputnik em 1957. A Arpanet não passava de um pequeno programa que surgiu de um dos departamentos da ARPA, o Information Processing Techniques Office (IPTO), fundado em 1962 com base numa unidade preexistente. O objetivo desse departamento (...) era estimular a pesquisa em computação interativa. (...) a montagem da Arpanet foi justificada como uma maneira de permitir aos vários centros de computadores e grupos de pesquisa que trabalhavam para a agência compartilhar, *on-line,* tempo de computação (CASTELLS, 2003, p.13-14).

Este fato impulsionou sobremaneira a microinformática e as engenharias com intenção comunicacional que contribuíram para o surgimento da sociedade em rede (Castells, 1999, p. 497-506). Sociedade esta, de economia globalizada com base informacional e culturalmente marcada pela crescente virtualização das relações sócio-econômicas, na qual as noções de tempo e espaço são redefinidas em função dos fluxos de informação e não mais com relação ao passado e ao futuro. Esta nova cultura global se propaga virtualmente, ultrapassando as fronteiras nacionais, globalizando costumes, entretenimento e experiências.

A globalização opera principalmente através da tecnologia, que deve ser entendida como o uso de conhecimentos científicos para especificar as vias de se fazerem as coisas de uma maneira reproduzível, com potencial de expansão muito grande. Deve possuir capacidade de criar interface entre campos tecnológicos mediante uma linguagem digital comum, através da qual a informação é gerada, armazenada, recuperada, processada e transmitida (CASTELLS; BROOKS; BELL apud CASTELLS, 1999, p. 49).

A tecnologia, ao transformar a informação, age sobre todos os domínios da atividade humana, possibilitando, dessa maneira, conexões infinitas entre

diferentes domínios, entre elementos e agentes de tais atividades. Ela se realimenta pelo seu uso, adicionado a mais inovação criando o chamado “círculo virtuoso”.

O avanço dessa tecnologia digital se faz notar em todas as dimensões da vida social: da agricultura aos serviços, dos crimes à religião, da medicina ao curandeirismo, da ciência às loterias: tudo pode se interligar na rede e, fora dela, milhões de pessoas, a maioria da população mundial, aparentemente não se encontra submetida aos seus ditames, pelo menos não se pensarmos em termos de inclusão digital[6].

No entanto, com respeito à globalização, alguns autores consideram que todos os povos (incluídos ou não digitalmente) sofrem seus efeitos:

> Os indivíduos, os grupos, as classes e todos os outros setores sociais adquirem distintas possibilidades de se desenvolverem e se expressarem. Diante de horizontes abertos, insuspeitados, uns e outros podem visualizar múltiplas perspectivas. Uns e outros deixam de estar vinculados a somente, ou principalmente, uma cultura, história, tradição, língua, religião, ideologia, utopia. O desenraizamento que acompanha a formação e o funcionamento da sociedade global põe uns e outros, situados em diferentes lugares e distintas condições sócio-culturais, diante de novas, desconhecidas e surpreendentes formas e fórmulas, possibilidades e perspectivas (IANNI, 1992, p.103).

Temos, assim, globalização e virtualização como fenômenos crescentes e interligados em um ambiente altamente conectivo:

> O resultado, em cerca de um par de décadas, será o de que um cidadão ativo de qualquer país desenvolvido encontrar-se-á ligado a esse universo por um cabo ou uma antena parabólica – ou por um terminal sem fio junto de um repetidor. Graças a essas ligações poderá sentir-se membro de uma comunidade ampliada e, muitas vezes, virtual, com limites geográficos difusos ou inexistentes, hierarquias sociais a serem estabelecidas e normas a serem regulamentadas (CEBRIÁN, 1998, p. 47).

A Globalização, como a entende Santos (2000, p. 16), é resultado das inovações técnicas e científicas que surgiram no período pós Segunda Guerra Mundial e significa um certo uso das condições materiais atuais que permitem: (...) comunicar todos os pontos do planeta (...); produzir uma mais-valia universal (...);

[6] No Brasil, apenas 24% da população tem computador em casa e 17% têm acesso à Internet de casa, segundo dados da Pesquisa sobre uso da Tecnologia da Informação e da Comunicação no Brasil (TIC Domicílios e TIC Empresas 2007).

produzir em toda parte e criar um produto global a partir de um único sistema técnico.

Um ou mais produtos globais, incluindo a Internet, distribuem-se, no entanto, de maneira desigual. No caso específico da Internet, Castells (2003, p. 215-216) mostra que a infra-estrutura de telecomunicações acaba atendendo à necessidade de grandes clientes, ao criar conexões específicas. Isso ocorre em virtude de que o sistema de comunicações, em especial nos países que integram o mundo em desenvolvimento, é arcaico e precisa ser reconstruído, passando por novas regulamentações, que demandam gestão governamental em um período de tempo maior, o que faz então com que grandes corporações financeiras e negócios dos mais diversos ramos, como grandes hotéis, forças armadas, mídia, transporte, entre outros, procurem alternativas que possam propiciar o binômio qualidade/velocidade de comunicação para expansão de seus negócios.

As questões que estão na base da desigualdade, no entanto, não se resumem apenas à capacidade financeira e política dos países em desenvolvimento para tratar com as questões de infra-estrutura de telecomunicações.

Para além dos fatores estritamente econômicos, outros aspectos se colocam como barreiras para que as populações sejam inseridas digitalmente no mundo global. Uma destas barreiras é o analfabetismo. A UNESCO (Organização das Nações Unidas para a Educação, a Ciência e a Cultura) informa em sua seção para Educação, que existem aproximadamente 781 milhões de analfabetos em todo o mundo, sendo que 64% deste total são mulheres (UNESCO, 2008). O analfabetismo funcional, que dificilmente é capturado nas estatísticas, também dificulta a navegação na Internet, cujos *links*, ao levarem os usuários de uma página a outra, podem confundi-los, uma vez que seu processo de letramento não foi realizado de forma completa.

Além disso, outras habilidades são exigidas para utilização dos computadores: é preciso utilizar as mãos e o cérebro em sintonia. Tais habilidades no trato com os computadores têm provocado alterações de comportamento que vêm merecendo a atenção de psicólogos, pais e autoridades, que acompanham com preocupação fatos envolvendo pessoas que chegaram até mesmo a falecer após um excessivo número de horas conectadas na Internet. Segundo informações do *site* de notícias G1, da Globo.com (MARATONA..., 2007), foi o que aconteceu em 2007, com Xu Yan, um internauta chinês de 26 anos de idade que faleceu após passar

quase sete dias *on-line*, jogando ininterruptamente. O *site* ainda informou que “(...) em 2005, autoridades da Coréia do Sul divulgaram que um homem de 38 anos morreu “por esgotamento” após ficar dez dias em frente ao computador. Também naquele ano, outro sul-coreano, esse com 28 anos, teve uma parada cardíaca e morreu depois de permanecer 50 horas conectado.”

O poder de sedução dos computadores conectados é explicado por Kerckhove (1995, p.34), para quem os media eletrônicos funcionam como extensões do nosso corpo, provocando impactos sobre o nosso sistema nervoso, acabando também por modificar nossa própria psicologia. Essa alteração psicológica, que este autor credita ao impacto das novas tecnologias (televisão e outros media, como telefone, rádio, computadores e outros) é capaz de prolongar as propriedades de envio e recepção da consciência, acabando por modificá-la.

Os media integrados tornam-se, assim, uma espécie de consciência a meio de caminho, uma compreensiva mediação entre eu e o mundo, entre eles e nós, entre os nossos cérebros e as coisas da vida. Assim, Kerckhove compreende os media, como órgãos de controle do corpo social.

Neste cenário de dominação e fascínio exercido pelos meios eletrônicos sobre os homens, é possível que uma transformação importante esteja em curso. Para Kerckhove, as redes de computadores poderão superar a televisão, alterando esse cenário de dominação que a mesma exerce sobre os homens, ao permitir a interatividade. É importante ressaltar que à época deste estudo, o desenvolvimento da Televisão digital estava em seu estágio inicial: “(...) no início da década de 90, a radiodifusão da Televisão Digital era impensável devido aos custos elevados para sua implementação” (MOURA, 2006, p. 3).

Dessa maneira e comparado à televisão aberta, segundo esse autor, o computador proporciona mais do que texto e imagem. O texto permite a crítica, enquanto a imagem, tridimensional, permite a observação em perspectiva e a noção de profundidade. A sensação tátil obtida por sucessivos cliques no mouse e por toques no teclado é capaz de transferir parte do processo cognitivo da visão para o tato.

Kerckhove confere importância especial à dimensão tátil – ele diz que as experiências intelectuais são experiências táteis. A conexão entre a inteligência e as mãos também foi também objeto de estudos de Piaget (apud GAIARSA, 1994, p. 64), que afirmou:

> Nada existe verdadeiramente na inteligência que não tenha passado pelas mãos! Se eu nunca juntei nada – com as mãos! – jamais saberei o que significa juntar. Se eu nunca desmontei nada – com as mãos! eu não sei o que significa desmontar. Se eu nunca pus nada em cima de nada, eu não sei o que significa "por em cima". Quem não tem experiência da manipulação de objetos, não pode ter uma noção atuante do que seja manipulação de idéias ou conceitos.

Uma curiosa identificação ocorre quando o usuário acessa o computador e se depara com sua tela, segundo Kerckhove (1995). O cursor, piscando na tela, aguarda a ação do usuário, o que dessa maneira o torna comandante na navegação eletrônica. O fato de adicionar a mão ao pensamento faz ainda tangíveis as coisas que eram apenas visíveis. Metaforicamente então "torna-se possível tocar os conteúdos do próprio pensamento".

Outro fato marcante na história dos computadores pessoais é relatado por Johnson (2001): a magnífica invenção do mouse por Doug Engelbart – cuja primeira demonstração pública ocorreu em 1968 em São Francisco (EUA) – e o quanto este engenhoso dispositivo revolucionou o contato homem/computador:

> A grande investida de Engelbart envolveu o princípio da *manipulação direta*. Representar um documento de texto como uma janela ou um ícone era uma coisa, mas, a menos que o usuário tivesse algum controle sobre essas imagens, a ilusão seria remota, pouco convincente, como um filme projetado a poucos fotogramas por segundo. Para que a ilusão de espaço-informação funcionasse, devíamos poder sujar as mãos, mexer as coisas de um lado para outro, fazer coisas acontecerem. Foi aí que entrou a manipulação direta. Em vez de teclar comandos obscuros, o usuário podia simplesmente apontar para alguma coisa e expandir seus conteúdos, ou arrastá-la através da tela. Em vez de dizer ao computador para executar uma tarefa específica – "abra este arquivo"-, os usuários pareciam fazê-los eles próprios. (...) a imediatez táctil da ilusão dava a impressão de que agora a informação estava mais próxima, mais à mão, em vez de mais afastada. Sentíamos que estávamos fazendo alguma coisa diretamente com nossos dados, em vez de dizer ao computador que a fizesse por nós (JOHNSON, 2001, p.21-22).

Castells (1999, p. 51) aprofunda a idéia de que, ao utilizar o computador, nós comandamos a experiência de forma muito próxima, graças aos dispositivos a ele anexados, ao afirmar que "(...) pela primeira vez na história a mente humana é uma força direta de produção e não apenas um elemento decisivo no processo produtivo".

2.2 Internet e indivíduo

A globalização como um todo, entendida em seus aspectos culturais e econômicos, coloca ao indivíduo inúmeras opções de consumo tanto de idéias quanto de produtos. Este indivíduo percebe-se em um mundo cada vez mais fragmentado, imprevisível, e, portanto, inseguro.

De acordo com Castells (2002, p. 25), uma das formas de resistência à fragmentação advinda dos efeitos globais, tem sido a construção da identidade de forma reflexiva pelos atores sociais. Essa identidade se define pelo reconhecimento do sujeito enquanto ser com determinados atributos culturais, construídos de modo a significar algo para si e para os outros. Castells distingue e confere especial importância à identidade, pois diferentemente dos papéis sociais, que organizam funções, a identidade organiza significados, e é capaz de se auto-sustentar ao longo do espaço e do tempo.

A identidade se estrutura em dois sentidos: de fora para dentro, através da contribuição da história, da geografia, da memória e das instituições e também de dentro para fora, sendo construída no caminho inverso, pois o indivíduo, ao processar as contribuições recebidas, as modifica, ressignificando-as.

No plano coletivo, Castells organiza as identidades em três categorias:

- ✓ Identidade legitimadora: o Estado projeta nos indivíduos valores culturais utilizando-se da força e/ou do poder. Neste caso, os valores projetados pelas fontes de dominação encontram guarida nos indivíduos, que, por este motivo, reconhecem tais valores como sendo seus, embora estejam estruturados de forma coercitiva.
- ✓ Identidade de resistência: nesta categoria, grupos excluídos ou desvalorizados constroem sua identidade, encontrando, através de princípios distintos dos valores socialmente reconhecidos, formas alternativas de sobrevivência. Por esta lógica, os excluídos negam os valores dos que os excluem. Ou nas palavras de Castells ocorre “a exclusão dos que excluem pelos excluídos” (CASTELLS, 2002, p.25).
- ✓ Identidade de projeto: grupos de atores sociais procuram reconstruir sua identidade com o objetivo de transformar aspectos da estrutura social de forma a ter suas posições nela reconhecidas e ao fazê-lo, acabam por estender essas transformações a outros domínios da vida

> social. Assim ocorreu com o feminismo, uma vez que, em decorrência desse movimento histórico, mudaram importantes dimensões da estrutura social então vigente, que era de caráter patriarcal, monogâmica e economicamente fundamentada no trabalho masculino.

Giddens (1991 apud CASTELLS, 2002, p.27) diz que a identidade não é um traço distintivo da pessoa, é o próprio ser que busca saber o quê e por que está fazendo algo, e ao fazê-lo, estrutura sua identidade através de um planejamento reflexivo.

Na sociedade em rede, segundo Castells (2002), o processo de construção de identidade de forma reflexiva (que poderia auxiliar as pessoas a se orientar no mundo onde não há mais referências sólidas) fica prejudicado, porque a maioria das pessoas está no local e a referência da sociedade em rede é este fluxo de valores que oscila entre o local e o global. A referência é a cidade e o mundo ao mesmo tempo. O segmento privilegiado neste contexto identitário são as elites transnacionais, uma vez que são as únicas a transitarem bem por este fluxo de valores, justamente porque têm acesso simultâneo ao local e ao global.

Segundo Castells (2002), a forma de construção de identidades coletivas que tende a predominar na sociedade em rede é a identidade de resistência. Através dela, os atores excluídos constroem comunidades e a comunicação que aí reside, resiste às ideologias dominantes, revertendo os valores a que estes atores estão submetidos. Como a força motriz da sociedade em rede é a informação, um dos terrenos férteis para que as identidades de resistência tenham voz são os diversos sítios construídos na Internet. Ainda que pela via negativa, alguns desses grupos se expressem de maneira contundente e até mesmo criminosa. É o que ficou evidente, por exemplo, no estudo revelado em recente dissertação de mestrado na área de antropologia defendida na Unicamp (DIAS, 2007), que caracterizou e mapeou mais de 13 mil sites neonazistas na Internet e cerca de 20 comunidades no *Orkut*, cujo conteúdo racista acabou sendo denunciado pela pesquisadora ao Ministério Público.

O processo histórico de construção da identidade também é relatado por Tedesco (2002, p. 74) em seus estudos sobre os caminhos da educação na era da informação. Nas sociedades tradicionais, as pessoas construíam as suas identidades considerando gênero, raça, etnia e religião, incorporando, dessa maneira, sistemas de vida ordenados e previsíveis. Com o capitalismo e a

democracia, esses fatores foram substituídos por nação, classe social e ideologia política. Os fatores introduzidos pelo capitalismo entram em crise com a globalização e assim as pessoas passam a incorporar fragmentos dispersos da realidade e são elas que devem reconstruir o sistema. Por conseguinte, a construção da identidade tornou-se um processo transformado de maneira substancial em nossos dias. Tedesco diz que tradicionalmente a construção da identidade passava inicialmente pela família, na denominada “socialização primária”, para ser complementada em seguida pela escola, a “socialização secundária”.

Hoje, a família não é mais capaz de realizar essa socialização primária, considerando os efeitos da entrada da mulher/mãe no mercado de trabalho e a remodelação das famílias, ficando a cargo de outras instâncias, como a escola e a mídia, o cumprimento desta tarefa. É claro que, em decorrência disso, a socialização primária não se cumpre, ao menos não como anteriormente. E o resultado, no campo social, são novas visões de mundo, novas relações com as instâncias coletivas e o enfraquecimento do sentido de pertencer a algo, seja a uma religião, a uma cidade ou a uma nação.

O multiculturalismo, ou seja, a existência de diferentes culturas numa sociedade, que é um modelo de diversidade (no qual a cultura ocidental não é mais hegemônica), trouxe insegurança, exigindo novas habilidades e capacidades que as pessoas em geral não aprendem nas escolas, que são as instituições nas quais passam grande parte de suas vidas. Além disso, os elementos da vida social estáveis são cada vez menores e os dinâmicos crescem, trazendo perdas de referências significativas.

Neste modelo, a solidariedade fragilizou-se e a exclusão aumentou, gerando novas formas de organização, nas quais sobressaem valores de intolerância, discriminação e exacerbação das diferenças. Como exemplo, Tedesco cita os movimentos neonazista e racista e ainda as gangues. Por outro lado, as elites transnacionais desapegam-se da nação e referenciam-se preponderantemente por valores financeiros. A situação piora com o declínio do Estado do Bem Estar Social, quando então todas as pessoas têm que passar a cuidar delas mesmas. Com o individualismo em alta, as responsabilidades pessoais aumentam e as pessoas não as assumem em sua integralidade, pois isso implica fazer escolhas que não estão preparadas para fazer.

É possível que a Internet seja um meio capaz de trazer gradativamente uma forma de pertencimento às comunidades que o declínio das sociedades tradicionais fez desaparecer. A solidão do indivíduo incluído digitalmente é, muitas vezes, minimizada pelo contato com pessoas através de “comunidades virtuais”.

Castells retoma os debates a respeito de como a Internet possibilitou a formação de comunidades virtuais, vistas inicialmente como instauradoras de novos padrões de sociabilidade. Na verdade, de acordo com sua visão, a Internet proporciona suportes tecnológicos para a sociabilidade, embora existam evidências de que a sociabilidade também tenha mudado na sociedade em rede. E esta mudança tem a ver com o que Castells chama de “privatização da sociabilidade”:

> Essa relação individualizada com a sociedade (...) enraíza-se, em primeiro lugar, na individualização da relação entre capital e trabalho, entre trabalhadores e o processo de trabalho, na empresa em rede. É induzida pela crise do patriarcalismo e a subseqüente desintegração da família nuclear tradicional, tal como constituída no final do século XIX. É sustentada (mas não produzida) pelos novos padrões de urbanização, à medida que subúrbios e condomínios de luxo ainda mais afastados proliferam, e a desvinculação entre função e significado nos microlugares das grandes cidades individualiza e fragmenta o contexto espacial da existência. E é racionalizada pela crise de legitimidade política, à medida que a crescente distância entre os cidadãos e o Estado enfatiza o mecanismo de representação e estimula a saída do indivíduo da esfera pública. O novo padrão de sociabilidade em nossas sociedades é caracterizado pelo individualismo em rede (CASTELLS, 2003, p. 108).

Conforme Castells (2003, p.99), estudos e pesquisas conduzidos nos Estados Unidos entre os anos de 1995 e 2001, com certos grupos de usuários da rede, mostraram que a sociabilidade não aumentou em decorrência de seu uso, mas reforçou os laços familiares e de interação social fora do meio tecnológico, fato que levou os pesquisadores a concluírem que a Internet acabou exercendo um efeito positivo na interação social.

Por outro lado, pesquisas levadas a efeito com grupos de pessoas menos afeitas ao uso das novas tecnologias, mostraram que um uso maior da Internet por essas pessoas resultou num declínio da interação social delas, em primeiro lugar, com suas próprias famílias, e em segundo lugar, com seus amigos, para na seqüência, culminar com sintomas sócio-psíquicos como depressão e solidão. Outros estudos conduzidos em 2000 e 2001 também nos Estados Unidos,

demonstraram que o uso dessa rede, além de um determinado limite e sob certas circunstâncias, pode sim, acabar substituindo outras atividades sociais.

No caso brasileiro, acompanha-se ainda de forma empírica, que a comunicação via Internet tem se mostrado como alternativa para o lazer dos jovens brasileiros, em especial, daqueles que moram nas grandes cidades. O tempo e os recursos financeiros necessários para locomoção física a bares, restaurantes, cinemas, teatros, entre outros, vêm diminuindo nos últimos anos no país, por conta de questões estruturais como o desemprego. O número de jovens que desenvolvem atividades de lazer na Internet, no item "Jogar ou fazer o *download* de jogos", foi de 37% no total Brasil em 2006[7], sendo que a faixa etária predominante situou-se entre 10 e 15 anos de idade (66,69%), seguida de 39,18% de jovens entre 16 e 24 anos. No item "Fazer o *download* de filmes, músicas e *softwares*" há uma distribuição mais eqüitativa entre todas as faixas etárias, que na amostra da pesquisa vão de 10 a mais de 60 anos. Assim mesmo, as faixas etárias que congregam pessoas jovens nesta atividade, concentraram as maiores participações (31,41% para 16 e 24 anos e 25,93% para 25 a 34 anos).

No caso específico de jovens e adolescentes, alguns estudos acadêmicos já demonstram a importância de seu pertencimento às comunidades virtuais de games. Pesquisa realizada entre os jogadores do *World of Warcraft* [8] (um dos jogos com maior número de jogadores e contas ativas no mundo), demonstrou que as relações estabelecidas durante os jogos tendem a perdurar e há desenvolvimento de afeto e compromisso de encontros virtuais regulares. Este jogo insere-se nos jogos chamados de RPG (*Rolle-Playing Game*), que são jogos de representação de papéis, nos quais os jogadores criam e assumem identidades para interpretar em um universo criado previamente.

Esses grupos formam, dentro do jogo, micro-esferas sociais nas quais se apóiam mutuamente dentro de dinâmicas específicas e representam uma espécie de fuga da realidade cotidiana:

> Como visto nas entrevistas, muitos apontam como motivo maior para jogar ou continuar jogando o apoio nas relações sociais de amizade cultivadas ao

[7] Pesquisa sobre o Uso das TIC's (Tecnologias da Informação e da Comunicação) no Brasil – 2006. TIC Domicílios.

[8] World of Warcraft é um MMO-RPG (*Massive Multiplayer Online*) da produtora Blizzard, um jogo massivo, on-line, de ação e aventura, no mundo fantástico de Azeroth, introduzido no primeiro jogo da série, Warcraft: Orcs & Humans em 1994. Disponível apenas para jogos *on-line*.

> longo do tempo. Revelam também como as ações coletivas muitas vezes acabam superando as individuais, sendo assim toda a estrutura do jogo demonstra funcionar, pois ela se apoiou e apostou no fato da interação humana, mesmo que virtual, mantivesse as pessoas jogando. Embora muitas adorem essa realidade virtual, elas também demonstram o interesse da fuga talvez como o antigo conceito árcade: fugere urbem (fugir da cidade), ou mesmo somente para fugir da rotina como muitos também caracterizaram o jogo, após jogar há muito tempo. E essa fuga, essa necessidade de dar um tempo na realidade, levou os jogadores a buscarem no WOW uma maneira rápida de se desligar dos problemas, de fugir para outra realidade, como disse o entrevistado Luiz: *"O jogo acaba levando a pessoa para outro mundo."* E esse mundo seria a pasárgada de Manuel Bandeira: é aquele mundo idealizado onde você pode fazer o que quiser. E ter amigos nesse outro universo, nessa realidade paralela (MAIA; CAMARGO, 2007, p. 16).

Com respeito a essa etapa da vida (adolescência/juventude), há que se destacar que estão construindo suas identidades através de um processo de auto-descobrimento e busca de referências para o "vir-a-ser". A interação *on-line* proporcionada pelo uso da Internet pode ser significativa para compreendermos melhor este processo (CASTELLS, 2003, p. 99).

Outra tendência que cresce entre os internautas é o "infoentretenimento" (mescla de informação e entretenimento). O índice de pessoas que ouvem rádio e/ou televisão na Internet chegou a 27% na Pesquisa sobre o Uso das TIC's (Tecnologias da Informação e da Comunicação) 2006, um dos importantes referenciais utilizados neste estudo. A gama de atividades desenvolvidas na Internet pelos indivíduos e sua adesão às comunidades virtuais, bate-papos, infoentretenimento, participação política, correio eletrônico, entre outros, atestam o que Castells denomina como virtualidade real, gerada pela comunicação eletrônica na rede:

> (...) É um sistema em que a própria realidade, (ou seja, a experiência simbólica/material das pessoas) é inteiramente captada, totalmente imersa em uma composição de imagens virtuais no mundo do faz-de-conta, no qual as aparências não apenas se encontram na tela comunicadora da experiência, mas se transformam na experiência. Todas as mensagens de todos os tipos são incluídas no meio porque este fica tão abrangente, tão diversificado, tão maleável, que absorve no mesmo texto de multimídia toda a experiência humana, passado, presente e futuro (...) (CASTELLS, 1999, p. 395).

A magia da Internet enquanto multimídia parece ser sua capacidade de aglutinar a grande diversidade de expressões culturais, na forma de texto, imagem e sons, construindo um ambiente simbólico significativo capaz de trazer ao indivíduo o global no local, possibilitando, ainda que virtualmente, a vivência de experiências que jamais teria fora da rede.

2.3 Gestão da Internet no mundo

A gestão da Internet no mundo ainda é uma abordagem de gerenciamento em fase experimental, quando se consideram os diferentes estágios nos quais se encontram os países com relação à inclusão e ao uso da comunicação mediada pela Internet.

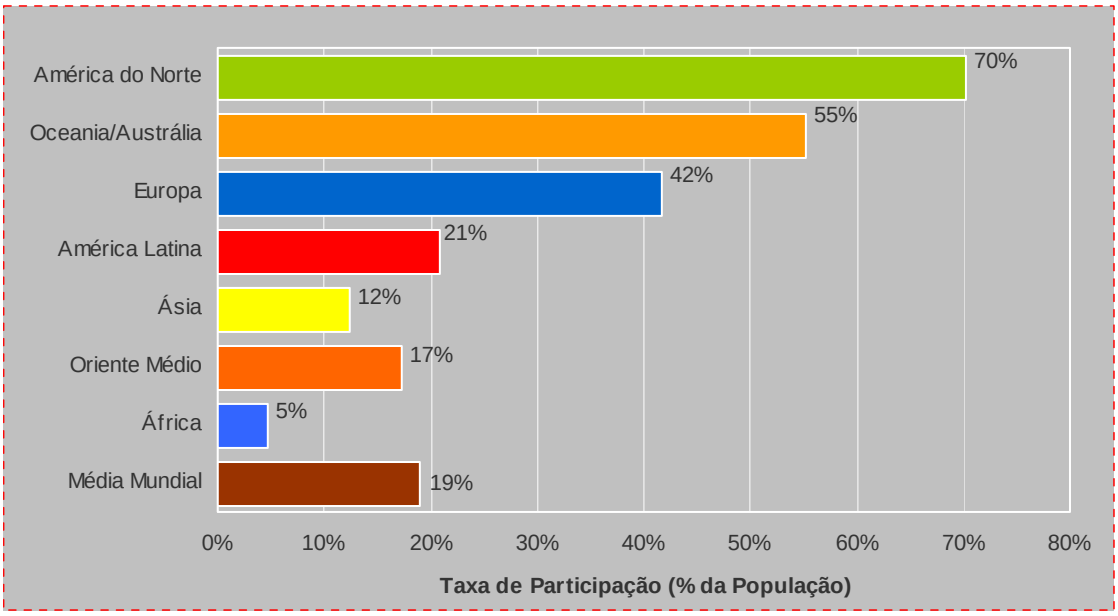
Estatísticas publicadas no *site* Internet World Stats, mostram o número de internautas e sua relação com a população das regiões do mundo.

Tabela 1 – Usuários de Internet e estatísticas populacionais (2000-2007)

Regiões do Mundo	População (2007) (Nº.)	Pop. do Mundo (%)	Usuários Internet (Data mais recente) (Nº.)	Pop./Participação (%)	Usuários Mundo (%)	Crescimento de Usuários 2000-2007 (%)
África	933.448.292	14,2	43.995.700	4,7	3,5	874,6
Ásia	3.712.527.624	56,5	459.476.825	12,4	36,9	302,0
Europa	809.624.686	12,3	337.878.613	41,7	27,2	221,5
Oriente Médio	193.452.727	2,9	33.510.500	17,3	2,7	920,2
América do Norte	334.538.018	5,1	234.788.864	70,2	18,9	117,2
Am. Latina/Caribe	556.606.627	8,5	115.759.709	20,8	9,3	540,7
Oceania/ Austrália	34.468.443	0,5	19.039.390	55,2	1,5	149,9
Total Mundo	6.574.666.417	100,0	1.244.449.601	18,9	100,0	244,7

Fonte: adaptado de Internet World Stats (2007).

O aumento da quantidade de usuários no período, nas regiões mencionadas na Tabela 1, evidencia a expansão de usuários de Internet do Oriente Médio (920,2%), seguido pela África (874,6%) e América Latina (540,7%), situadas bem acima da média mundial. Tal expansão indica que as populações dos países em desenvolvimento estão sendo incluídas nas novas tecnologias de informação e comunicação, com ênfase para a Internet.

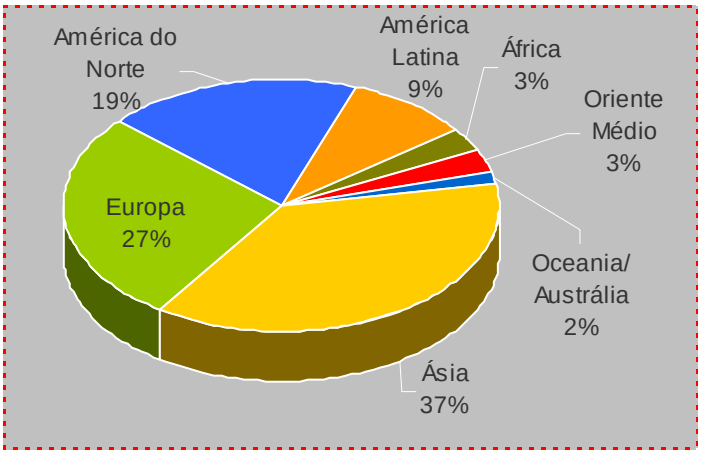


Fonte: adaptado de Internet World Stats (2007)

Figura 1 – Presença da Internet por região no mundo em percentagem (2007)

A Tabela 1 e a Figura 1, ao mostrarem a população das regiões mundiais em números absolutos, comparado ao número de internautas, demonstram que a participação em percentual do meio é muito maior na América do Norte, Oceania/Austrália e Europa, confirmando que a exclusão digital ainda é grande nos países em desenvolvimento.

A Figura 2, a seguir, demonstra a importância da Ásia no acesso à Internet: 459 milhões dos internautas são daquele continente, representando 37% de toda a população que se conecta à rede no mundo. Os internautas asiáticos se concentram principalmente nas áreas urbanas desenvolvidas, dos países chamados “Tigres Asiáticos” (Coréia do Sul, Hong Kong, Taiwan, Cingapura), “Novos Tigres Asiáticos” (Vietnã, Indonésia, Malásia, Filipinas) e no Japão e leste da China.



Fonte: Internet World Stats (2007)

Figura 2 – Percentual de usuários de Internet, segundo as regiões do globo (2007)

Os números demonstrados na Tabela 1 e nas Figuras 1 e 2 evidenciam o crescimento de usuários no período de 7 anos (2000 a 2007), bem como o potencial de expansão existente para que a Internet cresça exponencialmente em quantidade de usuários e em importância na comunicação e nos negócios.

Para que todo o aparato que envolve a rede funcione, há uma organização internacional que trabalha para garantir que todos os usuários da Internet possam encontrar seus endereços válidos. A entidade responsável por atribuir os domínios e os endereços e fixar regras para a utilização da rede mundial é a ICANN (*Internet Corporation for Assigned Names and Numbers*), que substituiu a IANA (*Internet Assigned Numbers Authority*), entidade que anteriormente realizava as funções de administração da Internet através de contratos firmados com o governo dos Estados Unidos e que hoje é subordinada à ICANN, realizando algumas de suas tarefas por delegação.

A ICANN é descrita em seu *site* (O que é a ICANN?), conforme a seguir:

> A ICANN - Internet Corporation for Assigned Names and Numbers (órgão mundial responsável por estabelecer regras do uso da Internet) é uma entidade sem fins lucrativos e de âmbito internacional, responsável pela distribuição de números de “Protocolo de Internet” (IP), pela designação de identificações de protocolo, pelo controle do sistema de nomes de domínios de primeiro nível com códigos genéricos (gTLD) e de países (ccTLD) e com funções de administração central da rede de servidores. Sendo uma sociedade de capital misto, a ICANN se dedica à manutenção da estabilidade operacional da Internet, à promoção da concorrência, a obter uma ampla representação das comunidades globais congregadas na Internet e ao desenvolvimento de uma política adequada à sua missão, com

> processos consensuais, implantados através da abordagem "bottom-up" (de baixo para cima) (ICANN, 2007ª, *online*).

O Relatório Anual 2007da ICANN define como seus valores-base:

> No desempenho da sua missão, os seguintes valores fundamentais dirigem as decisões e ações da ICANN:
>
> 1. Preservar e aumentar a estabilidade operacional, a confiabilidade, segurança e interoperabilidade global da Internet.
> 2. Respeitar a criatividade, inovação e o fluxo de informações que se tornaram possíveis graças à Internet, limitando as atividades da ICANN aos assuntos que fazem parte da sua missão e que exigem ou se beneficiam com a coordenação global.
> 3. Na medida do possível, delegar as funções de coordenação a outras entidades, ou reconhecer o papel normativo de outras entidades responsáveis que refletem os interesses das partes afetadas.
> 4. Procurar e incentivar a participação ampla e informada, de forma a refletir a diversidade funcional, geográfica e cultural da Internet em todos os níveis normativos e deliberativos.
> 5. Sempre que for viável e conveniente, depender de mecanismos de mercado para promover e manter um ambiente competitivo.
> 6. Introduzir e promover a concorrência no registro de nomes de domínio, sempre que isso for possível e vantajoso no interesse público.
> 7. Aplicar mecanismos normativos abertos e transparentes que (i) possibilitem decisões bem fundamentadas e baseadas no parecer de especialistas e (ii) garantam que as entidades mais afetadas possam participar do processo normativo.
> 8. Tomar decisões aplicando políticas documentadas de forma neutra e objetiva, com integridade e justiça.
> 9. Agir com a rapidez correspondente às necessidades da Internet e ao mesmo tempo, como parte do processo deliberativo, obter sugestões e comentários das entidades mais afetadas.
> 10. Prestar contas à comunidade da Internet por intermédio de mecanismos que aumentem a eficiência da ICANN.
> 11. Mesmo estando enraizada no setor privado, reconhecer que governos e autoridades públicas são responsáveis por políticas públicas e levar em conta as recomendações desses governos ou autoridades públicas (ICANN, 2007b, p. 8).

O principal compromisso da ICANN é operacional em relação à funcionalidade e estabilidade da rede, ou seja, as questões de controle de conteúdos veiculados, bem como o estabelecimento de regras para transações financeiras e proteção contra “spam” [9] não fazem parte de suas atribuições.

A ICANN trabalha através de parcerias com empresas e pessoas qualificadas em todo o mundo. A natureza mutável e em constante crescimento e inovação, trazida pela tecnologia Internet, faz com que a entidade seja auto-

[9] Mensagens eletrônicas comerciais não solicitadas.

regulamentada, isto é, não se submeta às políticas ditadas pelos Governos dos países. Como existe a clara necessidade de que as ações necessárias para gestão da rede sejam implementadas de forma imediata, a ICANN se apresenta com um modelo de gestão completamente inovador. De acordo com Castells, a ICANN:

> (...), é uma corporação privada, sem fins lucrativos, (...) Embora sua prática real e sua estrutura organizacional ainda estejam se desenvolvendo, suas normas incorporam o espírito de abertura da Internet, a descentralização, a formação de consenso e a autonomia que caracterizaram o governo *ad hoc* da Internet ao longo de trinta anos, acrescentando uma orientação global à composição da organização, embora tenha como sede Marina del Rey, na Califórnia (CASTELLS, 2003, p.31).

O modo como a ICANN nasceu e continua operando hoje é assim, considerado por Castells (2003, p. 32), um dos fatores-chave para o sucesso da Internet. Isso foi possível graças aos pioneiros da rede (especialmente os pesquisadores norte-americanos Vinton Cerf e John Postel), que compartilharam as inovações tecnológicas e conseguiram manter a liberdade que pressupõe sua estrutura.

De acordo com Cerf (ICANN, 2007b p. 11), que presidiu a entidade de 2000 a 2007, a revisão de desempenho e a estrutura da ICANN são as grandes forças de seu modelo. Isto é possível, segundo ele, graças a uma agenda em que constam as reavaliações de seus elementos organizacionais e uma visão clara dos objetivos operacionais. Cita também a comunidade da Internet e o Departamento de Comércio dos Estados Unidos como agentes questionadores da entidade de forma constante, o que acaba contribuindo para o processo que visa à transição contínua da coordenação técnica e do manejo do sistema de nomes e domínios da Internet para o setor privado.

A respeito do modelo de governança implementado na entidade, Cerf também reafirma o compromisso com a transparência no desenvolvimento e divulgação de suas políticas. Ele acredita que a entidade tem a oportunidade e a obrigação de continuar a melhorar a interação eficiente entre o Comitê Consultivo para Assuntos Governamentais e as demais estruturas da ICANN para alcançar cooperação avançada em áreas de política envolvendo interesses públicos. O Comitê Consultivo é constituído por membros de 120 governos ou instituições

governamentais em todo o mundo, que têm a missão de assessorar a diretoria da ICANN com respeito a políticas para Internet de seus respectivos países.

Na esfera individual, qualquer usuário da Internet, como membro da sociedade civil, tem assegurada sua entrada em assuntos de interesse público, através de representantes de organizações de usuários individuais e comunidades técnicas. Tal participação foi definida como sendo necessária para a atuação democrática da organização (ICANN, 2007a, p. 9).

Hoje, a ICANN realiza a governança eletrônica, que funciona mais como uma administração de consenso e busca de constante inovação realizada por uma estrutura descentralizada que se encontra periodicamente através de encontros de grupos de trabalho e conta com o apoio de comissões consultivas.

Governança é um conceito que vem sendo utilizado quando se pretende abordar gerenciamento, tanto do setor privado, quanto do setor público, e não apenas para caracterizar a gestão da Internet. No setor privado, a definição de governança é descrita no *site* do IBGC (Instituto Brasileiro de Governança Corporativa):

> Governança corporativa é o sistema que assegura aos sócios-proprietários o governo estratégico da empresa e a efetiva monitoração da diretoria executiva. A relação entre propriedade e gestão se dá através do conselho de administração, a auditoria independente e o conselho fiscal, instrumentos fundamentais para o exercício do controle. A boa governança corporativa garante eqüidade aos sócios, transparência e responsabilidade pelos resultados (accountability) (IBGC, 2008, *online*).

Frey (2002, p.144) descreve a origem da governança no setor público:

> A ampliação do debate sobre governança deve-se certamente à retração do Estado, promovida pelas estratégias neoliberais das últimas duas décadas, e à clara incapacidade das instituições públicas enfraquecidas para lidar eficientemente com os crescentes problemas urbanos, ou como mencionou STOCKER: “A governança é a parte aceitável dos cortes de gastos” (citado em Rhodes, 2000:55). Essa polêmica afirmação revela a ambigüidade da abordagem de governança. Se, por um lado, ela propõe ser uma abordagem neutra para descrever as transformações que estão realmente ocorrendo em sistemas políticos modernos, por outro, existem evidências claras acerca das premissas ideológicas das diferentes concepções. Em geral, podemos distinguir entre as versões de governança que enfatizam como objetivos principais o aumento da eficiência e da efetividade de aspectos governamentais e as que focalizam primariamente o potencial emancipatório de novas abordagens de governança.

A governança como opção para gerenciamento da Internet insere-se tanto no aumento da eficiência para lidar com as questões tecnológicas quanto está de acordo com o caráter multidisciplinar do conhecimento que é exigido para se tratar com elas. Ainda é necessário acrescentar que para além da governança eletrônica, o uso da Internet insere-se na dimensão política e já é palco para experiências nessa área, como por exemplo, as campanhas eleitorais e a votação eletrônica. Os partidos políticos têm utilizado os *websites* em suas campanhas eleitorais nos Estados Unidos, Austrália, Finlândia, Itália, Reino Unido, Alemanha e Brasil (IASULAITIS, 2008, p. 126).

As experiências mediando a esfera política através da Internet apresentam possibilidades e limites, conforme Gomes (2005, p.220-221):

> No rol das vantagens políticas da Internet, insiste-se com freqüência nas novas possibilidades de expressão que permitem a um cidadão ou a um grupo da sociedade civil alcançar, sem maiores mediações institucionais, outros cidadãos, o que promoveria uma reestruturação, em larga escala, dos negócios públicos e conectaria governos e cidadãos. (...) Por outro lado, apenas o acesso à Internet não é capaz de assegurar o incremento da atividade política, menos ainda da atividade política argumentativa. (...) Pesquisas sugerem que a esfera política virtual de alguma maneira reflete a política tradicional, servindo simplesmente como um espaço adicional para a expressão da política mais do que como um reformador radical do pensamento e das estruturas políticas.

É importante distinguir ainda a diferença entre governança eletrônica da Internet e governo eletrônico, sendo este último: “(...) a contínua otimização da prestação de serviços do governo, da participação dos cidadãos e da administração pública pela transformação das relações internas e externas através da tecnologia, da Internet e dos meios de comunicação” (GARTNER GROUP, 2000 apud FERGUSON, 2002, p.104). Dessa maneira, o governo eletrônico possibilita uma interação do cidadão com sua administração de forma direta, permitindo uma flexibilização no atendimento através do horário estendido (muitas vezes há serviços disponíveis 24 horas) e ainda uma democratização da esfera pública.

A governança eletrônica da Internet é fundamental para o funcionamento da rede. Conforme Gindre (2008, p. 68):

> Ao contrário do que o senso comum indica, a Internet não é uma rede anárquica e sem controle. De fato, existe um complexo, multifacetado e muitas vezes contraditório sistema internacional que garante a chamada

> "governança da Internet". Este modelo se constituiu historicamente mediante processos que ocorreram em paralelo, alguns em âmbito nacional (em especial nos Estados Unidos) e sem coordenação entre si.

O modelo de governança da Internet, cujo histórico é resgatado por Gindre, possui uma complexa estrutura de atuação internacional, que é a ICANN. O fato de a entidade responder diretamente ao Departamento de Comércio dos Estados Unidos da América é alvo de críticas, contudo reconhece-se a importância da ICANN, uma vez que a mesma administra com eficiência todo o sistema de nomes e números da Internet, sistema sem o qual, nas palavras de Gindre (2008, p. 69) "(...) ninguém 'vê' ninguém na Internet".

O fato de a ICANN ser a entidade responsável pela governança eletrônica mundial e ao mesmo tempo, estar sediada na Califórnia, território americano, é considerada por Getschko, como uma fase de transição neste processo de gestão:

> *(...) o Departamento de Comércio Americano, ficou encarregado, digamos, de supervisionar essa transição até o ICANN ser auto-suficiente e ter um funcionamento devidamente é, digamos, tranqüilo, garantido, correto, neutro e tudo mais. Por vários motivos, que é muito longo explicar agora e que depois podemos discutir com cuidado, essa transição até agora não acabou, isso gera evidentemente uma polêmica de porque um determinado governo tem mais controle do que o outro na rede, visto que está gerindo essa transição para o ICANN. O ICANN é uma organização na Califórnia, uma organização, portanto que segue as leis norte-americanas, e isso também pode ser um motivo de polêmica, talvez devesse ser uma organização mais neutra ou internacional de alguma forma, mas eu queria deixar muito claro isso, quer dizer, a Internet nunca foi ligada nem a governos, nem a empresas privadas e nem mesmo à academia em si, mas sim a grupos que cooperavam para que isso funcionasse, então, ela é o que a gente chama de uma rede multistakeholder, você tem vários segmentos interessados no seu desenvolvimento, interessados no seu progresso e esses segmentos cooperam entre si. Tanto a área acadêmica, quanto o governo, quanto o setor privado e, pelo menos em minha opinião, seria fundamental, "pra" liberdade da rede, para o crescimento da rede, que essa característica fosse mantida, essa característica de cooperação entre todos os segmentos e essa característica de não controle da rede por um determinado setor específico.*

Além da ICANN e de sua subordinada IANA (*Internet Assigned Numbers Authority*), outras entidades atuam para o funcionamento da Internet nos aspectos relativos à infra-estrutura, por onde trafegam os conteúdos e nos aspectos relativos aos parâmetros técnicos da rede, especialmente com respeito à padronização dos protocolos. Estas organizações que são a ITU (*Internacional Telecommunications Union*), a IETF (*Internet Engineering Task Force*) e o W3C (*World Wide Web Consortium*) tomam decisões que acabam influenciando o modelo de negócios da Internet, por mais técnicas que sejam, pois os padrões de software definidos por estas entidades, acabarão por beneficiar uma ou outra grande empresa, conforme relata Gindre (2008, p.70-71): “(...) Por exemplo, o resultado da disputa entre padrões abertos e proprietários é crucial para definir o sucesso, ou o fracasso, de gigantes como Microsoft, HP e Sun“.

