UNIVERSIDADE FEDERAL DA PARAÍBA - UFPB
CENTRO DE CIÊNCIAS JURÍDICAS - CCJ
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS JURÍDICAS - PPGCJ
ÁREA DE CONCENTRAÇÃO EM DIREITO ECONÔMICO

ARNALDO SOBRINHO DE MORAIS NETO

CIBERCRIME E COOPERAÇÃO PENAL INTERNACIONAL: UM ENFOQUE À LUZ DA CONVENÇÃO DE BUDAPESTE

JOÃO PESSOA
2009

ARNALDO SOBRINHO DE MORAIS NETO

CIBERCRIME E COOPERAÇÃO PENAL INTERNACIONAL: UM ENFOQUE À LUZ DA CONVENÇÃO DE BUDAPESTE

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Jurídicas da Universidade Federal da Paraíba, na área de concentração em Direito Econômico, como requisito parcial para obtenção do grau de mestre.

Orientador: Prof°. Dr. Manoel Alexandre Cavalcante Belo

JOÃO PESSOA
2009

M827c Morais Neto, Arnaldo Sobrinho de.
Cibercrime e cooperação penal internacional: um enfoque à luz da Convenção de Budapeste / Arnaldo Sobrinho de Morais Neto.- João Pessoa, 2009.
232p.
Orientador: Manoel Alexandre Cavalcante Belo
Dissertação (Mestrado) – UFPB/PPCJ
1. Criminalidade informática. 2. Cibercrime. 3. Cooperação penal internacional. 4. Convenção de Budapeste – cibercrime. 5. Criminalidade cibernética.

UFPB/BC CDU: 343.93:004(043)

ARNALDO SOBRINHO DE MORAIS NETO

CIBERCRIME E COOPERAÇÃO PENAL INTERNACIONAL: UM ENFOQUE À LUZ DA CONVENÇÃO DE BUDAPESTE

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Jurídicas da Universidade Federal da Paraíba, na área de concentração em Direito Econômico, como requisito parcial para obtenção do grau de mestre.

Banca Examinadora: Data de aprovação: _____

_____

Prof º. Dr. Manoel Alexandre Cavalcante Belo

_____

Prof º. Dr. Fernando Antônio de Vasconcelos

_____

Prof º. Dr. Mohamed Chawki

À Deus.

Meus pais Ardnildo e Maria Concebida.

À Carmen, Vinícius Kelsen, Heloísa Helena e Laura Victória,

aos meus irmãos Fernandes, Adenilson, Adenilda,

Adilson, Adenildo e Alenilda.

dedico.

AGRADECIMENTOS

Aos professores do Programa pelos brilhantes ensinamentos: Profa. Dra. Maria Luiza, Profa. Dra. Ana Luisa, Prof. Dra. Marcela Varejão, Prof. Dr. André Régis, Prof. Dr. Ernesto e aos amigos e mestres Prof. Dr Fernando Vasconcelos e Prof. Dr. Luciano Maia.

Devo agradecimento especial ao meu orientador Prof Dr. Alexandre Belo, pela paciência, pelas inestimáveis orientações que guiaram a conclusão do Mestrado

Aos meus colegas de Mestrado: Jacyara, Sancha, Márcio, Silmary, Adair, Luciano, Cláudio, Márcia, Thiago, Tertuliano e Ronny pelas inesquecíveis horas de debates e de convivência amistosa.

Aos amigos Onierbeth, Flórida pelo suporte E tradução dos textos para líNgua inglesa, sem os Quais em tempo hábil não seria possível concluir. AgradEcimento especial a Cinthya pela zelosa correção do texto e das idéias, imensamente grato pela Vitória.

Ao Juiz Dr. Mohamed Chawki pelas idéias compartilhadas no âmbito internacional, pela acolhida e oportunidades na cidade do Cairo, Egito, meu muito obrigado, também.

RESUMO

O desenvolvimento tecnológico revolucionou muitas atividades humanas, transformando o mundo numa sociedade global, na Era da Informação. Nesse novo contexto as novas Tecnologias da Informação e da Comunicação, apresentam-se como suporte indispensável em todas as áreas do conhecimento humano. Acompanhando esse novo panorama inúmeras condutas ilícitas passaram também a ser praticadas neste novo ambiente, neste novo mundo, na nova dimensão jurídica que desafia o Estado, pois o ciberespaço alterou as fronteiras geográficas de aplicação de instrumentos jurídicos em face do cibercrime. Estas condutas revelam-se um novo desafio para o Estado. Conceitos seculares e fundamentais do direito, relacionados aos aspectos de jurisdição e de aplicação da lei sofreram notáveis modificações, a exemplo da idéia de tempo e lugar do crime. Abordagem de uma nova dimensão para o termo soberania, em face do caráter transnacional da criminalidade cibernética, também. Ainda que o conceito e seus elementos caracterizadores possam comportar múltiplas interpretações de ordem doutrinária, sem consenso, o resultado de tais ações criminosas, muitas vezes ramificações ou instrumento da criminalidade organizada internacional, traduzem-se em prejuízos que ultrapassam a cifra de bilhões de dólares em todo mundo. O Brasil com suas dimensões continentais se insere de forma vigorosa neste novo contexto, ora como exemplo para a comunidade internacional em ações do Estado que visam combater o cibercrime; ora como um dos principais focos irradiadores de ações delituosas no ciberespaço. Por isso é possível observar no presente estudo os contornos deste novo fenômeno, seus aspectos jurídicos, a repercussão provocada em âmbito nacional e internacional, bem como os instrumentos jurídicos utilizados neste embate. Em face da nova dimensão e reordenamento dos espaços globais, há por conseqüência, a necessidade de adequação, do mesmo modo, da forma como os Estados devem estabelecer laços de cooperação internacional em matéria penal. A Convenção de Budapeste sobre o Cibercrime, neste sentido, mostra-se como instrumento jurídico eficaz a combater a criminalidade cibernética, ainda que possamos abordar as possibilidades, inclusive, de ampliação de algumas condutas à esfera de competência do Tribunal Penal Internacional e a necessidade de inserção da República Federativa do Brasil como signatário da Convenção do Conselho da Europa sobre o Cibercrime (Convenção de Budapeste).