A ITU (*Internacional Telecommunications Union*) editou uma recomendação descrita abaixo por Gindre (2008, p.70) e cujos efeitos são percebidos pelos usuários dos países mais pobres:

> É a sua Recomendação D.50 (*International Internet Connection*), por exemplo, que define os critérios para a cobrança dos “custos de interconexão das redes”. Esta é uma questão fundamental porque, para que um país tenha acesso à Internet, ele precisa garantir que sua(s) rede(s) irá (irão) se conectar a um (ou mais de um) *backbone* internacional, que são as espinhas dorsais da rede, capazes de distribuir o tráfego da Internet pelo mundo. Ocorre que estes *backbones* são privados e os custos de interconexão, além de altíssimos, acabam promovendo um subsídio cruzado às avessas, cobrando mais caro dos países mais pobres, que possuem menor poder de negociação frente às operadoras privadas dos *backbones*. Graças à fragilidade da Recomendação D.50 (e aos sucessivos repasses de custos ao longo da cadeia produtiva da conexão de Internet), o usuário final na cidade de Salvador paga R$ 0,16 à empresa Telemar por um Kbps enquanto em Londres ele pagaria R$ 0,01 à British Telecom (uma diferença de 1.600%).

Considera-se que a gestão da Internet no mundo não está suficientemente discutida e sua estrutura, tendo a ICANN como espinha dorsal, ainda responde diretamente a um único país, os Estados Unidos da América. Portanto, há um longo caminho a ser percorrido para que a gestão da Internet incorpore as necessidades dos países menos desenvolvidos no processo de inclusão digital.

2.4 Gestão da Internet no Brasil

No Brasil existem vários programas governamentais na área de inclusão digital. Um destes programas é o GESAC (Governo Eletrônico Serviço de Atendimento ao Cidadão), criado pelo Ministério das Comunicações em 2002. O GESAC tem como objetivo estar presente em todos os 5.565 municípios brasileiros, levando alternativas para acesso a computadores e à Internet. Segundo informa o site do Ministério, cerca de 5.000 prefeituras já estão equipadas com os Kits necessários à implantação dos telecentros comunitários, locais onde funcionarão os programas de acesso e inclusão digital (BRASIL, 2008b).

A inclusão digital, aparentemente, poderá não ocorrer primordialmente através de programas governamentais, e sim, impulsionada pela expansão mundial do comércio eletrônico, que inclui a venda de telefones celulares, linhas de TV's a cabo e câmeras digitais como chamarizes para a venda de computadores e conexão banda larga, no processo denominado "convergência das mídias".

Há visões críticas a respeito da real necessidade de inclusão digital como prioridade de governo. Esta é, por exemplo, a opinião de Antônio Tavares, membro do comitê Gestor da Internet e Presidente da ABRANET, na entrevista concedida a este trabalho, na sede DIALDATA Telecomunicações LTDA., em São Paulo (SP), no dia 16 de janeiro de 2008:

> *Eu sou um pouco crítico na forma com que se pensa a inclusão digital no Brasil, porque, num país em que nós temos que pensar ainda em bolsa família, pensar em inclusão digital é inverter a hierarquia das necessidades fisiológicas das pessoas. Habitação, alimentação, há que tratar primeiro disso. Só pra que nós possamos dizer que nós temos uma penetração de Internet de 90%, mas os meninos não podem se alimentar, morrem. Precisa ter muito cuidado da forma como se aborda isso. É muito lindo dizer: os meninos vão ter um computador, todo mundo vai ter um computador na escola. Ótimo. E os meninos vão à escola? Tá? E os meninos estão sendo alimentados? Gente que tem que receber do governo bolsa família, como se de uma esmola se tratasse, eu pergunto: isso serve para os políticos, para alavanca prá se eleger, ou vai servir efetivamente? Claro que a desigualdade é muito grande. Há que se criar desenvolvimento no país capaz de auto-sustentação das pessoas se cuidarem, das pessoas crescerem e terem direito à vida digna. E aí, a inclusão acontece naturalmente, não tem que ser um negócio forçado. Eu quando*

> *vejo um Presidente da República chegar e dizer: até 2010 eu quero todas as escolas com Internet, isso aí é muito bonito, mas isso interessa somente ao bolso de alguns que vão produzir bens, serviços e vão ter resultados políticos nisso. Então eu sou um pouco crítico e é a minha visão.*

Embora o tema da inclusão digital no Brasil suscite debates a respeito de melhores caminhos e alternativas com menores custos para alcançar as mais distantes localidades do país, os grandes centros urbanos já dispõem de uma estrutura de boa qualidade para o tráfego da Internet.

Os números da Internet no Brasil, embora ainda não sejam tão expressivos como aqueles apresentados pela América do Norte e Europa, já exibem uma penetração expressiva deste veículo de comunicação. Dessa maneira, já é possível efetuar algumas análises, a partir dos resultados das Pesquisas sobre o Uso das Tecnologias da Informação e da Comunicação no Brasil e que abrangem todo o território nacional (Anexo A).

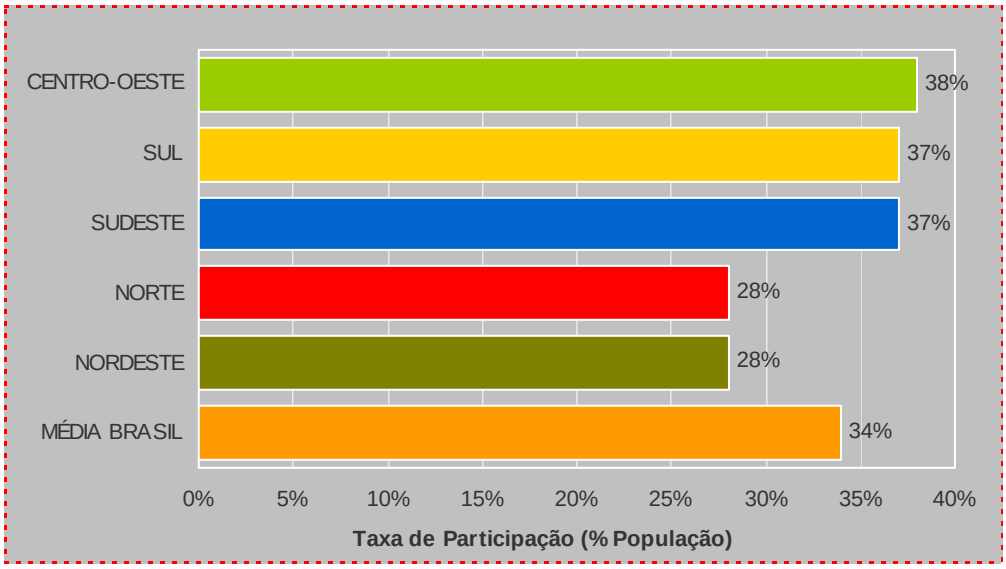
A Tabela 2 demonstra o percentual da população usuária de Internet de cada uma das regiões e o índice de suas participações no total Brasil.

Tabela 2 – Usuários de Internet e estatísticas populacionais do Brasil (2007)

Região do Brasil	População (IBGE, 2007)	População do Brasil (%)	Usuários de Internet	Participação (%)	Usuários em relação aos usuários total Brasil (%)
Sudeste	79.753.141	42,6	29.508.662	37	46,5
Nordeste	51.713.072	27,6	14.479.660	28	22,8
Sul	27.368.019	14,6	10.126.167	37	16,0
Norte	15.080.183	8,0	4.222.451	28	6,7
Centro-Oeste	13.313.377	7,2	5.059.083	38	8,0
Total Brasil	187.227.792	100	63.396.023	34	100

Fonte: Pesquisa TIC Domicílios – 2007 (BALBONI, 2008)

Na Figura 3, tem-se o percentual dos usuários de Internet considerando-se regiões do país.



Fonte: Dados extraídos da Pesquisa TIC Domicílios - 2007 (BALBONI, 2008).

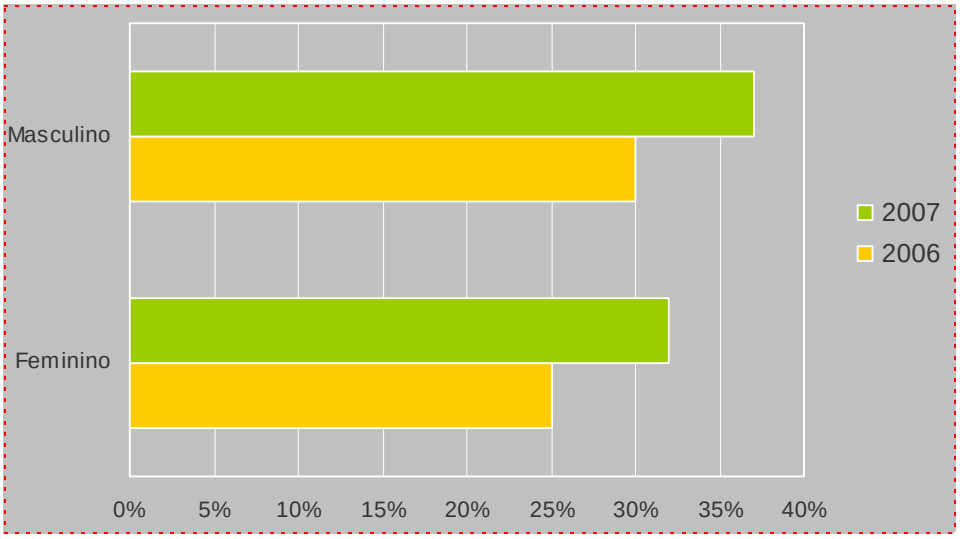
Figura 3 – Presença da Internet por Região no Brasil (2007)

Os estados do centro-oeste (38%) superaram percentualmente o número de usuários sediados no Sul e no Sudeste (37%), dado que, à primeira vista, surpreende um pouco, embora esta tendência tenha sido evidenciada desde a Pesquisa 2006, quando a Região Centro-Oeste apresentou 34% no índice de penetração, superando também os estados do Sul e Sudeste, que detinham 30 e 29%, respectivamente, deste índice.

As regiões Norte e Nordeste, ambas com 28% de penetração, mostram que há dificuldades ainda a serem superadas para aumento de suas plataformas digitais. Em 2006, essas regiões detinham 21 e 18% na participação de usuários Brasil. A região Nordeste mostrou crescimento expressivo de 10 pontos percentuais, o maior dentre todas as regiões brasileiras.

A média de usuários de Internet em relação à população total do Brasil situou-se em 26% em 2006 e 34% em 2007, acima da média mundial, que foi de 19% no ano de 2007, conforme demonstrado na Tabela 1.

A Figura 4 apresenta o perfil de gênero entre usuários da Internet no Brasil nos anos de 2006 e 2007.

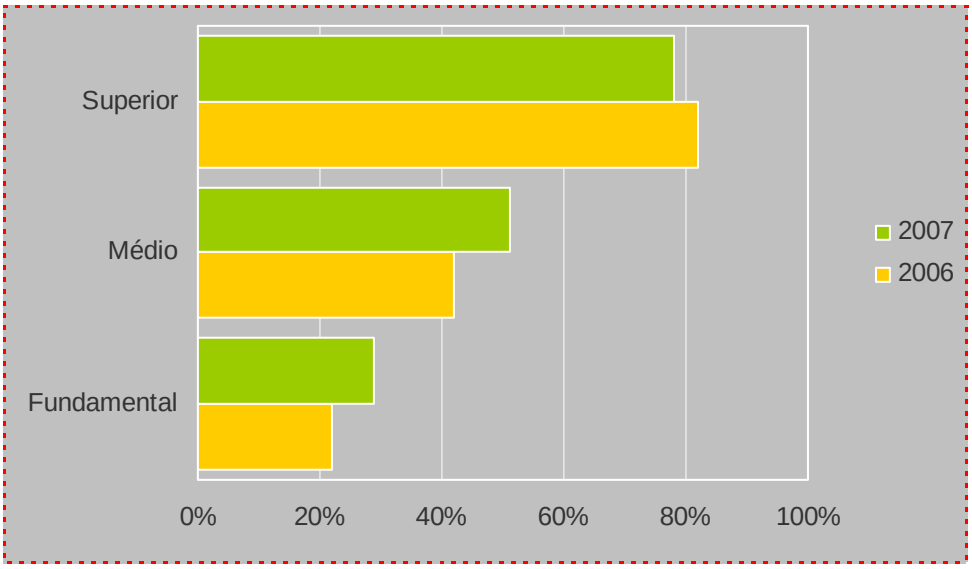


Fonte: Dados extraídos da Pesquisa TIC Domicílios 2006 e 2007 (BALBONI, 2007; 2008).

Figura 4 – Usuários de Internet por gênero (2006-2007)

Ambos os gêneros cresceram em participação no mesmo patamar: 7 pontos percentuais, embora a predominância na utilização seja masculina nos dois períodos analisados. Em 2006, a participação masculina ficou em cerca de 30% e a feminina em 25% sobre o total da população usuária. Em 2007, estes números situaram-se em 37% de participação para o público masculino e 32% para o público feminino.

O acesso à Internet continua sendo privilégio do público com maior formação educacional. As Pesquisas sobre o uso das Tecnologias de Informação e Comunicação (TIC Domicílios) 2006 e 2007 demonstram que o nível de participação na utilização da Internet ainda é maior nas populações com maior nível de estudos, porém apontam também o crescimento do acesso de um ano para o outro, das populações com grau de instrução fundamental e médio, como se pode comprovar na seqüência demonstrada pela Figura 5.



Fonte: Dados extraídos da Pesquisa TIC no Brasil 2006 e 2007 (BALBONI, 2007; 2008).

Figura 5 – Usuários de Internet por graus de instrução em percentual (2006-2007)

Curiosamente, a Figura 5 demonstra que o acesso à Internet diminuiu no público com grau de formação superior, o que pode significar uma acomodação no uso do veículo.

Tabela 3 – Classes sociais e o uso da Internet em percentual (2006-2007)

Classe Social	2006 (%)	2007 (%)
A	93	89
B	66	66
C	31	38
D/E	8	14

Fonte: Dados extraídos da Pesquisa TIC no Brasil 2006 e 2007 (BALBONI, 2007; 2008).

Quanto às classes sociais, o fenômeno a destacar é a expansão da Internet nas camadas sociais D/E, totalizando 13 pontos percentuais de crescimento no acesso para a somatória de ambas, conforme demonstra a Tabela 3. Segundo Gomes, a tendência crescente de acesso ao universo digital das classes menos privilegiadas em termos econômicos é verificada em todos os países, entretanto, em velocidades distintas:

> “(...) em toda parte há evidências de que o fosso que separa os ricos dos pobres em oportunidades de acesso à Internet vem diminuindo, numa velocidade maior nos países industrializados e com maior dificuldade nos outros países. De toda sorte, esta evolução tenderá a se estabilizar nos limites das classes sociais, isto é, conduzirá no máximo a que os integrantes das classes altas e médias tenham um acesso homogêneo ao mundo digital, a prescindir de diferenças de sexo, status e idade, por exemplo. No extremo, integrará, através do serviço público, os membros das classes baixas que possuam capital cultural semelhante àquele das classes superiores” (GOMES, 2005, p.72).

Embora no Brasil a Internet seja algo recente (sua história no Brasil começa a se delinear em 1988/1989), temos hoje pessoas e instituições extremamente profissionais a cuidar desta tecnologia surpreendentemente inovadora. Os dados exibidos nas Tabelas 2 e 3 e nas Figuras 4 e 5, constantes das edições anuais da Pesquisa sobre o uso das Tecnologias da Informação e da Comunicação no Brasil, de responsabilidade do Comitê Gestor da Internet no Brasil, através do CETIC (Centro de Estudos sobre as Tecnologias de Informação e Comunicação no Brasil) são gerados justamente por pessoas que realizam no país a coordenação das atividades de Internet, em uma gestão descentralizada.

Conforme descrito anteriormente, a entidade que realiza a governança da Internet em nosso país é o Comitê Gestor da Internet no Brasil, criado em 1995 através de Portaria Interministerial e redefinido em 2003, via Decreto Presidencial. Esta entidade vem atuando segundo o modelo *multistakeholder*, ou seja, uma gestão cooperativa, da qual participam membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica.

Procura-se, dessa maneira, que a sociedade efetivamente participe das decisões relativas ao funcionamento da Internet no Brasil nas suas dimensões vitais: registro de domínios, infra-estrutura de redes, prevenção e resposta para manutenção da segurança tecnológica e produção de indicadores e estatísticas. Além destas áreas, mantém os grupos de trabalho de engenharia e segurança de redes e formação de recursos humanos cuja importância é a de subsidiar as decisões do Comitê Gestor nos âmbitos operacionais, técnicos e administrativos que envolvem a governança da rede no Brasil.

O modelo de governança utilizado para Internet brasileira compartilha experiências com outros países que também adotam a mesma política de gestão, que é uma experiência bastante recente.

No Fórum para Governança da Internet[10], cujo programa consistiu no debate em torno de cinco grandes tópicos (Recursos críticos para Internet, acesso, diversidade, abertura ou eliminação de restrições e segurança), as seguintes recomendações/deliberações foram discutidas:

- a necessidade de ampliação do acesso à rede, especialmente com relação à educação e ao conhecimento, reconhecidos e enfatizados como um dos mais essenciais direitos humanos;
- a importância de aumentar a participação de todos os países no processo de governança da Internet e a discussão das práticas que norteiam estes processos de gestão e organização;
- a situação da Internet na África e a questão de adaptar a governança da rede à situação local;
- a conveniência de se inserir os mecanismos que envolvem a governança na Internet num contexto mais amplo como as políticas discutidas pelo Conselho da Europa, pelo Convênio Europeu de Direitos Humanos e pelo Convênio sobre Ciberdelinquência, que pretendem orientar os Estados em suas políticas relativas à Internet. Além disso, pautar-se pelas deliberações do Conselho da Europa, que definiu os marcos internacionais a serem seguidos para o desenvolvimento da Internet na sociedade da informação;
- o respeito aos direitos humanos, bem como o direito à liberdade de expressão devem ser observados nas práticas e processos relativos à governança da Internet;
- a discussão das políticas concretas definidas por organizações e redes intergovernamentais públicas e privadas que tratam das questões de segurança e governança.

O pensamento dos gestores brasileiros comunga de seus pares internacionais, no tocante à necessidade de se manter a Internet com sua característica de liberdade, sendo este fator considerado como chave para garantir

[10] 2º Reunião do IGF (*The Internet Governance Fórum*) realizada no Rio de Janeiro, entre os dias 12 e 15 de novembro de 2007 (IGF, 2007).

sua estabilidade e segurança. De acordo com essa visão, não há que se criarem quaisquer controles na rede com relação a seus participantes:

> A rede é uma construção coletiva que não pressupõe barreiras ou controles. Não tem porteiras, nem cancelas nem guardas. Quem tiver ao seu alcance os meios necessários para conectar-se deve ser estimulado a fazê-lo na forma que conseguir. É um participante na rede, tal como o é o transeunte na praça pública, o banhista do rio fresco, o viajante do panorama que se desdobra ante ele (GETSCHKO, 2007, p. 36).

No entanto, no mesmo artigo, Getschko (2007, p.36) faz a ressalva:

> Por outro lado, quem tem recursos alocados na rede – presença na rede – tem maior poder de ação sobre esta e sobre seus participantes e, desta forma, mais responsabilidades do que os que dela apenas usufruem como visitantes, ávidos leitores de informação ou meros espectadores. Quem mantém um domínio na rede para, a partir dele, criar seu sítio onde vai expor informações e serviços, quem tem um conjunto de números IP a ele atribuídos para a identificação de equipamentos ou a prestação de serviços à rede, esses têm responsabilidades específicas perante a comunidade.

Os provedores de serviço, que são na verdade os que têm presença na rede, segundo esta visão, devem zelar pela manutenção de boas práticas dos participantes. Para isso, é importante que os provedores mantenham os registros de seus usuários atualizados, e possam fornecer à Justiça, quando necessário, a identificação de endereços IP[11] que forem suspeitos de realização de fraudes ou crimes cibernéticos.

Na gestão da Internet brasileira, participam, além de representantes dos provedores, pessoas e associações interessadas de alguma maneira, na expansão do acesso à Internet com qualidade, e nas conseqüências do mau uso da mesma, como as organizações que denunciam crimes virtuais, como a SAFERNET (associação civil, com sede em São Paulo, que tem como objetivo principal promover o uso seguro das Tecnologias de Informação e Comunicação), por exemplo. O modelo de gestão da rede brasileira, que prevê a participação da sociedade civil é analisado por Gindre (2008, p. 72): "(...) O modelo de governança da Internet no Brasil é destacado, até mesmo internacionalmente, como referência,

[11] Endereço IP: número único para cada computador conectado à Internet, composto por uma seqüência de 4 números que variam de 0 a 255, separados por "." . Por exemplo: 192.168.34.25. (CGI, 2007a, p. 4/9).

por incorporar diferentes atores sociais e por ser o primeiro do mundo a ter membros eleitos".

Os membros do Comitê Gestor que representam o governo são indicados, porém aqueles pertencentes aos setores empresarial, terceiro setor e comunidade acadêmica e tecnológica são escolhidos através de votação não secreta, em colégio eleitoral, constituído por representantes legais de cada um dos segmentos.

As reuniões promovidas pelo Comitê Gestor têm periodicidade mensal e a pauta a ser discutida é pertinente a aspectos que necessitam de tomada de posição da entidade, sempre levando em consideração os interesses do país e a posição internacional.

Na visão de Tavares, o funcionamento do Comitê Gestor com respeito à gestão da Internet pode ser compreendido da seguinte maneira:

> *Comitê Gestor. Ele não existe "pra" fazer gestão de ninguém, ao mesmo tempo ele existe prá fazer gestão de tudo. E ele existe para cuidar de redes, pra cuidar das relações entre Governo e a sociedade civil (...) o Comitê Gestor ele tem um formato que é muito interessante, que é chamado de multistakeholder, todo tipo de segmento está representado. E isso é ótimo, quer dizer isso valoriza e revitaliza toda a sociedade envolvida, quer dizer qualquer problema que aconteça com determinado segmento é trazido para o Comitê Gestor para ser discutido e ali os vários parceiros podem interagir e o Comitê Gestor tomar decisões do tipo, sobre a forma de resolução. As resoluções do Comitê Gestor tem forma de lei? Não. Mas o interessante é isso, embora não tenham forma de lei, tem regras, normalmente técnicas, elas são auto-aplicáveis. Quem não aplicar vai estar fora do contexto, não consegue funcionar. Então, é muito efetivo e é muito respeitado.*

Embora tenha um formato de gestão democrático e esteja planejando e executando as diversas atividades exigidas para o adequado funcionamento da Internet brasileira, o Comitê Gestor enfrenta problemas que têm a ver muito mais com a ausência de políticas públicas claras para Internet, conforme a visão de Gindre (2008, p. 72):

> (...) o CGIbr paga o preço da inexistência de um marco regulatório capaz de lidar com o fenômeno da convergência das mídias, ao contrário do que foi feito em outros países. No Brasil, temos um Código Brasileiro de Telecomunicações (CBT), com exatos 45 anos de vida e que desde 1997

> ficou confinado a regular apenas a radiodifusão (mesmo assim, com regras totalmente defasadas). Bem como, uma Lei Geral de Telecomunicações (LGT) que, apesar de ter apenas 10 anos de existência, possui uma lógica anti-convergência e que, em nenhum momento menciona a expressão Internet e seus desdobramentos. Com a inexistência de um marco regulatório capaz de lidar com a Internet e a convergência de mídias, o CGIbr repousa como um corpo tão interessante quanto estranho ao funcionamento “normal” dos organismos de Estado.

Outros problemas estruturais do país se colocam como dificuldades para que se atinjam os objetivos definidos pelo Comitê Gestor da Internet, notadamente no que diz respeito ao “(...) estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil”, conforme descrito nas atribuições da entidade (CGI, 2008). Essas dificuldades se relacionam com a desigualdade entre os cidadãos, conforme analisa Gomes (2005, p.71):

> Uma autêntica experiência de democracia, acredita-se, depende basicamente de uma paridade fundamental dentre os cidadãos; paridade que deve ser superior e primária em face de todas as concretas disparidades que sobre ela se coloquem posteriormente. Daí a busca pela igualdade de oportunidades e pela equanimidade de meios e recursos, fenômenos que impõem naturalmente a busca de inclusão de todos os cidadãos na situação onde oportunidades, meios e recursos estão disponíveis para a ação política. Ora, sabe-se que nenhuma sociedade, nem mesmo aquelas mais homogêneas, até agora verificou uma distribuição equânime de acesso às oportunidades digitais de participação.

Nesse sentido, e não obstante os esforços de conselheiros e membros atuantes do Comitê Gestor, a gestão do veículo Internet empreendida por esta entidade, enfrenta, em sua dimensão política, problemas difíceis a serem superados a curto e médio prazo.

3 SEGURANÇA NA REDE

3.1 Internet e controles

A rapidez com que a Internet se desenvolveu desafia previsões quanto ao seu formato, expansão e usos. Há apenas alguns anos atrás, Castells (1999, p. 375), o cientista social que analisou os meandros da sociedade em rede, nos falava de uma rede cuja arquitetura impossibilitava quaisquer tipos de controles:

> Com base na tecnologia de comunicação por comutação de pacotes, o sistema tornou a rede independente de centros de comando e controle, de modo que as unidades de mensagem encontrariam suas rotas ao longo da rede, sendo remontadas com sentido coerente em qualquer ponto dela. Quando mais tarde, a tecnologia digital permitiu a compactação de todos os tipos de mensagens, inclusive som, imagem e dados, formou-se uma rede capaz de comunicar todas as espécies de símbolos sem o uso de centros de controle. A universalidade da linguagem digital e a lógica pura do sistema de comunicação em rede criaram as condições tecnológicas para a comunicação horizontal global. Ademais, a arquitetura dessa tecnologia de rede é tal, que sua censura ou controle se tornam muito difíceis. O único modo de controlar a rede é não fazer parte dela (...).

Apenas alguns anos mais tarde, o desenvolvimento das tecnologias da informação e comunicação possibilitou que esse paradigma da liberdade representado pela Internet pudesse, senão ser rigidamente controlado, sofrer a intervenção de mecanismos impostos pelos Governos, motivados por diversas razões, especialmente pelo aumento dos cibercrimes.

> Criada como um meio para a liberdade, nos primeiros anos de sua existência mundial a Internet pareceu prenunciar uma nova era. Os governos pouco podiam fazer para controlar fluxos de comunicação capazes de burlar a geografia e, assim, as fronteiras políticas. A liberdade de expressão podia se difundir através do planeta, sem depender da mídia de massa, uma vez que muitos podiam interagir com muitos de maneira irrestrita. (...) A privacidade era protegida pelo anonimato da comunicação na Internet e pela dificuldade de investigar as origens e identificar o conteúdo de mensagens transmitidas com o uso de protocolos de Internet. (...) No entanto, (...) os fundamentos da liberdade na Internet poderiam ser, e estão sendo de fato, desafiados por novas tecnologias e regulações (CASTELLS, 2003, p. 139-140).

A temática dos controles sociais é retomada sempre quando se pensa no paradigma da liberdade representado pela Internet, paradigma este que a considera um território livre, no qual todas as manifestações são possíveis e todos os usuários são bem vindos. Esta aura de liberdade que circunda a Internet está relacionada à proteção conferida ao direito de expressão nos Estados Unidos pela Primeira Emenda[12], que é referenciada cada vez que naquele país tenta-se regulamentar algum tipo de controle na rede mundial de computadores – Internet.

Nos Estados Unidos, as tentativas mais importantes de controlar a Internet tiveram como argumento preservar crianças e adolescentes de imagens e textos com apelativos sexuais a elas dirigidos. Mesmo com estes argumentos que têm, na verdade, fortes razões morais defendidas por políticos e juristas - pois tais atos são absolutamente condenáveis - e é necessário coibi-los, o governo Clinton não conseguiu aprovar as censuras à Internet pretendidas por sua administração. O governo americano foi derrotado em duas ocasiões: nos estados da Pensilvânia, em 1996 e na Filadélfia, em 2000 (CASTELLS, 2003, p.140).

Os governos americanos citados inicialmente, desejavam implantar o controle na rede, por razões morais, como relatado acima. No entanto, a tendência crescente para que se busquem as tecnologias de controle da Internet vêm ganhando outra motivação, desta vez econômica.

Empresas e autores se vêem preocupados com a eficácia das leis de direitos autorais, quando estes são desafiados via Internet. Como fazer para que esses direitos sejam respeitados, considerando o quadro atual existente (no qual os direitos intelectuais e artísticos contam com as proteções legais) é uma questão que exige, sem dúvida, uma intervenção na própria rede. Note-se que já existem experiências na *Web* trabalhando com modelos abertos. É o que mostra Spyer (2007, p. 202):

> No caso das gravadoras e também dos estúdios de cinema, que supostamente são os segmentos mais prejudicados pela pirataria, modelos abertos têm se mostrado vantajosos para criar frentes de trabalho para profissionais e artistas que não são aproveitados pela indústria estabelecida. Considere, por exemplo, o *site* Sellaband (www.sellaband.com), lançado em 2006 por um ex-executivo de gravadora, oferecendo uma solução viável para a produção de álbuns sem interferir com a livre troca de arquivos. O projeto tira proveito da redução de gastos

[12] A Primeira Emenda à Constituição dos Estados Unidos da América determina que “o Congresso não fará lei que limite a liberdade de expressão e de imprensa” (LINS, 2000, p.5).

> para comunicação e coordenação oferecidas pela Web para estabelecer parcerias produtivas entre profissionais da área, artistas e consumidores.

De acordo com Spyer (2007), projetos como o Sellaband e similares, procuram formas criativas de permitir os *downloads* gratuitos aos usuários, comercializando apenas algumas faixas de música em troca de CD's inteiros etc.

Para além das questões dos direitos autorais, há ainda as oportunidades de negócios advindas das tecnologias de controle. As empresas de marketing descobriram um filão especialmente generoso com os "cookies", pequenas informações que os *sites* visitados pelo usuário podem armazenar em seu *browser* (programas de navegação na rede). Costumam ser utilizados para guardar a identificação e senha pessoal dos usuários durante a navegação, manter listas de compras ou produtos preferidos em *sites* de comércio eletrônico, marcar a lista de páginas vistas pelo usuário em um *site*, para fins estatísticos, entre outras aplicações (CGI, 2007, p.7/14). Marcadores digitais, ou *cookies*, fazem parte das tecnologias de controle que identificam os usuários na rede. Também fazem parte deste grupo de tecnologias, as assinaturas digitais, baseadas em criptografia.

Há pelo menos mais dois grupos de tecnologia de controle, além da tecnologia de identificação da qual fazem parte os "*cookies*" e as assinaturas digitais. São as tecnologias de vigilância e as tecnologias de investigação.

Tal como as tecnologias de controle, as tecnologias de vigilância também usam as ferramentas de identificação, sendo ainda mais poderosas que as primeiras, uma vez que possuem a capacidade de identificar servidores em sua origem, interceptar mensagens, monitorar computadores todo o tempo e até mesmo seguir fluxos de comunicação a partir da instalação de marcadores nos computadores. Como todas as informações são gravadas, cada usuário de Internet pode ser identificado por um conjunto de informações e como vimos, também pode ser localizado pelas tecnologias de vigilância.

Através das tecnologias de investigação, que são mais complexas do que as tecnologias de vigilância, dados podem ser combinados, processados, cruzados com outros dados em um processo que tanto pode ser utilizado para publicidade e vendas, como também para atividades políticas (no caso de elaboração de perfis eleitorais) ou até mesmo para a polícia, quando se faz necessário perseguir criminosos virtuais.

Por outro lado, há quem resista a ser controlado na rede. São pessoas e empresas que, utilizando-se de tecnologias semelhantes as de controle, incluindo a criptografia, valem-se delas para proteger o anonimato e, em última instância, a liberdade:

> Firmas como a Disapperaring e a ZipLip criaram o e-mail que se apaga por si mesmo, que usa tecnologia de criptografia. A companhia canadense Zero-knowledge Systems decompõe identidades com um pacote de software chamado Freedom, que fornece cinco pseudônimos digitais que podem ser atribuídos a diferentes atividades. No sistema de Freedom, ninguém é capaz de descobrir a identidade real a partir dos pseudônimos. (...) A Zero-knowledge usa a mesma tecnologia, de tal modo que nem a própria companhia é capaz de vincular pseudônimos a clientes individuais. (...) A Anonymizer.com oferece “anonimizadores” gratuitos, em troca de sua publicidade. O “anonimizadores” são servidores extras que protegem o navegador do cliente de sua destinação final (CASTELLS, 2003, p.150-151).

O poder das tecnologias de controle tende a ser mais efetivo do que os sistemas que protegem a liberdade. O poder de controle, exercido formalmente pelo Estado, através de instituições como o exército e o sistema carcerário, pode passar, neste contexto informacional, a ser generalizado. Isto é possibilitado pelas tecnologias de informação e comunicação, aplicadas ao controle estatal, o que acaba resultando em um tipo de sociedade denominada por Deleuze (1992 apud HAESBAERT, 2006, p.268), como sociedade de controle: “(...) as sociedades de controle operam por máquinas de uma terceira espécie, máquinas de informática e computadores, cujo perigo passivo é a interferência, e, o ativo, a pirataria e a introdução de vírus”.

Os controles e o fluxo de pessoas são facilitados e permitem sua localização precisa, fato que pode ser utilizado, por exemplo, na condução de inquéritos policiais.[13]

> Pontos restritos (como uma antena para telefones celulares ou uma conexão de linha telefônica) adquirem um papel estratégico fundamental na organização do espaço social. Através deles pode-se fazer e desfazer conexões, abrir e fechar a circulação de fluxos imateriais, especialmente de informações e capitais, além de permitir o desencadeamento de outros, inúmeros, de caráter material (HAESBAERT, 2006, p.269).

[13] Em 2006, quando o Coronel da Polícia de São Paulo Ubiratan Guimarães foi assassinado, sua namorada Carla Cepollina foi acusada de mentir sobre uma ligação que não teria feito para o Coronel de seu celular, ligação que, no entanto, foi captada pela Estação Radiobase, que fica sobre o prédio onde residia o Coronel (BONADIO, 2007).

É possível pensar que no Brasil, as pessoas, notadamente os usuários das novas tecnologias, não se importam em ser identificados, mapeados, localizados e fotografados, fornecendo informações pessoais e financeiras em *sites* na Internet sem receio de quaisquer conseqüências.

Nos Estados Unidos há batalhas judiciais nas quais os advogados invocam o direito à privacidade na rede. O usuário, ao adentrar em determinado *site*, acaba aceitando, inadvertidamente, que seu nome seja incluído no *mailing* para receber ofertas e promoções diversas. Ocorre que para ser excluído desta lista, o usuário precisa clicar para ser excluído, o que na maioria das vezes, não é feito. E empresas de marketing e publicidade inseridas no comércio eletrônico americano se aproveitam disso, utilizando e vendendo banco de dados para aumentar suas fontes de receitas.

As batalhas entre liberdade e controle deverão se manter equilibradas por alguns anos. E embora as discussões sobre liberdade e controle na *Web* ainda estejam sem definição, acreditamos que os controles deverão predominar: primeiro porque as tecnologias o permitem; segundo, porque os Governos os querem e terceiro, porque as pessoas não se importarão com eles.

A privacidade já não é objeto de desejo. A tecnologia é tão mais importante do que a privacidade na sociedade da informação extremamente fragmentada e globalizada, pois:

> (...) é a prova, de que a técnica exerce a função de agregador para uma sociedade estilhaçada (...) essa sociedade fragmentada na qual vivemos sai então em busca de uma identidade e a encontra num consenso em torno de objetos indubitáveis, em torno de resultados objetivos, que formam um núcleo de certezas, compartilhados por todos. (...) Crê-se no progresso técnico porque ele se torna visível e palpável (SFEZ 1994, p.22).

Portanto, na sociedade da informação, as pessoas acreditam na tecnologia, tornando-a soberana, inquestionável; logo, os controles dela advindos são naturais, fazem parte deste novo mundo por ela mediado e os questionamentos ficam restritos à academia, às esferas de poder da sociedade civil e dos Governos.

O tema dos controles e da segurança na rede foi também amplamente discutido na segunda reunião do Fórum de Governança da Internet (IGF, 2007), ocorrido no Brasil, em dezembro de 2007. De maneira geral, todos os participantes

consideraram esta uma discussão fundamental para os Governos, por envolver a necessidade de cooperação internacional para resolução dos cibercrimes, uma vez que existem limitações técnicas, militares, financeiras, legislativas e judiciárias, dado o caráter sem fronteiras da Internet. Punir os criminosos que atuam fora de sua territorialidade exige tratamento cooperativo que deve se traduzir em um tipo de governança política que ainda não existe na prática. Segurança na rede é, pois, um tema multidimensional.

Os participantes do Fórum discutiram, ainda, a conveniência de se prevenirem os cibercrimes antes que aconteçam, ou providenciar a legislação necessária para puni-los, tão logo ocorram. Esta discussão na verdade retoma a divisão entre os que querem mais e entre os que querem menos legislação na Internet.

A segurança na Internet exige ainda o envolvimento de recursos humanos capacitados a tratar com estas questões e os países precisam tomar a iniciativa de treinar as pessoas. Criar uma cultura de ciber-segurança envolvendo grupos, associações e usuários foi um dos fatores apontados como necessário no conjunto de soluções para alcançar segurança na rede.

Com respeito ao *software* mais adequado para a segurança, se *software* livre ou proprietário, as discussões foram as seguintes:

> Comentou-se que a transparência é importante nas soluções de segurança, e um participante argumentou que softwares abertos oferecem mais segurança, e que segurança obtida com obscuridade é um conceito errôneo; sistemas e designs abertos que podem ser examinados são mais seguros. Outro participante observou que softwares proprietários são igualmente apropriados e alguém comentou que, do ponto de vista de um país em desenvolvimento, onde os criadores estão interessados em desenvolver novos sistemas, é importante proteger os direitos de propriedade intelectual e que por essa razão soluções proprietárias são importantes. Conforme comentou outro orador, uma política pública explícita que exija soluções de *open source*[14] em processos de procuração pode limitar o desenvolvimento da indústria nacional de software. Ficou claro que não existe uma solução única para todos na questão de sistemas proprietários ou não-proprietários (IGF, 2007, p. 10).

O consenso sobre a necessidade de proteção na Internet, nos aspectos de privacidade, identidade, direitos intelectuais e segurança internacional prevaleceu

[14] *Open source* é um método de desenvolvimento de software que explora o poder de distribuição por revisão e a transparência do processo. Os *softwares* (programas de computadores) desenvolvidos por este método possuem código aberto (SPYER, 2007, p. 245).

e as soluções que resultaram das discussões do Fórum apontam que o estabelecimento de um ambiente sustentável de confiança entre os países é fundamental na busca por segurança.

3.2 Cibercrimes

Cibercrimes constituem-se em delitos diversos praticados no ciberespaço. E o que seria este local? Fisicamente existente em potência e inexistente em ato, possibilitado por computadores conectados e suas memórias, “(...) o termo especifica não apenas a infra-estrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo” (LÉVY, 1999 apud HAESBAERT, 2006, p. 271).

A crescente expansão do número de usuários aliada à inovação constante dos produtos e serviços relacionados à Internet – cujo resultado direto é a criação do ciberespaço, um espaço multi-territorial que abriga informações, infra-estrutura digital e seres humanos – como define Lévy (1999 apud HAESBAERT, 2006), fez com que as pessoas, de todas as idades, níveis culturais e econômicos pudessem se comunicar nesta espécie de universo paralelo.

Claro, há que se lembrar da enorme exclusão digital ainda existente e sendo a Internet um universo no qual os conhecimentos podem ser produzidos e transmitidos, é de se considerar como sendo um direito de todos os cidadãos o acesso a ele. Afinal, “(...) a comunicação é um direito inalienável e privar o homem de sua capacidade de se comunicar é privá-lo de sua própria humanidade” (SOARES, 2007, p. 39).

Por outro lado, para quem acessa a Internet hoje, é possível encontrar os mais diversos temas, informações, imagens e conhecimento. *Sites,* como o *Youtube*, dispostos a atrair a atenção de um número cada vez maior de internautas, vêm utilizando recursos como imagens, sons, vídeos, charges e entrevistas em tempo real. É possível, via rede, tomar conhecimento dos fatos quase na medida em que eles acontecem. A divulgação da vida pessoal de celebridades é outro chamariz de peso na Internet. Os próprios internautas, por sua iniciativa, divulgam, cada vez mais freqüentemente, imagens pessoais e confissões íntimas no Orkut ou em

blogs/fotoblogs/videoblogs. Ocorre que nem tudo é proveitoso neste oceano de informações. Há uma parte da humanidade que, desviando-se das normas morais e cívicas definidas socialmente, posta na Internet todo o tipo de material relacionado às suas próprias normas e visões de mundo. Isto inclui, por conseguinte, práticas que a sociedade repudia em termos de valores morais, sociais e culturais.

A pedofilia é uma dessas práticas. Definida como desvio sexual que consiste na atração sexual do adulto por crianças, é um desses desvios e, certamente, o mais preocupante para famílias, juízes, procuradores e governos em todo o mundo, pois ocorre na infância, uma faixa etária na qual o desenvolvimento pleno de todas as capacidades humanas ainda não se completou, e os prejuízos decorrentes de uma perturbação ou traumas vividos nesta fase da vida, virão fatalmente a se manifestar cedo ou tarde, na forma de transtornos psicológicos graves ou sérias alterações comportamentais como o uso de drogas, álcool, prostituição, entre outros problemas. O estudo publicado na revista Pagu, de autoria da pesquisadora Jane Felipe, “Afinal, quem é pedófilo”, discute como na sociedade atual, as tecnologias permitem que novas formas de sedução, especialmente as imagéticas, dêem vazão a desejos sexuais adultos que utilizam os aparatos eletrônicos como estratégias de satisfação, coerentes com a lógica do consumo. Infelizmente neste caso, a criança aparece como o elo mais fraco, transformando-se num objeto a ser explorado.

> Um dos aspectos mais preocupantes, e que tem merecido a atenção do poder público e de várias entidades civis em defesa da criança e do adolescente, diz respeito à prática da pedofilia, especialmente aquela cometida através da Internet, uma vez que envolve a produção de material pornográfico utilizando imagens de crianças, muitas vezes submetidas a toda sorte de violência sexual. O Brasil ocupa o 4º lugar no ranking de material pornográfico, com pelo menos 1210 endereços na Internet. Um dos nichos desse material refere-se à pornografia infantil, com o intuito de abastecer o mercado da pedofilia. Essa rede se organiza internacionalmente, de modo que existem facções em todos os lugares onde há pessoas interessadas em obter acesso a esse tipo de material (FELIPE, 2006, p. 210).

Cabe ressaltar, no entanto, que, o estudo acima mencionado não relaciona as tecnologias à pedofilia, e também não é este o posicionamento deste trabalho, ou seja, não se afirma que as novas tecnologias estão a criar tais desejos. Através da Internet todos os tipos de pensamentos, sentimentos, conhecimentos e

informações podem ser manifestados, desde que o usuário disponha de um computador conectado à rede.

A situação fica mais grave, porque as crianças têm acesso cada vez mais cedo aos equipamentos de informática e a navegação na Internet é facilmente aprendida nas fases iniciais do desenvolvimento infantil. Os adultos não conseguem vetar o conteúdo de *sites* potencialmente perigosos. Dessa maneira, as crianças podem receber instruções que versam sobre formas de cometer suicídio, construir armas e bombas, baixar softwares de conteúdo criminoso, entre outros. Além disto, crianças podem ser orientadas a adotar posturas racistas e receber orientação sexual de pedófilos, cujos *sites* proliferam na rede.

A rede de adultos pedófilos é uma organização complexa, que conta com adeptos que utilizam a Internet para concretizar seus desejos na realidade material. Segundo essas organizações, as crianças têm desejos sexuais que são reprimidos pela sociedade adulta. Em contato uns com os outros, os pedófilos deixaram de se considerar “doentes” e “pervertidos”, para se sentirem perseguidos da mesma forma e pela mesma sociedade que discrimina as raças.

> Para os pedófilos, sua causa está alinhada com outros movimentos como a luta contra o racismo na década de 1960 nos Estados Unidos. Da mesma maneira como a discriminação racial já teve a anuência do poder público, eles entendem que o Estado não tem direito de regular a vontade de fazer sexo com quem quiser. Essa justificativa estimula discussões e trocas de dicas a respeito de como se aproximar de menores conseguindo empregos em acampamentos de verão ou atuando como DJ’s em festas para adolescentes. Alguns deles vão além: adotam crianças como pais solteiros, casam-se com mulheres que tenham filhos pequenos ou investem em carreiras que possibilitem o contato contínuo com a infância, como professores, enfermeiros, ou pediatras. E, apesar dos resultados do movimento até agora serem pequenos, a comunidade celebrou em maio de 2006 a fundação na Holanda de um partido político que defende a pedofilia (SPYER, 2007, p. 204).

Os cibercrimes vêm se diversificando. Filmes de agressões gratuitas a pessoas (transeuntes, por exemplo) por gangues européias vêm sendo veiculados na Internet. No Orkut, uma foto de uma criança negra foi postada por uma comunidade racista solicitando aos visitantes do site que “clicassem” na imagem para “desabafarem” todo o seu ódio na foto exposta. Denúncias de racismo como esta, apologia ao nazismo, tráfico de drogas e comercialização de medicamentos proibidos têm sido denunciadas ao Ministério Público Federal (SPYER, 2007, p.

206). A ocorrência de fatos como estes, fazem com que o combate aos cibercrimes venha ganhando espaço nas discussões acadêmicas e políticas, levantando questões como:

a) Deve haver limites à livre manifestação na rede?

b) Que Internet queremos para nossa sociedade?

As preocupações com respeito à ocorrência destes delitos cibernéticos têm levado alguns países, incluindo o Brasil, a colocarem em pauta, no âmbito dos poderes legislativo e judiciário, a questão da segurança e das práticas abusivas na rede.

O Ministério Público Federal e o Comitê Gestor da Internet no Brasil têm se pautado nos postulados acordados pela Convenção sobre a Cibercriminalidade, ratificada pelo Conselho da Europa[15] no ano de 2001 e assinada por alguns países não pertencentes ao Conselho, como a África do Sul, o Canadá, os Estados Unidos e o Japão (Anexo B).

Os principais termos acordados na referida Convenção tratam de tipificar diferentes cibercrimes, que vão muito além das práticas de pedofilia na rede.

Assim, o seu Capítulo 2, relaciona e define os seguintes cibercrimes:

- Infrações cometidas contra sistemas informáticos, com respeito à confidencialidade, integridade e disponibilidade de dados e sistemas: condena o acesso ilegítimo, a interceptação ilegítima, a interferência em dados e em sistemas e o uso abusivo de dispositivos (neste caso, os dispositivos são aqueles produzidos e vendidos com a intenção de incorrer nas práticas listadas nas infrações contra os sistemas informáticos).
- Infrações relacionadas com computadores:
  - ✓ falsidade informática: consiste na introdução, alteração, eliminação, supressão intencional e ilegítima de dados informáticos, resultando na produção de dados falsos que são comercializados como sendo autênticos;

[15] Conselho da Europa, criado à época da Segunda Guerra Mundial, teve como objetivo inicial reconstruir a Europa arruinada pelo conflito. Hoje possui 47 Estados membros que visam principalmente concluir acordos que harmonizem as práticas sociais e jurídicas dos países participantes. Disponível em: <http://www.coe.int/t/pt/com/about_coe/>.

- ✓ burla informática: também utiliza-se da introdução, alteração, eliminação, supressão intencional e ilegítima de dados informáticos, resultando na perda de bens de terceiros, obtendo lucros ilegítimos com estas práticas;

- Infrações relacionadas ao conteúdo: Infrações relacionadas à pornografia infantil[16]: neste item, considera-se crime a produção, a oferta, a difusão, a obtenção e o armazenamento de pornografia infantil;
- Infrações relacionadas com a violação dos direitos de autor e direitos conexos: especifica a proteção dos direitos do autor, com respeito à propriedade intelectual e artística anteriormente definidas pela Convenção Universal sobre os Direitos do Autor, realizada em Berna no ano de 1886 e revista em Paris em 1971;
- Outras formas de responsabilidade: tipifica a cumplicidade, em qualquer dos quesitos acima.

Quanto ao crime de racismo, não houve consenso entre os participantes da Convenção, de forma que não foi aposto no texto principal, constando, no entanto, de um aditivo, denominado como *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*[17] (CONCIL OF EUROPE, 2003), assinado por 33 países[18] e datado de março de 2006, trazendo em seu preâmbulo:

> *Many States have already criminalised certain acts related to racist or xenophobic content. However, the dissemination of such material through computer networks poses even greater challenges for law enforcement. It was thus necessary to adopt a co-ordinated approach which enables an effective domestic and international response, based on common elements to be included in an additional Protocol to the Convention. This Protocol entails an extension of the Cybercrime Convention's scope, including its substantive, procedural and international cooperation provisions, so as to cover also offences of racist or xenophobic propaganda. Thus, apart from harmonizing the substantive law elements of such behavior, the Protocol aims at improving the ability of the Parties to make use of the means and*

[16] Pornografia infantil: definida como material pornográfico que represente visualmente menor ou pessoa, que aparente menor, em atitudes sexualmente explícitas, tipificando também nesta categoria "imagens realísticas", que representem menores em comportamento sexualmente explícito.
[17] Protocolo adicional à Convenção sobre Cibercriminalidade, que versa a respeito da tipificação dos crimes de racismo e xenofobia cometidos através de sistemas computadorizados.
[18] Japão, África do Sul, Estados Unidos, Espanha, Rússia, Itália e Reino Unido são alguns dos países que não assinaram o Aditivo do Protocolo.

> *avenues of international cooperation set out in the Convention in this area* (CONCIL OF EUROPE, 2003, *online*).

O texto acima deixa claro que os países que assinaram o Aditivo consideram um desafio ainda maior a ser combatido, a disseminação de material de conteúdo racista e xenófobo através de redes de computadores. Consideram também, para que este adendo tenha êxito, a necessidade de uma ação coordenada e a cooperação internacional, o que requer dos países um treinamento para melhorar suas habilidades associativas.

O texto (principal) da Convenção sobre a Cibercriminalidade, como não poderia deixar de ser, não especifica as sanções e/ou penalidades, deixando a cada país a responsabilidade por analisar e aplicar as penas que julgar cabíveis para cada caso.

Não há dúvida de que existem duas grandes fontes de preocupação principais dos Governos no tocante ao cibercrimes: a pornografia e pedofilia infantis e os ataques a sistemas informáticos, em especial, os pertencentes às áreas estratégicas de segurança dos países e da administração pública de maneira geral.

3.3 Combate aos cibercrimes

As autoridades brasileiras responsáveis pela confecção e aplicação das leis, decretos e outros instrumentos necessários para a manutenção da ordem institucional vigente, começaram a preocupar-se mais seriamente com os denominados cibercrimes a partir de 2002, ano em que a Internet brasileira registrou 14,3 milhões de usuários, segundo o Manual Prático de Investigação de Crimes Cibernéticos (CGI, 2007).

As infrações cometidas contra sistemas informáticos, o primeiro dos cibercrimes tipificados pela Convenção da Europa, danificam sistemas em um ou mais de seus requisitos básicos: confidencialidade, integridade e disponibilidade. Por quebra de confidencialidade entende-se o acesso não autorizado a informações pessoais dos usuários. Os ataques à integridade alteram informações diversas enviadas por usuários em transações na rede. E os ataques à disponibilidade impedem que provedores possam funcionar, através de envio de sobrecarga de

dados ou ataque de negação de serviço. Este tipo de infração, quando cometido em sua forma pura, ou seja, realizado apenas com o intuito de causar danos à hardware, software, dados e sistemas, concretiza-se na desestabilização e/ou destruição de programas instalados em computadores, por meio da inoculação de softwares que utilizam códigos maliciosos (*malwares*). A Cartilha de Segurança na Internet (NIC.BR 2006, p. 9-14), define *malwares*: "*malwares (malicious software*) é um termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador", como vírus, *worms* e *bots*, *backdoors*, cavalos de tróia, *keyloggers* e programas *spyware* e *rootkits*.[19]

Os delitos informáticos são também definidos pela Organização para Cooperação Econômica e Desenvolvimento de Informática da ONU como "qualquer conduta ilegal, não-ética ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados" (NETO; GUIMARÃES, 2003, p. 69).

Informações detalhadas sobre as infrações cometidas contra sistemas telemáticos geralmente não são divulgadas, em especial se atacam sistemas de segurança dos Governos.

3.4 Crimes financeiros

As infrações cometidas através de computadores visando a obtenção de lucros através de falsificação, adulteração e roubo de dados obtidos na *Web*, ocasionam perdas financeiras de grande expressão. Estatísticas divulgadas pelo *Internet Crime Report* [20], mostram que em 2006 foram registradas mais de 200 mil reclamações sobre fraudes na Internet nos Estados Unidos, o que representou 44% de todas as reclamações sobre cibercrimes naquele país.

Estes crimes cometidos utilizando-se a Internet, e que visam lesar contas bancárias e cartões de crédito têm crescido também no Brasil. As fraudes em contas bancárias ocorrem com freqüência maior do que se veicula na imprensa. A operação

[19] Programas diversos que duplicam, espionam e/ou invadem computadores (NIC.BR, 2006)
[20] Relatório preparado em conjunto pelo *National White Collar Crime Center* e pelo *Federal Bureau Investigation* (FBI) nos Estados Unidos da América (INTERNET CRIME COMPLIANCE CENTER, 2006).

Scan[21], da Polícia Federal, prendeu uma quadrilha, em fins de fevereiro de 2006, acusada de aplicar um golpe de mais de R$ 10 milhões em sete estados.

Os golpes mais comuns, relacionados a fraudes bancárias, consistem em simular a página do *site* no qual o usuário é correntista. O simulacro é quase idêntico, a não ser por alguns detalhes que escapam às pessoas que não são especialistas no assunto, ou não estão acostumadas a enxergar detalhes. Por exemplo, para checar se um *site* é verdadeiro ou falso, pode-se clicar com o mouse em qualquer outro *link* da página aberta. Se não for possível a conexão no *link,* a página provavelmente é falsa.

Uma vez simulado o acesso, o criminoso aguarda a vítima digitar o número de sua conta corrente ou cartão de crédito, seguida de sua senha. Enquanto isso, em seu computador, vai registrando todos os movimentos da "vítima", utilizando um tipo de vírus muito comum, mas extremamente poderoso, conhecido como *trojan*, ou cavalo-de-tróia. Mais tarde, o criminoso usa um boleto bancário emitido em nome da vítima por uma empresa de falsas vendas *on-line*, empresas chamadas de "boleteiras". O criminoso, então, efetiva o pagamento deste boleto (cuja dívida é falsa) via Internet, desta vez no *site* verdadeiro do Banco, utilizando-se da conta bancária da vítima. A empresa emissora do falso boleto e o criminoso digital dividem então os lucros provenientes da falsa operação.

Cavalo-de-tróia também foi o nome utilizado pela Polícia Federal do Brasil para denominar uma grande operação policial destinada a investigar crimes digitais. Segundo informou o *site* do Globo (JUSTIÇA..., 2007), uma das maiores prisões desta operação aconteceu no estado do Pará, em julho de 2007, quando foram presas 65 pessoas que faziam parte de uma quadrilha especializada nestes crimes. A Polícia Federal não divulga os procedimentos utilizados nestas operações, por motivos que envolvem o sigilo necessário para o sucesso das mesmas. Ainda segundo o G1 (JUSTIÇA..., 2007), os prejuízos causados foram de aproximadamente R$ 100 milhões, para apenas uma das instituições financeiras lesadas. Normalmente, quando isso ocorre, os clientes destas instituições são ressarcidos pelas mesmas, após um processo de investigação que pode demorar alguns meses.

[21] Operações Scan, Clone e Replicante denominam ações empreendidas pela Polícia Federal do Brasil com o objetivo de investigar e prender pessoas ou provedores que violam e roubam contas bancárias via Internet.

Um dos tipos mais comuns de ataques a computadores, é denominado pelo CERT.br com o termo de Engenharia Social:

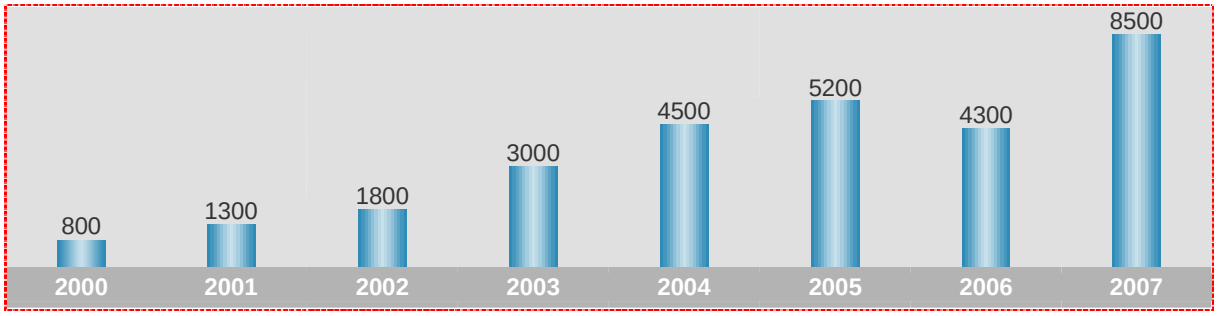
> (...) definida como um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações (NIC.BR, 2006, *online*).

Neste tipo de ataque, o criminoso envia *e-mails* falsos (normalmente com o cabeçalho em nome de órgãos públicos como Receita Federal e Tribunal Superior Eleitoral ou de bancos como o Banco do Brasil, por exemplo). O usuário, ao abrir o *e-mail*, é induzido a digitar sua senha secreta ou dados pessoais, ou mesmo é orientado a clicar em um aplicativo anexo ao *e-mail*. Outras vezes, o criminoso telefona para o usuário, se passando por funcionário de suporte técnico de seu provedor de acesso e pede sua senha para corrigir um suposto problema. O CERT alerta que o sucesso deste tipo de ataque depende unicamente da colaboração do usuário, ou seja, de sua decisão em informar seus dados ao falsário.

3.5 Pornografia infantil

Com respeito às infrações relacionadas ao conteúdo, as que mais preocupam as autoridades públicas e os gestores da Internet estão relacionadas à pornografia infantil.

O crescente número de sites de pornografia infantil em toda a Internet é demonstrado na Figura 6, que se segue:



Fonte: ASACP (2008)

Figura 6 - Número anual de endereços IP suspeitos de hospedar pornografia infantil (2000-2007)

Organizações não-governamentais têm se constituído com a finalidade de combater a ciberpedofilia.

Nos Estados Unidos, uma destas entidades é a *Association of Sites Advocating Child Protection* (ASACP), uma organização sem fins lucrativos, dedicada a eliminar a pornografia infantil da Internet. A ASACP combate a pornografia infantil por meio de sua linha de ação de denúncias, que organiza esforços para combater o que esta associação considera como "crime hediondo do abuso infantil na indústria da Internet". A ASACP também ajuda os pais a evitar que suas crianças vejam material inapropriado na rede mundial de computadores. Esta organização argumenta que capturar pedófilos que postam páginas suspeitas na Internet é difícil para os Governos, que recebem as denúncias, mas não têm condições de investigá-las. Assim, o *site* da ASACP promete investigar tais denúncias - pois possui aparato tecnológico para tal fim - e coloca à disposição de seus visitantes *on-line*, um *link* para que estes possam reportar suspeitas de crimes de pedofilia e pornografia infantil. Considera também que os usuários da Internet podem sentir-se mais à vontade contatando a Associação do que as agências governamentais. Dessa maneira, a própria ASACP pode contatar as autoridades, priorizando denúncias que realmente forem consideradas graves. No *site* da entidade, o *modus operandi* para o combate a estes crimes é descrito:

> **O que fazemos e como fazemos**
>
> - A ASACP providencia uma linha de denúncias para usuários da Internet e donos de páginas virtuais para reportarem suspeitas de pornografia infantil. Muitos de nossos membros possuem URLs[22] para a linha. Assim recebemos milhares de denúncias todo mês.
> - A ASACP investiga estas denúncias e determina o servidor, a fatura, o endereço IP, o dono e ligações para páginas suspeitas. A ASACP, então, envia o alerta vermelho para autoridades e associações apropriadas, incluindo o FBI e o Centro Nacional de Crianças Abusadas e Desaparecidas, assim como linhas européias. Nós também falamos com os servidores e processadores de pagamento que hospedam operadores de pornografia infantil.
> - O programa de membros aprovados da ASACP oferece um modelo de auto-regulagem efetivo para a indústria adulta da Internet. Páginas de membros aprovados devem seguir nosso código de ética.
> - A ASACP estabeleceu melhores práticas para seus membros, que são recomendadas não só para os mesmos, como também para páginas de busca, páginas de encontro virtual, entre outras.
> - A ASACP criou a marca RTA (Restrito a Adultos) para melhorar o filtro adulto, e para demonstrar o compromisso da indústria adulta da Internet em ajudar os pais a impedirem que seus filhos sejam expostos a material

[22] URL (Universal Resource Locator) Sequência de caracteres que indica a localização de um recurso na Internet. Ex.: http://www.asacp.org/page.php.

inapropriado.

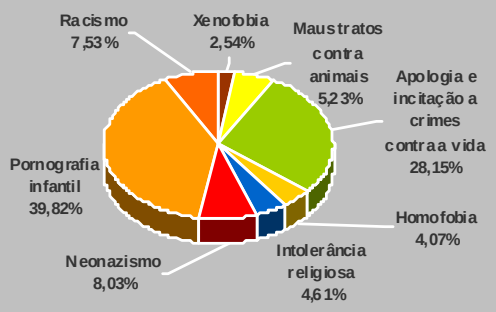
- A ASACP mantém seus membros informados sobre as atuais leis e regulamentos condizentes à pornografia infantil e proteções da criança, assim como a legislação nova e a pendente.
- A ASACP trabalha para informar e educar seus membros, a indústria adulta da Internet, mentores das políticas governamentais, e o público geral sobre temas relacionados à proteção da criança, atividades virtuais ilícitas, e os esforços da indústria adulta da Internet em combater a pornografia infantil (ASACP, 2008, *online*).

No Brasil, a entidade similar à ASACP é a SaferNet, uma organização não-governamental que assim se define em seu *site*:

> A SaferNet Brasil é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos e econômicos, de duração ilimitada e ilimitado número de membros, sem vinculação político- partidária, fundada em 20 de Dezembro de 2005 por um grupo formado por cientistas da computação, professores, pesquisadores e bacharéis em Direito, reunidos com o objetivo de materializar as diretrizes e linhas de ação empreendidas ao longo dos anos de 2004 e 2005, quando estiveram diretamente envolvidos na realização de pesquisas e no desenvolvimento de projetos sociais relacionados ao combate a pornografia infantil (pedofilia) na Internet no Brasil (SAFERNET BRASIL, 2008, *online*).

A Figura 7 demonstra que esta entidade registrou mais de cinco mil denúncias destes crimes, que incluíram pornografia infantil, racismo, neonazismo e intolerância religiosa. Segundo dados desta ONG, o Brasil está em terceiro lugar no *ranking* da pornografia mundial, perdendo apenas para os Estados Unidos e a Rússia.

	Conteúdo denunciado à Safernet	Removido pelo Orkut/Google	Removido pelo usuário
Perfis pedófilos	4.135	7.991	2.020
Comunidades com pornografia infantil	1.693	1.472	719
Total de páginas denunciadas	5.878	9.463	2.784
Número estimado de imagens publicadas	49.620	113.556	24.240



Fonte: Safernet Brasil (2007).

Figura 7 – Páginas do Orkut denunciadas à Safernet contendo pornografia infantil (janeiro de 2006 a junho de 2007)

Atualmente, o Ministério Público Federal trabalha em parceria com a SaferNet, com o Comitê Gestor da Internet no Brasil e com a Associação Brasileira de Provedores de Internet (ABRANET) no combate a estes crimes, tendo sido fruto destas parcerias as seguintes ações:

- a confecção do Manual Prático de Investigação para Crimes Cibernéticos, colocado à disposição de delegados, membros do Ministério Público, juízes e auxiliares de justiça. O manual em referência não pode ser reproduzido, pois contém descritos os passos necessários para investigar os cibercrimes, contendo inclusive anexos de peças processuais relativas à busca e apreensão de computadores por crime de racismo, pedido de interceptação de dados telemáticos por pornografia infantil, pedido de quebra de sigilo para provedores que hospedam *sites* de pornografia infantil, entre outros;

- acordos celebrados entre o Ministério Público Federal e o *Google* em pelo menos quatro estados brasileiros (Ceará, Minas Gerais, Pernambuco e Rio de Janeiro). Tais acordos consistem, na verdade, de um compromisso do *Google* com o Ministério Público Federal, em fornecer indicações, arquivar dados, facilitar o acesso e até mesmo retirar páginas suspeitas de ilegalidades, como pedofilia e racismo, postados no Orkut (PICHONELLI; FERNANDES, 2007).

Os cibercrimes envolvendo menores vêm crescendo no Brasil. Segundo informa a SaferNet, em Juiz de Fora (MG), uma garota de 15 anos fugiu de casa para encontrar-se com um homem de 30 anos que conheceu pela Internet e com o qual passou dois meses, sem que a família recebesse quaisquer notícias. Em Nova Friburgo (RJ), dois homens foram presos por terem divulgado fotos pornográficas de adolescentes no Orkut. Casos como esses são cada vez mais comuns, e envolvem crianças e adolescentes muito jovens – existem registros envolvendo crianças de 9 anos ou menos.

Falta é claro, uma educação digital que poderia ser realizada pela televisão aberta, escolas, universidades e associações profissionais. Os jornais e a própria Internet já são porta-vozes dessas mensagens de alerta, que, entretanto,

não conseguem chegar a um grande número de internautas. As conseqüências do desconhecimento das práticas de segurança na rede acabam favorecendo o aumento das ocorrências criminosas. Medidas básicas de proteção para diminuir tais problemas podem ser adotadas, bastando, para isso, que se tomem cuidados como instalar antivírus nos computadores e adotar a prática de alterar senhas de acesso com freqüência.

Essas medidas poderiam também ser amplamente divulgadas pelo Governo brasileiro, pelo Ministério Público Federal, pelo Comitê Gestor e pelos Provedores de acesso, especialmente os maiores, que têm a responsabilidade de operacionalizar uma campanha nacional em rede de televisão aberta para informar a sociedade civil das possibilidades e dos perigos que existem na rede.

3.6 Direitos do autor

A tipificação das infrações relacionadas com a violação dos direitos do autor objetiva proteger principalmente a indústria do entretenimento, que tem se queixado de perdas financeiras causadas pelos canais abertos de compartilhamento de arquivos na rede, “(...) e, por isso, vem fazendo lobby para impor ao mercado a utilização dos *digital rights management* ou DRM – programas e equipamentos que impossibilitam a cópia de conteúdo protegido por direitos autorais” (SPYER, 2007, p. 200).

Tipificar como crimes as violações dos direitos do autor talvez não seja, na opinião de Demi Getschko, a solução para o problema causado com relação à propriedade intelectual:

> *A propriedade intelectual baseou boa parte da sua operação, no fato de que existia um meio de suporte físico onde a propriedade intelectual se expressa, então o autor de um livro, ele imprime um livro, e pelo fato de imprimir n exemplares do livro, ele pode ter uma conta que vai gerar à ele uma receita, porque o livro carrega a idéia dele em papel. Da mesma forma que um compositor de música grava um meio físico, onde a música dele, de alguma forma, pode ser transportada e ele pode controlar isso. Mas, se nós voltarmos ao passado, não tão distante assim, na época dos compositores clássicos, Bach e outros, a coisa não era assim. Na verdade Bach, quando*

> *compunha um oratório, ou o que fosse, ele ganhava "pra" fazer aquilo, mas ele não ganhava para que estocassem aquilo, ao contrário, ele gostaria que tocassem bastante aquilo, porque toda vez que tocavam aquilo, provavelmente ele iria receber uma encomenda de um novo oratório, e ele ia ser pago pra produzir mais uma missa ou uma cantata, ou o que fosse. Então os meios de remunerar o autor a partir dos meios de reprodução geraram o suporte físico da idéia. A Internet, de alguma forma, volta a destruir esse negócio, quer dizer, o suporte físico da idéia desaparece. Além de desaparecer o suporte físico da idéia, o intermediador desaparece. A rede desintermedia as coisas: quer dizer, o autor e o consumidor são colocados diretamente em contato. Eu posso gerar um texto e passar diretamente "pros" meus leitores através do meu blog sem ninguém no meio do caminho. E eu não tenho como numerar quantas vezes aquilo foi lido ou não lido, porque uma vez lido por alguém isso sempre pode ser espalhado pela rede e, uma vez gerada a informação, ela se distribui e é muito difícil controlá-la. Então, certamente, eu acho que nós teremos algum impacto na área de propriedade intelectual, as coisas vão ter que ser revistas, provavelmente conceitos serão revistos provavelmente a forma de remunerar o autor será revista, porque certamente não há como tampar as infinitas possibilidades que a rede tem de você copiar algo. Se tentou fazer assinaturas e formas de criptografia e de fazer, mas, uma vez que esteja disponibilizado para leitura, "ta" na rede, e como nós já falamos, todos os bits são iguais e não tem mais como segurar. Esse é um ponto que eu acho que a rede vai trazer impacto.*

Algumas regiões, como a Escandinávia e a Suécia procuram outras alternativas para permitir a "pirataria". Há propostas que viabilizam *downloads* mediante valores mensais destinados a pagamentos relativos aos direitos autorais, que estariam inclusos nas contas de acesso à *Web*. Como ainda não é possível viabilizar esta solução, devido à existência de uma multiplicidade de autores e obras, o impasse permanece e o download de filmes, músicas e obras não autorizadas continua sendo considerado um cibercrime.

3.7 Liberdade versus controle

Os países têm procurado colaborar mutuamente no combate aos cibercrimes, inaugurando uma espécie de "governança política coletiva", algo que

suscita algumas novas situações, como o acesso a informações confidenciais de cidadãos que vivem distantes de seu país local: “(...) o compartilhamento de acesso global a redes de informação é uma forma decisiva de impor poder estatal coletivo sobre todos os cidadãos em toda a parte, já que as conseqüências da informação obtida guiarão a repressão em contextos específicos” (CASTELLS, 2003, p.148).

Quando se trata de combater crimes como o racismo ou a pedofilia, a intervenção da “governança política coletiva” ou “ciber-governança internacional” de países pode ter bons resultados de maneira geral. Porém, o compartilhamento de informações entre os países possibilitados por esta governança coletiva pode levar a perseguições políticas ou de natureza discriminatória a cidadãos de “esquerda” ou de “direita” e a homossexuais. Malásia e Arábia Saudita são países cuja legislação é punitiva para gays ou lésbicas. Isto pode levar a intervenção em assuntos privados destes cidadãos, que eventualmente morem nos Estados Unidos, por exemplo. O resultado por vezes pode se concretizar de forma inusitada, conforme explica Castells:

> Ademais, a vigilância global invade a liberdade de expressão. Isto ocorre em menor grau em países como os Estados Unidos, onde há forte proteção legal desse direito básico. Mas uma vez que o tráfego seja conjuntamente interceptado por agências de vários países, os usos dos dados obtidos mediante a vigilância não ficarão restritos à jurisdição dos tribunais norte-americanos (CASTELLS, 2003, p.148).

É por esse motivo, que os gestores da Internet no Brasil e nos Estados Unidos, consideram a intervenção e monitoramento da Internet um tema que merece muita atenção. O matemático e cientista da computação americano Vinton Cerf, que presidiu a ICANN (*Internet Corporation for Assigned Names and Numbers*), de 2000 a 2007 e foi o idealizador da Internet e criador dos protocolos que deram origem a toda a rede de computadores, expressou suas preocupações com respeito às questões envolvendo a segurança da comunicação e outras práticas que podem tornar-se abusivas. De acordo com Vinton, a Internet precisa evoluir para desenvolver novas formas de tratar tais temas. O problema é definir uma política que possa gerir todo este conjunto de informações, conhecimento e entretenimento, conciliando o respeito à liberdade de expressão. No entanto, definir uma política para comunicação virtual não é algo simples. Os argumentos a favor da proibição

dos excessos, partem, na maioria das vezes, de juristas, desembargadores e promotores, que consideram que a esfera digital não deve estar à parte das ocorrências do ambiente físico e temem que a falta de controle na rede leve à impunidade para crimes de todos os gêneros (BUARQUE, 2006).

De acordo com Lucena (2007), alguns gestores da rede, como é o caso de Susan Crawford,[23] defendem que a rede seja um ambiente de livre manifestação, e quaisquer censuras ou bloqueios serão ineficazes, pois os internautas sempre conseguirão encontrar maneiras de contornar tais bloqueios. Além de que, está em discussão, neste caso, a liberdade de expressão, que tem nos Estados Unidos, garantia da *Primeira Emenda*. Demi Getschko, representante de notório saber sobre assuntos de Internet, membro do Comitê Gestor e conselheiro da ICANN, considera importante manter a característica de liberdade na rede:

> *(...) conforme existe risco na rede, porque, como a rede está disponível a todos que colocarem o que acham, existe certamente uma facilidade de propagação de coisas que não são verdadeiras, ou não são corretas. Agora, eu acho que esse é um custo a pagar pela liberdade da rede, acho que é importante que nós mantenhamos essa abertura e que todos possam dizer o que queiram, evidentemente o pessoal da legislação, da justiça e tal, vai ter que ver como coíbe os que falam coisas inadequadas ou falsas ou inverídicas sem que o abuso impeça o uso, não é, uma das regras básicas em geral que se tem, liberais, abertas, democráticas, é que o abuso não deve tolher o uso. Se alguém abusa de algo, isso não quer dizer que devemos tirar o uso legal daquilo, porque está havendo um abuso.*

Os cientistas e filósofos tendem à opinião semelhante a dos gestores da rede, ressalvando, no entanto, que os cibercrimes devam ser punidos, especialmente aqueles relacionados à pornografia infantil e à pedofilia. Tavares (Presidente da ABRANET e membro do Comitê Gestor da Internet no Brasil) considera que tais problemas devam ser resolvidos através de ferramentas de proteção:

> *Muito bem, ah, em termos comportamentais, portanto, o que é que nós passamos a ter como preocupação: algumas coisas que*

[23] Professora de direito cibernético e direito das comunicações na *Cardozo Law School*, em Nova York, e diretora da Icann, a entidade internacional que coordena a Internet.

> *não eram transparentes ao ser humano comum eram as redes de pedofilia por exemplo. E nesse caso, fica muito claro a Internet, ela é, protege de certa forma o anonimato, algumas pessoas, de formação, lamentavelmente baixa e, portanto, permite que aconteça esse tipo de coisa. Por isso, é preciso desenvolver a ferramentas de filtro de proteção para evitar que isso cresça, prá se fazer a correção do rumo e a boa utilização de uma mídia como a Internet.*

Estudiosos de comunicação, filosofia, sociologia e política, especialmente na Europa e nos Estados Unidos, têm sua atenção voltada à expansão da cibercultura e seus efeitos no tecido social. Segundo Veras (2000), há estudiosos otimistas, como o filósofo Pierre Lévy, que acreditam nas possibilidades abertas pelo ciberespaço em direção a um futuro promissor, no qual a humanidade terá a sua disposição uma enorme inteligência e um grande cérebro do mundo. Outros, como o pesquisador e professor da Universidade de Toronto, Derrick de KERCKHOVE (1995, p. 113), são cautelosos e consideram, em seus estudos, a complexidade das relações na era da comunicação eletrônica, em que as fronteiras entre o público e o privado e o local e o global esmaeceram, pois as nações estão se integrando em outro nível histórico, no qual as formas tradicionais de identidade estão ameaçadas. Este autor também percebe o impacto do avanço das telecomunicações nas diferentes culturas, avaliando a importância da globalização na expansão das fronteiras culturais – criando uma nova cultura mundial - porém alerta para o problema da necessidade de preservar a regionalização, a manutenção das identidades e do sentimento de unidade, essenciais para manter um país ou uma empresa. A questão dos controles para a Internet irá demandar, nos próximos anos, discussões mais aprofundadas e abrangentes entre os gestores da rede, legisladores, políticos e sociedade civil organizada.

3.8 Legislação Brasileira

No Brasil, encontra-se em tramitação no Senado Federal, o substitutivo de lei apresentado pelo Senador Eduardo Azeredo, PSDB/MG (Anexo C), que abrange três projetos de lei anteriormente existentes que versam sobre os cibercrimes, que

são: o Projeto de Lei da Câmara dos Deputados número 89, de 2003, de autoria do Deputado Luiz Piauhylino, PDT/PE, o Projeto de Lei do Senado Federal número 76, de 2000, de autoria do Senador Renan Calheiros, PMDB/AL e o Projeto de Lei do Senado Federal número 137, de 2000, de autoria do Senador Leomar Quintanilha, PMDB, TO.

Desde o início da discussão empreendida por Azeredo no Senado em 2005, quando sua iniciativa foi bastante criticada, o texto de seu substitutivo tem avançado nas discussões, uma vez que está de acordo com os princípios definidos pela Convenção sobre a Cibercriminalidade, ratificados pelo Conselho da Europa e ainda pelas modificações posteriores que lhe foram apostas. As críticas ao texto original tomavam como base o artigo que regulamentava a identificação do usuário:

> A identificação do usuário de rede de computadores poderá ser definida nos termos de regulamento, sendo obrigatórios para a pessoa natural os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento, um número de documento hábil e legal de identidade e endereço completo (AZEREDO, 2007, *online*)

As dificuldades de ordem econômica para a aplicação deste artigo ficaram evidenciadas nas palavras de Antônio Alberto Tavares, presidente da ABRANET (Associação Brasileira dos Provedores de Acesso):

> No seio do projeto pode perceber-se uma preocupação muito grande com os processos de validação dos dados cadastrais de usuários - não apenas de Internet, mas também de celulares, de telefones (este é um dos erros) e por outro lado se induz a certificação digital como a fórmula salvadora para todos os males da Internet. Ora, mesmo reconhecendo a eficiência e importância da certificação digital, ao se aprovar tal projeto e ao olhar para os preços elevadíssimos praticados hoje, nós corremos o risco de iniciar um processo de segregação - A Internet do Bem (dos ricos, certificados) e a Internet geral ou dos pobres. Ora, isso é imperdoável (PROJETO..., 2006, *online*).

Segundo os termos do artigo proposto originalmente no Substitutivo, não existiria privacidade para os usuários na rede, o que contraria os preceitos de liberdade preconizados pela Internet. Todavia, após discussões com representantes da sociedade civil e do Comitê Gestor da Internet, o referido artigo foi retirado.

No texto atual o Senador Azeredo ainda mantém o artigo pelo qual os provedores de acesso são obrigados a identificar e guardar os dados completos dos endereços eletrônicos acessados pelos usuários em seu sistema de acesso pelo prazo de três anos, sendo que a redação atual do Substitutivo, com relação a esse tópico, assim se encontra:

> **Art. 23.** O responsável pelo provimento de acesso a rede de computadores é obrigado a: I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o estrito 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 por esta gerados, cujo fornecimento será feito exclusivamente à autoridade investigatória e dependerá de prévia e expressa autorização judicial (PORTUGAL, 2007, p. 20).

A polêmica ainda está instaurada, porque tal identificação e guarda fazem parte de um processo que envolve alto custo para os provedores de acesso, uma vez que "(...) cada provedor ou operadora precisaria de *data centers*[24] gigantescos para guardar tudo isso e de equipamentos de *storage*[25] caríssimos" (PROJETO..., 2006). Este custo acabaria sendo repassado para os usuários, o que tornaria o acesso à Internet restrito às camadas sociais mais elevadas, impossibilitando que a grande maioria da população brasileira um dia tenha acesso à rede. Bancos e Instituições Financeiras têm procurado soluções complexas para conferir maior segurança às transações financeiras realizadas por seus clientes pela Internet, através da adoção do processo de certificação digital. Este processo demanda grande investimento financeiro, uma vez que inclui o uso de criptografia, chaves públicas/privadas e uma conexão com a Internet bastante segura. Além disso, é preciso que os certificados digitais sejam emitidos por Autoridades Certificadoras (AC), que são empresas que realizam a emissão dos certificados seguros na rede. Tais certificados precisam ser solicitados por Autoridades de Registro (AR), que no Brasil obtêm o credenciamento necessário junto ao ITI (Instituto Nacional de Tecnologia da Informação). Assim mesmo, os Bancos não têm cobrado pelas transações efetivadas via Internet, pois o custo da transação virtual possivelmente ainda é menor que o custo de recepcionar as transações dos clientes diretamente

[24] Centro de processamento de dados.
[25] Área de armazenamento de dados.

nos caixas das agências. No tocante à tipificação dos cibercrimes, o Substitutivo apresenta as alterações necessárias na legislação brasileira, fundamentado em três aspectos-chave (Anexo D):

> **Por que é preciso tipificar os crimes de informática ou cibercrimes**
> Porque a Constituição Federal diz em seu art. 5º, do Título I, Capítulo I, dos Direitos e Garantias Fundamentais, no inciso XXXIX, que:
> "XXXIX – não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;"
>
> No Direito Penal não se admite a analogia para prejudicar o réu; ou seja, a conduta deve estar claramente definida no texto da lei. Assim, algumas condutas criminosas mediante o uso de rede de computadores, dispositivo de comunicação ou sistema informatizado, devem estar claramente definidas na lei.
>
> **Por que é preciso alterar o Código Penal:**
> Porque a Constituição Federal em seu art. 59, parágrafo único, diz que "Lei complementar disporá sobre a elaboração, redação, alteração e consolidação das leis." Esta lei é a Lei Complementar nº. 95, de 26 de fevereiro de 1998, que no seu art. 7º, inciso IV, diz que:
> "IV – o mesmo assunto não poderá ser disciplinado por mais de uma lei, exceto quando a subseqüente se destine a complementar lei considerada básica, vinculando-se a esta por remissão expressa.".
> No nosso caso, a lei básica é o Código Penal, que está sendo alterado com mudanças de redação ou inclusão de novos artigos, parágrafos, incisos etc., em complemento à lei existente.
>
> **Por que é preciso criar medidas administrativas como, por exemplo, a guarda de dados:**
> Porque a Constituição Federal diz em seu art. 5º, do Título I, Capítulo I, dos Direitos e Garantias Fundamentais, no inciso II, que:
> "II – ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;"
>
> E a Lei Complementar nº. 95, de 26 de fevereiro de 1998, que no seu art. 3º, inciso III, prescreve que:
> "Art. 3º A lei será estruturada em três partes básicas:
> III – parte final, compreendendo as disposições pertinentes às medidas necessárias à implementação das normas de conteúdo substantivo [...]."
> No nosso caso, como acontece hoje, se a autoridade judicial requerer as informações de conexões informáticas, a parte responsável pela conexão pode alegar que não é obrigado por lei a guardar e muito menos a fornecer as informações (PORTUGAL, 2007, p. 7-8).

Os crimes/delitos tipificados no Substitutivo com base nestes aspectos-chave são: roubo de senha através de difusão de código malicioso (*malware*); falsificação de cartão de crédito; falsificação de telefone celular ou meio de acesso a sistema; calúnia, difamação e injúria - crimes contra a honra; difusão de código malicioso para causar dano; acesso não autorizado; obtenção não autorizada de informação e manutenção, transporte ou fornecimento indevido de informação obtida

desautorizadamente; divulgação não autorizada de informações disponíveis em banco de dados; furto qualificado por uso de informática; atentado contra a segurança de serviço de utilidade pública; ataques a redes de computadores - interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado.

Oficialmente, o Brasil não assinou a Convenção sobre a Cibercriminalidade definida pelo Conselho da Europa. Porém se houver interesse manifesto formal do país ao referido Conselho, este será convidado a participar, segundo informou ao Ministério das Relações Exteriores, o Chefe de Cooperação Técnica do Departamento de Problemas Criminais da Secretaria Geral do Conselho da Europa em fevereiro de 2007 (PORTUGAL, 2007, p. 3).

O importante a observar é a correspondência existente entre os princípios da Convenção e as Leis brasileiras (Anexo E), a partir da vigência do Substitutivo, caso seja aprovado e conforme ilustra a Figura 8.

Recomendação da Convenção	**Artigos das leis ou códigos**
1- do acesso ilegal ou não autorizado a sistemas informatizados	154-A e 155 § 4º,V do **Código Penal** 1 339-A e 240 § 6º,V do **Código Penal Militar** 2
2- da interceptação ou interrupção de comunicações	art. 16 do **Substitutivo**
3- da interferência não autorizada sobre os dados armazenados	154-D, 163-A e 171-A do **Código Penal** 339-D, 262-A e 281-A do **Código Penal Militar**
4- da falsificação em sistemas informatizados	163-A, 171-A, 298 e 298-A do **Código Penal** 262-A e 281-A do **Código Penal Militar**
5- da quebra da integridade das informações	154-B do **Código Penal** 339-B do **Código Penal Militar**
6- das fraudes em sistemas informatizados com ou sem ganho econômico	163-A e 171-A do **Código Penal** 262-A e 281-A do **Código Penal Militar**
7- da pornografia infantil ou pedofilia	241 da Lei 8.069, de 1990, Estatuto da Criança e do Adolescente (**ECA**), alterado pela Lei 10.764, de 2003;
8- da quebra dos direitos de autor	Lei 9.609, de 1998, (a **Lei do Software**), da Lei 9.610 de 1998, (a **Lei do Direito Autoral**) e da Lei 10.695 de 2003, (a **Lei Contra a Pirataria**);
9- das tentativas ou ajudas a condutas criminosas	154-A § 1º do **Código Penal** 339-A do **Código Penal Militar**
10- da responsabilidade de uma pessoa natural ou de uma organização	art. 21 do **Substitutivo**
11- das penas de privação de liberdade e de sanções econômicas	penas de detenção, ou reclusão, e multa, com os respectivos agravantes e majorantes, das **Leis citadas** e dos artigos do **Substitutivo**.

Fonte: Resenha didática com Substitutivo apresentado à CCT (PORTUGAL, 2007)

Figura 8 – As leis brasileiras e a Convenção de Budapest

A situação atual do Substitutivo é descrita por José Henrique Santos Portugal[26], assessor do Senador Eduardo Azeredo:

> O Projeto de Lei 76 de 2000, que tem apensados o PLC 89 de 2003 e o PLS 137 de 2000, foi aprovado na Comissão de Educação do Senado Federal em maio de 2005. Está com o Substitutivo apresentado à CCJ do Senado Federal desde 30 de maio de 2007. Está em tramitação suspensa na Comissão de Constituição de Justiça - CCJ. Já foi ouvida a Comissão de Ciência e Tecnologia - CCT que aprovou o Substitutivo anexado na Resenha em dezembro de 2007. Vai agora ser ouvida a Comissão de Assuntos Econômicos - CAE e de lá voltará à CCJ para continuar a ser discutido lá.
> Em agosto de 2007 recebeu a Emenda 03, aditiva, do Senador Walter Pinheiro, incluindo a alteração da Lei Afonso Arinos, crimes de discriminação de raça e cor e na Comissão de Ciência e Tecnologia o Relator incluiu a alteração do Estatuto da Criança e Adolescente para tipificar o crime de “manter consigo” vídeos, fotos etc. relativos à pedofilia.

Com respeito à pornografia infantil e pedofilia, a legislação brasileira é expressa no Estatuto da Criança e do Adolescente, de 1990 e alterado em 2003:

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar, ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.
> Pena – reclusão de 2 (dois) anos a 6 (seis) anos, e multa.
> § 1° Incorre na mesma pena quem:
> I – agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;
> II – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do caput deste artigo;
> § 2° A pena é de reclusão de 3 (três) a 8 (oito) anos:
> I – se o agente comete o crime prevalecendo-se do exercício de cargo ou função;
> II – se o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial (BRASIL, 2003, *online*).