Palavras-chave: cibercrime; criminalidade informática; cooperação penal internacional; Convenção de Budapeste.

ABSTRACT

The development revolutionized many human activities, transforming the world in a global society, in Information Age. In this new context the new Information Technology and Communication, are as essential support in all areas of human knowledge. Accompanying this new panorama numerous illegal conduct have also to be applied in this new environment, this new world, the new legal dimension that challenges the State, as the cyberspace has changed the geographical boundaries of application of legal instruments in the face of cybercrime. These behaviors seem to be a new challenge for the State. Concepts and principles of secular law, related to issues of jurisdiction and law enforcement have suffered significant changes, like the idea of time and place of the crime. Approach to a new dimension to the word sovereignty, given the transnational nature of cybercrime. Although the concept and its characteristic elements may include multiple interpretations of a doctrine, without consensus, the result of such criminal actions, often branching or instrument of international organized crime, result in losses that exceed the amount of billions of dollars in everyone. Brazil with its continental size comes in a robust manner in this new context, either as an example for the international community in the state actions to combat the crime, either as a main focus of radiators criminal actions in cyberspace. It is therefore possible to observe in this study the contours of this new phenomenon, its legal aspects, the impact caused at the national and international, as well as legal instruments used in this clash. In light of the new scale and global reordering of the spaces, there is therefore the need for adequacy, the same, of how States should establish links to international cooperation in criminal matters. The Budapest Convention on Cybercrime, in this sense, it is as an effective legal instrument to combat cybercrime, yet we can address the possibilities, including the expansion of some pipes to the sphere of competence of the International Criminal Court and the need for integration of the Federative Republic of Brazil as a signatory of the Council of Europe Convention on Cybercrime (Budapest Convention).

Keywords: cybercrime, computer crime, international criminal cooperation, the Budapest Convention.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS

APC - Associação para Comunicações Progressiva

ARPANET -Advanced Research Projects Agency Net

BBSs - Bulletin Board Systems

CDA - Communications Decency Act

CDPC - Comitê Europeu para os Problemas Criminais

CECA - Comunidade Europeia do Carvão e do Aço

CERN - Centro de Estudos de Energia Nuclear

CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CPI - Comissão Parlamentar de Inquérito

DNS - Domain Name System,

DOD - Departamento de Defesa dos Estados Unidos

EUA – Estados Unidos da América

EMBRATEL - Empresa Brasileira de Telecomunicações

FAPESP - Fundação de Amparo a Pesquisa do Estado de São Paulo

FAPESQ - Fundação de Apoio a Pesquisa da Paraíba

Fermilab - Laboratório de Física de Altas Energias

FTP - File Transfer Protocol

IBASE - Instituto Brasileiro de Análises Sociais e Econômicas

ICANN - Internet Corporation for Assigned Names and Numbers

IDH – índice de desenvolvimento humano

IGC - Institute for Global Communication

IP - internet protocol

LNCC - Laboratório Nacional de Computação Científica

MCT - Ministério da Ciência e Tecnologia

MPF – Ministério Público Federal

MIT - Massachussetts Institute of Technology

NCSA - Centro Nacional de Aplicações em Supercomputação

OAB **-** Ordem dos Advogados do Brasil

OECD - *Organization for Economic Cooperation and Development*

OMC - Organização Mundial do Comércio PAQTC - Parque Tecnológico da Paraíba

PNUD - Programa das Nações Unidas para o Desenvolvimento

RNP - Rede Nacional de Pesquisa

RPP - Rede Paraibana de Pesquisa

SEPFIN – Serviço de Perícias de Informática

SPCI - International Conference on Security, Privacy and Confidentiality Issues in Cyberlaw

TCP/IP - Transmission Control Protocol/Internet Protocol

TIC – telecomunicações, informática e comunicações

TRIPS - Trade-Related Aspects of Intellectual Property Rights

UNCITRAL – *United Nations Commision on International Trade Law*

UCLA **-** Universidade da Califórnia

UFPB - Universidade Federal da Paraíba Fundação

URSS - União das Repúblicas Socialistas Soviéticas

WWW **-** World Wide Web

SUMÁRIO

1 INTRODUÇÃO

As transformações vivenciadas pela humanidade em pouco mais de meio século tem proporcionado mudanças em muitos conceitos que levaram séculos para serem construídos e efetivados. Estas mudanças indicam um novo caminho, uma nova cultura, uma nova dimensão para fenômenos sociais que estão provocando uma mutação no pensamento tradicional de enunciados do mundo jurídico em face da necessidade de adequação ao estabelecimento de novas interações entre os Estados, organizações e pessoas.