A análise da legislação brasileira mostra que o Substitutivo apresentado pelo Senador Azeredo tem méritos, pois abrange os principais cibercrimes definidos pelo Conselho da Europa e os tipifica, algo considerado realmente necessário, pois não há crime sem lei que o defina anteriormente.

O crime de racismo veiculado via Internet, que não se encontra tipificado pela Convenção sobre Cibercriminalidade ratificada pelo Conselho da Europa

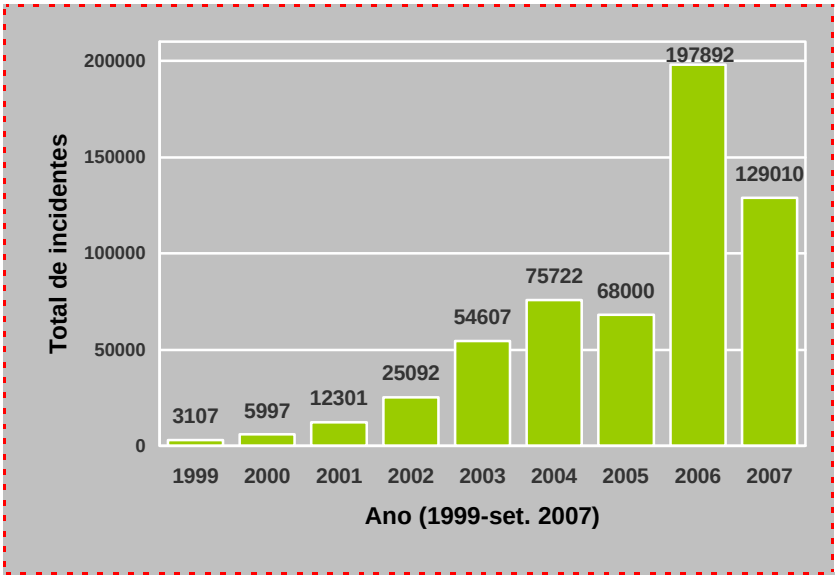
[26] Texto recebido em correspondência eletrônica pessoal (e-mail) em 23/01/2008.

(consta apenas do Adendo de março de 2006 e não assinado por todos os membros), está previsto no Substitutivo. Isto o torna mais completo que a referida Convenção, embora o crime de racismo já conste da Constituição de 1988, em seu artigo 5º, que considera a prática do racismo inafiançável e imprescritível. A Lei 8081, de 1990, "(...) estabelece os crimes e as penas aplicáveis aos atos discriminatórios ou de preconceito de raça, de cor, religião, etnia ou procedência nacional, praticados pelos meios de comunicação ou por *publicação de qualquer natureza,* estipulando penas de 2 a 5 anos para a prática desses crimes" (BRASIL, 1990). De qualquer maneira, o Substitutivo inclui a emenda 03, aditiva, de autoria do Senador Walter Pinheiro, PT/BA, que dispõe sobre o racismo difundido via Internet.

O Substitutivo ainda não pôde ser votado e a sociedade civil o desconhece, dois fatores que podem contribuir para o aumento dos cibercrimes no Brasil. É o que demonstra o texto abaixo, de autoria do Senador Eduardo Azeredo (2007, p. 11):

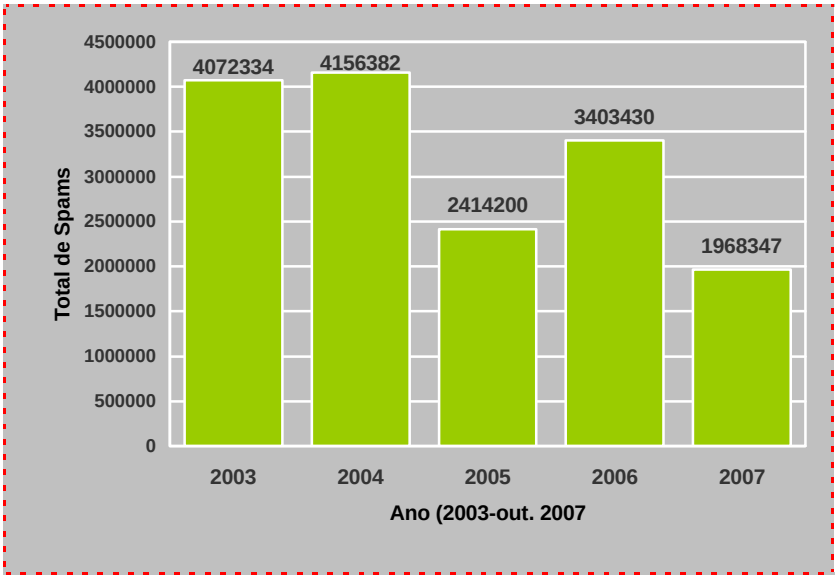
> O tema é atual e merece a devida atenção do Congresso Nacional. Segundo recentes dados divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (www.cert.br), os códigos maliciosos, classificados como *worm*, representam 40%, ou 51 mil, de todos os incidentes reportados ocorridos na Internet no Brasil até setembro de 2007.
>
> Em segundo lugar aparecem as tentativas de fraudes, que chegam a pouco mais de 50 mil e representam 39% dos mesmos incidentes. Segue-lhes os 22 mil incidentes, ou 17%, relativos a leitura simples ou busca, no jargão técnico, *scan*. Em menor volume, mas com mesmo grau de periculosidade ou até maior, os incidentes restantes, são distribuídos em 1.800 ataques de negação de serviço (*DoS - Denial of service*), ou 1,5%, 1.350 ataques a servidores (*aw*), ou 1%, e 200 invasões.
>
> Os números, frise-se bem, podem ser muito maiores, dado que o CERT.br considera apenas as informações reportadas espontaneamente pelos usuários e administradores de redes. Ao todo, o CERT.br recebeu, no ano passado, 197 mil comunicações de incidentes relacionados à Internet, alta de 191% em relação a 2005. Este ano já chegam a 129.010 em setembro, mostrando que há uma tendência de ligeira queda, mas o volume é preocupante.
>
> Em relação ao SPAM os números também são preocupantes. Até o momento não foi possível a sua tipificação penal, embora inúmeros projetos de lei estejam em tramitação. Tratando-se de uma mensagem sem autorização prévia, ele é tecnicamente correto como conceito fundamental de uma rede de computadores, mas é perigoso pois é freqüentemente usado como vetor de disseminação de códigos maliciosos de qualquer tipo e objetivo.

O relatório do Senador Eduardo Azeredo anexa as Figuras 9 e 10, que registram a quantidade de incidentes reportados ao Comitê Gestor da Internet.



Fonte: CERT.br (2008b)

Figura 9 – Total de incidentes reportados ao CERT.br no período de 1999 a setembro de 2007



Fonte: CERT.br (2008b)

Figura 10 - Total de spams reportados ao CERT.br no período de 2003 a outubro de 2007

> Os bancos e o comércio continuam os principais alvos, com perdas estimadas em mais de R$ 300 milhões por ano em fraudes virtuais, mas os crimes contra a honra, calúnia, difamação e injúria, incomensuráveis no mal que provocam, e de difícil ou impossível reparação, são fortes concorrentes aos crimes econômicos, não em volume, mas no aumento relativo, face ao covarde anonimato na rede e à expansão, ou explosão, do uso de computadores no país.
>
> Com esses números, o Brasil ficou, em 2006, na segunda colocação entre os dez países com maior número de incidentes reportados. O líder são os Estados Unidos da América (EUA), com 24,61% dos incidentes, seguido pelo Brasil, com 21,18% deles, e o Canadá, em terceiro lugar, 9,45%.
>
> De acordo com a Comissão Federal de Comércio dos EUA, o custo de crimes de furto pela Internet para pessoas físicas e jurídicas no país atinge US$ 50 bilhões por ano. No Reino Unido, o custo para a economia, segundo o Ministério do Interior, foi de US$ 3,2 bilhões nos últimos três anos.
>
> Como se pode observar, trata-se de problema sério e que precisa ser enfrentado pela legislação brasileira (AZEREDO, 2007, p. 11-13).

Os gestores da Internet, de maneira geral, não acreditam que as questões criminosas na Internet serão resolvidas com a legislação ou com o cerceamento da liberdade dos usuários na rede. Para eles, é necessário um processo de educação digital.

Na área preventiva, o Comitê Gestor da Internet desenvolveu dois projetos educativos considerados de grande interesse para todos os usuários de Internet: a Cartilha de Segurança para Internet e o projeto Anti-Spam, ambos disponíveis no endereço eletrônico do CGI (www.cgi.br).

A Cartilha de Segurança para Internet está dividida em 8 tópicos: Conceitos de segurança; Riscos envolvidos no uso da Internet e métodos de prevenção; Privacidade; Fraudes na Internet; Redes de banda larga e redes sem fio (*wireless*); *Spam*; Incidentes de segurança e Uso abusivo da rede e *Malware* (códigos maliciosos). Cada um destes tópicos desvenda e detalha, de forma didática, os mecanismos de proteção e os dispositivos que atacam os computadores, em conexão na Internet.

O Projeto Anti-Spam relaciona em seu *site* os tópicos: o que é *spam*; problemas causados pelo *spam*; origens e curiosidades; tipos de *spam*; como identificar; boas práticas; dicas; como reclamar; dúvidas mais freqüentes; vídeos educativos e glossário.

Os vídeos educativos trabalham em seqüência: Navegar é preciso; Os invasores; *Spam* e A Defesa. São vídeos de boa qualidade e têm curta duração (6

minutos em média, para cada um). A narrativa e os desenhos mostram ao usuário como navegar com segurança na Web. Tais vídeos poderiam já estar sendo veiculados nas escolas como parte da necessária campanha de segurança na rede da qual falou-se anteriormente.

O desenvolvimento destes dois projetos demonstra, portanto, a importância do tema segurança para os usuários de Internet, notadamente para os novos internautas, que ingressam no meio a cada ano, e que, raramente, recebem a correta orientação para navegar na Web com segurança.

As questões de segurança também remetem às questões de privacidade na rede. Pensar no futuro da Internet é também retomar esta discussão, porque a rede possibilita que os dados e registros pessoais possam ser capturados por sistemas e programas que os usuários comuns não podem controlar, ocasionando o acesso a dados de caráter privado dos usuários.

A privacidade de uma pessoa consiste em seu poder de controle sobre seus dados, imagens e registros de maneira geral, de maneira que não possam ser utilizados por terceiros de forma indevida ou não autorizada. Registros pessoais armazenados nos servidores e capturados posteriormente são freqüentemente utilizados por empresas especializadas para montar perfis de compra comercializáveis, obtidos na maioria das vezes à revelia dos usuários. Além disso, é possível postar na rede informações, vídeos e fotografias de pessoas famosas ou não, e instantaneamente milhares de outras pessoas terão acesso a estes registros. Estes fatos tem causado alguns impactos na vida das pessoas de difícil resolução apenas com a legislação. Foi o que ocorreu, por exemplo, com a modelo e apresentadora de TV Daniela Cicarelli em 2006, quando foi postado um vídeo no *site YouTub*e, revelando cenas de intimidade em um passeio na praia com seu namorado. Na época, o referido *site* foi retirado do ar, por ordem judicial, gerando protestos dos internautas. Demi Getschko considera:

> *(...) quem foi punido foi o acesso ao YouTube, que não tinha nada a ver com o caso Cicarelli em si. Quer dizer, se alguém fez um vídeo inadequado, que ele seja justiciado de alguma forma, punido de alguma forma, mas não que percamos o acesso a um recurso como o YouTube, que era usado pelo governo do Rio Grande do Sul, por exemplo, na campanha contra a dengue, então, é muito importante separar a rede em si, que na minha*

> *opinião é inimputável, dos usuários da rede que obviamente são responsáveis pelos seus atos.*

A sociedade da informação traz, então, de forma concomitante, as possibilidades de vigilância e a exposição dos cidadãos. Cabe indagar até que ponto esta nova sociedade, permeada pelas tecnologias da informação e comunicação ainda preza a privacidade? Ou em outras palavras, a privacidade é um valor para as pessoas que vivem no contexto da digitalização e informatização crescente da vida cotidiana?

Na era das câmeras digitais que gravam pequenos vídeos e dos celulares que tiram fotos instantâneas, todos os indivíduos podem ser produtores de cultura visual. O que importa a exposição quando esta é objeto de desejo? Que sentido há proteger a privacidade e/ou o anonimato na Web se o monitoramento e vigilância sobre os cidadãos são possíveis a partir de redes bluetooth em celulares?[27]

Todos os espaços públicos na cidade e em breve, todos os espaços privados têm e terão possibilidades de se constituir em mídias locativas:

> Podemos definir mídia locativa (*locative media*) como um conjunto de tecnologias e processos info-comunicacionais cujo conteúdo informacional vincula-se a um lugar específico. (...) As mídias locativas são dispositivos informacionais digitais cujo conteúdo da informação está diretamente ligado a uma localidade. Trata-se de processos de emissão e recepção de informação a partir de um determinado local. Isso implica uma relação entre lugares e dispositivos móveis digitais até então inédita. Esse conjunto de processos e tecnologias caracteriza-se por emissão de informação digital a partir de lugares/objetos. Esta informação é processada por artefatos sem fio como GPS, telefones celulares, *palms* e *laptops* em redes Wi-Fi ou Wi-Max, *Bluetooth*,ou etiquetas de identificação por rádio freqüência, RFID4. As mídias locativas são utilizadas para agregar conteúdo digital a uma localidade, servindo para funções de monitoramento, vigilância, mapeamento, geoprocessamento (GIS), localização, anotações ou jogos. Dessa forma, os lugares/objetos passam a dialogar com dispositivos informacionais, enviando, coletando e processando dados a partir de uma relação estreita entre informação digital, localização e artefatos digitais móveis (LEMOS, 2007, p.1-2).

Assim como os espaços físicos podem ser controlados, o ciberespaço também poderá. O tema dos controles na Internet tende a ser resolvido a médio e longo prazo, focado nas possibilidades de redução de custos das tecnologias de

[27] A base de celulares ativos no Brasil atingiu 99,9 milhões de assinantes em 2006 e mais de 120 milhões em 2007, segundo dados da Agência Nacional de Telecomunicações (ANATEL, 2008).

controle. É o que prevê Yochai Benkler, professor de Direito da Universidade de Yale, segundo relato de Spyer (2007, p.212):

> Para ele, a Internet é apenas temporariamente indestrutível e se não for defendida pelos indivíduos, em 20 anos terá sido “domesticada” pelos governos e pelos grupos de poder da sociedade, da mesma forma como aconteceu com mídias igualmente descentralizadas e baratas como o rádio.

Diante das redes de crimes digitais, constituídas por pessoas que se reúnem com objetivos que colocam em risco a vida de outras pessoas e diante de uma sociedade na qual a privacidade não é mais um valor, ou, deixa de ser gradativamente um valor em função do desenvolvimento das tecnologias de controle, deixar a Internet como um espaço totalmente livre para todas as manifestações, não deve ser a opção dos Governos.

No mesmo sentido, segmentos organizados da sociedade começam timidamente a repensar as conseqüências éticas e legais que advêm do uso das tecnologias da comunicação e informação.

> Há uma minoria de pessoas que exploram o poder da Internet para finalidades criminosas e terroristas. A ciber-ética pode minimizar estes problemas, por ensinar a utilizar a Internet com responsabilidade e de forma segura. Um comportamento seguro pode ser ensinado, especialmente aos jovens, para que se protejam e protejam os outros conhecendo quais são os riscos de condutas ilegais na rede de computadores (USA, 2008, *online*).

A ciber-ética, ou seja, a utilização da ética na produção e disseminação de informações no ambiente eletrônico é um tema novo que vem sendo pensado e discutido no bojo das transformações da era virtual, na qual aumentam as oportunidades de comunicação e de aprendizado disponibilizadas por computadores e por conexões possibilitadas pela Internet, ao mesmo tempo em que identidades são roubadas, fraudes são praticadas e muitos outros delitos que desconhecemos ameaçam a integridade e o ambiente virtual, no qual todos estaremos inseridos dentro de poucos anos.

Este capítulo mostrou como os problemas de segurança na rede vêm aumentando consideravelmente, devido à ocorrência dos denominados cibercrimes que, para além de danos financeiros e morais, trazem à tona o debate sobre o direito

de expressão na Web, à primeira vista colocado como irrestrito, e que tem sido defendido por alguns segmentos da sociedade, uma vez que é o primeiro meio de expressão global sem fronteiras e sem censuras.

Embora ainda não exista um consenso, governos, legisladores e gestores da rede no mundo começam a pensar e discutir formas de governança mais focada em controles, visando principalmente conferir maior segurança na comunicação para os milhões de usuários que se utilizam da Internet diariamente.

4 A INTERNET BRASILEIRA E O COMITÊ GESTOR

Há consenso entre os estudiosos, especialistas e autoridades envolvidas com as atividades relacionadas à Internet, com o fato de que esta é uma poderosa ferramenta de comunicação, conhecimento e informação que, embora de recente criação e ainda em desenvolvimento, está se expandindo no mundo todo com rapidez notável.

Fenômeno de comunicação, no formato “de muitos para muitos”, tem se inserido no cotidiano das pessoas como instrumento de trabalho, entretenimento, obtenção de serviços públicos, compra eletrônica, pertencimento a comunidades virtuais, entre outras aplicabilidades. Dessa maneira, tem facilitado a comunicação corporativa, familiar, social, política e cultural, especialmente por esta capacidade de aproximar pessoas através de mensagens, textos, vídeos, *chat’s* etc.

Todo esse rápido desenvolvimento rendeu fortunas e provocou prejuízos, como aconteceu com o *site Yahoo!*, que segundo Vieira (2003, p.13), em 2000, contava com 180 milhões de usuários e faturamento de 1,1 bilhão de dólares/ano, possuindo valor de mercado de 100 bilhões de dólares. Em 2001, o *Yahoo* teve perda de receitas que fizeram seu faturamento cair para a marca de 717 milhões de dólares. Segundo informou o *site* Folha *On line*, em 11 de fevereiro de 2008, o *Yahoo* recusou oferta da Microsoft para sua aquisição no valor de US$ 42,6 bilhões e estava acordando aliança corporativa com outra empresa, a NewsCorp, como forma de resistir à fusão com a Microsoft (YAHOO!..., 2008). Atualmente, a Microsoft desistiu de adquirir o Yahoo que não se fundiu com a News Corp e firmou um acordo operacional com o Google. Pelos termos do acordo, o Yahoo pode utilizar tecnologia de busca nos arquivos do Google e ao exibir os resultados, apresentar anúncios contextualizados do Google em suas páginas e em *websites* parceiros nos Estados Unidos e no Canadá (CHAVES, 2008).

A Internet, para além de seu alcance comunicacional, pode ser vista também como grande negócio:

> (...) Assim como a máquina a vapor na segunda metade do século XIX, a indústria automobilística no início do século XX e a televisão na década de 1950, a Internet vive atualmente dias comuns a qualquer indústria em

> formação. Sofreu, até o momento, todos os altos e baixos inerentes a qualquer tipo de negócio em seu início (...) (VIEIRA, 2003, p.xx).

Embora tendo que enfrentar prejuízos, provedores e grandes empresas brasileiras não se furtaram a participar do *e-commerce* (comércio eletrônico), que vem ganhando adeptos entre os consumidores em todo o país.

O temor de utilizar o cartão de crédito nas compras *on-line* não intimida os consumidores das Americanas.com. "(...) 100% dos usuários cadastrados possuem esse meio de pagamento e são responsáveis por um tíquete médio de 350 reais (contra 14 reais das lojas de tijolo e cimento da rede)" (VIEIRA, 2003, p. 217).

Outras redes consolidam sua participação no comércio eletrônico. Lojas que vendem de eletrodomésticos a roupas de cama, mesa e banho decidiram-se por colocar seus produtos também na venda *on-line*. É o caso do Ponto Frio, Magazine Luíza e Casas Pernambucanas. Estas empresas também estão apostando na venda de computadores, celulares e câmeras digitais em suas lojas físicas e virtuais, aproveitando a inserção do consumidor comum no mundo da *Web*[28].

Esta inserção é disponibilizada no Brasil pelas operadoras e empresas de TV por assinatura através de acesso discado e banda larga, sendo que o acesso à Internet originário dos domicílios brasileiros apresenta a seguinte configuração:

Tabela 4 - Tipo de conexão à Internet no domicílio

Tipo de Conexão	Total (%)*	Entre os que utilizaram a Internet somente no domicílio *
Somente acesso discado	52,1	57,4
Somente acesso banda larga	41,2	36,3
Acesso discado e por banda larga	6,7	6,2

Fonte: Teleco (2007a)
* percentual das pessoas na população de 10 anos ou mais de idade que utilizou a Internet nos últimos três meses (PNAD 2005)

Na modalidade de conexão à Internet através de acesso discado, a própria linha telefônica do usuário é utilizada, ocasiões nas quais seu telefone fica indisponível.

[28] *World Wide Web* (rede de alcance mundial) é a interface gráfica da Internet. Sistema de informações organizado de maneira a englobar todos os outros sistemas de informação disponíveis na Internet (USP, 2003).

A conexão banda larga possibilita diferentes tipos de inserção, classificados nas modalidades ADSL (*Assymetric Digital Subscriber Line*), TV por assinatura, conexão via rádio direto ou redes locais e banda larga via satélite. A modalidade ADSL utiliza os cabos telefônicos e é oferecida pelas operadoras de telefonia fixa, como o *Speedy* (*Telefonica*), Velox (Telemar) e Turbo (Brasil Telecom). Conexões banda larga oferecidas pelas empresas de TV's por assinatura, como a Net por exemplo, utilizam dispositivos modem ou *wireless* (redes sem fio). Quando o dispositivo usado é o *modem*[29], o acesso é feito por meio dos cabos que fazem parte da estrutura para distribuição da TV a cabo. Os sistemas de redes sem fio (wireless) operam por meio da emissão de ondas eletromagnéticas de rádio, transmitidas pelo provedor conectado à Internet.

O perfil da banda larga no país pode ser observado na Tabela 5.

Tabela 5 - Internet Banda Larga no Brasil: total de conexões (2002-2006)

Milhares	2002	2003	2004	2005	2006
ADSL	526	993	1.880	3.152	4.341
TV assinatura (Cabo)	135	203	342	629	1.200
Outros (Rádio) *	31	40	50	75*	115*
Total Brasil	692	1.236	2.272	3.856	5.656

Fonte: Teleco (2007b).
* estimativa Teleco. Não inclui satélite. (Dados revisados em ago./2007)

A conexão via banda larga através dos cabos telefônicos, como é o caso do Speedy da Telefônica, cuja tecnologia ADSL utiliza a própria infra-estrutura de par de cobre da concessionária para levar Internet veloz aos seus clientes, começa a ser também ofertada através de fibra óptica. Segundo Demi Getschko, a questão da infra-estrutura é bastante importante para que o usuário possa ter uma experiência completa de acesso à Internet e o Comitê Gestor está atento a isso:

> *Eu acho que o papel fundamental aí de Governo, do Comitê Gestor e outros aí, é estimular a penetração da infra-estrutura para que a rede possa ser accessível de todos os pontos do país. O nosso país é gigantesco, nós temos pontos em que a infra-*

[29] *Modem*: dispositivo que permite o envio e recebimento de dados utilizando as linhas telefônicas (CGI, 2006b, p. 82).

> *estrutura de telecomunicações ainda é extremamente precária e à vezes nem existe. Um bom acesso à rede exige estruturas de superfície; satélite nunca é uma boa alternativa, porque o satélite tem um atraso grande, então, o ideal seria que tivéssemos uma estrutura em cima de fibra óptica (...).*

A infra-estrutura em fibra óptica, no entanto, exige maiores aportes financeiros, justamente pela necessidade de construir uma nova rede de transmissão com outro material. A principal diferença entre a banda larga por fio de cobre e a fibra óptica é a velocidade. Segundo reportagem da Gazeta Mercantil, "(...) enquanto o Speedy consegue chegar a 8 Megabits por segundo (Mbps), a fibra óptica leva 30 Mbps ou até mais à casa do cliente ou a seu escritório, no caso de profissionais liberais" (TELEFÔNICA..., 2008).

A velocidade passa a ser cada vez mais importante, na medida em que jogos interativos e entretenimento (filmes e vídeos) ocupam espaço cada vez maior na Internet. Assistir a filmes sem ter que baixar arquivos, como por exemplo, os vídeos exibidos pelo site YouTube, ou jogar determinados jogos *on line*, através da tecnologia de banda larga via fibra óptica, são experiências bem diferentes das demais tecnologias, cuja velocidade é menor, inclusive a do Speedy, que está entre as mais rápidas.

Para além dos aspectos financeiros e técnicos, cujos números são expressivos, a Internet tem despertado a atenção para discussão de outros temas que dizem respeito à formação de identidades, como a sociabilidade *on-line* e as comunidades virtuais; a novos formatos educativos, como a educação à distância; à participação política e religiosa via *Web* e as produções artísticas (ainda em debate sobre como fazer valer os direitos autorais e/ou procurar novas formas de comercializá-lo via rede).

A comunicação no ciberespaço é uma experiência que vem proporcionando maior liberdade em relação aos padrões convencionais presentes na comunicação face-a-face.

Segundo Wertheim (2001, p. 19), a interação no ciberespaço:

> Para os que de fato têm acesso a ele, há algo de potencialmente positivo em interagir no ciberespaço, pois a bagagem suscetível de gerar prevenção – um corpo sexuado, colorido e em processo de envelhecimento – fica oculta sob a tela. Invisíveis no mar do ciberespaço, quando estamos on-line

> não podemos ser avaliados sumariamente, de relance, pela cor de nossa pele ou as protuberâncias sob nossos suéteres. Um dos atrativos do ciberespaço é precisamente o alívio que proporciona do inexorável escrutínio físico que se tornou uma marca registrada da vida nos Estados Unidos de hoje. No fluxo de bits, ninguém pode nos ver vacilar. Ali, gordura, rugas, cabelo grisalho, acne, calvície, baixa estatura e outros “pecados” estéticos da carne ficam todos (literalmente) encobertos. Como a comunicação on-line é basicamente textual (pelo menos por enquanto), o cibernauta se vê liberto da pressão constante que o obriga a ter boa aparência.

Esconder a aparência ou escolher uma outra identidade no ciberespaço é possível. Algumas modalidades de salas de bate-papos, mais conhecidas como *chat’s*, possibilitam:

> (...) que os usuários incorporem alteregos virtuais chamados popularmente de avatares. Nos novos ambientes de *chat*, os participantes não dependem exclusivamente das palavras publicadas na janela do texto para interagir. Ao entrar no chat, cada pessoa escolhe características visuais como cor da pele, sexo, roupas e outros objetos de identificação. As salas recriam espaços físicos como bares, café ou boates, que podem ter, dependendo da sofisticação do programa e da conexão do usuário, duas ou três dimensões e oferecer elementos como som ambiente, que façam com que a experiência pareça mais realista (SPYER, 2007, p. 42).

De acordo com Lévy (2004, p. 158), o ciberespaço representa a terceira etapa da evolução cultural da humanidade, baseado em três de suas proposições - a primeira, de que existe uma evolução cultural na história humana; a segunda, que a evolução cultural dá continuidade à evolução biológica e a terceira refere-se ao ciberespaço como a etapa mais recente da evolução cultural/biológica e a base para evoluções posteriores. Para ele, o ciberespaço:

> (...) integra todas as mídias anteriores, como a escrita, o alfabeto, a imprensa, o telefone, o cinema, o rádio, a televisão e, adicionalmente, todas as melhorias da comunicação, todos os mecanismos que foram projetados até agora para criar e reproduzir signos. O ciberespaço não é um meio, é um metameio (LÉVY, 2004, p. 165).

Este autor considera que meios de comunicação como o telégrafo, o telefone, o rádio, a televisão; meios de expressão artística como o cinema, a música

e a fotografia e meios eletrônicos como o computador foram “(...) começos dispersos do processo embriônico de criação do ciberespaço” (LÉVY, 2004, p. 162).

Espaço este que confere duas características à Internet que a tornam revolucionária:

> A primeira é o fato de que as mensagens serem enviadas à velocidade da luz; desse modo, pela interface da navegação, tudo o que estiver na rede está contido virtualmente em cada nó dela, à distância apenas de um clique. A rede é proximidade tecnológica de todos com todos e, como asseguram as diversas peças publicitárias, traz o mundo para a ponta de nossos dedos. A segunda (...), é a possibilidade de os nós serem também emissores de informação. A Internet como meio de comunicação rompe com a distribuição hierárquica entre emissores e receptores ao possibilitar que cada nó possa produzir e distribuir mensagens. Eis o sonho: com a Internet, enfim, a troca de mensagens assemelha-se a um diálogo ou ao que ocorre numa praça ou numa festa (VAZ, 2004, p. 225).

Percebemos, portanto, que o alcance da Internet, tal qual a teia que a representa, está presente em muitas áreas da atividade humana, sendo, ela própria, definida como “(...) ‘mídia social’ – termo que descreve ferramentas, plataformas e práticas usadas para o compartilhamento de opiniões e experiências via Internet” (SPYER, 2007, p.16).

Como entidade gestora da Internet no Brasil, o Comitê Gestor precisou também espelhar esta multiplicidade de aspectos que constituem a Internet, através de uma gestão compartilhada com setores da sociedade civil que fossem representativos dos interesses legítimos na administração deste que vem se tornando um veículo essencial na comunicação.

Nos dois capítulos anteriores, foram destacadas e analisadas a governança eletrônica e a segurança na Internet, dois temas que se encontram ainda em aberto por estarem em debate por segmentos da sociedade civil e do Governo brasileiro, quanto aos aspectos que deverão nortear os rumos dessa mídia nos próximos anos.

Para o presente capítulo, analisar-se-á o trabalho de gestão realizado pelo CGI, cujas decisões e projetos são implementadas pelo Nic.br (Núcleo de Informação e Coordenação do Ponto.br.). O Nic.br, por sua vez, é uma entidade civil sem fins lucrativos que, desde 1995 vem atuando na efetivação das ações planejadas pelo Comitê Gestor, através de seus quatro núcleos que cuidam, respectivamente de: administração de nomes de domínio; tratamento e resposta às

questões de segurança; infra-estrutura de redes e suas interconexões e produção de indicadores sobre a Internet brasileira.

O Nic.br é regido por estatuto próprio, no qual são especificados sua natureza, características e atividades. Trata-se de pessoa jurídica, de direito privado, na modalidade associação, sem fins lucrativos, que obedece às regras estabelecidas pelo Comitê Gestor da Internet no Brasil.

4.1 Registro de nomes de domínio para a Internet no Brasil – registro.br

O Comitê Gestor da Internet no Brasil coordena as atividades de atribuição de nomes de domínio no território nacional, através do registro.br.

> O sistema de nomes de domínio (DNS) na Internet permite que usuários acessem sites e outros recursos da Internet usando nomes de domínio de fácil memorização (como "www.icann.org") ao invés dos endereços IP totalmente numéricos (como "192.0.34.65") que são atribuídos a cada computador na Internet. Cada nome de domínio compõe-se de uma série de seqüências de caracteres (chamadas "labels" ou "rótulos") separadas por pontos. O rótulo na extremidade direita de um nome de domínio é conhecido como o seu "domínio de primeiro nível" (DPN). O DNS forma uma hierarquia semelhante a uma árvore. Cada DPN inclui muitos domínios de segundo nível (como "icann" em "www.icann.org"); cada domínio de segundo nível pode incluir vários domínios de terceiro nível ("www" em "www.icann.org"), e assim por diante. A responsabilidade por operar cada DPN (inclusive mantendo um registro dos domínios de segundo nível dentro do DPN) é delegada a uma determinada organização. Essas organizações são conhecidas como "operadores de registro", "patrocinadores" ou simplesmente "delegados" (ICANN, 2003, *online*).

Os países recebem como domínio duas letras. Assim, os domínios no Brasil são terminados em (br); na Argentina (ar), no Chile (cl), no Japão (jp) e assim todos os países seguem o mesmo padrão, tendo duas letras como terminações em seus domínios. É importante mencionar que essas duas letras que constituem os códigos dos países (ccTLD´s) são delegados a pessoas que respondem por sua administração e devem zelar para que estes domínios estejam adequados à situação legal, cultural, lingüística e econômica de cada país no âmbito dessa codificação e em tudo o que ela representa. Hoje há 240 países e territórios que são detentores de códigos pertencentes aos domínios de primeiro nível (DPN´s).

Existem ainda os domínios genéricos, que são identificados por três ou mais letras.

Os principais domínios genéricos são em número de dezenove e vêm sendo criados desde a década de oitenta. Estes domínios são administrados por organizações que podem ou não ser patrocinadas. O fato de determinado domínio ser patrocinado faz com que certas regras definidas pelo patrocinador precisem ser seguidas, em conformidade com a comunidade atendida pelo domínio em questão.

A Figura 11 mostra os domínios genéricos e suas respectivas finalidades.

DPN´s Genéricos	Introduzido em	Patrocinado (S/N)	Finalidade
.aero	2001	S	Indústria de transporte aéreo
.biz	2001	N	Empresas
.cat	2005	S	Comunidade lingüística e cultural catalã
.com	1995	N	Irrestrito (mas destinado a registrantes comerciais)
.coop	2001	S	Cooperativas
.edu	1995	S	Instituições educacionais dos Estados Unidos
.gov	1995	S	Governo dos Estados Unidos
.info	2001	N	Uso irrestrito
.int	1998	N	Organizações criadas por tratados internacionais entre governos
.jobs	2005	S	Comunidade internacional de administradores de recursos humanos
.mil	1995	S	Exército dos Estados Unidos
.mobi	2005	S	Comunidade de fornecedores e usuários de conteúdo para telefonia móvel
.museum	2001	S	Museus
.name	2001	N	Para registro por indivíduos
.net	1995	N	Irrestrito (mas destinado a provedores de redes, etc.)
.org	1995	N	Irrestrito (mas destinado a organizações que não se encaixam em outro domínio)
.pro	2002	N	Contadores, advogados, médicos e outros profissionais
.tel	2006	S	Específico para http://www.telnic.org
.travel	2005	S	Comunidade de viagens e turismo

Fonte: adaptado de ICANN (2006).

Figura 11 – Domínios genéricos

Os domínios genéricos com, net e org permitem que sejam registrados sob seu nível novos sub-domínios sem restrições.

Existem regras definidas por políticas especialmente formuladas para atribuição de nomes de domínio, que contribuem para a transparência do processo e possibilitam que todos os interessados dele participem em igualdade de condições.

As políticas que pautam o processo de registro procuram dirimir disputas por domínios, prazos ou propriedades intelectuais e marcas específicas e se subdividem em tipologias, entre as quais citamos:

- resolução de disputas por nomes de domínios (procura combater a ciberpirataria, protegendo os domínios registrados de eventuais abusos na utilização de marcas registradas);
- resolução de disputas quanto à qualificação do regimento (relacionam-se à disputas relacionadas aos nomes de domínio aero, .coop, .museum e .travel) ;
- resolução de disputas sobre os critérios de qualificação (arbitram as contestações relacionadas ao registro de domínios name, que disciplinam registros de nomes próprios ou fictícios de indivíduos);
- contestação de registros defensivos sob alegação de propriedade intelectual (referem-se aos registros de domínio pro, exclusivos de membros cujas profissões sejam das áreas médicas, jurídicas e contábeis);
- resolução de disputas por restrições (registros de domínios biz podem se valer desta política, quando domínios registrados neste nível não seguirem as orientações do segmento);
- resolução de disputas por transferências (regula as transferências entre nomes de domínio biz, .com, .info, .name, .net, .org e .pro).

A ICANN (*Internet Corporation for Assigned Names and Numbers*) é a entidade responsável por formular tais políticas e suas respectivas regras. O Comitê Gestor da Internet no Brasil tem como princípios as políticas gerais definidas pela ICANN e o Registro.br é o responsável pela administração e resolução de conflitos relativos a nomes de domínio. No processo brasileiro, as etapas são estruturadas da seguinte maneira: inicialmente o Registro disponibiliza a pesquisa de domínios em seu *site*, para que o interessado possa verificar se já existe nome idêntico ao que pretende requisitar.

Caso haja um único candidato, o domínio será a ele atribuído. Para domínios especiais, o requisitante deverá informar ao CGI (Comitê Gestor da Internet), através de contato com o Registro, se o nome é vinculado à sua empresa/marca, de forma que este possa caracterizá-la como diferencial, e ainda, deverá comprovar que o utiliza há mais de trinta meses.

Cada entidade poderá se candidatar a vinte nomes diferentes. O reconhecimento de uma entidade ou pessoa física se faz pelo CNPJ (Cadastro Nacional de Pessoas Jurídicas) ou CPF (Cadastro de Pessoas Físicas).

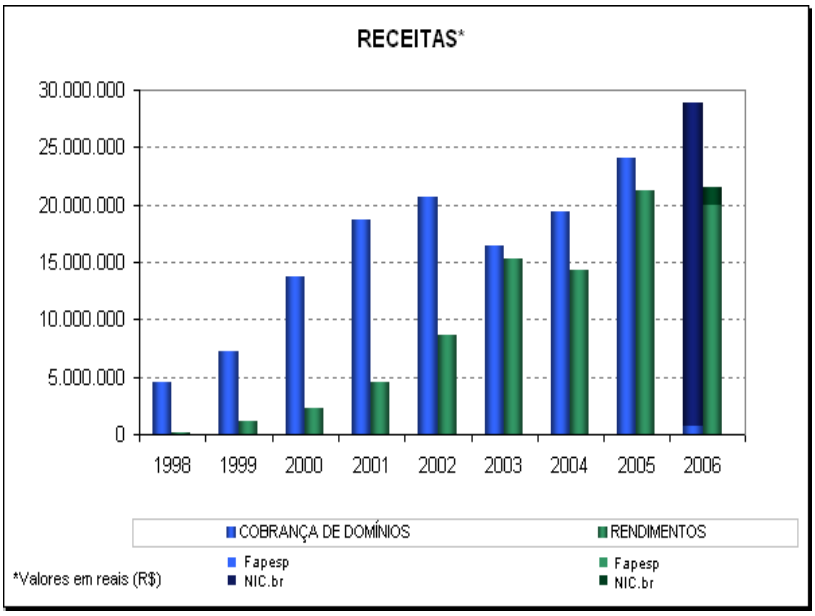
Este processo envolve custos estabelecidos pelo Comitê Gestor, que apresenta, em sua página, os seguintes valores:

Período	Registro (R$)	Manutenção Anual (R$)	Mínimo 1 ano	3 anos	Para cada ano adicionado durante o processo de registro ou renovação
Até Dez/2000	50,00	50,00			
de Jan./2001 até 22/Jan./2003	40,00	40,00			
A partir de 23/Jan/2003	0,00	30,00			
A partir de 26/Set/2007					
NOM.BR	0,00			30,00	9,00
*.BR			30,00		27,00
Exemplos					
Domínio COM.BR pelo período de 1 ano: R$ 30,00 Domínio COM.BR pelo período de 4 anos: R$ 30,00 + 3 x R$ 27,00 = R$ 111,00					
Domínio NOM.BR pelo período de 3 anos: R$ 30,00 Domínio NOM.BR pelo período de 10 anos: R$ 30,00 + 7 x R$ 9,00 = R$ 93,00					

Fonte: Registro.br (2007b).

Figura 12 - Valores definidos para aquisição de nomes de domínios

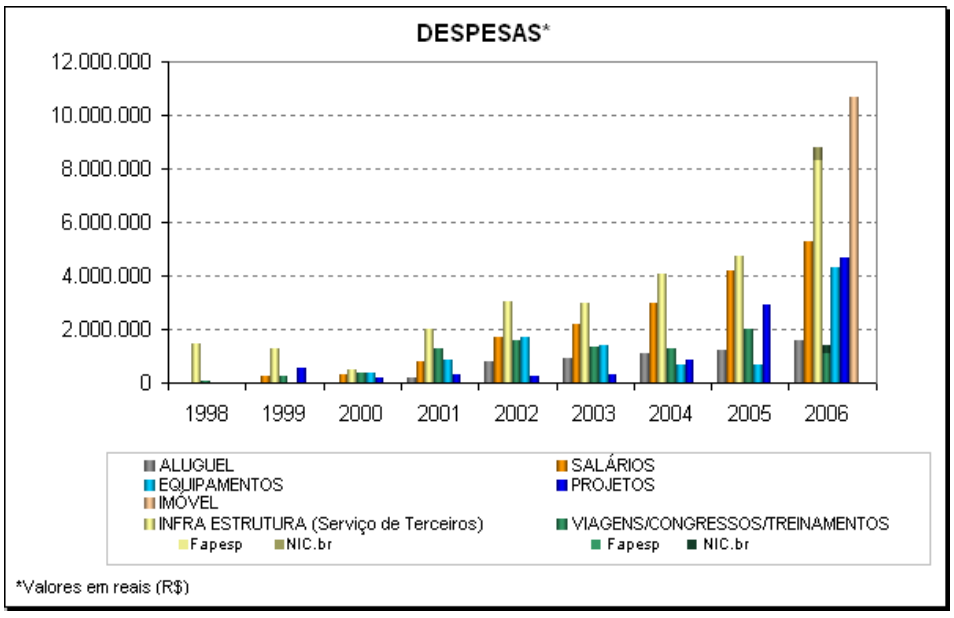
As receitas obtidas com o processo de registro de domínios até o ano de 2005 são administradas em conjunto pela FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) e pelo Comitê Gestor da Internet no Brasil. A partir de 2006, o Nic.br (Núcleo de Informação e Coordenação do Ponto.br), a quem foi delegada a atribuição e permissão de registros de nomes e distribuição de números IP para Internet (endereços eletrônicos), passou a ser o órgão responsável pela gestão destas receitas. A seguir, são demonstradas as receitas e despesas relacionadas às atividades de registro (Figura 13).



Fonte: Nic.br (2007)

Figura 13 – Receitas provenientes do registro de domínios

Observa-se, na Figura 13, que os recursos captados no processo de atribuição de registros de domínios na Internet brasileira e seus rendimentos, passaram de cerca de R$ 5 milhões, para R$ 50 milhões, no período de 8 anos (1998-2006), indicando uma expansão de 900%.



Fonte: Nic.br (2007)

Figura 14 – Despesas relacionadas ao registro de domínios

As despesas, demonstradas na Figura 14, também evoluíram com a expansão das atividades de registro. Ficaram em torno de R$ 25 milhões no ano de 2006, um período atípico, pois foi o ano em que o Núcleo de Informação e Coordenação do ponto.br adquiriu sede própria, cujo valor ficou situado em aproximadamente R$ 10 milhões.

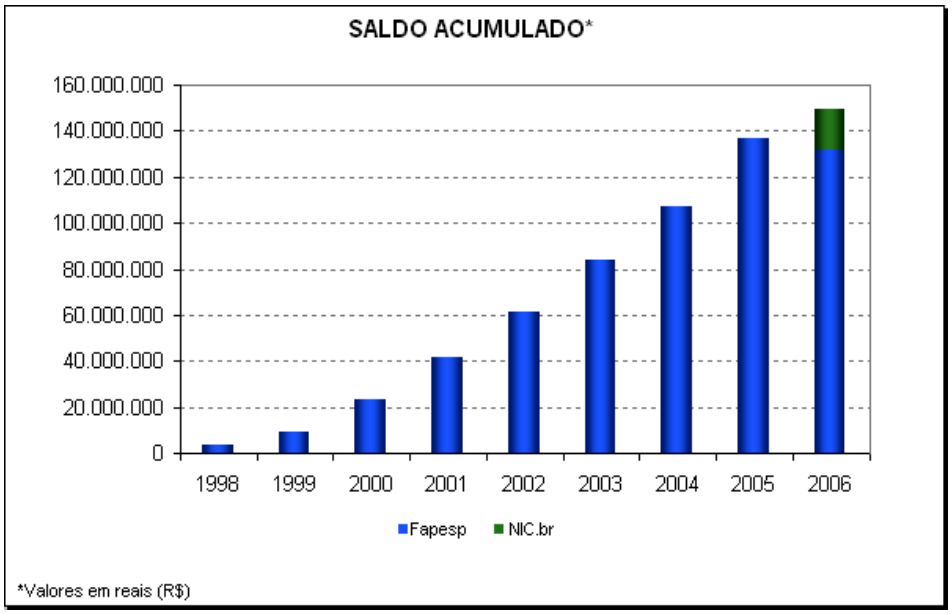
A análise ano a ano, de 1998 até 2006, excluída a aquisição deste imóvel que é, na realidade, um investimento, indica uma despesa anual da ordem de 30% do total de receitas.

Fonte: Nic.br (2007)

Figura 15 – Saldos apurados por exercício

Verifica-se, que o saldo no exercício, não apresenta crescimento do ano de 2003 para o ano de 2004, em razão da redução de valores efetivada a partir de janeiro de 2003, que eliminou o custo de registro de domínio e reduziu a sua manutenção anual em 25%.

Em 2006, o saldo no exercício apresenta-se negativo na coluna FAPESP, por ter a administração de recursos migrado para o Núcleo de Informação e Coordenação do ponto.br, conforme demonstrado na Figura 15.



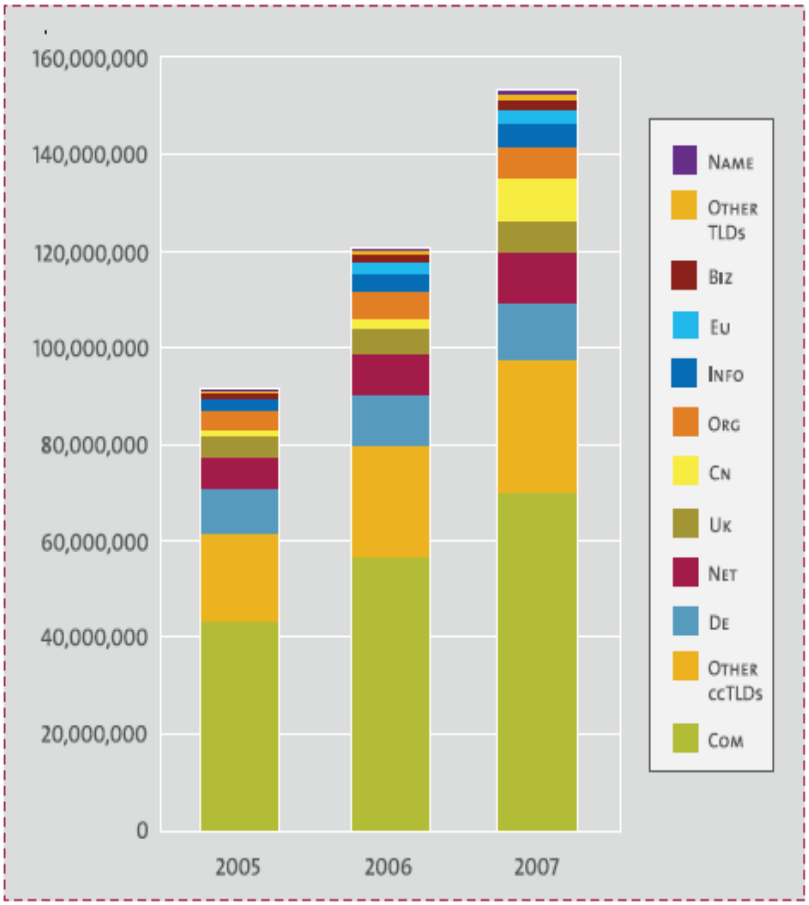
Fonte: Nic.br (2007)

Figura 16 – Saldo acumulado no período de nove anos

O saldo acumulado no período mostra recursos da ordem de R$ 150 milhões de reais, sendo que o valor administrado em conjunto pela FAPESP e Comitê Gestor são da ordem de R$ 132 milhões e de R$ 17,5 milhões, valor referente ao ano de 2006, quando o Nic.br passou a administrar o registro de domínios.

Os custos para registro de nomes de domínio são accessíveis aos usuários (proprietários de nomes de domínio) e são bloqueados apenas por falta de pagamento.

No entanto, o desconhecimento do processo é evidenciado pelo pequeno número de nomes de domínios registrados em território brasileiro (1.358.222 – ver figura 19), se compararmos com os indicadores de registro de domínios mundiais, apresentados na Figura 17.

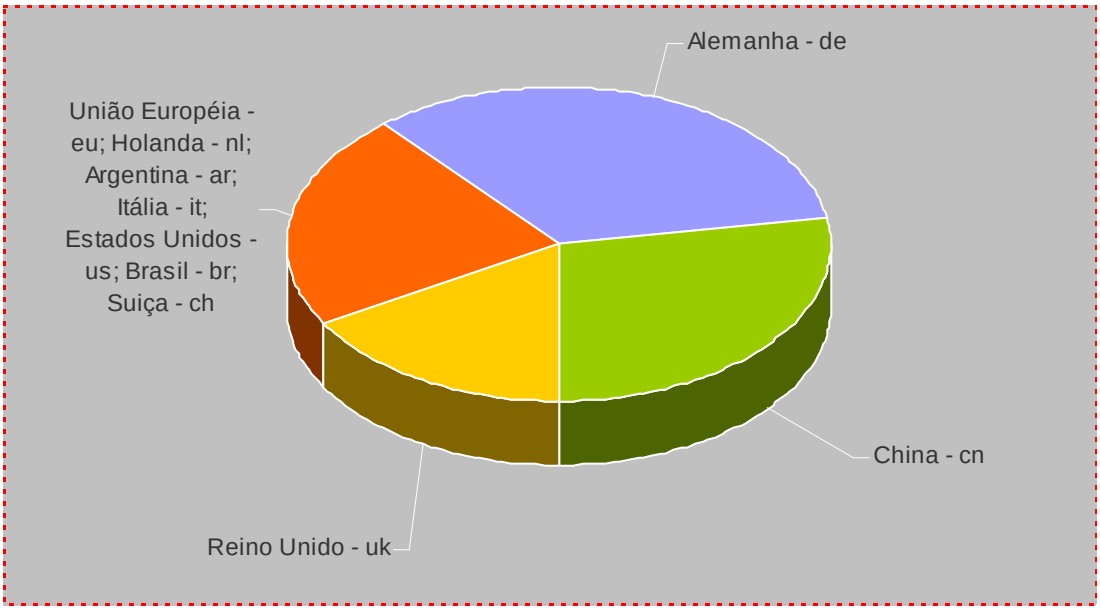


Fonte: VeriSign (2008, p. 2).

Figura 17 – Total de nomes de domínios registrados no mundo (2005-2007)

Os domínios destinados a organizações comerciais, representam o maior volume de registros, seguidos pelos domínios de países e provedores de rede.

O Brasil, embora não apresente um número de registros bastante expressivo, figura na lista de países que mais cresceram em registro de domínios específicos para países, e encontra-se, portanto, entre os dez países campeões neste quesito, conforme ilustra a Figura 18.



Fonte: adaptado de VeriSign (2008.

Figura 18 - Os dez maiores em registros de nomes de domínio de primeiro nível (ccTLDs) no mundo (jan./abr. 2007)

O crescimento de registro de nomes de domínio deve intensificar-se nos próximos anos, em razão do novo comportamento de compra adotado pelas próprias empresas: levantamento feito em 2007 pelo Comitê Gestor de Internet revelou que 64% das empresas realizam pelo menos uma parte de suas compras via *Web*. O estudo em questão teve como amostra 2,3 mil empresas com dez funcionários ou mais. As compras são feitas por *e-mail*[30] ou formulários disponibilizados pelos *sites*. Conforme Demi Getschko (REGISTRO.BR, 2008), esta evolução no comportamento de negócios via *Web*, segue os padrões internacionais.

Há produtos que, antes da compra, requerem a presença física do comprador, para que se observem suas condições *in loco*. Nestes casos, a Internet vem sendo utilizada para as pesquisas preliminares de preço, condições de pagamento, características do produto e empresa, entre outros fatores.

Os serviços públicos disponíveis nas páginas do governo eletrônico (federal, estadual e municipal) são acessados por 89% das empresas, como as consultas aos respectivos saldos de FGTS (Fundo de Garantia por Tempo de Serviço) e situações cadastrais e/ou fiscais.

[30] *E-mail:* ou correio eletrônico, é um serviço disponível na Internet que possibilita o envio e o recebimento de mensagens (UFPA, 2008).

No Brasil, o Registro.br disponibiliza categorias para registro de domínios destinados a atividades comerciais genéricas (que são os ponto com.br); domínios para pessoas jurídicas que querem especificar suas atividades (como por exemplo, as entidades de ensino superior, que utilizam edu.br) e para pessoas físicas profissionais liberais e outras atividades.

O Registro.br também atende às demandas de órgãos do Governo para ações específicas, como por exemplo, a criação de domínios para a utilização dos candidatos em suas campanhas eletrônicas, como ocorreu na campanha eleitoral de 2006, por solicitação do TSE (Tribunal Superior Eleitoral). Naquele evento, os candidatos poderiam solicitar o cadastro no registro.br., após obter a aprovação de sua candidatura junto ao TSE.

Naquela ocasião, após o registro, o candidato recebia um domínio, com o modelo <http://www.nomedocandidatonumerodocandidato.can.br>, pelo qual ficaria então responsável durante sua permanência na rede. Os custos de criação, hospedagem e manutenção dos *sites* seriam pagos pelo candidato, ficando os mesmos isentos apenas da taxa de registro junto ao Comitê Gestor. Estes domínios foram cancelados de forma automática após a realização do primeiro turno de eleições, exceto quando os candidatos foram qualificados a concorrer em segundo turno.

O processo de atribuição de registro de nomes e respectivos endereços eletrônicos é bastante dinâmico e vem se alterando constantemente, de forma a acompanhar a própria evolução das atividades econômicas e culturais na Internet.

Uma das permissões de registros mais recentes ocorreu em 16 de abril de 2008, quando o registro.br anunciou que pessoas físicas com CPF também podem obter o domínio com.br, anteriormente destinado somente a pessoas jurídicas que exercem atividades comerciais. A partir deste anúncio, a permissão começou a vigorar no mês de maio de 2008.

A Figura 19 apresenta o total de domínios utilizados e registrados no Brasil.

	DPN	Quantidade	%
Pessoas Físicas	BLOG.BR	2680	0.19
	FLOG.BR	188	0.01
	NOM.BR	2715	0.20
	SEC3.BR	17	0.00
	VLOG.BR	90	0.01
	WIKI.BR	301	0.02
		5887	**0.43**
Profissionais Liberais	ADM.BR	1655	0.12
	ADV.BR	9515	0.70
	ARQ.BR	2173	0.16
	ATO.BR	111	0.01
	BIO.BR	351	0.03
	BMD.BR	17	0.00
	CIM.BR	658	0.05
	CNG.BR	14	0.00
	CN.BR	1408	0.10
	ECN.BR	135	0.01
	ETI.BR	3158	0.23
	FND.BR	49	0.00
	FOT.BR	928	0.07
	FST.BR	138	0.01
	GGF.BR	21	0.00
	JOR.BR	548	0.04
	LEL.BR	103	0.01
	MAT.BR	148	0.01
	MED.BR	2815	0.21
	MUS.BR	1224	0.09
	NOT.BR	92	0.01
	NTR.BR	84	0.01
	ODO.BR	989	0.07
	PPG.BR	886	0.07
	PRO.BR	3103	0.23
	PSC.BR	629	0.05
	QSL.BR	71	0.01
	SLG.BR	21	0.00
	TRD.BR	133	0.01
	VET.BR	351	0.03
	ZLG.BR	3	0.00
		35342	**2.60**

	DPN	Quantidade	%
Pessoas Jurídicas	AGR.BR	472	0.03
	AM.BR	122	0.01
	ART.BR	3848	0.28
	COOP.BR	338	0.02
	ESP.BR	609	0.04
	ETC.BR	872	0.06
	FAR.BR	222	0.02
	FM.BR	230	0.02
	G12.BR	601	0.04
	GOV.BR	947	0.07
	IMB.BR	793	0.06
	IND.BR	7711	0.57
	INF.BR	3243	0.24
	JUS.BR	175	0.01
	MIL.BR	28	0.00
	NET.BR	1058	0.08
	ORG.BR	33597	2.47
	PSI.BR	238	0.02
	REC.BR	97	0.01
	SRV.BR	2751	0.20
	TMP.BR	44	0.00
	TUR.BR	3102	0.23
	TV.BR	254	0.02
		61352	**4.52**
Univer-sidades	BR	1196	0.09
	EDU.BR	1544	0.11
		2740	**0.20**
Gene-ricos	COM.BR	1252901	92.25
		1252901	**92.25**
	Total	**1358222**	**100.00**
	IDNA	**1366**	**0.10**
	DNSSEC	**238**	**0.02**

Fonte: Registro.br (2008)

Figura 19 - Domínios registrados no país de 01/01/1996 a 15/06/2008

Através deste quadro, percebemos que os domínios pertencentes a atividades comerciais, que desde 1996 são registrados apenas para pessoas

jurídicas, contam com cerca de 1,2 milhões de nomes, representando 92% do total. São seguidos por pessoas jurídicas com atividades específicas (61.352 – 4,52%), profissionais liberais (35.342 – 2,60%) e pessoas físicas (5.887 – 0,43%). As universidades representam apenas 0,2% do total, com 2.740 registros.

4.2 Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – cert.br

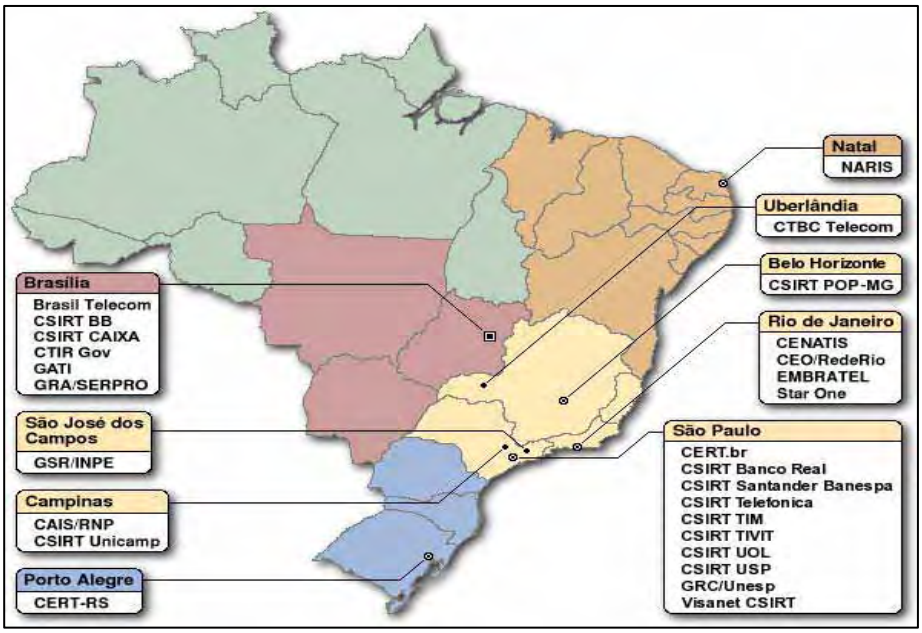
O núcleo CERT.Br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) apresenta como missão:

> (...) receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à Internet brasileira. Além do processo de resposta a incidentes em si, o CERT.br também atua através do trabalho de conscientização sobre os problemas de segurança, da correlação entre eventos na Internet brasileira e do auxílio ao estabelecimento de novos CSIRTs (Grupos de Segurança e Resposta a Incidentes) no Brasil (CERT.Br, 2008ª, *online*).

O CERT.br pretende centralizar as notificações a respeito dos incidentes de segurança, procurando respondê-los e acionar as partes envolvidas, sempre que necessário. O trabalho deste núcleo envolve a parceria com entidades, provedores de acesso e *backbones*[31], bem como apoiar investigações iniciadas pela Polícia Brasileira. Com relação à parte técnica, fornece suporte necessário para recuperar sistemas danificados por ataques de vírus. Oferece, ainda, treinamento na área de resposta a incidentes de segurança, em especial para instituições que estejam interessadas em formar seus próprios grupos de segurança e resposta a incidentes.

O Brasil conta hoje com 27 CSIRT´s, distribuídos em seis estados (Figura 20).

[31] Provedores de *backbone*: entidades que transportam tráfego agregado de seus clientes, detêm blocos de endereços IP por delegação do Comitê Gestor Internet Brasil e vendem conectividade para acesso à rede Internet (CGI, 2008, *on line*).



Fonte: CERT.br (2008a)

Figura 20 – Grupos de segurança e resposta a incidentes no Brasil

Este formato de organização demonstra como a segurança das instituições precisa ter estrutura própria de tratamento e resposta e não pode, assim, depender de um único órgão gestor, como é o CERT.Br.

Os prejuízos à segurança dos computadores serão bem maiores caso as grandes empresas e instituições não dispuserem de grupos próprios de resposta, uma vez que a capacidade de identificar rapidamente ataques de *vírus*[32]*, rootkits*[33] *e worms*[34] são determinantes para combatê-los e, muitas vezes, somente a aquisição de softwares de proteção poderão ser medidas insuficientes.

Quanto ao tamanho, estes grupos de segurança podem ser dimensionados de modo a atender a um continente, a um país, uma instituição ou prestar serviços para pequenas organizações, de forma terceirizada.

Os grupos de resposta podem receber diversas denominações, todas no mesmo padrão em língua inglesa, mesmo em países cuja língua oficial não seja o idioma inglês. Esta forma de denominação garante uma nomenclatura padrão, fator

[32] Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros arquivos e programas de computador.
[33] *Rootkit*: conjunto de programas que tem por finalidade esconder a presença de invasores nos computadores comprometidos.
[34] *Worm*: programa que também se propaga automaticamente como o vírus, no entanto, não necessita ser executado para se propagar (CGI, 2007a, p. 83-85).

importante, considerando a característica internacional da Internet, como se pode observar na Figura 21.

CSIRT	Computer Security Incident Response Team
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
IRC	Incident Response Center or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

Fonte: CERT.br (2008a)

Figura 21 - Nomenclaturas padrão - Grupos de resposta a incidentes na Internet

Estes grupos situam-se na estrutura organizacional das instituições de forma não padronizada, podendo estar ligados às áreas de tecnologia da informação, telecomunicações ou até mesmo auditoria. Atuam de forma pró-ativa e reativa, tratando os incidentes de segurança na seqüência: notificação do incidente, análise e resposta. As três etapas de tratamento, embora inter-relacionadas, demandam ações distintas (Figura 22):

Figura 22 – Três etapas de tratamento dos incidentes de segurança

Na recepção do incidente, é importante ter um único ponto de contato. Quanto à sua análise, é importante reconhecer o grau do incidente, para, uma vez

determinada sua gravidade, estabelecer ações necessárias para uma pronta resposta e erradicação.

Os custos de criação dos grupos de resposta, bem como sua estrutura organizacional, recursos humanos e instalações são de responsabilidade de cada instituição, não havendo recursos governamentais para financiá-los. O CERT.br. oferece um treinamento de 8 horas, destinado a apoiar a formação inicial destes grupos. Neste curso, são destacados os princípios fundamentais para a criação do grupo, especialmente relativas ao seu planejamento e implementação. O CERT.br também disponibiliza dois documentos essenciais para suporte à organização/funcionamento destes grupos:

> Forming an Incident Response Team: Um artigo examinando o papel que um grupo de resposta a incidentes pode ter na comunidade e quais as questões que devem ser consideradas durante a sua formação e depois do início das operações. Este artigo foi escrito por um membro do AusCERT (Australian Computer Emergency Response Team).
>
> Handbook for Computer Security Incident Reponse Teams: Um handbook que provê orientações a respeito de questões genéricas a serem consideradas quando se está formando ou operando um CSIRT. Em particular, ele ajuda a organização a definir e documentar a natureza e o escopo de um serviço de resposta a incidentes em computadores, que é o serviço principal de um CSIRT, bem como a criar as políticas e os procedimentos de um CSIRT. O handbook foi escrito por três destacados membros da comunidade de grupos de resposta a incidentes e tem o objetivo de auxiliar outras organizações a formar CSIRTs (CERT.BR, 2008a, *online*).

Existem ainda outros documentos de interesse para formação de grupos de resposta a incidentes na Internet, disponíveis no *site* do CERT.br. Além de todo este suporte documental, as instituições que desejam organizar grupos de segurança e resposta a incidentes, podem participar do FIRST.

O FIRST (*Forum of Incident Response and Security Teams*) é um fórum internacional, que ocorre anualmente, desde 1990, e reúne grupos de segurança acadêmicos, empresariais e governamentais. O décimo nono encontro mundial do FIRST ocorreu em Sevilha, na Espanha, em junho de 2007. O próximo encontro será realizado em Vancouver, Canadá.

Na análise do trabalho desenvolvido pelo CERT.br, percebe-se que as questões de segurança estão na esfera eminentemente técnica. Não há menções aos aspectos sociais envolvidos nas ações dos diversos grupos de segurança e

resposta a incidentes, exceto na conscientização dos usuários comuns, feito ainda de maneira incipiente através da Cartilha de Segurança e dos vídeos institucionais realizados pelo CERT.br.

A sociedade desconhece a existência dos grupos de resposta (denominados no Brasil como CSIRT´s). Isso pode dificultar que pequenas empresas se beneficiem dos serviços de segurança da informação, oferecidos tanto pelo CERT quanto pelos diversos CSIRT´s existentes no país.

4.3 Centro de Estudos sobre as Tecnologias da Informação e da Comunicação - cetic.br

Através de pesquisas de periodicidade anual, o Centro de Estudos sobre as Tecnologias da Informação e da Comunicação produz indicadores que são essenciais para que o Comitê Gestor possa medir a evolução das Tecnologias de Informação e Comunicação no país, possibilitando, assim, a análise das necessidades e demandas sociais na área tecnológica frente às ações e projetos que precisam ser empreendidos pelo Governo e iniciativa privada e ainda a comparação com a realidade de outros países neste contexto.

Em junho deste ano (2008), o Cetic.br divulgou os resultados da Pesquisa TIC (Tecnologias da Informação e Comunicação) Domicílios 2007 (BALBONI,2008), na qual verificou o acesso, uso do computador, uso da Internet, segurança da rede, o uso do *e-mail*, *spam*[35], utilização do governo eletrônico, comércio eletrônico, habilidades no uso das tecnologias da informação e comunicação, o acesso sem fio e a intenção e aquisição de equipamentos e serviços TIC's.

No mesmo volume, encontram-se também os resultados da TIC (Tecnologias da Informação e Comunicação) Empresas, que contém indicadores quantitativos sobre empresas e funcionários que utilizam computadores, uso da Internet, interação com instituições governamentais, segurança na Rede, comércio eletrônico via Internet e as habilidades no uso das das tecnologias da informação e comunicação.

A pesquisa foi realizada entre os meses de setembro e novembro de

[35] *Spam*: termo utilizado para se referir a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas (CGI, 2006b, p. 84).

2007, em todo o território urbano pelo CETIC e consistiu numa amostra de 17.000 domicílios, que entrevistou indivíduos de mais de 10 anos de idade. Amostras de domicílios e respondentes tiveram como base indicadores oficiais do PNAD (Pesquisa Nacional por Amostra de Domicílios) 2006 e do Censo IBGE (Instituto Brasileiro de Geografia e Estatística) 2000. O padrão metodológico utilizado seguiu os critérios definidos pela OCDE (Organização para a Cooperação e Desenvolvimento Econômico) e da Eurostat (Instituto de Estatísticas da Comissão Européia), permitindo, dessa maneira, a comparabilidade internacional.

A Tabela 6 indica o universo amostral da Pesquisa TIC Domicílios 2007 (BALBONI, 2008).

Tabela 6 – Estratos de Região

Região Brasileira	PNAD 2006				Internet		
	População	Domicílios	Amostra Principal	Erro amostral	Amostra extra	Total Usuários	Erro amostral
Norte	15.080.183	3.781.989	2.200	2,1%	332	2.532	2,0%
Centro-Oeste	13.313.377	3.976.706	1.500	2,6%	168	1.668	2,4%
Nordeste	51.713.072	13.818.092	5.800	1,3%	600	6.400	1,3%
Sudeste	79.753.141	24.577.689	4.400	1,5%	268	4.668	1,5%
Sul	27.368.019	8.564.286	3.100	1,8%	132	3.232	1,8%
Total	187.227.792	54.718.762	17.000	0,8%	1.500	18.500	0,7%

Fonte: Adaptada TIC Domicílios 2007 (BALBONI 2008, p. 70).

Os indicadores específicos sobre o uso da Internet revelaram o número de usuários em 2007, a participação por região do país, por faixa etária, gênero, grau de instrução e classe social. Além destes macro-indicadores, comentados anteriormente, a Pesquisa 2007 trouxe ainda outros números no módulo “Uso da Internet”: a frequência de uso, as atividades desenvolvidas na Internet, o local de acesso e as barreiras de uso.

4.3.1 Frequência de uso

A frequência da utilização da Internet cresce de acordo com a escolaridade e a renda. Para 53% desses usuários, a frequência na utilização da

rede é diária. Nos segmentos com menor renda e escolaridade (34% dos usuários), a freqüência de uso diminui para uma vez por semana. Os demais usuários responderam que sua freqüência de utilização da Internet é mensal.

4.3.2 Atividades desenvolvidas na Internet

A Internet, ao permitir a escolha da atividade a ser desenvolvida pelo usuário, em seu tempo livre, é uma mídia capaz de responder a diversas necessidades comunicativas dos internautas, conforme os resultados apresentados abaixo:

> Entre as principais atividades desenvolvidas na Internet em 2007 destacaram-se as ações relacionadas à comunicação, lazer e busca de informações *on-line*, que foram realizadas por quase 90% dos internautas brasileiros. No que diz respeito às atividades relacionadas à comunicação, a Internet foi usada principalmente na troca de e-mails (78%), na participação em sites de relacionamento como o Orkut (64%) e no envio de mensagens instantâneas (55%). A principal atividade de lazer realizada pelos internautas brasileiros é ler jornais e revistas (47%), seguida por "jogar ou fazer download de jogos" (43%) e "assistir filmes ou vídeos" utilizando sites como o You Tube (43%) (BALBONI, 2008, p.84).

Dessa maneira, seja pela troca de *e-mails*, que é o maior indicador no item comunicação, seguido pela participação no *Orkut* e no envio de mensagens instantâneas, especialmente pelo MSN *messenger* (programa da Microsoft que permite o encontro em tempo real entre os internautas), observa-se que a necessidade de socialização via rede é muito importante para os internautas brasileiros. Segundo Getschko, esta comunicação viabilizada pela rede derrubou alguns paradigmas que se tinha a este respeito no início do fenômeno Internet:

> *Se dizia o seguinte, na Internet nós vamos ter que aprender a falar inglês, e com isso vai ser, digamos uma ferramenta contra a manutenção de culturas locais e de idiossincrasias locais, de especificidades de cada país – isso, na minha opinião se mostrou totalmente errado – a Internet, ao contrário, ela privilegia e ela permite que pequenas comunidades possam se reforçar comunicando-se pela rede e com isso, não só se manterem vivas, como até se expandirem, então não é verdade que haverá uma capa única de cultura e ela será anglo-saxã, e cobrirá aí como*

> *um todo; na verdade, todas as culturas que existem e que acessam a rede, usam a rede, se beneficiam da rede "pra" poder até reforçar a própria existência, quer dizer, é um fato que é interessante.*

Além do estabelecimento de laços de amizade, as comunidades virtuais, como o *Orkut*, por exemplo, acabam por se constituir em um público potencial para ações de marketing via rede: "(...) O *Orkut* vem se tornando uma ferramenta de marketing muito utilizada hoje por ser um dos sites mais acessados. Muitas pessoas, candidatos políticos, e até mesmo empresas de nome estão aproveitando seus benefícios" (DOILE; FIABANE; AREU, 2007, p. 7).

A pesquisa apontou ainda as atividades de treinamento e educação com 64% de participação em 2006 e 73% em 2007. O item uso do *Internet Banking* (acesso às contas bancárias e movimentos financeiros via Internet) evoluiu de 17% no ano de 2006 para 18% no ano de 2007.

4.3.3 Local de acesso individual à Internet

Os brasileiros passaram a acessar a Internet predominantemente de locais de acesso pago:

> O ano de 2007 foi definitivo para impulsionar o crecimento do uso da Internet em centros públicos de acesso pago (lanhouses, Internet cafés, etc.), que se transformou no local predominante para o acesso à Internet no Brasil, com 49% das menções. (...) O uso da Internet nestes centros cresceu 19 pontos percentuais em relação ao ano passado, um aumento muito significativo, o que mostra o grande potencial da iniciativa privada para combater o problema da exclusão digital no país (BALBONI, 2008, p.84).

A inclusão digital por esta via, do acesso pago em local público, pode não propiciar uma das melhores alternativas de utilização da rede para os usuários, na visão de Getschko. Para ele, além da barreira imposta pela necessidade de infra-estrutura de qualidade para Internet no país, para que se possa chegar aos mais distantes pontos do território nacional, tem-se a segunda barreira, que é a falta do computador no domicílio:

> *(...) Uma vez estabelecida a infra-estrutura, nós temos uma segunda barreira a vencer, que é a barreira do computador, quer dizer, uma experiência completa à Internet, uma experiência completa da rede, envolve você ter disponibilidade do equipamento a hora que você precisa, e não, a hora que você pode usar, então você precisa ler seu e-mail, ler o noticiário, se aculturar do que "tá" acontecendo, e depois, então, também, interagir. Na verdade a rede, na minha opinião, também passa a fazer parte do dia-a-dia das pessoas dessa forma: em primeiro lugar uma forma de você ganhar informação, se instruir, ganhar acesso ao que há no mundo, e numa segunda fase, você participar, gerando sua própria informação.*

Quem acessa a Internet do domicílio situa-se nas faixas da população com maiores renda mensal, grau de instrução e idade. Pessoas jovens e com menor renda são o público que freqüenta os locais públicos de acesso pago.

4.3.4 Barreiras de uso

A pesquisa apontou os principais motivos pelos quais os brasileiros não estão acessando a Internet, por região do país. No total Brasil, a maior barreira de uso é a falta de habilidade com o computador e com a própria Internet (55%) e o menor percentual de dificuldade foi indicado por falta de local de acesso (18%). A região na qual os usuários relatam a falta de habilidade com os computadores e a Internet como sendo sua maior dificuldade é a região Norte, com 62% neste indicador, enquanto na região Sul, a falta de habilidade foi a menor barreira, com 41%.

Neste sentido, a principal barreira apontada pela Pesquisa TIC Domicílios 2007 (BALBONI, 2008), ou seja, a falta de habilidades com os computadores e com a Internet, demonstra que a inclusão digital não é apenas uma questão técnica. Na verdade, aponta que os fatores educacionais são de primordial importância na aquisição deste conhecimento e a partir daí, o que fazer com ele, pois participar de comunidades virtuais, jogar e assistir a vídeos pela Internet não significam que as pessoas estão se apropriando de maior conhecimento. O fato de a rede permitir que

as pessoas produzam conteúdos e ali as publiquem, torna muito grande e nem sempre positiva a quantidade de informações disponíveis. Na opinião de Getschko,

> *(...) é essa geração de conteúdo na mão do indivíduo, quer dizer hoje todos podem gerar conteúdo e colocar na rede e você vê isso pela proliferação de blogs, de wicks, de sítes em que existe informação, evidente que com isso a qualidade é muito variável, existem informações corretas, existem informações falsas, existem calúnias, existem difamações, existem todo tipo de coisas boas e ruins.*

Durante a Reunião do Fórum de Governança da Internet, a questão das habilidades digitais foi debatida entre os participantes, no Painel dedicado à diversidade na Internet, cujos trabalhos foram presididos pelo Ministro da Cultura, Gilberto Gil. Na discussão, os participantes concordaram com a premissa de que a partilha digital entre os povos é essencialmente uma partilha de conhecimento. O entendimento geral é de que a Internet na língua local pode ajudar a transformar a sociedade, sendo uma das alternativas facilitadoras para tal objetivo, a incorporação da cultura da Internet à cultura local.

O que se pode concluir a princípio é um certo grau de dificuldade nesta transposição para a realidade prática desta “fusão” da Internet com a cultura local, embora se possam localizar comunidades étnicas, religiosas e políticas organizadas através de *sites* na rede.

4.4 Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações – ceptro.br

Composto por duas unidades, o Ponto de Troca de Tráfego (PTT.br) e o *Network Time Protocol* (NTP.br), o Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações é o núcleo gestor responsável dentro da estrutura do Comitê Gestor, por administrar e inovar em todas as atividades relacionadas à tecnologia de informações e comunicações (CEPTRO, 2008).

4.4.1 Ponto de Troca de Tráfego – Ptt.br

Núcleo eminentemente técnico, responsável por viabilizar a infra-estrutura necessária à interconexão direta entre as redes das áreas metropolitanas brasileiras, tem como objetivo promover uma ótima conexão para estas regiões estratégicas, racionalizando custos e resolvendo questões rapidamente, facilitadas por sua gerência centralizada e próxima às áreas em questão. Características como neutralidade (independência dos provedores comerciais), qualidade (trocas de tráfego eficientes), baixo custo de alternativas, com alta disponibilidade e matriz de troca de tráfego regional única são necessárias para a implantação de um ponto de troca de tráfego.

As regiões metropolitanas brasileiras que apresentam características que as credenciam a possuir um ponto de troca de tráfego são: Belo Horizonte, Brasília, Curitiba, Florianópolis, Porto Alegre, Rio de Janeiro, Salvador e São Paulo.

Em São Paulo, algumas das organizações que participam do PTT.br, área São Paulo são: RNT (Rede Nacional de Ensino e Pesquisa), At&T (*American Telephone and Telegraph*), Oi, Brasil Telecom, Telefônica, SERPRO (Serviço de Processamento de Dados), Terra, Uol, *Yahoo*, entre outras.

4.4.2 *Network Time Protocol* – NTP.br

Através da estrutura do NTP.br, todos os servidores de Internet no Brasil podem ser sincronizados com a Hora Legal Brasileira, estabelecida pelo Observatório Nacional, órgão vinculado ao Ministério da Ciência e Tecnologia. A Hora Legal Brasileira é um projeto do Observatório Nacional, que objetiva gerá-la, conservá-la e transmiti-la por sinais horários e freqüência padrão para todo o território nacional através de radiofreqüência. Para a interconexão dos computadores à rede, é fundamental que a hora esteja sincronizada com o horário do país e o NTP é o órgão habilitado para isso.

O sincronismo da Hora Legal Brasileira é fornecido pelo Observatório Nacional ao Núcleo de Informação e Coordenação do Comitê Gestor, que, por sua vez, disponibiliza os equipamentos necessários a este processo, o qual ocorre sem

ônus para as partes envolvidas, tornando o processo de sincronismo da Hora Legal Brasileira seguro e confiável.

Problemas diversos podem ocorrer com computadores não sincronizados à hora legal. Os prejuízos mais comuns são aqueles relacionados a aplicativos (programas ou *softwares*) afetados pelo tempo, como os sistemas de distribuição de conteúdo, de arquivo, agendadores de eventos, técnicas de criptografia, protocolos de comunicação e aplicações de tempo real, sistemas transacionais e banco de dados distribuídos. Cada um destes aplicativos exige sincronias específicas de tempo:

> Para algumas aplicações, exatidão da ordem de segundos pode ser suficiente. Para outras, é necessário manter os relógios com diferenças na ordem dos milisegundos entre si e em relação à referência legal. (...) O NTP (Network Time Protocol), se corretamente utilizado, é capaz de garantir as propriedades necessárias ao relógio do computador para o bom funcionamento das aplicações (NTP.BR, 2008, *online*).

Os países e seus órgãos disseminadores de tempo e freqüência participam do Tempo Universal Coordenado (TUC) ou *Coordinated Universal Time* (UTC), rastreado ao *Bureau International des Poids et Mesures* (BIPM), na França, do qual também faz parte o Observatório Nacional brasileiro. O UTC é a base legal para o tempo em todo o mundo e é disciplinado pelo período solar e acompanha também o tempo atômico, que é uma leitura de cerca de 260 relógios atômicos no mundo todo. O tempo atômico representa a mensuração de tempo mais próxima de um relógio imaginário perfeito. A cada 18 meses, torna-se necessário um ajuste na UTC (acrescentando-se ou removendo-se um segundo) de forma a equipará-lo ao período solar. Através destes ajustes, objetiva-se garantir que o Sol esteja exatamente às 12 h sobre o meridiano de Greenwich.

Os países adotam ainda o tempo local, para adaptar o relógio de suas regiões à UTC. No Brasil, a hora oficial é a hora da capital de Brasília, cujo Tempo Universal Legal é UTC-3, ou seja, tempo universal coordenado menos três horas. Também são adotados no país quatro fusos horários diferentes, que são utilizados em função da região e do horário de verão, conforme Figura 23.

Diferença em relação ao UTC	Sem horário de Verão	No horário de Verão
UTC - 2	Ilhas de Fernando de Noronha, Trindade, Martin Vaz, Penedos de São Pedro e São Paulo e o Atol das Rocas.	Ilhas de Fernando de Noronha, Trindade, Martin Vaz, Penedos de São Pedro e São Paulo e o Atol das Rocas. Estados da região Sudeste e Sul, Goiás e o Distrito Federal (hora oficial do Br.).
UTC - 3	Estados da região Nordeste, Sudeste, Sul, além do Distrito Federal (hora oficial do Brasil), Goiás, Tocantins, Amapá e a porção oriental ou leste do estado do Pará.	Estados da região Nordeste, Tocantins, Amapá e a porção oriental ou leste do estado do Pará, Mato Grosso e Mato Grosso do Sul.
UTC - 4	Estados de Roraima, Rondônia, Mato Grosso, Mato Grosso do Sul, a porção oeste do estado do Pará e a maior parte do estado do Amazonas.	Estados de Roraima, Rondônia, a porção oeste do estado do Pará e a maior parte do estado do Amazonas.
UTC - 5	Porção oeste do Amazonas e todo o estado do Acre.	Porção oeste do Amazonas e todo o estado do Acre.

Fonte: NTP (2008)

Figura 23 – Regiões brasileiras e tempo universal coordenado

Durante o horário de verão, cada localidade passa a ter uma nova correção em relação ao UTC, devido ao acréscimo de uma hora ao tempo local.

O *site* do *Network Time Protocol* possui um serviço adicional de apoio aos internautas que desejem sincronizar os relógios de seus computadores com a Hora Legal Brasileira.

5 CONSIDERAÇÕES FINAIS

O estudo apresentado analisou a Internet no aspecto gestão da comunicação, evidenciando o histórico deste veículo e sua trajetória tecnológica, trajetória esta, que aglutinou e incorporou dimensões da vida social contemporânea, tal qual faz um rio caudaloso, ao transbordar e arrastar de suas margens, as terras, arbustos, árvores e tudo o mais que esteja a seu alcance, especialmente quando extravasa com as chuvas.

A Internet não pára de se transformar, portanto, este estudo e outros que forem feitos a seu respeito não serão conclusivos. Estarão na condição de abertos, inacabados, incompletos, dada a característica *mutatis mutandis* desta *dona mobile*.

Assim mesmo, a contribuição de tais estudos é fundamental, ao abrir caminhos, levantar questões, provocar reflexões, que é da própria natureza da academia. Neste sentido, também situa-se esta pesquisa, que em seus resultados evidencia a importância de se pensar como a gestão da Internet é capaz de interferir positiva ou negativamente no acesso de milhões de pessoas no mundo.

Conclui-se, que a gestão internacional realizada pela ICANN mostra-se eficiente e fundamental no que diz respeito ao estabelecimento de padrões técnicos para toda a rede, às parcerias realizadas com outras entidades para viabilizar seu funcionamento e ainda à preocupação que começa a demonstrar com os efeitos sociais e políticos da disseminação da Internet em todo o mundo.

No Brasil, o Comitê Gestor vem desempenhando suas atribuições no tocante à gestão da rede brasileira nos padrões estabelecidos pela ICANN e procurando observar os aspectos da realidade do país. Considera-se que esta entidade vem se revelando uma instância importante na coordenação técnica e na construção de uma referência nacional para Internet no Brasil e internacional do país no exterior.

Tecnicamente, o trabalho de gestão realizado pelo CGI.br, não deixa margem para críticas importantes. Há algumas discordâncias com relação às normas estabelecidas pelo Comitê Gestor para registro de domínios por parte de alguns grupos empresariais, que se ressentem de não poder comercializar domínios, o que contraria a finalidade do núcleo de Registro, que fixa valores baseados em

critérios técnicos e é a única entidade que está habilitada para isto no Brasil. Mas até mesmo estas críticas perderão a razão de ser. A nova regra que amplia os domínios *Web* já foi aprovada pela ICANN e deverá entrar em vigor em 2009, segundo informa a *Associated Press* (2008, p. 8). De acordo com essa nova regra, entidades e empresas poderão possuir mais de um domínio de Internet. A expectativa é que apareçam centenas de novos endereços a co-existir com os tradicionais ponto com e ponto org.

Com respeito à gestão política da Internet, o Comitê Gestor apresenta debilidades, pois no contexto brasileiro a política pública não propicia a atuação desta entidade como força integradora do universo digital no Brasil. A falta de autonomia do Comitê Gestor para assumir a liderança do processo de inclusão digital no país também diminui seu poder de gestão.

O Governo Brasileiro não está paralisado na questão digital, uma vez que possui algumas iniciativas na área de inclusão – projetos com características específicas e direcionados a alguns segmentos da sociedade. Alguns destes projetos incluem programas como o “Computadores para Inclusão”, que recondiciona microcomputadores e os disponibiliza a oficinas profissionalizantes e o TIN (Telecentros de Informação e Negócios), destinado a treinamento presencial e à distância, de micro e pequenas empresas que desejam preparar seus funcionários no manejo das TIC’s (Tecnologias de Informação e Comunicação). O Ministério da Ciência e Tecnologia coordena o “Programa 1008 – Inclusão Digital”, cujo “(...) objetivo é promover o acesso às tecnologias de informação e comunicação e ao acervo de informações e de conhecimentos, contribuindo para inclusão social dos cidadãos brasileiros” (BRASIL, 2006). O Ministério da Cultura desenvolveu o “Cultura Digital”, que “(...) permite a implantação de equipamentos e formação de agentes locais para produção e intercâmbio de vídeo, áudio, fotografia e multimídia digital com uso de software livre e conexão à Internet” (BRASIL, 2008a).

Todos esses programas parecem se constituir em paliativos para suprir esta fragilidade de uma política pública que possa funcionar como eixo norteador para a convergência das mídias, que acabam por se tornar alvo de programas e projetos de diversos ministérios, interessados em promover ações de suas pastas para cumprir uma agenda digital.

Conclui-se, ao mesmo tempo em que se responde à primeira das questões propostas (vide p. 20), **que a governança eletrônica nos padrões atuais**

não é a mais adequada para a expansão da rede brasileira com qualidade. O Comitê Gestor da Internet no Brasil, ao realizar a gestão da Internet nos padrões americanos fixados pela ICANN, não consegue ainda adaptá-lo à realidade brasileira, marcada pela exclusão digital e por medidas governamentais isoladas para saná-la. Para resolver este problema de gestão, seria necessária uma reformulação no papel do Comitê Gestor, conferindo-lhe autoridade para gerir de fato a Internet brasileira em todas as suas dimensões.

As tecnologias aplicáveis para a Internet desafiam previsões conservadoras e novas descobertas científicas na área de computação provam que as inovações possíveis são, de fato, imprevisíveis e imponderáveis. Na área de segurança da informação, por exemplo, pesquisadores da Universidade de Princeton, nos Estados Unidos, revelaram a descoberta de um método capaz de captar dados criptografados guardados nos discos rígidos de computadores, provando, desta maneira, a vulnerabilidade dos softwares criptográficos, utilizados principalmente para salvaguardar informações sigilosas de agências governamentais e empresas. "(...) A técnica, que poderia solapar os softwares de segurança que protegem dados importantes em computadores, é bastante simples: basta resfriar o chip de memória do computador com uma rajada de ar frio de um spray removedor de poeira" (MARKOFF, 2008, p. 15).

Esta descoberta poderá, eventualmente, ser desenvolvida de tal maneira que possa ser comercializada como uma solução para os internautas que desejem obter proteção adicional para seus dados pessoais contra ações de invasão de privacidade perpetradas por autoridades públicas.

Tornar disponível o conhecimento em domínio público e permitir a apropriação da tecnologia da Internet através da *Web 2.0*[36] são algumas transformações culturais já em curso e que, no futuro, tendem a se intensificar. Para Demi Getschko, o que irá importar no futuro, serão os serviços possibilitados pela Internet:

> *(...) nesses serviços é que nós faremos as transações e compraremos coisas e trocaremos informações e iremos ao banco e faremos tudo o mais, e com as novas ferramentas 2.0 e as demais, tudo isso se mistura de tal forma que no meu próprio*

[36] *Sites* de networking social, ferramentas de comunicação, *wikis* (artigos eletrônicos editáveis) e etiquetagem eletrônica (*tags*), baseados na colaboração (SPYER, 2007, p. 17).

> *site, ou no meu próprio blog, eu tenho o mapa da minha cidade, que é baseado num site que "tá" lá fora, no serviço de outra instituição e também tem um acesso ao banco que também não é do meu site, em suma: a Web 2.0 permitirá que todas essas comunidades se interliguem de forma indistinguível e ficará difícil até saber o que faz parte da minha estrutura e o que tá fora dela.*

As modificações tecnológicas na Internet, que já influenciam a vida cultural de pessoas e comunidades, estão em estudo e novas aplicações permitirão, por exemplo, um acesso maior ao conteúdo existente hoje neste ambiente virtual, graças ao desenvolvimento de uma nova linguagem que possibilitará a indexação de informações que hoje as limitadas linguagens de busca atuais não conseguem exibir. Esta nova linguagem faz parte do projeto IEML (*Information Economy Meta Language*), coordenado pelo teórico e filósofo Pierre Lévy (STRECKER, 2007, p.3).

A ampliação do acesso e conseqüentemente de informações disponíveis na rede, podem não se traduzir em um real aumento das habilidades para trabalhar os conteúdos de maneira a ampliar o capital cultural dos indivíduos. O estudo de Ian Rowlands, pesquisador da *University College* de Londres, mostra que o uso da Internet tem se limitado a coleta de informações superficiais que estejam dispostas nas páginas mais citadas da Internet, pouco importando se estas provêm de um *site* acadêmico ou de um *blog* de alguém que posta suas opiniões sobre determinado tema, conforme informa Murta (2008, p. 16).

Portanto, a resposta à segunda questão sobre que tecnologias esperam os novos usuários de rede, é de que inúmeras possibilidades estão colocadas; pessoas no mundo inteiro trabalham nisto. E as transformações poderão se refletir no corpo humano. Conforme Tavares:

> *Ah, obrigatoriamente o corpo humano mudará, em função da Internet. Imagino o seguinte. Eu não imagino que uma criança, dentro de duas ou três gerações escreva manualmente, ela vai teclar. Então, a parte do cérebro que ela utilizava para o desenvolvimento da escrita vai ser modificada, vai ser diferente, o condicionamento vai ser diferente. E da mesma forma, o tipo da consciência. Por quê? Porque o que ele precisava desenvolver em termos lógicos, passa a ter ferramentas que fazem isso. Ele não precisa saber que 2 + 2 são 4. Coloca 2 asterisco 2, ele sabe que é 4. Então, vai haver*

> *efetivamente uma liberalização de espaço de memória que nós hoje utilizamos pra fazer isso, e com certeza, isso propiciará um crescimento real.*

Enquanto a cultura se modifica, em função de novos ambientes virtuais e novas tecnologias de informática, a infra-estrutura para que o aparato da rede funcione também evolui. Do acesso discado passou-se ao acesso via banda larga com fio de cobre, ambos estruturados sobre o cabeamento de telefonia existente; a passagem do acesso banda larga com fio de cobre para acesso via fibra óptica é questão de investimento e as empresas dedicadas a este negócio têm realizado os aportes necessários para que isso aconteça. Assim, a conexão por fibra óptica, que confere maior velocidade ao tráfego de dados e informações via Internet, é realidade em algumas grandes cidades brasileiras, como São Paulo, por exemplo. A este respeito Getschko considera:

> *Eu acho que o papel fundamental aí de Governo, do Comitê Gestor e outros aí, é estimular a penetração da infra-estrutura "pra" que a rede possa ser accessível de todos os pontos do país. O nosso país é gigantesco, nós temos pontos em que a infra-estrutura de telecomunicações ainda é extremamente precária e à vezes nem existe. Um bom acesso à rede exige estruturas de superfície; satélite nunca é uma boa alternativa, porque o satélite tem um atraso grande, então, o ideal seria que tivéssemos uma estrutura em cima de fibra óptica .*

Quanto às tecnologias sem fio, a expectativa é a de que evoluam e superem as dificuldades hoje existentes, que estão basicamente relacionadas ao desenvolvimento de novas soluções que superem os problemas de conexão a menores custos. As características do acesso sem fio são descritas por Gouveia (2006, *online*):

> O acesso à Internet em banda larga sem fio ocorre por meio de ondas de rádio, que podem ser enviadas pelos sistemas WiFi (Fidelidade Sem Fio), WiMax (Interoperabilidade Mundial para Acesso de Microondas) e WiMesh (Rede em Malha Sem Fio). A tecnologia **WiFi** consiste na emissão de sinais de rede para serem captados por usuários com equipamentos apropriados. Esse tipo de conexão trabalha com radiofreqüências de 2,4Ghz (também utilizadas em telefones sem fio e fornos microondas), atinge a velocidade de 11Mbps e alcança até 100m a partir da fonte emissora. Portanto, é um

> sistema geralmente usado em ambientes internos. Desenvolvido por um consórcio mundial e certificado pelo IEEE (Institute of Electrical and Electronicas Engeneers), o padrão de transmissão **WiMax** difere do WiFi principalmente porque pode alcançar distâncias e velocidades muito maiores, com limites de 50 km e 75Mbps, respectivamente. Assim, o WiMax pode cobrir localidades de grandes dimensões, como as cidades. Estão disponíveis no Brasil para a transmissão WiMax as freqüências de 2,5Ghz, 3,5Ghz, 10,5Ghz (que necessitam de autorização da Anatel) e 5,8Ghz (livre). Quanto às redes Mesh, elas podem utilizar os sistemas sem fio WiFi/WiMax ou cabos, para conectar os usuários. O **WiMesh** é uma rede composta por várias antenas com capacidade de cobertura menor que o WiMax e maior que o WiFi. As antenas ficam mais próximas umas das outras e tornam a transmissão mais densa e segura, com velocidades de 54 Mbps e alcance de até 400 metros.

Os projetos Cidades Digitais, que já são realidade no Brasil, são baseados na conexão via rádio. Em Tiradentes (MG), uma das tecnologias via rádio mais avançadas, a *WiMesh*, foi implantada em um telecentro e quatro escolas, que oferecem Internet gratuita e de qualidade, cujo acesso é sem fio. Esta iniciativa foi patrocinada pelo Ministério das Comunicações em conjunto com a empresa Cisco (especializada em hardware, software e serviços para Internet). Sud Menucci, cidade do interior de São Paulo, possui a tecnologia sem fio *WiFi,* disponível a toda a população da cidade, mediante a aquisição do *Kit* necessário para a recepção do sinal, cujo custo estimado está em torno de dois salários mínimos. Assim, a resposta à terceira questão: **que conexões teremos disponíveis**, permitem dizer que novos tipos de conexão poderão influenciar no aumento expressivo do número de usuários. “Em 2009, os projetos de WiMax e redes Wi-Fi chegarão a mais de 500 milhões de pessoas em todo o mundo” (BARBOSA, 2005, p. 81).

A segurança do acesso sem fio à Internet é menor nos padrões atuais de conexão. A respeito deste tipo de conexão, Tavares considera que ele propicia uma zona cinzenta, pois a rede *Wireless*, mesmo com a proteção da senha de acesso, permite sua burla por pessoas com habilitação técnica para isso. E assim, o caminho pode ser aberto para os delitos cibernéticos. Neste sentido, conclui-se, para responder à quarta questão: **se é preciso investir em segurança na Internet,** que tais investimentos são necessários, embora as críticas que ponderam que os controles ferem a liberdade na rede tenham seus fundamentos. Mas as práticas de racismo e pedofilia na rede, as fraudes bancárias, roubos de informações sigilosas entre outros cibercrimes vêm crescendo e com isso, os investimentos no desenvolvimento de novas tecnologias de controle, além dos tipos citados neste

estudo (vide p. 56), deverão se intensificar nos próximos anos e as futuras gerações poderão ter que se identificar a todo o momento. Este cenário é antecipado por Tavares:

> *Se você vai usar o seu celular, você deixará de ter um CPF, um RG, um número de título de eleitor e no seu celular, você terá um número IP e você será um número IP. Você será Débora ou 201 ponto e quando você chegar com o celular ou qualquer outra ferramenta que ainda venha a surgir perto de uma caixa de banco, perto de uma urna eletrônica de uma votação, perto de qualquer portaria de prédio, você não precisa nem se identificar porque já tem um sensor que leu que você "ta"passando ali, "tá". Enfim, essa é a evolução e esse obrigatoriamente será o futuro. Pode-se chamar esse de futuro da Internet? Não é só a Internet, é a tecnologia em geral. A Internet é mola mestra pra esse desenvolvimento.*

De acordo com tal visão, os cenários tecnológicos que permearão o cotidiano das populações urbanas terão aparatos de identificação que extrapolarão os ambientes virtuais. Na Internet, por onde trafegarão milhões de usuários, incluindo um número crescente de crianças, há indicativos de que os cuidados com a segurança na comunicação deverão também evoluir juntamente com as tecnologias.

Portanto, a resposta à última questão (vide p. 20) conclui que é fundamental a **conscientização dos usuários a respeito das boas práticas na rede mundial de computadores**. As melhores maneiras para alcançar as consciências a este respeito, terão que ser desenvolvidas pelos diversos segmentos da sociedade, interessados na partilha de conhecimento digital. Para Tavares, a Internet oferece riscos, porém o caminho para bem utilizá-la é a educação:

> *E nesse caso, fica muito claro a Internet, ela é, protege de certa forma o anonimato, algumas pessoas, de formação, lamentavelmente baixa e, portanto, permite que aconteça esse tipo de coisa. Por isso, é preciso desenvolver as ferramentas de filtro de proteção para evitar que isso cresça, "pra" se fazer a correção do rumo e a boa utilização de uma mídia como a Internet. (...) Criar novas leis não é, nunca foi solução. Se fosse solução criar novas leis, as cadeias não estariam cheias (...) Temos é que educar. É importante que, o mais rapidamente possível, tudo isso esteja nas escolas, desde o nível mais*

> *elementar, mais básico, sem esquecer que não é apenas, não pode ser apenas uma promessa política de que vamos levar a Internet até as escolas; é preciso pensar que há necessidade de capacitar, e bem, os monitores, os professores, aqueles que vão estar ensinando a utilizar a Internet, para que de uma forma condicionadora, se faça um bom curso de Internet desde criança. Se nós permitirmos – o Brasil infelizmente tem um histórico, um vício, de não educar e não se preocupar em investir bastante em educação, de tal forma que o resultado "ta" aí, nos jornais, no dia-a-dia.*

A educação, cuja função principal é manter a coesão social ao mesmo tempo em que transforma indivíduos em sujeitos é, de fato, importante para a apropriação dos conhecimentos encontrados na Internet. Mas não é condição excludente para o acesso e, nesse sentido, a Internet é extremamente democrática.

Os problemas para os quais buscou-se resposta na pesquisa – ou seja, [a)] como administrar a comunicação mediada pela rede conciliando a liberdade que a caracterizou desde o início de seu desenvolvimento, com os controles que vêm se tornando necessários, na medida em que aumentam os incidentes que ameaçam, em graus e circunstâncias distintas, a segurança dos internautas; e, [b)] é possível que o atual modelo de gestão da Internet, a governança eletrônica, preserve a confidencialidade, a integridade, a ética e a disponibilidade da informação, sem ferir os princípios de liberdade permitidos pela rede mundial de computadores? – podem ser finalmente respondidos, após análises das estruturas de gestão da comunicação da Internet.

Os problemas apontados pela pesquisa não encontraram evidências no sentido de que é possível manter o atual modelo de gestão da Internet a médio e longo prazos. Os controles irão prevalecer sobre a liberdade, possibilitadas pelas tecnologias específicas.

Conclui-se que a Internet irá se transformar continuamente e sua essencialidade como veículo mediador de todas as tecnologias de comunicação estará fundamentada. Em outras palavras, a vida social estará irremediavelmente associada à Internet. E a comunicação, mediada pela rede mundial de computadores, contribui assim, definitivamente para a entrada da humanidade em outro estágio da história humana, a ser descoberto pelas futuras gerações.

Aponta-se, finalmente, que a comunidade acadêmica da área de comunicação poderá concorrer, de maneira significativa, para o aprimoramento da gestão e da expansão da Internet com qualidade e segurança.

REFERÊNCIAS

A SAGRAÇÃO da web. Pai da Internet, Vinton Cerf diz que celulares ultrapassarão computadores como meio de acesso e prevê um novo conceito para definir a rede. **Folha de São Paulo**, São Paulo, 15 jun. 2008. Suplemento Mais. Caderno Tecnologia, p. 4.

ANATEL. **Base de celulares ativos no Brasil.** 2008. Disponível em: <http://www.anatel.gov.br/Portal/exibirPortalInternet.do#>. Acesso em: 15 jan. 2008.

ASACP. Association of Sites Advocating Child Protection. About ASACP. **Statistics.** 2008. Disponível em: <http://www.asacp.org/page.php?content=statistics& PHPSESSID=14e389c7d4ef5fc9f4163bbc390b3f86>. Acesso em: 02 jan. 2008.

ASSOCIATED PRESS. Regra de domínio na Internet é ampliada. **Folha de São Paulo**, São Paulo, 27 jun. 2008. Folha Dinheiro, Caderno B, p.8.

AZEREDO, E. **Parecer sobre o projeto de lei da câmara nº. 89, de 2003, e Projetos de Lei do Senado nº. 137, de 2000, e nº. 76, de 2000***,* Brasília: Senado Federal, 2007. Disponível em: <http://webthes.senado.gov.br/sil/Comissoes/ Permanentes/CCT/Pareceres/PLC2007121289.rtf. Acesso em: 05 fev. 2008.

BALBONI, M. (Coord.). **Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil:** TIC domicílios e TIC empresas 2006. São Paulo: Comitê Gestor da Internet no Brasil, 2007.

_____. (Coord.). **Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil:** TIC domicílios e TIC empresas 2007. São Paulo: Comitê Gestor da Internet no Brasil, 2008.

BARBOSA, A. **Cuidado, a Internet está viva!** São Paulo: Terceiro Nome, 2005.

BONADIO, L. Carla mentiu sobre local de telefonema para Ubiratan, diz Promotor. **G1.** Globo.com. 25 abr. 2007. Disponível em: <http://g1.globo.com/ Noticias/SaoPaulo/0,, MUL27063-5605,00.html>. Acesso em: 10 jan. 2008.

BRASIL. Lei 8081, de 21 de setembro de 1990. Estabelece os crimes e as penas aplicáveis aos atos discriminatórios ou de preconceito de raça, cor, religião, etnia ou procedência nacional, praticados pelos meios de comunicação ou por publicação de qualquer natureza. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 24 set. 1990. Disponível em: <http://www6.senado.gov.br/sicon/ ListaReferencias.action?codigoBase=2&codigoDocumento=134249>. Acesso em: 5 fev. 2008.

_____. Congresso Nacional. Projeto de Lei Nº 84 DE 1999. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Autor: Deputado Federal Luiz Piauhylino, PDT/PE. Brasília, 1999. Disponível em: <http://www.cedeca.org.br/PDF/projeto_lei_8499_phyauilino.pdf>. Acesso em: 27 jan. 2008.

BRASIL. Lei n. 10.764, de 12 de novembro de 2003. Altera a Lei no 8.069, de 13 de julho de 1990, que dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 13 nov. 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/2003/L10.764.htm#art4>. Acesso em: 5 fev. 2008.

_____. Ministério da Ciência e Tecnologia. **Programa 1008 - Inclusão Digital.** 2006. Inclusão Digital. Disponível em:<http://www.mct.gov.br/index.php/content/view/42303.html>. Acesso em: 30 jun. 2008.

_____. Ministério da Cultura. **Cultura Digital**. 2008a. Disponível em: <http://www.cultura.gov.br/programas_e_acoes/cultura_viva/programa_cultura_viva/cultura_digital/> Acesso em: 30 jun. 2008.

_____. Ministério das Comunicações. Inclusão Digital. Gesac. **Apresentação** 2008b. Disponível em: <http://www.mc.gov.br/>. Acesso em: 30 jun. 2008.

BUARQUE, D. O meio sem a mensagem. Entrevistado: Vinton Cerf. **Folha de São Paulo**, São Paulo, 29 jan. 2006. Suplemento Mais.

CASTELLS, M. **A sociedade em rede.** São Paulo: Paz e Terra, 1999.

_____. **O poder da identidade.** A era da informação: economia, sociedade e cultura, São Paulo: Paz e Terra, 2002. v. 2.

_____. **A galáxia da Internet:** reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

CEBRIÁN, J. L. **A rede:** como nossas vidas são transformadas pelos novos meios de comunicação. São Paulo: Sumus, 1999.

CEPTRO.BR. Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações. **Conheça os projetos**. 2008. Disponível em: <http://www.ceptro.br/> Acesso em: 15 jun. 2008.

CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Informações de contato de grupos de respostas brasileiros**. 2008a. Disponível em: <http://www.cert.br/contato-br.html>. Acesso em: 15 jun. 2008.

_____. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Estatísticas dos Incidentes Reportados ao CERT.br**. 2008b. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 15 jun. 2008.

CETIC.BR. Centro de Estudos sobre as Tecnologias da Informação e da Comunicação. **Centro de Estudos sobre as TICs**. 2008. Disponíveis em <http://www.cetic.br/>. Acesso em: 30 jun. 2008.

CGI. Comitê Gestor da Internet no Brasil. Ministério Público Federal. **Crimes cibernéticos:** manual prático de investigação. São Paulo: Comitê Gestor da Internet no Brasil, Ministério Público Federal, 2007.

CGI. Comitê Gestor da Internet no Brasil. **Sobre o CGI.br:** quem somos*.* 2008. Disponível em: <http://www.cgi.br/sobre-cg/definicao.htm>. Acesso em: 02 jan. 2008.

CHAVES, D. Yahoo! e Google anunciam acordos de anúncios online. **O Estado de S. Paulo**, São Paulo, 12 jun. 2008. Disponível em: <http://www.estadao.com.br/ tecnologia/not_tec188571,0.htm>. Acesso em: 15 jun.2008.

CONCIL OF EUROPE. **Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems http.** Strasbourg, 28 Jan. 2003. Disponível em: <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>. Acesso em: 20 jan. 2008.

CUBA descarta acesso de moradores à Internet a curto prazo. **G1.** Globo.com. São Paulo, 12 mai. 2008. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/ 0,,MUL466874-6174,00.html>. Acesso em: 04 jun. 2008.

DIAS, A. A. M. **Os Anacronautas do teutonismo virtual**: uma etnografia do neonazismo na Internet. 2007. F. Dissertação (Mestrado em Antropologia Social) – Instituto de Filosofia e Ciências Humanas Campinas, Unicamp, Campinas, 2007.

DOILE, R.; FIABANE, V.; AREU, G. I. P. New Mídia: o Orkut, uma poderosa ferramenta de segmentação. In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 30., 2007, Santos. **Anais eletrônicos…** Santos: Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2007. Disponível em: <http://www.intercom.org.br/papers/nacionais/2007/resumos/R1886-1.pdf>. Acesso em 20 fev. 2008.

E-COMMERCE. Dados estatísticos sobre Internet e comércio eletrônico. **Vendas comércio eletrônico – Brasil.** 2008. Disponível em: <http://www.e-commerce.org. br/STATS.htm#H>. Acesso em: 12 jan. 2008.

FELIPE, J. Afinal, quem é mesmo pedófilo?*.* **Cadernos Pagu**, Campinas, n.26, p. 201-223, jan./jun. 2006.

FERGUSON, M. Estratégias de governo eletrônico: o cenário internacional em desenvolvimento. In: EISENBERG, J.; CEPIK, M. (Orgs.). **Internet e política:** teoria e prática da democracia eletrônica. Belo Horizonte: UFMG, 2002. p. 103-140.

FREY, K. Governança eletrônica. In: EISENBERG, J.; CEPIK; M. (Orgs). **Internet e política:** teoria e prática da democracia eletrônica. Belo Horizonte: UFMG, 2002, p.141-163.

GAIARSA, J. A., **O que é corpo**, São Paulo: Brasiliense, 1994.

GETSCHKO, D. Participação e presença na rede*.* In: BALBONI, M. (Coord.). **Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil:** TIC domicílios e TIC empresas 2006**.** São Paulo: Comitê Gestor da Internet no Brasil, 2007. , p. 35-37.

GINDRE, G. Os desafios da governança na Internet. **Revista ADUSP**, São Paulo, n. 42, p.66-73, jan. 2008.

GOMES, W. A democracia digital e o problema da participação civil na decisão política. **Revista Fronteiras**, v. 7, n. 3, p. 214-222, set./dez. 2005.

_____. Internet e participação política em sociedades democráticas. **Revista FAMECOS**, Porto Alegre, n. 27, p. 58-78, ago. 2005.

GOUVEIA, F. Internet sem fio em benefício de quem? 2006. **Com Ciência.** Revista Eletrônica de Jornalismo Científico. Seção Reportagem. Disponível em: <http://www.comciencia.br/comciencia/?section=8&edicao=18&id=188 Acesso: 30 jun. 2008

HAESBAERT, R. **O mito da desterritorialização***:* do "fim dos territórios" à multiterritorialidade. Rio de Janeiro: Bertrand Brasil, 2006.

IANNI, O. **A sociedade global.** Rio de Janeiro: Civilização Brasileira, 1992.

IASULAITIS, Sylvia. **Internet, democracia e eleições**: as cibercampanhas presidenciais brasileiras em 2006. 2008. 272 f. Dissertação (Mestrado em Ciências Sociais) – Universidade Federal de São Carlos, São Carlos, 2008.

IBGC. **Governança corporativa**. 2008. Disponível em: <http://www.ibgc.org.br/Secao.aspx? CodSecao=17>. Acesso em: 10 fev. 2008.

ICANN. Internet Corporation for Assigned Names and Numbers. **Domínios de primeiro nível (gTLDs)**. 16 dez. 2003. Disponível em: <http://www.icann.org.br/tlds/>. Acesso em: 15 jan. 2008.

_____. Internet Corporation for Assigned Names and Numbers. **Relação dos registros**. 5 jun. 2006. Disponível em: <http://www.icann.org.br/registries/ listing.html>. Acesso em: 15 jan. 2008.

_____. Internet Corporation for Assigned Names and Numbers. A comunidade internacional da Internet trabalha em equipe para promover a estabilidade e a integridade da Internet. **O que é a ICANN?**. 26 mar. 2007a Disponível em:<http://www.icann.org/tr/portuguese.html>. Acesso em: 15 jan. 2008.

_____. Internet Corporation for Assigned Names and Numbers. **ICANN Annual Report 2007**. 2007b. Disponível em: <http://www.icann.org/annualreport/annual-report-2006-2007.pdf>. Acesso em: 20 jan. 2008.

IGF. Internet Governance Fórum. **Relatório da Segunda Reunião do Fórum de Governança da Internet (IGF)**. Rio de Janeiro, 12-15 nov. 2007. Disponível em: <http://governanca.cgi.br/documentos/intgovforum-org_rio_meeting_chairmansummary-final-16-11-2007-revisado-final.pdf>. Acesso em: 10 jan. 2008.

INTERNET CRIME COMPLIANCE CENTER. **Internet crime report.** 1 Jan./ 31 Dec. 2006. Disponível em: <http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf>. Acesso em: 10 jan. 2008.

INTERNET WORLD STATS. **Uso da internet no mundo e estatísticas populacionais.** 2007. Disponível em: <www.internet worldstates.com/stats.htm>. Acesso em: 7 dez. 2007.

JOHNSON, S. **Cultura da interface:** como o computador transforma nossa maneira de criar e comunicar. Rio de Janeiro: Jorge Zahar, 2001.

JUSTIÇA condena 65 por crimes via Internet. **G1.** Globo.com. São Paulo, 17 jul. 2007. Disponível em: <http://g1.globo.com/Noticias/Brasil/0,,MUL71642-5598,00.html>. Acesso em: 20 jan. 2008.

KERCKHOVE, D. **A pele da cultura:** uma investigação sobre a nova realidade eletrônica. Lisboa: Relógio D´Agua, 1997.

LEMOS, A. Mídia locativa e territórios informacionais. In: ENCONTRO ANUAL DA ASSOCIAÇÃO NACIONAL DOS PROGRAMAS DE PÓS-GRADUAÇÃO EM COMUNICAÇÃO, 16., 2007, Curitiba. **Anais eletrônicos...** Curitiba: COMPÓS, 2007. Disponível em: <http://www.compos.org.br/data/ biblioteca_168.pdf>. Acesso em: 13 jun. 2007.

LÉVY, P. O ciberespaço como um passo metaevolutivo. In: MARTINS, Francisco Martins; SILVA; J. M. (Orgs.). **A genealogia do virtual:** comunicação, cultura e tecnologias do imaginário. Porto Alegre (RS): Sulina, 2004. p. 157-170.

LINS, B. **Privacidade e Internet.** Brasília: Câmara dos Deputados, Praça dos Três Poderes, Consultoria Legislativa, Anexo III, Térreo, mar. 2000.

LUCENA, R. Superproteção traz ainda mais danos. **Folha de São Paulo**, São Paulo, 14 jan 2007. Suplemento Mais. Disponível em: <http://www1.folha.uol.com.br/fsp/mais/fs1401200711.htm>. Acesso em 4 dez. 2007.

MAIA, A.; CAMARGO, F. **World of warcraft**. Análise antropológica do game. 2007. Trabalho apresentado à disciplina Antropologia, do Curso de Desenho Industrial. Bauru: FAAC/Unesp, 2007.

MARATONA de jogos mata chinês de 26 anos. **G1.** Globo.com. São Paulo, 28 fev. 2007. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL7971-6174,00.html>. Acesso em: 4 fev. 2008.

MARKOFF, J. Spray “rouba” dado criptografado de HD. **Folha de São Paulo**, São Paulo, 23 fev. 2008. Folha Dinheiro, Caderno B, p. 15.

MATTELART, A. A era da informação: gênese de uma denominação descontrolada. In: MARTINS, F. M.; SILVA, J. M. (Orgs). **A genealogia do virtual:** comunicação, cultura e tecnologias do imaginário. Porto Alegre: Sulina, 2004, p. 81-107.

MOURA, A. P. Tv digital no Brasil: do SBTVD ao impasse. In: SIMPÓSIO DE CIÊNCIAS DA COMUNICAÇÃO NA REGIÃO SUDESTE - INTERCOM SUDESTE 2006, 11., 2006, Ribeirão Preto. **Anais...** Ribeirão Preto: Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2006. p. 1-14.

MURTA, A. Estudo destrói mito de que geração Google é melhor no mundo virtual. **Folha de São Paulo**, 9 fev. 2008. Folha Mundo, Caderno A, p.16.

NETO, M. F.; GUIMARÃES, J. A. C. Crimes na Internet: elementos para uma reflexão da ética informacional. **R. CEJ**, Brasília, n. 20, p.67-73, jan./mar./2003.

NIC.BR. Núcleo de Informações e Coordenação do Ponto br. **Cartilha de Segurança para Internet 3.1**. 2006. Disponível em: <http://cartilha.cert.br/>. Acesso em: 12 dez. 2007.

_____. Núcleo de Informações e Coordenação do Ponto br. **Prestação de contas.** 2007. Disponível em: <http://nic.br/index.shtml>. Acesso em: 12 dez. 2007.

NTP.BR. Network Time Protocol. Projeto NTP.br. **O tempo.** 2008. Disponível em: <http://ntp.br/tempo.html>. Acesso em: 15 jun. 2008.

PICHONELLI, M.; FERNANDES, K. Acordo libera dados do Orkut em 4 estados. **Folha On Line**. 6 jul. 2007. Disponível em: <http://www1.folha.uol.com.br/fsp/cotidian/ff0607200729.htm>. Acesso em: 07 jul. 2007.

PORTUGAL, J. H. S. **Resenha didática:** tipificação e punição dos crimes de informática. Brasília: Senado Federal, Gabinete do Senador Eduardo Azeredo, 2007.

PROCON. Fundação Procon de São Paulo. Equipe de Pesquisas – DEP. **Pesquisa:** "comércio eletrônico". jul. 2007. Disponível em: <http://www.procon.sp.gov.br/pdf/comercio_eletronico.pdf>. Acesso em: 10 jan. 2008.

PROJETO de lei que coíbe crimes na Internet teria erros crassos. InfoMediaTv. **Terra**. 3 out. 2006. Disponível em: <http://infomediatv.terra.com.br/infomediatv/?section=10&article=140>. Acesso em: 10 out. 2006.

REGISTRO.BR. Registrando Domínios. **Registrando um novo domínio via interface web**. 16 fev. 2007a. Disponível em: <http://registro.br/info/novo-registro.html>. Acesso em 15 dez. 2007.

_____. Valor. **Valores das retribuições**. 26 set. 2007b. Disponível em: <http://registro.br/info/valor.html>. Acesso em 15 dez. 2007.

_____. Categorias disponíveis para registro. **Lista de categorias de domínios**. 30 abr. 2008. Disponível em: <http://registro.br/info/dpn.html>. Acesso em 15 mai. 2008.

SAFERNET BRASIL. **Estatísticas da central de denúncias**. 2007. Disponível em: <http://www.denunciar.org.br/twiki/bin/view/SaferNet/Estatisticas>. Acesso em: 15 jan.2008.

_____. **Quem somos.** 2008. Disponível em: <http://www.denunciar.org.br/twiki/bin/view/SaferNet/QuemSomos>. Acesso em: 15 jan.2008.

SANTOS, M. Globalização, cidadania e meio técnico-científico-informacional. In: Souza, A. J. et al. (Orgs.). **Milton Santos:** cidadania e globalização. São Paulo: Saraiva; Bauru, SP: Associação dos Geógrafos Brasileiros, 2000, p. 15-20. p. 15-20.

SANTOS, R. S (Coord.). **Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil:** TIC domicílios e TIC empresas 2005. São Paulo: Comitê Gestor da Internet no Brasil, 2006.

SFEZ, L. **Crítica da comunicação**. São Paulo: Edições Loyola, 1994.

SOARES, G. G. M. Por uma inclusão digital para além do mercado. In: BALBONI, M. (Coord.). **Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil:** TIC domicílios e TIC empresas 2006. São Paulo: Comitê Gestor da Internet no Brasil, 2007. p.39-42.

SPYER, J. **Conectado:** o que a Internet fez com você e o que você pode fazer com ela. Rio de Janeiro: Jorge Zahar, 2007.

STRECKER, M. Web 2.0 não é inovação, diz Pierre Lévy. **Folha de São Paulo**, São Paulo, 14 ago. 2007. Folha Ilustrada, Caderno E, p. 3.

TEDESCO, J. C. **O novo pacto educativo:** educação, competitividade e cidadania na sociedade moderna. S.Paulo: Ática, 1998.

TELECO. Informação em Telecomunicações. Seção: Banda larga e VOIP. **Perfil usuários**. 26 mar. 2007a. Disponível em: <http://www.teleco.com.br/internet_usu.asp>. Acesso em: 12 fev. 2008.

_____. Informação em Telecomunicações. Seção: Banda larga e VOIP. Estatísticas de Banda Larga no Brasil. **Dados Anuais**. 2007b. Disponível em: <http://www.teleco.com.br/blarga.asp>. Acesso em: 12 fev. 2008.

TELEFÔNICA vai investir este ano R$ 623 milhões em banda larga. **Gazeta Mercantil.** Empresas e Negócios. São Paulo, p. 29, 3 jun. 2008.

UFPA. **O serviço de e-mail.** 2008. Disponível em: <http://www2.ufpa.br/dicas/net1/mailtipo.htm>. Acesso em: 15 jun. 2008

UNESCO. Organização das Nações Unidas para a Educação, a Ciência e a Cultura. **Em foco:** alfabetização e educação de jovens e adultos. 2008. Disponível em: <http://www.unesco.org.br/areas/educacao/areastematicas/alfabeteja/index_html/mostra_documento>. Acesso em: 10 fev. 2008.

USA. United States Department of Justice. Computer crime & intelectual property section. **Cyberethics** Disponível em: <http://www.cybercrime.gov/cyberethics.htm. Acesso em: 20 jan. 2008.

USP. Tutorial HTML. Instituto de Ciências Matemáticas e de Computação. Universidade de São Paulo em São Carlos. **O que é World-Wide Web**. 9 set. 2003. Disponível em: <http://www.icmc.usp.br/ensino/material/html/www.html>. Acesso em: 15 jun. 2008.

VAZ, P. Mediação e tecnologia. In: MARTINS**,** F. M.; SILVA**,** J. M. (Orgs). **A genealogia do virtual:** comunicação, cultura e tecnologias do imaginário. Porto Alegre: Sulina, 2004. p. 216-238.

VERAS, E. Previsões otimistas sobre o futuro da humanidade. Um “chat”com Pierre Lévy. **Computação e sociedade**, Universidade Federal do Espírito Santo, 23 mai. 2000. Disponível em: <http://www.compsociedade.hpg.ig.com.br/pierre/terra.htm>. Acesso em: 08 nov. 2007.

VERISIGN. Provider of Internet infrastructure services for the digital world. The VeriSign Domain Report. **The domain name industry brief**, v.5, issue 1, March 2008. Disponível em: <http://www.verisign.com/static/043939.pdf>. Acesso em: 15 jun. 2008.

VIEIRA, E. **Os bastidores da Internet no Brasil.** As histórias de sucesso e fracasso que marcaram a Web brasileira. São Paulo: Manole, 2003.

WERTHEIM, M. **Uma história do espaço de Dante à Internet**. Rio de Janeiro: Jorge Zahar, 2001.

YAHOO! negocia acordo com a News Corp., dona do MySpace. **Folha On Line**. 13 fev. 2007. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u372142.shtml>. Acesso em: 14 fev. 2008.

APÊNDICES

APÊNDICE A

Entrevista com Demi Getschko

(Diretor Presidente do Comitê Gestor da Internet no Brasil)

Data: 08/01/2008 16h00min h

Local: Sede do CGI
Avenida das Nações Unidas, 11-541, 7º. Andar, Brooklin Novo,
São Paulo (SP)

GOVERNANÇA ELETRÔNICA

Bom, a gente “tá” discutindo governança na Internet, então é importante primeiro pegar as origens da administração da Internet, prá ver como é que foram geradas as estruturas que nós temos hoje. Importante a notar é que ela nasce dentro de um projeto chamado ARPANET, patrocinado pelo governo americano, pelo departamento de defesa, mas rapidamente se descola desse segmento da sociedade e vira algo que fica na mão da academia, então basicamente, a academia, evidentemente com verbas federais dos Estados Unidos, foi a principal responsável pelo desenvolvimento dos protocolos e dos padrões que geraram a Internet, aliás a palavra Internet ela não é usada na origem da rede, a rede chamava-se ARPANET e Internet ela vai dar um pedaço do nome do protocolo que chama-se *Internet protocol,* quer dizer o protocolo que liga as diversas redes e este pedaço de nome do protocolo acabou dando a nome a rede como um todo. Ela passa a se chamar Internet a partir de 86 mais ou menos, um pouquinho antes, talvez 82, 84, quando ela começa a ter popularidade na versão TCP/IP. Antes da versão TCP/IP, ARPANET tentou outras soluções em termos de protocolos, que depois foram abandonados em função de que o TCP/IP foi considerado o mais adequado. TCP/IP foi escrito pelo Vinton Cerf e pelo Robert Cant, dois pesquisadores aí que até hoje estão por aí e que são considerados pais desse protocolo e, portanto, pais da rede. Bom, então, a rede começa com uma administração informal, a partir de algumas pessoas da academia envolvidas diretamente com a estruturação da rede e baseia-se especificamente em colaboração - que se quer dizer com isso - a rede é formada de vários segmentos de

rede, vários milhares de segmentos de rede, todos trabalhando com mesmo protocolo e com uma fraca administração central, cuja única função é garantir que os números que são atribuídos às máquinas e os nomes que são atribuídos às máquinas de serviço são únicos – quer dizer, se eu garantir que de alguma forma, minha máquina tem um nome único na rede e tem um número único na rede, é isso que eu preciso, em termos de administração central, eu não preciso mais do que isso.E assim foi no começo.

Então por exemplo, quando John Postel que faleceu há 10 anos atrás, não, 8 anos atrás, passou a administrar nomes e números e foi criado um negócio chamado IANA, (*Internet Assigned Numbers Authority*) que era praticamente o próprio Postel e mais alguns estagiários e ele passou então a pensar em estruturas de nomes que pudessem permitir a expansão da rede mundialmente e então o que que ele fez – ele pegou uma tabela por exemplo da ISO, a ISO 3166, que tinha acrônimos de duas letras associados a territórios no mundo – ele pegou cada um desses acrônimos e atribuiu a ele uma entrada na raiz de nomes da rede chamada DNS (*Domain Name Systems*) e passou a atribuir prá cada um desses acrônimos, quando havia no território específico uma iniciativa de redes, alguém que cuidasse daquilo. Então por exemplo, o Brasil, foi incluído nessa raiz em 89 (Ponto br. foi registrado em 18 de abril de 89) e foi apontado pra vida acadêmica brasileira na época, então quais eram as redes acadêmicas, havia a rede da ANSP (*Academic Network at* São Paulo), que ficava na FAPESP, e a RNP, a Rede Nacional de Pesquisa, no caso como a FAPESP era o lugar onde a operação central da rede acontecia, foi pra atribuído o apontador do ponto br. Então, o que eu quero dizer com isso é que o br, que representa o território associado ao Brasil, foi atribuído a um grupo envolvido em redes, sem nenhum envolvimento, nem do governo americano, nem do governo brasileiro, nem de nenhuma instância oficial, mas simplesmente dos atores envolvidos em redes naquele instante.

Então eu tava falando que o br foi atribuído a esse grupo de pessoas – outros domínios, o ponto ar, da Argentina, o ponto cl do Chile, etc. tal, foram atribuídos a outros grupos de pessoas, normalmente da área de universidades, ou da área de academia, porque era o pessoal envolvido com redes na época. Então, a Universidade do Chile tocava o ponto cl, e assim por diante. Com o tempo, a partir de 86 principalmente, a rede começa a ter um afluxo cada vez maior de serviços não acadêmicos, então a área comercial começa a descobrir a rede, e com isso,

algumas novas preocupações surgem, não é, como garantir que aquela estrutura informal pudesse de fato ser sólida, como garantir, se houvesse necessidade de incluir outros nomes na raiz, isso fosse feito de uma forma justa, homogênea, coerente, tudo mais, e com isso, em vários lugares do mundo que foram criados, foram, nasceram discussões sobre como isso seria feito.

No Brasil, por exemplo, em 95, foi criado o Comitê Gestor, por uma portaria de dois ministros, o ministro da Ciência e Tecnologia e o Ministro das Telecomunicações e o Comitê Gestor então, chamou a si aquela administração que era inicialmente feita de forma informal pelo grupo operador inicial, que trabalhava na , então, tanto o domínios, nomes, quanto números passaram a ser, digamos a ter responsabilidade administrativa do Comitê Gestor.

Analogamente, no cenário mundial, a IANA começou a sentir que poderia ser complicada a gestão informal que havia e aí houve uma proposta do governo americano de criar então uma transição para um órgão que fizesse o que a IANA fazia em termos de nomes e números e esse órgão então, devia ser um órgão neutro e pluralista, etc. e tal, e foi feita uma chamada de propostas, foi escrito um texto chamado *Green Paper* e que gerou então depois as propostas e, a proposta de uma organização da Califórnia chamada ICANN, que é *Internet Corporation for Assigned Names and Numbers,* um pedaço do IANA está no meio do nome dele, acabou sendo digamos, a organização eleita para operar isso aí numa fase de transição e, o Departamento de Comércio Americano, ficou encarregado, digamos, de supervisionar essa transição até o ICANN ser auto-suficiente e ter um funcionamento devidamente é, digamos, tranqüilo, garantido, correto, neutro e tudo mais. Por vários motivos, que é muito longo explicar agora e que depois podemos discutir com cuidado, essa transição até agora não acabou, isso gera evidentemente uma polêmica de porque um determinado governo tem mais controle do que o outro na rede, visto que está gerindo essa transição para o ICANN, o ICANN é um organização na Califórnia, uma organização portanto que segue as leis norte-americanas, e isso também pode ser um motivo de polêmica, talvez devesse ser uma organização mais neutra ou internacional de alguma forma, mas eu queria deixar muito claro isso, quer dizer, a Internet nunca foi ligada nem a governos, nem a empresas privadas e nem mesmo à academia em si, mas sim a grupos que cooperavam para que isso funcionasse, então, ela é o que a gente chama de uma rede *multistakeholder*, você tem vários segmentos interessados no seu

desenvolvimento, interessados no seu progresso e esses segmentos cooperam entre si.

Tanto a área acadêmica, quanto o governo, quanto o setor privado e, pelo menos em minha opinião, seria fundamental, pra liberdade da rede, para o crescimento da rede, que essa característica fosse mantida, essa característica de cooperação entre todos os segmentos e essa característica de não controle da rede por um determinado setor específico.

PARTICIPAÇÃO NA HISTÓRIA DA INTERNET

Bom, meu envolvimento com redes, essas coisas, começa em, eu me formei na Poli em 75, como engenheiro, mas desde 71, já estagiava no centro de computação lá da USP e lá já tínhamos um envolvimento com computador, etc., tal; na época redes, não se falava em redes de computadores, se falava no máximo, redes em que terminais acessavam um computador central, então havia uma rede, chamada de rede USP na época, que era de terminais acessando um computador central, eu me envolvi na montagem dessa rede, mas nada parecido com o que nós temos agora. Depois do CCE, do Centro de Computação da USP, eu fui pra FAPESP, em 85, tive sorte de estar então na FAPESP, no momento em que havia uma grande pressão pra que fossem montados acessos internacionais do Brasil às redes acadêmicas que já eram uma realidade em 85. Então, nós montamos uma equipe lá a partir de 86, 87, o Professor Oscar Sala, que era o presidente da FAPESP, um físico que é muito importante, foi presidente da Academia Brasileira de Ciências e tudo o mais, ele encabeçou a iniciativa, resolveu que a FAPESP era o lugar certo pra fazer isto, porque era neutra em relação às três universidades e também englobava a Secretaria de Ciência e Tecnologia, hoje o IPT e tudo o mais, então, nós montamos lá um grupinho e fizemos uma conexão internacional, um laboratório de Física, chamado *Fermlab*, que fica perto de Chicago, uma cidade chamada Batávia e acessamos uma rede chamada *Bitnet*, é *Bitnet* é "*Becouse it's time network*", porque "ta" na hora da Rede. É, na verdade nós, nessa iniciativa, nessa iniciativa, também houve uma iniciativa ao mesmo tempo no Rio de Janeiro, que aliás, conectou-se também à *Bitnet* um mês antes da FAPESP, no LNCC (o Laboratório Nacional de Computação Científica), então, no final de 88, haviam duas conexões do Brasil ao exterior, uma da FAPESP ao Ferm, e outra do LNCC à

Maryland, à Universidade de Maryland, as duas trabalhando com *Bitnets*, e, além de *Bitnet*, que era uma rede muito boa pra correio eletrônico, mas não tinha nenhuma outra interatividade, não tinha vídeo, não tinha imagem, a rede era uma rede de terminais a caracter, na época os terminais, os microcomputadores basicamente trabalhavam com caracteres, tela de 24 linhas por 80 colunas, não tinha imagem, essas coisas que nós temos hoje, mas era muito boa por causa do correio eletrônico, correio eletrônico foi uma ferramenta sensacional, ainda é uma ferramenta sensacional e abriu um horizonte de uso que ninguém tinha, quer dizer, você podia falar com seu orientador, podia continuar seus projetos, podia continuar usando os aceleradores do exterior, fazer experimentos, sem ter que se deslocar “pra” fora.

Então, isso foi um sucesso, rapidamente, várias universidades puxaram linhas por conta própria até São Paulo ou Rio e montou-se uma rede então, totalmente espontânea, de conexões desorganizadas “pra” espalhar a *Bitnet* pelo país. Em breve se viu, que além da *Bitnet*, havia outras redes interessantes, no caso da FAPESP, a gente também usou uma rede chamada *Hafnet* (*Hinet Fisics network*) , uma rede de físicos, trabalhava em outro protocolo e, finalmente...

Então, em 88, 89 então, as conexões brasileiras, tanto da FAPESP, quanto do Rio de Janeiro iam “pros” Estados Unidos e traziam *bitnet* “pro” país. *Bitnet* era boa “prá” correio eletrônico, era uma rede muito econômica em termos de banda, para você ter uma idéia, a linha que ligava o Brasil aos Estados Unidos era de 4.800 *bits* por segundo e hoje não é nada, quer dizer, ninguém consegue fazer nada com isso, depois nós subimos pra 9.600 *bits* por segundo, mas pra correio eletrônico é suficiente, porque era só texto não tinha imagem, não tinha carga adicional nenhuma. Então, primeiro *Bitnet*, depois *Hacnet* (*Hinet Fisics Network*) e, rapidamente nos anos 90, ficou claro que as duas, a *Bitnet* e a *Hacnet* iam ser substituídas por uma única nova estrutura, baseada em TCP/IP, que era a Internet, então nós, rapidamente tentamos nos incluir também pela Internet e aí, foi na FAPESP que isso aconteceu, o *Ferm* ia participar de uma rede chamada *Easnet* (*Energy Ciences Network*), que era um dos *backbones* americanos, uma das espinhas dorsais americanas, que rodaria o TCP/IP e estariam integradas na Internet. O *Ferm* entrou no *Easnet* no final de 90, e já em 91, em janeiro, nós estávamos ligados, carregando os mesmos pacotes TCP/IP na linha São Paulo/Batávia, essa que ia até o *Ferm* e, a partir daí, nós vimos que rapidamente a

banda seria consumida muito rapidamente, 9.600 não dava pra nada, fomos pra 64, depois fomos pra 128, 256, e rapidamente a linha internacional foi sendo aumentada.

Eu posso comentar que em 92, teve um evento importante, que foi a Eco 92, no Rio, e na Eco 92 no Rio, nós conseguimos disponibilizar Internet pro pessoal que tava lá no Rio e isso foi um dos fatores de amadurecimento da rede brasileira também, então aí, tanto São Paulo quanto o Rio colaboraram pra que a Eco 92 tivesse acesso à Internet, como falei, na época, com linhas de 64 K, que eram consideradas de alta velocidade.

Aí, em 93, acontece um fenômeno muito importante, que é a entrada do *World Wide Web*. Hoje nós confundimos www com a própria Internet, elas são coisas distintas, quer dizer, www é uma aplicação sobre a rede, que começa a ganhar força a partir de 93. Na época, a gente era muito cético com relação a isso, porque achava que não haveria banda suficiente pra acomodar uma imagem e porque as imagens não só valem mais que mil palavras como pesam também mais que mil palavras, uma imagem é um negócio muito maior que um texto. Então, mas por sorte, também na época, as infra-estruturas de telecomunicação foram melhorando, o Brasil foi passando a ter fibra entre as cidades, nas áreas metropolitanas e a linha internacional pôde ser aumentada 2 megabytes por segundo, que também é uma miséria hoje, mas na época, era considerada uma grande velocidade, então, de alguma forma, a rede conseguiu sobreviver à enchente de dados que o www representou e no Brasil começaram a aparecer os grandes provedores, em 94/95.

INFRA-ESTRUTURA, PROVEDORES, CULTURA, CUSTOS

Nós temos um outro fator interessante no Brasil que é o seguinte: vários provedores de Internet no Brasil vieram de meios de comunicação de massa, de mídia, é Uol, Bol, e tudo, e vários outros desse tipo. Então, com isso, nós temos a seguinte vantagem que outros países não tiveram: um afluxo de conteúdo em português rapidamente disponível, não é, a rede antes de 94, 95 a linguagem franca era o inglês, e praticamente tudo que tinha na rede tava em inglês. A partir da entrada de provedores de acesso e de serviços em cada país, eles traziam conteúdo do país, e como no Brasil esses provedores também eram veículos de mídia, eles já

tiveram mais facilidade de produzir conteúdo, então rapidamente o conteúdo em português abundou na rede e tivemos facilidade pra incluir pessoas que não teriam, digamos, formas de se comunicar, falando em inglês. Então, a partir de 93, 94, nós passamos a ter provedores e esses provedores como vinham da área de mídia também, esses provedores, eles geraram bastante conteúdo, então, em 95, houve o boom, a explosão da Internet comercial no Brasil que também coincidiu com a explosão da Internet comercial nos Estados Unidos, então no Brasil nós seguimos mais ou menos no mesmo ritmo dos demais, talvez em escala menor, porque os nossos meios de comunicação eram piores, não tínhamos a mesma banda disponível, mas os eventos que aconteciam lá também aconteciam aqui, quer dizer, quando havia um grande afluxo de provedores e um grande interesse pelo comércio na rede também no Brasil, então isso começou a acontecer mais ou menos ao mesmo tempo. E daí a coisa evidentemente foi florescendo e hoje nós temos aí toda a riqueza da Web 2.0, etc. e tal. Mas o que eu queria dizer é que, desde o começo algumas noções que a Internet trazia ou alguns riscos que estavam embutidos nisso não se mostraram digamos tão reais, outros evidentemente são reais, então, vou dar um exemplo:

Se dizia o seguinte, na Internet nós vamos ter que aprender a falar inglês, e com isso vai ser, digamos uma ferramenta contra a manutenção de culturas locais e de idiossincrasias locais, de especificidades de cada país – isso, na minha opinião se mostrou totalmente errado – a Internet, ao contrário, ela privilegia e ela permite que pequenas comunidades possam se reforçar comunicando-se pela rede e com isso, não só se manterem vivas, como até se expandirem, então não é verdade que haverá uma capa única de cultura e ela será anglo-saxã, e cobrirá aí como um todo; na verdade, todas as culturas que existem e que acessam a rede, usam a rede, se beneficiam da rede pra poder até reforçar a própria existência, quer dizer, é um fato que é interessante. Um outro fato que tem que ser explorado com mais detalhe é essa história da colaboração que eu falei no começo e a colaboração da rede tem uma segunda visão que é o software, quer dizer desde o começo da rede e TCP/IP progrediu por causa disso e os serviços em TCP/IP e as aplicações em TCP/IP tenderam a ser gratuitas, se vocês lembram, no começo da *World Wide Web* como uma tendência de cobrar o browser, rapidamente isso foi é, demolidos e os browsers continuam gratuitos, os navegadores que é o primeiro navegador, o mosaic era grátis, mas aí houve uma tendência da Microsoft cobrar, outros também pensaram

em cobrar, aí no final se viu que isso aí era inviável – os navegadores continuaram grátis.

Então, a rede permitiu que a colaboração em cima dela gerasse software de boa qualidade, de excelente qualidade, através da colaboração de milhares de indivíduos de todos os lugares do mundo e esse software tende a ser grátis porque ele não tem um dono específico. Então, é um software aberto, livre, e em geral disponível e de boa qualidade. A rede usa isso pra se expandir e o software livre usa a rede pra poder gerar mais software, então isso é uma sinergia, uma simbiose muito interessante que a rede trouxe e que certamente não era imaginável antes da rede, quando o software era produzido em grandes organizações que controlavam completamente o seu fonte, o seu conteúdo e a sua forma de distribuição.

A rede, de alguma forma, tornou impossível esse controle, fazendo com que o software fosse difundido rapidamente, porque afinal de contas, bits são bits, independente se isso é um software, um texto, uma imagem ou o que for. Eu acho que tem alguns paradigmas que a rede quebra e que são muito difíceis de se controlar, então por exemplo um deles é, um problema de fronteiras geo-políticas. Certamente na rede não há fronteiras claras e você pode ter um brasileiro escrevendo no seu blog, na China e armazenando o blog nos Estados Unidos e orientando o blog aos brasileiros. Você pode ter alguém fazendo um conteúdo inadequado, indevido, ilegal, pornográfico em algum lugar na África mandando pra um servidor na Europa pra ser usado por brasileiros, quer dizer, não há uma identificação clara de territorialidade.

CONTROLES/LEGISLAÇÃO/SEGURANÇA

Com isso também, é muito difícil de se aplicar legislação na rede. Fora isso, a rede não é de ninguém. Então, por exemplo, algumas iniciativas do tipo identificar o acesso do usuário à rede é uma coisa estranha porque eu posso identificar o acesso de alguém a minha casa, mas eu não posso identificar o acesso de alguém à rua ou à praia, quer dizer, se eu não tenho um sujeito que é responsável pela estrutura em si, eu não posso botar uma porteira em algo que é aberto, então eu acho que nós temos de tomar o máximo de cuidado pra quem entra na nossa casa, no nosso *site*, no nosso banco, na nossa loja, mas nós não podemos impedir que alguém entre na rede, porque a rede não é especificamente nossa; se a gente dificultar a entrada na

rede aqui, ele vai entrar por outro lugar, quer dizer, não há como você cercar a praia e impedir o acesso ao oceano – então, é muito importante o balanço entre, digamos o serviço de Internet, de acesso livre, de conteúdo disponível, etc. e tal, e as formas que você tem de controlar os mal feitos sobre a rede, acho que é fundamental que se consiga inibir e punir os que cometem delitos na rede, mas temos que tomar muito cuidado pra não punir a rede, acho que a rede em si é inimputável – eu “to” dizendo isso porque tem uma pergunta que envolve o caso Cicarelli no *YouTube*, onde quem foi punido foi o acesso ao *YouTube*, que não tinha nada a ver com o caso Cicarelli em si. Quer dizer, se alguém fez um vídeo inadequado, que ele seja justiciado de alguma forma, punido de alguma forma, mas não que percamos o acesso a um recurso como o *YouTube*, que era usado pelo governo do Rio Grande do Sul, por exemplo, na campanha contra a dengue, então, é muito importante separar a rede em si, que na minha opinião é inimputável, dos usuários da rede que obviamente são responsáveis pelos seus atos. Então, continuando nessa parte digamos de conceitos da Internet que de alguma forma vão afetar o nosso dia a dia – além desse aspecto de legislação que eu comentei, que é muito difícil ter uma legislação sobre a rede em si, porque a rede não tem fronteiras, a legislação nacional não se aplica a rede como um todo, então na minha opinião a legislação tem que se aplicar aos que atuam na rede, e eles devem ser punidos se cometerem delitos ou não mas a rede em si é inimputável, eu diria que tem mais alguns aspectos da rede que são muito interessantes e que provavelmente nós estamos examinando só no começo desse seu efeito e não sabemos como é que será daí pra frente.

Um deles, por exemplo, é essa geração de conteúdo na mão do indivíduo, quer dizer hoje todos podem gerar conteúdo e colocar na rede e você vê isso pela proliferação de blogs, de wicks, de sites em que existe informação, evidente que com isso a qualidade é muito variável, existem informações corretas, existem informações falsas, existem calúnias, existem difamações, existem todo tipo de coisas boas e ruins, mas de qualquer forma o poder do usuário de poder colocar informação na rede é algo muito importante e não havia... Então, estávamos falando da capacidade de cada um editar conteúdos na rede, isso inclusive gerou por exemplo (...) a Wikipedia, que é uma enciclopédia gigantesca, com a colaboração de milhares de indivíduos, e que tem uma qualidade bastante boa, eu diria, na verdade, o fato de a coisa ser aberta, de todos colaborarem, não é obrigatório que se gere

informação distorcida, mas conforme existe risco na rede, porque, como a rede está disponível a todos que colocarem o que acham, existe certamente uma facilidade de propagação de coisas que não são verdadeiras, ou não são corretas.

Agora, eu acho que esse é um custo a pagar pela liberdade da rede, acho que é importante que nós mantenhamos essa abertura e que todos possam dizer o que queriam, evidentemente o pessoal da legislação, da justiça e tal, vai ter que ver como coíbe os que falam coisas inadequadas ou falsas ou inverídicas sem que o abuso impeça o uso, não é, uma das regras básicas em geral que se tem, liberais, abertas, democráticas, é que o abuso não deve tolher o uso. Se alguém abusa de algo, isso não quer dizer que devemos tirar o uso legal daquilo, porque está havendo um abuso. Mas, outros dois aspectos que também queria comentar que acho que são fundamentais nessa história, é que alguns dos conceitos que nós temos de algumas áreas certamente serão afetados pela rede de uma forma muito profunda que nós ainda não conseguimos entender em toda a sua extensão.

Um deles, por exemplo, é toda a parte ligada à propriedade intelectual. A propriedade intelectual baseou boa parte da sua operação, no fato de que existia um meio de suporte físico onde a propriedade intelectual se expressa, então o autor de um livro, ele imprime um livro, e pelo fato de imprimir n exemplares do livro, ele pode ter uma conta que vai gerar à ele uma receita porque o livro carrega a idéia dele em papel.Da mesma forma que um compositor de música grava um meio físico, onde a música dele, de alguma forma, pode ser transportada e ele pode controlar isso.Mas, se nós voltarmos ao passado, não tão distante assim, na época dos compositores clássicos, Bach e outros, a coisa não era assim. Na verdade Bach, quando compunha um oratório, ou o que fosse, ele ganhava pra fazer aquilo, mas ele não ganhava para que estocassem aquilo, ao contrário, ele gostaria que tocassem bastante aquilo, porque toda vez que tocavam aquilo, provavelmente ele iria receber uma encomenda de um novo oratório, e ele ia ser pago pra produzir mais uma missa ou uma cantata, ou o que fosse. Então, o meio de remunerar o autor a partir que os meios de produção geraram o suporte físico da idéia. A Internet, de alguma forma, volta a destruir esse negócio, quer dizer, o suporte físico da idéia desaparece. Além de desaparecer o suporte físico da idéia, o intermediador desaparece. A rede “desintermedia” as coisas: quer dizer, o autor e o consumidor são colocados diretamente em contato. Eu posso gerar um texto e passar diretamente pros meus leitores através do meu *blog* sem ninguém no meio do caminho. E eu não tenho

como numerar quantas vezes aquilo foi lido ou não lido, porque uma vez lido por alguém isso sempre pode ser espalhado pela rede e, uma vez gerada a informação, ela se distribui e é muito difícil controlá-la.Então, certamente, eu acho que nós teremos algum impacto na área de propriedade intelectual, as coisas vão ter que ser revistas, provavelmente conceitos serão revistos, provavelmente a forma de remunerar o autor será revista, porque certamente não há como tampar as infinitas possibilidades que a rede tem de você copiar algo.

Se tentou fazer assinaturas e formas de criptografia e de fazer, mas, uma vez que esteja disponibilizado para leitura, ta na rede, e como nós já falamos, todos os bits são iguais e não tem mais como segurar. Esse é um ponto que eu acho que a rede vai trazer impacto.

Um outro ponto, que a rede também vai trazer impacto é o seguinte: muitos dos serviços nossos de telecomunicação passarão a ser feitos sobre a rede, como nós já estamos vendo hoje; então, estruturas específicas não é, muito custosas que eram operadas por grandes operadoras e, portanto, tinham uma barreira de entrada muito grande pra competição, por exemplo, telefonia, perdem essa barreira de entrada, no momento em que telefonia vira simplesmente mais um serviço sobre a rede, e da mesma forma que correio eletrônico, e som e texto e o diabo andam em cima de pacotes TCP/IP. Então, telefonia é um exemplo, mas na verdade, uma porção de serviços que nós temos hoje, migrarão para serem operacionalizados sobre o protocolo da rede e com isso, o modelo econômico muda drasticamente. Então, os modelos de várias indústrias, não é, que existem hoje, na área de comunicação, serão afetados pelo fato da rede existir. Isso envolve jornais, envolve TV, envolve telefonia, envolve todos os meios de comunicação, por quê? Porque hoje a rede é um meio ubíquo, não é, está em todo o lugar, e ela transporta informação de uma forma neutra, sem que a gente saiba se aquela informação é uma notícia importante, ou um pedaço de uma piada, ou um pedaço de uma imagem, com isso, os modelos econômicos dessas indústrias, desses segmentos serão afetados pela existência da rede. Não há uma conta específica que alguém esteja pagando, quer dizer, a Internet não é um serviço que seja subsidiado por alguém. Na verdade, todos pagam a conta de alguma forma. As linhas de telefone são pagas aos provedores de telecomunicação, as infra-estruturas de comunicação de dados são pagas de alguma forma a provedores. A Internet trouxe um novo modelo em que a integração de milhões de pequenos pagamentos geram uma

grande conta, então isso é um outro ponto muito interessante pra notar, quer dizer, veja por exemplo, um buscador como o *Google*, que tem um investimento de infra-estrutura enorme: são milhares e milhares de máquinas, sem contar uma tecnologia extremamente sofisticada da distribuição da carga pelas máquinas e uma confiabilidade muito grande e que, a ponto que todos usamos esse serviço diariamente. Essa empresa hoje vale muito dinheiro, é uma das empresas mais valiosas do mundo, mas se se pensar bem, porque ela vale tudo isso? Quer dizer, ela vale tudo isso porque ela tem milhões de usuários o tempo todo no mundo e porque ela “ta” usando um modelo de micro-pagamentos que vem a partir dos anúncios classificados que eles têm, que são ligados à busca que você faz, que cada um deles é extremamente barato, portanto, várias pequenas empresas podem pagar esse tipo de anúncio, mas a integral, quer dizer, a soma desses pequenos pagamentos dá um montante que justifica o valor que a *Google* tem.Então, essa mesma tendência que a Internet traz, uma tendência em que nós diluímos os pagamentos, ninguém ta subsidiando nada, a rede em si se mantém, mas a soma de pequenas frações de pagamentos que todos nós fazemos de alguma forma no nosso dia-a-dia sustenta os serviços.

INCLUSÃO DIGITAL

Eu acho que o papel fundamental aí de Governo, do Comitê Gestor e outros aí, é estimular a penetração da infra-estrutura “prá” que a rede possa ser accessível de todos os pontos do país. O nosso país é gigantesco, nós temos pontos em que a infra-estrutura de telecomunicações ainda é extremamente precária e à vezes nem existe. Um bom acesso à rede exige estruturas de superfície; satélite nunca é uma boa alternativa, porque o satélite tem um atraso grande, então, o ideal seria que tivéssemos uma estrutura em cima de fibra óptica, e uma vez estabelecida a infra-estrutura, nós temos uma segunda barreira a vencer, que é a barreira do computador, quer dizer, uma experiência completa à Internet, uma experiência completa da rede, envolve você ter disponibilidade do equipamento a hora que você precisa, e não, a hora que você pode usar, então você precisa ler seu e-mail, ler o noticiário, se aculturar do que “tá” acontecendo, e depois, então, também, interagir. Na verdade a rede, na minha opinião, também passa a fazer parte do dia-a-dia das pessoas dessa forma: em primeiro lugar uma forma de você ganhar informação, se

instruir, ganhar acesso ao que há no mundo, e numa segunda fase, você participar, gerando sua própria informação. É o que a gente tem visto, na sociedade como um todo, quer dizer, o Brasil, o brasileiro primeiro acessa a rede e passa a se informar por ela, depois rapidamente ele passa a querer gerar sua própria informação, e discutir, e participar de comunidades, etc. e tal.

Eu ainda aproveito para fazer mais um parêntese: nós temos dois pontos que são muito interessantes, que são específicos do Brasil. Primeiro: nós temos um tempo de conexão à rede muito grande, aparentemente é o líder não é, e o segundo é que nós gostamos muito de comunidades, brasileiro é o líder em comunidades virtuais tipo Orkut. Bom, agora eu acho que nós temos uma grande campanha “prá” expansão da banda larga, o próprio governo está empenhado nisso, existiu uma consulta pública na ANATEL no final do ano passado, para que as teles, as empresas de comunicação provessem acesso em banda larga em cidades com certa quantidade de habitantes pra cima, que praticamente envolveria todos os municípios de algum porte no país, então a gente espera que pelo menos a infra-estrutura esteja disponível, aí faltará o equipamento, mas os equipamentos têm barateado, nós vimos esse ano, ainda não sabemos aí o que é que deu no Natal, mas eu acredito que microcomputadores devem ter sido campeões de venda, porque os preços têm caído muito, mesmo os de portáteis, que eram muito caros no passado, e então, a gente imagina que rapidamente, mais e mais brasileiros terão acesso à rede.

FUTURO DA INTERNET

Eu não acredito que nós tenhamos os números que têm os países escandinavos e os Estados Unidos num prazo curto, mas certamente talvez o dobro do que nós temos hoje. Chegar talvez a uns 20, 25, 30 por cento da população talvez não seja um sonho exagerado. Agora, em relação à Internet em si, a gente “tá” vendo, por exemplo, essa história da *Web* 2.0, da *Web* semântica e outras coisas, eu acho que a tendência, se eu quisesse, digamos, tentar resumir, seria que a gente passasse a enxergar cada vez menos a Internet, quer dizer, eu imaginaria que a Internet deverá diluir-se e sumir do ponto de vista que ela não será sensível, não será visível ao usuário. O usuário verá os serviços e não a rede. “Prá” fazer uma analogia que eu já tenho feito em outros casos, hoje, por exemplo, ninguém se

preocupa em qual é o futuro da eletricidade, você usa os aparelhos que consomem eletricidade e esquecemos que a eletricidade existe. Você compra televisores, geladeiras e o que for e vai ligando na tomada e a eletricidade “tá” lá. Então, a Internet como rede, deve seguir mais ou menos esse caminho: deve ser algo que permeia tudo, mas que ela em si, não é objeto de preocupação ou sequer é notada. Com isso, a governança da rede em si, também deve cair para um plano muito simples de geração e de manutenção das estruturas básicas. O que vai importar cada vez mais são os serviços sobre ela, porque nesses serviços é que nós faremos as transações e compraremos coisas e trocaremos informações e iremos ao banco e faremos tudo o mais e com as novas ferramentas 2.0 e as demais, tudo isso se mistura de tal forma que no meu próprio site, ou no meu próprio *blog*, eu tenho o mapa da minha cidade, que é baseado num site que “ta” lá fora, no serviço de outra instituição e também tem um acesso ao Banco que também não é do meu site, em suma: a *Web* 2.0 permitirá que todas essas comunidades se interliguem de forma indistinguível e ficará difícil até saber o que faz parte da minha estrutura e o que “tá” fora dela. Então eu acho que a tendência é essa, é que cada vez mais nós tenhamos uma eliminação de fronteiras, uma eliminação de barreiras e que a rede em si, passe a ser cada vez menos uma preocupação e passe a ser realmente invisível.

Observações: O entrevistado solicitou o roteiro com as questões previamente e optou por respondê-las na ordem de sua preferência, sem interrupções.
Tempo total: 00:33:83
Transcrito por Débora Corrêa Chama
São Paulo (SP), 09/01/08: 14:37:00

APÊNDICE B

Entrevista com Antônio Alberto Tavares

(Presidente da Associação Brasileira de Provedores de Acesso, Serviços e Informações da Rede Internet e Diretor da Dialdata Telecomunicações Ltda.)

Data: 16/01/2008 15:00 h

Local: Sede da Dialdata Telecomunicações Ltda
Rua Nova York, no. 421, São Paulo (SP)

PARTICIPAÇÃO NA HISTÓRIA DA INTERNET

Primeiro, a minha participação na Internet, ela vem desde o início da Internet, 1994/95, a Dialdata, a empresa que eu fundei, junto com o sócio, foi um dos primeiros provedores de acesso, e naquela altura nós já tínhamos uma experiência de alguma coisa que era precursora da Internet, que eram os BBS's (...), então nós tivemos nos Estados Unidos...tivemos um pouco no mercado e percebemos claramente que a tendência era que a comunicação Internet, comunicação eletrônica se fizesse através da Internet. Nesse sentido, como lhe disse, criamos esse provedor de acesso e começamos a nos envolver no sentido de: primeiro, garantir que as telecomunicações, que eram naquela altura, alguma coisa estatizada, (Telebrás) precisassem de ser desmembradas...ou de alguma forma garantir que se constituísse uma cadeia de valor, cadeia essa de valor que garantisse competitividade, garantisse o aumento da capilaridade e que não estivesse engessado pelas coisas típicas de órgãos governamentais. Nesse sentido, foi negociado com a Rede Nacional de Pesquisa (RNP), que estava muito próxima do Ministério de Ciência e Tecnologia e do Ministério das Comunicações, cujo ministro era o ministro Sérgio Motta, pessoa muito forte no governo Fernando Henrique Cardoso, pessoa muito capaz de reconhecer os interesses e ele publicou em 1995, uma norma que dizia que quem deveria dar acesso ao público à Internet eram os provedores de acesso, sem que isso considerasse que os provedores de acesso eram provedores de telecomunicações, ou seja, as operadoras de telecomunicação públicas ou privadas, elas tinham que dar condições para que os provedores

existissem e, eles sim, fariam o acesso a autenticação do usuário na rede.

Naquela altura, evidentemente o acesso era feito via a ligação telefônica, acesso discado e através dos tempos, esse acesso veio a transformar-se em acesso banda larga, acesso via televisão a cabo, via satélite, via Wi-fi, enfim todas essas formas que já estão disponíveis no mercado. Foi um trabalho muito difícil, primeiro lugar, explicar o que era Internet ao mundo, ao mercado, formar a Internet; eu me lembro, as primeiras páginas que apareceram eram uma coisa muito insípidas, não só aqui no Brasil mas também no estrangeiro. E me lembro também que a adesão do brasileiro foi muito natural, foi muito grande, dentro das possibilidades e as possibilidades aí eram as limitações que existiam em função da pouca quantidade de linhas telefônicas disponíveis e as linhas telefônicas naquela altura eram compradas e eram caríssimas e também da pouca penetração do computador, havia ainda muito poucos computadores naquela altura. Estamos falando de 96. Dez anos atrás, onze anos atrás. Foi bastante difícil. Mas aí, grandes empresas passaram já a se envolver, perceberam que havia um potencial grande na exploração da Internet, e que potencial era esse? É que a Internet era uma nova mídia, uma nova forma de comunicação. Ela iria substituir algumas mídias existentes, alguns meios existentes, não eliminá-los, da mesma forma que televisão não acabou com o rádio e nem era essa a proposta, não se esperava isso, mas permitir que a Internet crescesse e servisse à sociedade a uma sociedade que tendia, desde logo já se falava nisso, à globalização, ou seja, a troca intensa de bens e serviços e que eram os aspectos políticos, os aspectos sociais, etc. Esse início da Internet, eu diria, foi um início heróico, estóico e heróico e foi preciso muita força, muita coragem e os provedores que apareceram, salvo algumas grandes empresas como a Folha de São Paulo, que criou o Uol e outros que vieram mais tarde foram pequenas empresas que eram, foram criadas e alimentadas com capitais próprios, economias de pessoas e etc. que, com coragem, foram comprando as linhas telefônicas, modens, enfim, os servidores, etc. e foram construindo essa parte da rede no Brasil, como você sabe, a Internet é rede das redes, uma pequena rede montada aqui se liga a outra e a outra e é por aí que se pode navegar.

Para avançar um pouco nessa conversa, uma vez que o histórico você conhece, as estatísticas mostram, que o crescimento foi grande, nós percebemos e é uma coisa que nos preocupa muito é que a evolução disso mostrou as preocupações do tipo comportamental. A tal ponto que há uma questão que eu

sempre coloco que é o seguinte: o que é que vem primeiro, a tecnologia ou o comportamento, ou seja, é o comportamento que demanda ah, novas tecnologias ou novos equipamentos, novas formas de se comunicar ou é o contrário, são essas tecnologias que são desenvolvidas e elas transformam o comportamento. Por quê? Porque é, um exemplo claro é a televisão. A televisão, enquanto você estava, ah, quando a televisão surgiu aquilo que você fazia indo a um estádio de futebol ou indo a um cinema, passou a fazer menos, passando dentro de casa, na tranqüilidade da sua casa, etc. etc. Ah tem vantagens? Ah, claro que tem vantagens, tem comodidade, muitas vezes de segurança, você acaba se protegendo de alguns atos violentos e tem desvantagens, porque você se torna mais sedentário, enfim, mas o mundo evolui sempre nesse sentido.

CONTROLES/LEGISLAÇÃO/SEGURANÇA

Já naquela altura se falava que a tendência de se passar a se fazer muitas operações do comércio ah via Internet, ou seja, você poderia obter produtos e serviços. Isso ainda era complicado nos primeiros momentos, inclusive isso criou uma grande dificuldade porque colocar o número de cartão de crédito na Internet era perigoso. E não estou em desacordo, se não houver um mínimo de cuidado isso pode ser realmente perigoso. Mas é tão perigoso quanto você carregar uma carteira no bolso no meio da rua. É preciso tirar... não é a Internet que é culpada disso, é preciso dar um valor real coisas. Se há violência, esta violência não é apenas física, acontece no dia-a-dia, na rua, acontece também nos meios virtuais. Uma das coisas que se atribui à televisão era de trazer exemplos maus, de filmes bastante agressivos, enfim de outras mídias. Enfim, isso seria a parte má da televisão. Só que, em muitos casos, isso se chama entretenimento, e entretenimento é uma indústria muito grande, que cresce cada vez mais, e o mundo é isso mesmo, ele vai evoluindo no bom e no mau sentido. Muito bem., ah, em termos comportamentais, portanto, o que é que nós passamos a ter como preocupação: algumas coisas que não eram transparentes ao ser humano comum eram as redes de pedofilia por exemplo. E nesse caso, fica muito claro a Internet, ela é, protege de certa forma o anonimato, algumas pessoas, de formação, lamentavelmente baixa e portanto, permite que aconteça esse tipo de coisa. Por isso, é preciso desenvolver a ferramentas de filtro de proteção para evitar que isso cresça, “pra” se fazer a

correção do rumo e a boa utilização de uma mídia como a Internet. Entretanto, há diferentes pensamentos, diferentes interpretações. Enquanto que algumas pessoas pensam que isso possa ser feito através da criação de novas leis, nós entendemos que - eu pessoalmente – e tenho procurado defender isso, que nós temos que criar, cercear essas atitudes tanto quanto pudermos tecnicamente e, utilizar todos os aparatos que existem, mas não criar novas leis. Por quê? Criar novas leis não é, nunca foi solução. Se fosse solução, criar novas leis as cadeias não estariam cheias, então, nós temos tido alguma dificuldade muitas vezes em discutir com ah, políticos, sejam senadores, sejam deputados, enfim, sejam até ministros que tendem a se inclinar para recomendar e solicitar que se criem novas leis. Não vai resolver absolutamente nada. São aquelas leis que, tipicamente, não vão ser respeitadas e, portanto, elas serão inócuas. Temos é que educar. É importante que, o mais rapidamente possível, tudo isso esteja nas escolas, desde o nível mais elementar, mais básico, sem esquecer que não é apenas, não pode ser apenas uma promessa política de que vamos levar a Internet até as escolas; é preciso pensar que há necessidade de capacitar, e bem, os monitores, os professores, aqueles que vão estar ensinando a utilizar a Internet, para que de uma forma condicionadora, se faça um bom curso de Internet desde criança. Se nós permitirmos – o Brasil infelizmente tem um histórico, um vício, de não educar e não se preocupar em investir bastante em educação, de tal forma que o resultado “tá” aí, nos jornais, no dia-a-dia.

Então, se nós não olharmos a Internet e deixarmos ir por este mesmo caminho, nós vamos ter, não apenas a fama que de certa forma já se tem hoje, que o Brasil é uma das principais pragas que permite que se façam muitas fraudes através da Internet, etc., e não é, eu vou já esclarecer isso. Mas não é. Precisamos então de cuidar. Por que é que o Brasil não é um dos principais responsáveis e praticantes ou promotor de fraudes na Internet? O Brasil, por falta de preparação, muitas pessoas não usam os recursos de segurança em suas máquinas, nas suas redes, que são o minimamente necessário e que deveriam ser conhecidos. E por isso permitem que outros, de fora, muito mais experts nessa história, invadam as suas próprias máquinas brasileiras e as utilizem, como se brasileiros se tratassem, cometendo essas fraudes. E eles tão no estrangeiro. Então, mais de 70% dos ataques que são feitos e aparentemente partidos do Brasil, na realidade eles são originários de Taiwan, na China. Depois vem os Estados Unidos.

Esse negócio é o seguinte: nesses centros onde a inteligência, a quantidade de gente, o acesso é grande “ta” (esse pessoal se utiliza muito) para fazer fraude. Isso isenta todos os brasileiros? Não, já há verdadeiras quadrilhas no Brasil organizadas nesse sentido e, algumas já estão presas, outras estão sendo processadas. Mas o principal problema é o problema da segurança, o problema da formação das pessoas que utilizam a Internet, “ta”, da ingenuidade, da curiosidade, você vê, por exemplo, alguma coisa que é um site de relacionamento como o *Orkut*. O *Orkut* nasceu, não pertenceu ao *Google*, ele nasceu de uma iniciativa de duas pessoas do leste europeu e os americanos começaram a utilizá-lo. Quando os brasileiros descobriram que ali havia alguma coisa tão fácil de usar, tão fácil, tão prática, “tomaram de assalto”, no bom sentido, o *Orkut* e se tornaram a maior comunidade dentro do *Orkut*.

Então, da mesma forma que hoje, o *Orkut* pertence ao *Google*, é praticamente dominado pelas comunidades brasileiras. Agora, é num *site* destes que se pode avaliar, quanto se pode fazer de bem e de mal para o uso da Internet, já que existe a liberdade de você colocar o que quer, se você não tiver a boa e a clara noção do respeito para com a sociedade, você escreve, publica ali como se um jornalista, um editor fosse, aquilo que te apetece, seja atacando o próprio país, atacando governos, atacando outras pessoas, às vezes sem provas, etc., etc. Evidentemente que isso tem que começar a ser resolvido de uma forma educacional. Usando leis? Sim. Que leis são essas então?

Eu disse há pouco que não deviam criar-se leis, por quê? Por que, muito embora, o Código Penal e o Código de Processo Penal sejam de 1940 e 1941, de lá “pra” cá houve atualização através de legislação complementar e, basicamente os crimes que se praticam hoje no dia-a-dia, na vida do ser humano comum, são os mesmos que se praticam na Internet. Então faz-se naturalmente uma coisa que se chama tipificação do crime, ou seja, aplicar aquele mesmo conceito da coisa na Internet e, 95% destes casos já estão portanto resolvidos, sem necessidade de se criar novas leis. Não é, portanto, à toa que se diz: não precisa de novas leis. Há leis específicas referentes a uns pontos que são característicos da Internet, por exemplo, os vírus, etc. Estou totalmente de acordo: é preciso criar uma legislação que tipifique e crie as penas necessárias para esses tipos de atitude. Então, nós temos na mão, um instrumento fantástico de comunicação com uma ferramenta maravilhosa de

educação, de conhecimento, mas precisamos aprender a usá-la. “Tá” tudo muito no início. A Internet é uma criança.

INFRA-ESTRUTURA, PROVEDORES, CULTURA, CUSTOS

Primeiro, vamos falar dos nomes de domínio, eles têm vários níveis “tá”, a raiz do nome do domínio é o ponto br. Essa á a sigla que representa o Brasil “tá”. Digamos, o segundo nível é que tipo de atividade se refere aquele domínio. Então você tem o ponto com que é comercial, você tem o ponto eng que é relativo à uma profissão, como a engenharia, você pode ter o ponto nom que é de um nome próprio de uma pessoa que pode registrar nesta categoria, você tem o ponto psi que é o provedor de serviço de informação. Você tem vários sub-níveis que você pode utilizar. No caso do br, do ponto br, eles são utilizados exclusivamente pelas organizações de registro, ou seja, o Comitê Gestor e as organizações a que se refere e para as escolas e Universidades, etc., “pra” área acadêmica. Até o governo, ele tem o ponto.gov ponto br, a justiça tem jus ponto br. Então todos tem um nível, exceto Universidades. Inclusive no caso das Universidades, houve a suspensão da concessão desse domínio, do uso da raiz, em função dos abusos que houve. Houve Universidades que começaram a tentar no ponto br, registrar nomes que não obrigatoriamente tinham a ver com Universidades, mas que seriam diferenciais, por exemplo, engenheiros ponto br ou igrejas ponto br e isso não era a finalidade então foi obrigado a se cancelar numa ação que eliminou esses registros que poderiam ter sido naturalmente concedidos. Há provedores gratuitos, há. Ou seja, que dão acesso gratuito. Nas Universidades como o objetivo não é de lucro, muitas vezes permitem que os alunos, exclusivamente os alunos usem, que os professores usem, enquanto na Universidade. Isso não significa exatamente ser um provedor público. É um direito do aluno de poder usar como ferramenta de trabalho enquanto está na Universidade. Por princípio ele não poderia usar este acesso fora da Universidade. O provedor normal, o que que o provedor faz? O provedor é aquele elemento que faz a interligação entre o usuário e a operadora de telecomunicações, que por sua vez, coloca na rede Internet, ou seja, eu tenho um provedor, uma série de conexões, dependendo da quantidade de usuários, dos serviços oferecidos, uma série de conexões com as operadoras de telecomunicações. O usuário, a Débora quando quer entrar na Internet, ela escolheu o provedor A, que sou eu para ela

entrar na Internet, então ela tem que discar para o provedor A e dizer eu sou a Débora e a minha senha é 123, o provedor A checa. Libera você pra entrar na Internet, esse é o papel do provedor. O provedor o que é que ele dá além de o seu acesso na Internet? O provedor oferece serviços de *e-mail* onde você pode utilizar o seu *e-mail*, com mais ou menos possibilidade de arquivo, de guardar mais ou menos tempo de *e-mail*, enfim, com antivírus, essas coisas todas. Ah, ele lhe dá direito também a arquivar uma página, ele lhe oferece voz por IP, enfim, sobre essa, em cima dessa conexão, dessa relação comercial, os provedores vão criando as várias camadas de valor para atrair o usuário. E faz com que o seguinte: no início, os provedores começaram a cobrar R$ 35,00 por 10 horas de uso, pra fazer face aos elevados custos que eram cobrados pelas operadoras. Depois, com a vinda da competição, passou a ser R$ 35,00 por 20 horas de uso, até que chegou um provedor, que foi o Uol e disse: não, vão ser R$ 35,00 e eu vou dar acesso ilimitado. As operadoras que existem no Brasil. Existem três grandes operadoras, quatro, cinco, uma em cada região, regiões 1, 2 e 3. Região 3 em São Paulo, é a Telefônica, isto para telefonia fixa, “ta”. Na zona do Rio é a Telemar, que agora se chama Oi, e a Brasil Telecom “ta” lá no Centro-Oeste, Brasília centro-oeste. Então essas são as três grandes operadoras, e tem a Embratel que atuava no Brasil inteiro, então a Embratel continua atuando no Brasil inteiro. Essas poucas operadoras também trabalham com Internet Então, hoje nós temos um nível de concentração muito elevado e que tende a aumentar. Então, em São Paulo hoje, você tem basicamente a Telefônica, e hoje você tem o acesso pelas redes de TV a cabo. Então você tem a Net que é da Globo e você tem a TVA, a TVA é da Abril. Hoje você tem outros tipos de acesso, especialmente em redes sem fio, via rádio, etc., etc., um pouco mais raros, mas que tendem a crescer muito. Então essas são basicamente as opções que você tem de acesso. Agora, também, o celular vem se transformando, vem sendo cada vez mais um instrumento, vem sendo mais um PC praticamente e, portanto você talvez veja na Internet com o celular também e aí praticamente já não tem como competir: o que era obrigatório entre a operadora e o usuário e o provedor está começando a se desmontar pela força do poder econômico, então os provedores começam a perder espaço, o que é muito ruim, é muito ruim porque a competição tende a desistir, você começa a ver a perda da qualidade pelas operadoras, o número de clientes que eles tem para atender começa a ser sacrificado, porque não vão atender bem a tanta gente, não vão ser eficientes no

atendimento, não vão se preocupar com o serviço porque não tem competição nessas regiões e existe, queira ou não, como um “cartel". Oi/Telemar que poderia estar entrando em São Paulo para competir e não vem e a Telefônica não vai pra o Rio. Então, quer dizer, nós vivemos uma situação onde a política infelizmente hoje, “ta” praticamente fechando os olhos e permitindo que a competição não aconteça. Então nós estamos pagando muito caro por essa guerra pelo acesso à Internet comercial.

Quanto à segurança, você falou do livro (o manual prático para investigação dos crimes cibernéticos), porque do surgimento dele. Os juízes, especialmente os procuradores, tiveram que começar a entender como entender, como cuidar destes fatos. Não que as leis não existissem, mas como eles passariam a cuidar do tratamento das fraudes, dessas histórias que começaram a acontecer na Internet. E aí, a cada exemplo que foi surgindo, foi sendo criada a necessidade de uma solução. Eles se encontraram e começaram a pensar, começaram a se reunir, começaram a julgar. Se o problema, se o processo chegava para ser avaliado, pra ser julgado por eles, eles tinham que encontrar as peças, as formas de aplicar as regras, e por isso, o que eles fizeram aí foi a compilação de algumas regras, de alguns princípios, que nacionais, quer exemplos do estrangeiro “tá” e esses livros se destinam essencialmente a procuradores, a juízes, para que eles saibam como olhar, como interpretar e como aplicar as regras. E aí tem algo muito simbólico que está neste livro que é assim: existe um acordo entre os Provedores e a Justiça no sentido de que uma vez configurado o ilícito, o Provedor ele não pode, não tem o direito, nem o poder de polícia de prender ninguém, agora, na medida em que ele receber uma informação, até da Polícia, de que há um indiciante praticado por um usuário daquele provedor, o provedor imediatamente toma medidas no sentido de se fazer os registros, como se fosse fazer uma gravação telefônica, de registro telefônico para que, quando vier a solicitação da justiça, ele já tenha pronto para lhe entregar. Então, num entendimento precípuo e de colaboração entre órgãos judiciários e os provedores e a comunidade.

GOVERNANÇA ELETRÔNICA

Comitê Gestor. Ele não existe “prá” fazer gestão de ninguém, ao mesmo tempo ele existe “prá” fazer gestão de tudo. E ele existe para cuidar de redes, “prá”

cuidar das relações entre Governo e a sociedade civil, o Comitê Gestor ele tem um formato que é muito interessante, que é chamado de *multistakeholder*, todo tipo de segmento está representado. E isso é ótimo, quer dizer isso valoriza e revitaliza toda a sociedade envolvida, quer dizer qualquer problema que aconteça com determinado segmento é trazido para o Comitê Gestor para ser discutido e ali os vários parceiros podem interagir e o Comitê Gestor tomar decisões do tipo, sobre a forma de resolução.

As resoluções do Comitê Gestor têm forma de lei? Não. Mas o interessante é isso, embora não tenham forma de lei, tem regras, normalmente técnicas, elas são auto-aplicáveis. Quem não aplicar vai estar fora do contexto, não consegue funcionar. Então, é muito efetivo e é muito respeitado. A ICANN, ela tem muito mais, em alguns pontos sim. Nós estamos falando agora de governança da Internet “ta”? A ICANN, ela tem que olhar, tem que cuidar da distribuição dos números IP, com certeza o Demi já falou sobre isso, “tá”, o que é que significam os números IP, da distribuição de nomes, dos servidores que fazem as funções do DNS ( ), então a ICANN tem uma visão muito mais globalizada. Nós hoje, até bem pouco tempo, usávamos apenas o alfabeto latino, ou arábico, para qualquer comunicação. E os chineses, que são a maior população, porque não utilizar os caracteres da linguagem deles. Por que não usar caracteres árabes? Enfim, começaram a surgir estas questões que são questões importantes. Os russos, eles disseram: olha, nós somos muito importantes, não podemos ser entendidos e temos que entender todo mundo. Ou eles vão ter que usar os caracteres que não nos lhe são familiares, do alfabeto cirílico pra poder se fazer entender isso não é justo. Então, fazer com que essas diferentes coisas se comuniquem entre si e possam ser entendidas. E ao mesmo tempo, colocar nisso, camadas de segurança. Agora, isso pressupõe e envolve, muito dinheiro, muito tempo, muita inteligência.

Mas no nível Brasil, é o Brasil que cuida. Por exemplo, se os provedores têm esse problema de que a polícia quer que eles dêem uma informação que eles não podem dar com autorização judicial, nós temos que ter uma solução que deixe isso claro, então nós fizemos um acordo, cujo resultado está aí, com o Ministério Público, que as coisas ficaram claras. Ah, vamos fazer pontos de troca de tráfego por que: antigamente, quando você entrava na Internet, e eu queria estar fazendo um *chat* com você, você podia estar na casa ao lado da minha, mas nossa comunicação ia até Miami e voltava, porque esse era o circuito, nós, o que que o Comitê Gestor fez:

concluiu pontos de troca de tráfego, que identificaram que o destino daqueles pacotes, daquela comunicação era local, não precisava ir a Miami. Isto foi reduzindo custos. O papel do Comitê Gestor é de governança da Internet, mais do que a gestão propriamente dita. E governança é uma palavra que se está usando cada vez mais, porque ela tem: um cunho político, técnico, científico, acadêmico, comercial, tem um pouco de tudo isso embutido nela.

FUTURO DA INTERNET

Olha, o futuro é assim, eu tenho a impressão que o futuro tende em que as pessoas cada vez mais a viverem em comunidades, e em comunidades pequenas. Nós estamos voltando ao início dos tempos, eu acho que vai haver uma regressão sim. Hoje você "ta" aqui fazendo uma entrevista. Nós poderíamos estar fazendo esta entrevista você em Bauru, e eu aqui, através de uma videoconferência, isso vai ser cada vez mais disponível no futuro. Ah, obrigatoriamente o corpo humano mudará, em função da Internet. Imagino o seguinte. Eu não imagino que uma criança, dentro de duas ou três gerações escreva manualmente, ela vai teclar. Então, a parte do cérebro que ela utilizava para o desenvolvimento da escrita vai ser modificado, vai ser diferente, o condicionamento vai ser diferente. E da mesma forma, o tipo da consciência. Por quê? Porque o que ele precisava desenvolver em termos lógicos, passa a ter ferramentas que fazem isso. Ele não precisa de saber que 2 + 2 são 4. Coloca 2 asterístico 2, ele sabe que é 4. Então, vai haver efetivamente uma liberalização de espaço de memória que nós hoje utilizamos pra fazer isso, e com certeza, isso propiciará um crescimento real. Ah, seremos tão sedentários porque vamos estar sentados na frente do computador? Não, como lhe disse, a vida continuará porque aqui num celular desses "ta" lá tudo que nós precisamos para acessar a Internet; hoje aqui eu tenho comunicação, eu tenho planilha eletrônica, eu tenho *e-mail*, eu tenho tudo o que eu quiser. Então eu vou continuar, poder continuar me movimentando e tendo, privacidade. Com certeza, privacidade se perde num ônibus porque não é qualquer pessoa vai sentada onde você está. Se você vai usar o seu celular, você deixará de ter um CPF, um RG, um número de título de eleitor e no seu celular, você terá um número IP e você será um número IP. Você será Débora ou 201.ponto e quando você chegar com o celular ou qualquer outra ferramenta que ainda venha a surgir perto de uma caixa de banco, perto de uma

urna eletrônica de uma votação, perto de qualquer portaria de prédio, você não precisa nem se identificar porque já tem um sensor que leu que você ta passando ali, ta. Enfim, essa é a evolução e esse obrigatoriamente será o futuro. Esse. Pode-se chamar esse de futuro da Internet? Não é só a Internet é a tecnologia em geral. A Internet é mola mestra pra esse desenvolvimento.

INCLUSÃO DIGITAL

Eu sou um pouco crítico na forma com que se pensa a inclusão digital no Brasil, porque, num país em que nós temos que pensar ainda em bolsa família, pensar em inclusão digital é inverter a hierarquia das necessidades fisiológicas das pessoas. Habitação, alimentação, há que tratar primeiro disso. Só pra que nós possamos dizer que nós temos uma penetração de Internet de 90%, mas os meninos não podem se alimentar, morrem. Precisa ter muito cuidado da forma como se aborda isso. É muito lindo dizer: os meninos vão ter um computador, todo mundo vai ter um computador na escola. Ótimo. E os meninos vão à escola? Ta? E os meninos estão sendo alimentados? Gente que tem que receber do governo bolsa família, como se de uma esmola se tratasse, eu pergunto: isso serve para os políticos, para alavanca pra se eleger, ou vai servir efetivamente. Claro que a desigualdade é muito grande. Há que se criar desenvolvimento no país capaz de auto-sustentação das pessoas se cuidarem, das pessoas crescerem e terem direito à vida digna. E aí, a inclusão acontece naturalmente, não tem que ser um negócio forçado. Eu quando vejo um Presidente da República chegar e dizer: até 2010 eu quero todas as escolas com Internet, isso aí é muito bonito, mas isso interessa somente ao bolso de alguns que vão produzir bens, serviços e vão ter resultados políticos nisso. Então eu sou pouco crítico e é a minha visão.

PERGUNTAS COMPLEMENTARES

Débora: E só pra finalizar. Crimes cibernéticos, essas ocorrências são preocupantes?
Antônio: Claro que preocupam.
Débora: Então eles têm crescido.

Antônio: Mas o caminho que nós temos que escolher é o caminho da educação, não é o caminho da punição.

Débora: Embora essas pessoas têm como ser punidas, você falou, com a legislação que "a gente" já tem.

Antônio: Sem dúvida. Não existe nem Internet 100% segura, nunca vai existir, nada é 100% seguro, nem existe irreastribilidade, tudo é rastreável. Pensem o que quiserem, não existe crime perfeito também no mundo virtual.

Débora: Então, o criminoso não pode alegar: eu não cometi crime nenhum, porque foi na Internet, você não tem lei pra me punir. Ele pode? Ele não pode alegar isso?

Antônio: O que ele pode alegar e aí é, digamos uma zona cinzenta que existe é a seguinte: eu aqui no nosso escritório eu tenho uma rede *wireless*, *Ok*? Se eu não tiver o cuidado suficiente e proteger essa rede *wireless*, você vai parar o teu carro ali na porta, vai ligar o teu *notebook* e vai ter o acesso.

Débora: É, ele conseguiu detectar.

Antônio: *Ok*. Ele conseguiu detectar, mas não conseguiu entrar na rede.

Débora: Não, porque elas (as redes sem fio) pedem a chave.

Antônio: Isso. Mas quem é malandro, e sabe das coisas consegue burlar isso. Então vai fazer o seguinte: vai entrar na rede e vai cometer uma fraude, vai entrar numa conta bancária e vai tirar um dinheiro. E aí, vai acontecer o seguinte: o cara de segurança do Banco vai dizer: olha, foi através do IP 201.010.350.001. A quem estava atribuído esse IP nessa hora? Ao Antônio Tavares.Vai lá o Antônio Tavares. Eu vou dizer: eu não fiz, mas eu vou ter que provar que não fiz, ta? E é difícil você, o ônus da prova é meu e é difícil provar que não estava.

Débora: E no Senado, na Câmara, tem algum projeto interessante sobre isso?

Antônio: Tem verdadeiros monstros, verdadeiros absurdos, não tem nada que... O do Eduardo Azeredo.

Débora: O do Eduardo Azeredo.

Antônio: São peças jurídicas que, sinceramente...

Débora: Não são necessárias?

Antônio: Elas estão desalinhadas com o futuro. Elas poderão eventualmente servir alguns interesses que eu não vou querer referir aqui.

Débora: E a Polícia Federal, como você vê, ela tem atuado em relação aos crimes cibernéticos?

Antônio: A Polícia Federal tem muito boa vontade, a Polícia Federal tem os seus próprios vícios, seus próprios métodos. Nós entendemos que a Polícia Federal tem que ter uma integração muito grande com a inteligência do país, com a Associação Brasileira (ABIN) sobre inteligência, isso sim, nós entendemos, é natural. Agora, a Polícia Federal não é o órgão supremo da Justiça tá? Ela cumpre sua função. Então, ela tem que se submeter da mesma forma às regras que valem pra todos, ou seja: a Polícia Federal não pode chegar, e, sem autorização judicial, sem um mandado, interferir. Seja no provedor, seja na casa do usuário. Agora, quando ela investiga, quando ela tem provas e quando ela consegue o mandado judicial, ela pode e deve fazer isso.

Débora: Eu tenho acompanhado a atuação deles, especialmente com crimes bancários.

Antônio: É notável. Embora ainda falte um pouquinho de sincronia internamente entre o policial federal, comum e o policial federal especializado na área de cibernética. Falam e pensam...

Débora: Então obrigada. Bom dia.

Observações: O entrevistado também optou por conhecer o roteiro previamente e respondê-lo, de acordo com sua própria dinâmica narrativa. No final, acrescentamos questões complementares, de modo a esclarecer alguns pontos.

Tempo total: 00:41:98

Transcrito por Débora Corrêa Chama

Bauru (SP), 14/02/08: 22:28

ANEXOS

ANEXO A

TABELAS

C2 – PROPORÇÃO DE INDIVÍDUOS QUE ACESSARAM A INTERNET – ÚLTIMO ACESSO

Percentual sobre o total da população[1]

Percentual (%)		Há menos de 3 meses	Nos últimos 12 meses	Há mais de 12 meses	Nunca acessou a Internet
Total		**27,82**	**31,25**	**2,07**	**66,68**
REGIÕES DO PAÍS	SUDESTE	30,76	34,56	2,33	63,11
	NORDESTE	18,38	21,02	1,38	77,59
	SUL	29,37	33,57	2,61	63,81
	NORTE	21,59	24,2	1,34	74,46
	CENTRO-OESTE	34,37	37,06	1,88	61,06
SEXO	Masculino	30,3	33,79	2,24	63,97
	Feminino	25,59	28,97	1,91	69,12
GRAU DE INSTRUÇÃO	Analfabeto/Ed. infantil	4,29	5,19	0,48	94,33
	Fundamental	22,17	26,3	1,57	72,14
	Médio	42,31	48,52	4,54	46,94
	Superior	82,03	84,7	2,25	13,05
FAIXA ETÁRIA	De 10 a 15 anos	38,42	44,88	1,59	53,53
	De 16 a 24 anos	48,71	55,15	3,68	41,17
	De 25 a 34 anos	35,13	39,13	3,74	57,12
	De 35 a 44 anos	20,63	22,43	1,36	76,21
	De 45 a 59 anos	11,25	11,84	0,66	87,5
	De 60 anos ou mais	2,62	3,07	0,13	96,79
RENDA FAMILIAR	ATÉ R$300	5,07	6,12	1,2	92,68
	R$301-R$500	10,43	12,53	1,39	86,07
	R$501-R$1000	23,26	27,25	2,24	70,52
	R$1001-R$1800	45,66	49,82	2,66	47,52
	R$1801 OU MAIS	64,39	67,87	2,05	30,08
CLASSE SOCIAL[3]	A	93,43	94,85	0,23	4,92
	B	66,63	70,56	1,72	27,71
	C	31,21	36	2,86	61,15
	DE	8,73	10,74	1,49	87,77
SITUAÇÃO DE EMPREGO	Trabalhador	30,8	33,87	2,31	63,81
	Desempregado	26,94	34,91	1,85	63,23
	Não integra a pop. ativa[2]	22,97	26,59	1,68	71,74

Fonte: Nic.br – jul/ago 2006.

1 Base: 10.510 entrevistados.

2 Na categoria não integra população ativa estão contabilizados os estudantes, aposentados e as e donas de casa.

3 O critério utilizado para classificação leva em consideração a educação do chefe de família e a posse de uma série de utensílios domésticos, relacionando-os a um sistema de pontuação. A soma dos pontos alcançada por um domicílio é associada a uma classe sócio-econômica específica (A, B, C, D, E).

C2 – PROPORÇÃO DE INDIVÍDUOS QUE ACESSARAM A INTERNET – ÚLTIMO ACESSO

Percentual sobre o total da população[1]

Percentual (%)		Há menos de 3 meses	Nos últimos 12 meses	Há mais de 12 meses	Nunca acessou a Internet
Total		**34**	**38**	**3**	**59**
REGIÕES DO PAÍS	SUDESTE	37	41	2	57
	NORDESTE	28	31	2	67
	SUL	37	42	4	54
	NORTE	28	31	1	68
	CENTRO-OESTE	38	42	3	55
SEXO	Masculino	37	40	2	58
	Feminino	32	36	3	61
GRAU DE INSTRUÇÃO	Analfabeto/Ed. infantil	7	8	1	91
	Fundamental	29	33	2	66
	Médio	51	59	5	36
	Superior	78	81	4	15
FAIXA ETÁRIA	De 10 a 15 anos	53	58	1	41
	De 16 a 24 anos	60	66	4	30
	De 25 a 34 anos	45	49	4	47
	De 35 a 44 anos	24	28	4	69
	De 45 a 59 anos	12	14	1	85
	De 60 anos ou mais	3	4	-	96
RENDA FAMILIAR	Até R$380	12	15	1	84
	R$381-R$760	21	25	3	72
	R$761-R$1140	38	42	3	54
	R$1141-R$1900	51	55	2	43
	R$1901-R$3800	67	73	1	25
	R$3801 ou mais	72	74	3	23
CLASSE SOCIAL[3]	A	89	92	2	6
	B	66	70	3	27
	C	38	43	3	53
	DE	14	16	1	83
SITUAÇÃO DE EMPREGO	Trabalhador	37	41	3	57
	Desempregado	35	40	6	54
	Não integra a pop. ativa[2]	30	33	2	65

Fonte: Nic.br – set/nov 2007.
1 Base: 17.000 entrevistados. Entrevistas realizadas em zona urbana.
2 Na categoria não integra população ativa estão contabilizados os estudantes, aposentados e as e donas de casa.
3 O critério utilizado para classificação leva em consideração a educação do chefe de família e a posse de uma série de utensílios domésticos, relacionando-os a um sistema de pontuação. A soma dos pontos alcançada por um domicílio é associada a uma classe sócio-econômica específica (A, B, C, D, E).
Veja a tabela de erros estatísticos aproximados para cada variável deste indicador.
Números calculados sobre bases estatísticas pequenas e que possuem erro estatístico acima de 4%.

ANEXO B

Países signatários da Convenção sobre os Cibercrimes de Budapest

Opening for signature: Place: Budapest Date : 23/11/2001
Entry into force: Conditions: 5 Ratifications including at least 3 member States of the Council of Europe Date : 1/7/2004

Status as of: 24/1/2008 - Member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra										
Armenia	23/11/2001	12/10/2006	1/2/2007							
Austria	23/11/2001									
Azerbaijan										
Belgium	23/11/2001									
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X				
Croatia	23/11/2001	17/10/2002	1/7/2004							
Cyprus	23/11/2001	19/1/2005	1/5/2005							
Czech Republic	9/2/2005									
Denmark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Finland	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia										
Germany	23/11/2001									
Greece	23/11/2001									
Hungary	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Iceland	30/11/2001	29/1/2007	1/5/2007		X		X			
Ireland	28/2/2002									
Italy	23/11/2001									
Latvia	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein										
Lithuania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003									
Malta	17/1/2002									
Moldova	23/11/2001									
Monaco										
Montenegro	7/4/2005			55						
Netherlands	23/11/2001	16/11/200	1/3/2007				X	X		
Norway	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Poland	23/11/2001									
Portugal	23/11/2001									
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005			55						
Slovakia	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spain	23/11/2001 r									
Sweden	23/11/2001									
Switzerland	23/11/2001									
the former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Turkey										
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
United Kingdom	23/11/2001									
Non-member States of the Council of Europe										
Canada	23/11/2001									
Costa Rica										
Japan	23/11/2001									
Mexico										
South Africa	23/11/2001									
United States	23/11/2001	29/9/2006	1/1/2007		X	X	X			
Total number of signatures not followed by ratifications:				**21**						
Total number of ratifications/accessions:				**22**						

Source: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=1/24/2008&CL=ENG **Notes**:(55) Date of signature by the state union of Serbia and Montenegro.
a: Accession - s: Signature without reservation as to ratification - su: Succession - r: Signature "ad referendum".
R.: Reservations - D.: Declarations - A.: Authorities - T.: Territorial Application - C.: Communication - O.: Objection.

ANEXO C

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 9.296, de 24 de julho de 1996, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, 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 9.296, de 24 de julho de 1996, Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, 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 Capítulo V do Título I da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do seguinte art. 141-A:

"**Art. 141-A.** As penas neste Capítulo aumentam-se de dois terços caso os crimes sejam cometidos por intermédio de rede de computadores, dispositivo de comunicação ou sistema informatizado."

Art. 3º O Título I da Parte Especial do Código Penal fica acrescido do Capítulo VI-A, assim redigido:

"Capítulo VI-A

DOS CRIMES CONTRA REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

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

Art. 154-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 1º Nas mesmas penas incorre quem, permite, facilita ou fornece a terceiro meio não autorizado de acesso a rede de computadores, dispositivo de comunicação 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, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.
§ 3º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de acesso.

Obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica ou digital ou similar

Art. 154-B. Obter dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:
Pena – detenção, de 2 (dois) a 4 (quatro) anos, e multa.

§ 1º Nas mesmas penas incorre quem mantém consigo, transporta ou fornece dado ou informação obtida nas mesmas circunstâncias do “caput”, ou desses se utiliza alem do prazo definido e autorizado.
§ 2º Se o dado ou informação obtida desautorizadamente é fornecida a terceiros pela rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.
§ 3º 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 suas subsidiárias.

Dispositivo de comunicação, sistema informatizado, rede de computadores e defesa digital

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

I – dispositivo de comunicação: o computador, o telefone celular, o processador de dados, os instrumentos de armazenamento de dados eletrônicos ou digitais ou similares, os instrumentos de captura de dados, os receptores e os conversores de sinais de rádio ou televisão digital ou qualquer outro meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar;

II – sistema informatizado: o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III – rede de computadores: os instrumentos físicos e lógicos através dos quais é possível trocar dados e informações, compartilhar recursos, entre máquinas, representada pelo conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem de comum acordo a um conjunto de

regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial;

IV - código malicioso: o conjunto de instruções e tabelas de informações ou programa de computador ou qualquer outro sistema capaz de executar uma seqüência de operações que resultem em ação de dano ou de obtenção indevida de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal;

V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob uma forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado, incluindo um programa, apto a fazer um sistema informatizado executar uma função;

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.

Divulgação ou utilização indevida de informações contidas em banco de dados

Art. 154-D Divulgar, utilizar, comercializar ou disponibilizar informações contidas em banco de dados com finalidade distinta da que motivou o registro das mesmas, incluindo-se informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas naturais ou jurídicas, ou a dados de pessoas naturais referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, 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.

§ 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

§ 2º Se o crime ocorre em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.“

Art. 4º O § 4º do art. 155 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte inciso V:

“**Art. 155.** .....
.....

§ 4º .....
.....

V - mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares”.
..... (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:

“**Dano por difusão de código malicioso eletrônico ou digital ou similar**

Art. 163-A. Criar, 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.

Dano qualificado por difusão de código malicioso eletrônico ou digital ou similar

§ 1º Se o crime é cometido com finalidade de destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado 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.

Difusão de código malicioso eletrônico ou digital ou similar seguido de dano

§ 2º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado, e as circunstâncias demonstram que o agente não quis o resultado, nem assumiu o risco de produzi-lo:

Pena – reclusão, de 3 (dois) a 5 (cinco) anos, e multa.

§ 3º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

Art. 6º O Capitulo VI do Título II do Código Penal passa a vigorar acrescido do seguinte artigo:

“**Difusão de código malicioso**

Art. 171-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por qualquer forma indevida, induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, à rede de computadores, dispositivo de comunicação ou a sistema informatizado, com obtenção de vantagem ilícita, em prejuízo alheio:

Pena – reclusão, de um a três anos.

§ 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de difusão de código malicioso.

Art. 7º O Código Penal passa a vigorar acrescido do seguinte art. 183-A:

“**Art. 183-A.** Para efeitos penais, equiparam-se à coisa o dado, informação ou unidade de informação em meio eletrônico ou digital ou similar, a base de dados armazenada, o dispositivo de comunicação, a rede de computadores, o sistema informatizado, a senha ou similar ou qualquer instrumento que proporcione acesso a eles.”

Art. 8º 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. 9º O art. 298 do Código Penal passa a vigorar acrescido do seguinte parágrafo único:

“**Art. 298**. .....

.....

Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico ou digital ou similar portátil de captura, processamento, armazenamento e transmissão de informações.

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer outro dispositivo portátil capaz de capturar, processar, armazenar ou transmitir dados, utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar.(NR)”

Art. 10. O Código Penal passa a vigorar acrescido do seguinte art. 298-A:

“**Falsificação de telefone celular ou meio de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado**

Art. 298-A. Criar ou copiar, indevidamente, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de rádio freqüência ou telefonia celular, ou qualquer instrumento que permita o acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado:

Pena – reclusão, de um a cinco anos, e multa.”

Art. 11. O § 6º do art. 240 do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar acrescido do seguinte inciso V:

“**Art. 240.** .....

.....

Furto qualificado

§ 6º .....

.....

V – mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra rede de computadores, dispositivos de comunicação ou sistema.

..... (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:

Dano por difusão de código malicioso eletrônico ou digital ou similar

Art. 262-A. Criar, 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.

Dano qualificado por difusão de código malicioso eletrônico ou digital ou similar

§ 1º Se o crime é cometido com finalidade de destruição, inutilização, deterioração, alteração, dificultação 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.

Difusão de código malicioso eletrônico ou digital ou similar seguido de dano

§ 2º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento não autorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado, e as circunstâncias demonstram que o agente não quis o resultado, nem assumiu o risco de produzi-lo:

Pena – reclusão, de 3 (dois) a 5 (cinco) anos, e multa.

§ 3º A pena é aumentada de sexta parte se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

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

Capítulo VII-A

DOS CRIMES CONTRA REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

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

Art. 339-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado sem autorização do legítimo titular, quando exigida:

Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 1º Nas mesmas penas incorre quem permite, facilita ou fornece a terceiro meio não autorizado de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado.

§ 2º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de acesso.

Obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica ou digital ou similar

Art. 339-B. Obter dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

Pena – detenção, de 2 (dois) a 4 (quatro) anos, e multa.

§ 1º Nas mesmas penas incorre quem mantém consigo, transporta ou fornece dado ou informação obtida nas mesmas circunstâncias do *caput*, ou deles se utiliza além do prazo definido e autorizado.

§ 2º Se o dado ou informação obtida indevidamente é fornecida a terceiros pela rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.

Dispositivo de comunicação, sistema informatizado e rede de computadores

Art. 339-C. Para os efeitos penais considera-se:

I – dispositivo de comunicação: o computador, o telefone celular, o processador de dados, os instrumentos de armazenamento de dados eletrônicos ou digitais ou similares, os instrumentos de captura de dados, os receptores e os conversores de sinais de rádio ou televisão digital ou qualquer outro meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar;

II – sistema informatizado: o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

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

IV – código malicioso: o conjunto de instruções e tabelas de informações ou programa de computador ou qualquer outro sistema capaz de executar uma seqüência de operações que resultem em ação de dano ou de obtenção indevida de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal;

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, incluindo-se programas, apta a fazer um sistema informatizado executar uma função;

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.

Divulgação ou utilização indevida de informações contidas em banco de dados

Art. 339-D Divulgar, utilizar, comercializar ou disponibilizar informações contidas em banco de dados com finalidade distinta da que motivou o registro das mesmas, incluindo-se informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas naturais ou jurídicas, ou a dados de pessoas naturais referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, 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.

§ 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

§ 2º Se o crime ocorre em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.

Art. 14. O 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 Capítulo VIII-A, assim redigido:

Capítulo VIII-A

DISPOSIÇÕES GERAIS

Art. 267-A. Para efeitos penais, equiparam-se à coisa o dado, informação ou unidade de informação em meio eletrônico ou digital ou similar, a base de dados armazenada, o dispositivo de comunicação, a rede de computadores, o sistema informatizado, a senha ou similar ou qualquer instrumento que proporcione acesso a eles.

Art. 15. O Capítulo I do Título VI 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. 281-A, assim redigido:

Difusão de código malicioso

Art. 281-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por qualquer forma indevida, induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, à rede de computadores, dispositivo de comunicação ou a sistema informatizado, com obtenção de vantagem ilícita, em prejuízo alheio:

Pena – reclusão, de um a três anos.

Parágrafo único. A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de difusão de código malicioso.

Art. 16. O art. 2º da Lei nº 9.296, de 24 de julho de 1996, passa a vigorar acrescido do seguinte § 2º, renumerando-se o parágrafo único para § 1º:

"Art. 2º .....
.....

§ 2º O disposto no inciso III do *caput* não se aplica quando se tratar de interceptação do fluxo de comunicações em rede de computadores, dispositivo de comunicação ou sistema informatizado." (NR)

Art. 17. O art. 313 do Decreto-Lei nº 3.689, de 3 de outubro de 1941, Código do Processo Penal (CPP), passa a vigorar acrescido do seguinte inciso V:

"**Art. 313.** .....
.....

V – punidos com detenção, se tiverem sido praticados contra rede de computadores, dispositivo de comunicação ou sistema informatizado, ou se tiverem sido praticados mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado, nos termos da lei penal.(NR)"

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

Art. 19. 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. 20. O art. 9º da Lei nº 8.078, de 11 de setembro de 1990 passa a vigorar com a seguinte redação:

"**Art. 9º** .....
.....

Parágrafo único. O disposto neste artigo se aplica à segurança digital do consumidor, mediante a informação da necessidade do uso de senhas ou similar para a proteção do uso do produto ou serviço e para a proteção dos dados trafegados, quando se tratar de dispositivo de comunicação, sistema informatizado ou provimento de acesso a rede de computadores ou provimento de serviço por meio dela.(NR)"

Art. 21 O art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

"**Art. 20**. .....
.....

§ 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza, inclusive pela criação, manutenção ou divulgação de sítios, páginas, portais ou comunidades na rede mundial de computadores:

.....

§ 3º .....

.....

III – a retirada do sítio, página, portal ou comunidade de conteúdo discriminatório ou preconceituoso.

..... (NR)”

Art. 22 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, fornecer, divulgar, publicar ou manter consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente: (NR)”

Art. 23. O responsável pelo provimento de acesso a rede de computadores é obrigado a:

I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o estrito 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 por esta gerados, cujo fornecimento será feito exclusivamente à autoridade investigatória e dependerá de prévia e expressa autorização judicial;

II – tornar disponíveis à autoridade competente, por expressa autorização judicial, os dados e informações mencionados no inciso I, no curso de auditoria técnica a que forem submetidos;

III – fornecer, por expressa autorização judicial, no curso de investigação, os dados de que cuida o inciso I deste artigo;

IV – preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de que cuida o inciso I deste artigo e outras informações solicitadas por aquela investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

V – informar, de maneira sigilosa, à autoridade policial competente, denúncia da qual tenha tomado conhecimento 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;

VI – informar ao seu usuário que o uso da rede sob sua responsabilidade obedece às leis brasileiras e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras;

VII – alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores, dispositivo de comunicação e sistema informatizado;

VIII – divulgar aos seus usuários, em local destacado, as boas práticas de segurança no uso de rede de computadores, dispositivo de comunicação e sistema informatizado.

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

§ 2º Os dados e procedimentos de que cuida o inciso I deste artigo deverão estar aptos a atender ao disposto nos incisos II , III e IV no prazo de cento e

oitenta dias, a partir da promulgação desta Lei.

§ 3º O responsável citado no *caput* deste artigo que não cumprir o disposto no § 2º, 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 verificação ou solicitação, aplicada em dobro em caso de reincidência, que será imposta mediante procedimento administrativo, pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração.

§ 4º 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. 24. Não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso, hospedagem e dados de conexões realizadas, quando constatada qualquer conduta criminosa.

Art. 25. Esta Lei entrará em vigor sessenta dias após a data de sua publicação.

Sala da Comissão,

, Presidente

, Relator

ANEXO D

Por que é preciso tipificar os crimes de informática ou cibercrimes

- ✓ Porque a Constituição Federal diz em seu art. 5º, do Título I, Capítulo I,dos Direitos e Garantias Fundamentais, no inciso XXXIX, que:
- ✓ "XXXIX – não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;"

- ✓ No Direito Penal não se admite a analogia para prejudicar o réu; ou seja, a conduta deve estar claramente definida no texto da lei. Assim, algumas condutas criminosas mediante o uso de rede de computadores, dispositivo de comunicação ou sistema informatizado, devem estar claramente definidas na lei.

Por que é preciso alterar o Código Penal:

- ✓ Porque a Constituição Federal em seu art. 59, parágrafo único, diz que "Lei complementar disporá sobre a elaboração, redação, alteração e consolidação das leis." Esta lei é a Lei Complementar nº 95, de 26 de fevereiro de 1998, que no seu art. 7º, inciso IV, diz que:
  "IV – o mesmo assunto não poderá ser disciplinado por mais de uma lei, exceto quando a subseqüente se destine a complementar lei considerada básica, vinculando-se a esta por remissão expressa.".

No nosso caso, a lei básica é o Código Penal, que está sendo alterado com mudanças de redação ou inclusão de novos artigos, parágrafos, incisos etc., em complemento à lei existente.

Considerações Gerais sobre Direito Penal

O Direito Penal é um dos ramos do Direito Público que define as infrações que devem ser punidas com mais rigor pelo Estado, e suas respectivas penas, estando a maior parte delas previstas no Código Penal. Inclui os crimes punidos com privação da liberdade, restrição de direitos e, também, multa. Inclui também as contravenções, definidas na Lei de Contravenções Penais e punidas com prisão simples, com a possibilidade de aplicação isolada de multa.

Em regra, para que exista a responsabilidade penal de uma pessoa em relação a um crime é necessário que ela tenha agido, ou se omitido, com intenção ou vontade, ou seja, com dolo.

Quando expressamente previsto na lei penal, é possível responsabilizar penalmente uma pessoa que age ou se omite por negligência, imprudência ou imperícia, ou seja, com culpa.

O Código Penal

O Código Penal está dividido em duas partes: a Parte Geral (arts. 1º a 120) e a Parte Especial (arts. 121 a 361). Cada parte é dividida em Títulos, estes em Capítulos e estes em Seções, de acordo com o bem jurídico que se quer proteger (como a vida, o patrimônio etc.). A essa divisão dá-se o nome de topologia, ou localização dos crimes dentro do código.

A Parte Geral trata da Aplicação da Lei Penal (arts 1º a 12), do Crime (arts. 13 a 24), da Imputabilidade Penal (arts. 26 a 28), do Concurso de Pessoas (arts. 29 a 31), das Penas (arts. 32 a 95), das Medidas de Segurança (arts. 96 a 99), da Ação Penal (arts. 100 a 106), da Extinção da Punibilidade (arts.107 a 120).

A Parte Especial trata dos Crimes contra a Pessoa (arts. 121 a 154), dos Crimes contra o Patrimônio (arts. 155 a 183), dos Crimes contra a Propriedade Imaterial (arts. 184 a 196), dos Crimes contra a Organização do Trabalho (arts. 197 a 207), dos Crimes contra o Sentimento Religioso e contra o Respeito aos Mortos (arts. 208 a 212), dos Crimes contra os Costumes (arts. 213 a 234), dos Crimes contra a Família (arts. 235 a 249), dos Crimes Contra a Incolumidade Pública (arts. 250 a 285), dos Crimes contra a Paz Pública (arts. 286 a 288), dos Crimes contra a Fé Pública (arts. 289 a 311), dos Crimes contra a Administração Pública (arts. 312 a 359) e Disposições Finais (arts. 360 e 361).

Por que é preciso criar medidas administrativas como, por exemplo, a guarda de dados:

- ✓ Porque a Constituição Federal diz em seu art. 5º, do Título I, Capítulo I, dos Direitos e Garantias Fundamentais, no inciso II, que:
  "II – ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;"

- ✓ E a Lei Complementar nº 95, de 26 de fevereiro de 1998, que no seu art. 3º, inciso III, prescreve que:
  "Art. 3º A lei será estruturada em três partes básicas:
  .....
  III – parte final, compreendendo as disposições pertinentes às medidas necessárias à implementação das normas de conteúdo substantivo [...]."

No nosso caso, como acontece hoje, se a autoridade judicial requerer as informações de conexões informáticas, a parte responsável pela conexão pode alegar que não é obrigado por lei a guardar e muito menos a fornecer as informações.

A situação do SUBSTITUTIVO em Janeiro de 2008

O Projeto de Lei 76 de 2000, que tem apensados o PLC 89 de 2003 e o PLS 137 de 2000, teve o Substitutivo aprovado na Comissão de Educação (CE), está com o Substitutivo apresentado à Comissão de Constituição e Justiça (CCJ) do Senado Federal desde 30 de maio de 2007.

Sua tramitação foi suspensa para que fossem ouvidas a Comissão de Ciência e Tecnologia – CCT e a Comissão de Assuntos Econômicos – CAE. Na CCT em dezembro de 2007 o Substitutivo foi aprovado, tendo incorporado as emendas apresentadas na CCJ. Falta ser ouvida a CAE, o que deverá acontecer no primeiro trimestre de 2008.

As emendas na CCJ foram:

- ✓ - Emenda 01, supressiva, do Senador Flexa Ribeiro, excluindo a Defesa Digital;
- ✓ - Emenda 03, aditiva, do Senador Walter Pereira, a alteração da Lei Afonso Arinos, crimes de discriminação de raça e cor.
- ✓ - Emenda 04, de redação, do Senador Antonio Carlos Valadares, alterando a redação dos incisos I (guarda dos dados de conexões) III, IV (preservação imediata de dados) e V (repasse de denúncia à autoridade policial), e § 1º, todos do art. 21 antigo, agora art. 23 no novo Substitutivo.

Na CCT o Relator incluiu a alteração do Estatuto da Criança e Adolescente para tipificar o crime de “manter consigo” vídeos, fotos etc. relativos à pedofilia.

ANEXO E

RESENHA DIDÁTICA COM SUBSTITUTIVO APRESENTADO À CCT (COMISSÃO DE CIÊNCIA E TECNOLOGIA)

Resenha didática - tipificação e punição dos crimes de informática

PLS 76/2000 (PLC 89 de 2003 e PLS 137 de 2000)

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 ou similares, de rede de computadores, ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências (veja as razões em detalhe no Apêndice B).

O PLC 89, de 2003, de autoria do Deputado Luiz Piauhylino, altera:

- ✓ o **Código Penal**, Decreto-Lei nº 2.848, de 7 de dezembro de 1940;
- ✓ a **Lei de Interceptações Telefônicas**, Lei nº 9.296, de 24 de julho de 1996.

O PLS 76, de 2000, de autoria do Senador Renan Calheiros, tipifica crimes cometidos com o uso de informática mas sem alterar o Código Penal.

O PLS 137, de 2000, de autoria do Senador Leomar Quintanilha, determina o aumento das penas ao triplo para delitos cometidos com o uso de informática.

O substitutivo aos três projetos altera as duas leis acima e mais:

- ✓ o **Código Penal Militar**, o Decreto-Lei nº 1.001, de 21 de outubro de 1969;
- ✓ o **Código do Processo Penal**, Decreto-Lei nº 3.689, de 3 de outubro de 1941;
- ✓ a **Lei da Repressão Uniforme**, a Lei nº 10.446, de 8 de maio de 2002;
- ✓ o **Código do Consumidor**, Lei nº 8.078, de 11 de setembro de 1990;
- ✓ a **Lei Afonso Arinos,** Lei nº 7.716, de 5 de janeiro de 1989;
- ✓ o **Estatuto da Criança e do Adolescente**, a Lei nº 8.069, de 13 de julho de 1990.

A Convenção sobre o Cibercrime, do Conselho da Europa

A Convenção sobre o Cibercrime, celebrada em Budapest, Hungria, a 23 de novembro de 2001, pelo Conselho da Europa, teve como signatários 43 paises, europeus na sua maioria (veja lista detalhada no Apêndice A) e ainda Estados Unidos, Canadá e Japão. Cada Estado signatário deve ratificar as disposições constantes da Convenção no seu ordenamento jurídico interno.

Embora o Brasil ainda não seja signatário da Convenção sobre o Cibercrime, pode ser considerado um país em harmonia com suas deliberações, pois o presente Projeto de Lei já atende às recomendações do seu Preâmbulo, como, por exemplo, “a adoção de poderes suficientes para efetivamente combater as ofensas criminais e facilitar a sua detecção, investigação e persecução penal, nos níveis doméstico e internacional e provendo protocolos para uma rápida e confiável cooperação internacional”.

A harmonia é importante para otimizar a repressão dos crimes de informática, notadamente transnacionais. O presente Projeto de Lei coloca o Brasil em condições de

poder tratar e acordar de maneira diferenciada, o que facilitará em muito a cooperação judiciária internacional e eventuais extradições, com os países signatários da Convenção de Budapest e outras, inclusive os EUA, país sede dos maiores provedores de acesso à rede mundial de computadores.

Em resumo a Convenção recomenda 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, trata da necessária cooperação internacional, das questões de extradição, da assistência mútua entre os Estados, da denúncia espontânea e sugere procedimentos na ausência de acordos internacionais específicos, além da definição da confidencialidade e limitações de uso. Define também a admissão à Convenção de novos Estados por convite e a aprovação por maioria do Conselho.

A harmonia crescente da legislação brasileira com a Convenção sobre o Cibercrime

A legislação brasileira em vigor já tipifica alguns dos crimes identificados pela Convenção, como os crimes contra os direitos do autor e crimes de pedofilia, e, caso a caso, cuida de alguns outros já tipificados no Código Penal. Veja abaixo o que segundo a Convenção, a legislação penal em cada Estado signatário deve tratar e a sua correspondência na legislação brasileira:

As leis brasileiras e a Convenção de Budapest
(CP – Código Penal CPM – Código Penal Militar)

Recomendação da Convenção	Artigos das leis ou códigos
1- do acesso ilegal ou não autorizado a sistemas informatizados	154-A e 155 § 4º,V do **Código Penal** 1 339-A e 240 § 6º,V do **Código Penal Militar** 2
2- da interceptação ou interrupção de comunicações	art. 16 do **Substitutivo**
3- da interferência não autorizada sobre os dados armazenados	154-D, 163-A e 171-A do **Código Penal** 339-D, 262-A e 281-A do **Código Penal Militar**
4- da falsificação em sistemas informatizados	163-A, 171-A, 298 e 298-A do **Código Penal** 262-A e 281-A do **Código Penal Militar**
5- da quebra da integridade das informações	154-B do **Código Penal** 339-B do **Código Penal Militar**
6- das fraudes em sistemas informatizados com ou sem ganho econômico	163-A e 171-A do **Código Penal** 262-A e 281-A do **Código Penal Militar**
7- da pornografia infantil ou pedofilia	241 da Lei 8.069, de 1990, Estatuto da Criança e do Adolescente (**ECA**), alterado pela Lei 10.764, de 2003;
8- da quebra dos direitos de autor	Lei 9.609, de 1998, (a **Lei do Software**), da Lei 9.610 de 1998, (a **Lei do Direito Autoral**) e da Lei 10.695 de 2003, (a **Lei Contra a Pirataria**);
9- das tentativas ou ajudas a condutas criminosas	154-A § 1º do **Código Penal** 339-A do **Código Penal Militar**
10- da responsabilidade de uma pessoa natural ou de uma organização	art. 21 do **Substitutivo**
11- das penas de privação de liberdade e de sanções econômicas	penas de detenção, ou reclusão, e multa, com os respectivos agravantes e majorantes, das **Leis citadas** e dos artigos do **Substitutivo**.

A posição oficial do Brasil em relação à Convenção sobre o Cibercrime

Em dezembro de 2006 a Comissão de Relações Exteriores e Defesa Nacional do Senado Federal (CRE) aprovou Requerimento de Informações, de autoria do Senador Eduardo Azeredo, solicitando ao Ministério das Relações Exteriores qual o posicionamento oficial do Brasil em relação à Convenção, uma vez que ele ainda não é dela signatário.

Em fevereiro de 2007 o Senador Eduardo Azeredo foi recebido em audiência pelo Senhor Ministro das Relações Exteriores, Celso Amorim, tratando, entre outros assuntos, da Convenção sobre o Cibercrime e a posição do Brasil.

Em março de 2007 o Senador Eduardo Azeredo recebeu em audiência o Chefe de Cooperação Técnica, do Departamento de Problemas Criminais, da Secretaria Geral do Conselho da Europa. Ele sugeriu à Coordenadora Geral contra o Crime Transnacional do Ministério das Relações Exteriores, o envio de carta ao Conselho manifestando o interesse do Brasil à Convenção, após o que o Conselho ouvirá os seus Membros para que então o Brasil seja convidado a participar.

Em junho de 2007 o Senador Eduardo Azeredo participou da Conferência sobre o Cibercrime, em Estrasburgo, França, onde expôs a situação da legislação brasileira no contexto.

São 13 os crimes ou delitos tipificados no Substitutivo:

1. **Roubo de senha - Difusão de Código Malicioso – inclusão do art. 171-A – Fraude:** É a tipificação do “phishing” com pena de reclusão, de um a três anos. Foi incluída a majorante de pena de uma sexta-parte se o autor se vale de nome falso ou da utilização da identidade de terceiros.
2. **Falsificação de cartão de crédito – inclusão de parágrafo único ao art. 298:** Mantida a pena, passa a ser “Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico ou digital ou similar portátil de captura, processamento, armazenamento e transmissão de informações”.
3. **Falsificação de telefone celular ou meio de acesso a sistema – inclusão do art. 298-A:** Mantida a pena, passa a ser “Falsificação de telefone celular ou meio de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado incluindo outros dispositivos falsificáveis”.
4. **Calúnia, difamação e injúria - crimes contra a honra – inclusão do art. 141-A:** Substitutivo inclui majorante de dois terços da pena para os casos em que os crimes do capítulo de “Crimes contra a Honra” – calúnia, difamação e injúria – são praticados mediante uso de informática.
5. **Difusão de Código Malicioso para causar dano – inclusão do art. 163 – A – “vírus”:** O texto atualizou a redação dos projetos originais, colocando a difusão de código malicioso que cause dano, como, por exemplo, o “vírus”, o “worm”, o trojan”, o “zumbi” etc. A pena prevista para quem comete esse crime foi alterada para reclusão.
6. **Acesso não autorizado – inclusão do art. 154-A:** Aumenta a pena de uma sexta-parte, se o autor se vale de nome falso ou da utilização da identidade de terceiros.
7. **Obtenção não autorizada de informação e manutenção, transporte ou fornecimento indevido de informação obtida desautorizadamente – inclusão do art. 154–B:** Foi incluída a conduta da utilização de informação além do prazo autorizado. A pena prevista é de detenção, de dois a quatro anos, e multa. Aumenta-se a pena de um terço se o dado ou informação obtida

desautorizadamente é fornecida a terceiros pela rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa.

8. **Divulgação não autorizada de informações disponíveis em banco de dados - inclusão do art. 154–D:** A pena é de detenção, de um a dois anos, e multa. Aumenta-se de pena se o autor se vale de nome falso ou da utilização da identidade de terceiros. Também aumenta a pena se o dado ou informação é fornecida indevidamente em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa.
9. **Furto Qualificado por uso de informática – art. 155 - Furto – inclusão do § 4º, V:** O Substitutivo tipificou o crime, mantendo a pena, a exemplo do tipo "o furto qualificado por uso de chave falsa".
10. **Atentado contra a segurança de serviço de utilidade pública – alteração do art. 265:** Mantida a pena, incluído no tipo o serviço de "informação ou telecomunicação".
11. **Ataques a redes de computadores - Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado – alteração do art. 266:** Os novos serviços no tipo incluem os ataques a redes de computadores tipo DoS, DdoS etc.
12. **Discriminação de raça ou de cor, disseminados através de rede de comutadores etc..** Alteração do art. 20, §§ 2º e 3º, da Lei Afonso Arinos, Lei nº 7.716/1989.
13. **Manter consigo arquivos digitais de vídeos, fotos etc. relativos a pedofilia:** Alteração do *caput* do art. 241, do Estatuto da Criança e Adolescente, Lei 8.069/1990.

Glossário – inclusão do art. 154-C

Para efeitos penais são definidos o que é "Dispositivo de Comunicação", "Sistema Informatizado", "Rede de Computadores", "Código Malicioso", "Dados Informáticos", "Dados de Tráfego".

Equiparação à coisa – inclusão do art. 183-A

Para efeitos penais, equiparam-se à coisa o dado, informação ou unidade de informação em meio eletrônico, digital ou similar, a base de dados armazenada, o dispositivo de comunicação, a rede de computadores o sistema informatizado, a senha ou similar ou qualquer instrumento que proporcione o acesso a eles.

Sobre as obrigações do responsável por liberar acesso a uma rede de computadores ou prestar serviços mediante o seu uso:

- ✓ Guardar os dados aptos à identificação do usuário e das conexões por ele realizadas;
- ✓ Atendendo expressa autorização judicial, tornar disponíveis os dados à autoridade de auditoria técnica que será definida em regulamento;
- ✓ Atendendo expressa autorização judicial, fornecer os dados no curso de investigação;

- ✓ Atendendo expressa autorização judicial, preservar imediatamente os dados aptos à identificação do usuário e das conexões por ele realizadas no curso de investigação;
- ✓ Repassar à polícia as denúncias que receber de crimes cometidos na rede;
- ✓ Dar esclarecimentos aos usuários que estão sob a lei brasileira;
- ✓ Fazer campanhas de alerta quanto ao uso criminoso da rede de computadores;
- ✓ Divulgar boas práticas de segurança;
- ✓ Pagar multa variável, de R$2mil a R$100 mil, aplicada pela autoridade definida em regulamento, caso não atenda às obrigações de guarda e/ou fornecimento dos dados, independentemente de indenização à pessoa lesada.