Não se trata de um processo estanque, separado do processo histórico. Estas forças transformadoras são frutos do conhecimento técnico-científico experimentadas, sobretudo, a partir do pós Segunda Guerra Mundial, sintetizadas com a Revolução Tecnológica, fruto da simbiose entre as telecomunicações e o emprego de recursos de informática e aceleradas com o fim da Guerra Fria, transformando, pois, o mundo numa aldeia global, uma das faces do processo de globalização.

O que interessa nesse contexto, notadamente, enquanto objeto para pesquisa científica, são os efeitos desse fenômeno sobre a sociedade. Uma das faces carente de investigação indica o surgimento de novos conceitos, abordagens e práticas sociais que ligam as dimensões de um novo mundo proporcionadas pela internet e pelo ciberespaço, um novo ambiente onde se estabelecem práticas que requerem a tutela jurídica do Estado.

Num primeiro momento, enquanto restrita à área acadêmica não havia registro de situações que viessem desafiar as ações do Estado, mas com a sua exploração numa escala comercial, passaram a surgir conflitos ligados ao comércio, direito do consumidor, direitos civis e políticos, direitos humanos e economia, cuja movimentação financeira anual ultrapassa bilhões de dólares.

Nesta perspectiva, é conveniente, num primeiro momento, analisar como o processo de globalização e a Revolução Tecnológica deram novas feições a postulados tradicionais do mundo jurídico, como a perspectiva da soberania em relação à internet e ao ciberespaço e como as questões inerentes à prática de ilícitos transnacionais podem ser enfrentadas, também, num esforço que não esteja restrito a um único Estado.

As primeiras projeções sobre as ações criminosas têm se confirmado, numa migração real, inclusive, do crime organizado para o novo ambiente virtual onde as pessoas realizam grande parte de suas atividades econômicas e consequentemente têm sofrido os efeitos da nova realidade: a criminalidade cibernética. Este tem sido o novo desafio aos

poderes constituídos do Estado, numa perspectiva de proteção jurídica de interesses e também de estabilidade nas relações sociais.

Assim, em face desse novo fenômeno, a presente pesquisa procurou analisar, como ponto de partida, os efeitos desse processo sobre conceitos tradicionais da Ciência Jurídica, como a noção de soberania, território, fronteiras e os aspectos peculiares que fizeram emergir o cibercrime como fenômeno da pós-modernidade.

Neste sentido, a pesquisa foi conduzida com o ideal de analisar o problema gerado pelo cibercrime. O que o Estado pode fazer para enfrentar este novo fenômeno e que instrumentos jurídicos seriam eficazes para dar um tratamento efetivo a estas novas demandas em suas mais variadas formas numa escala mundial?

Desta forma, procurou-se uma delimitação para o campo de trabalho que se volta para a perspectiva da Cooperação Penal Internacional, tendo a Convenção de Budapeste Sobre o Cibercrime como elemento balizador, uma vez que os ordenamentos jurídicos nacionais têm se mostrado ineficazes quando o crime se concretiza numa dimensão multifronteiras.

Sob o aspecto medotológico, procurou-se nortear a pesquisa sob uma base qualitativa, com caráter teórico-instrumental, utilizando para tanto o método dedutivo, focando-se a temática, num primeiro momento, com uma análise geral do tema e em seguida efetivando sua delimitação com a análise dos aspectos de Cooperação Penal Internacional presentes na Convenção de Budapeste Sobre Cibercrime.

Ousa-se a utilização de notas de rodapé para comentários essenciais e referências (simultaneamente) de forma a facilitar a identificação das obras originalmente consultadas, remetendo-se ao final com a indicação bibliográfica completa em ordem alfabética.

Como técnica de pesquisa fez-se uso da pesquisa documental, complementada com uma considerável base bibliográfica, parte dela alienígena. Procuro-se, ainda, observar o tratamento jurídico dado à temática no âmbito nacional, mediante a participação de um seminário sobre cibercrime patrocinado pela Ordem dos Advogados do Brasil – OAB, seccional São Paulo, em março de 2008, bem como com a participação, como conferencista da "*1st International Conference on Security, Privacy and Confidentiality Issues in Cyberlaw - (SPCI 2008),* realizada no mês de junho de 2008, na cidade do Cairo, Egito e Cyberspace 2008, na cidade de Brno, República Tcheca, onde nos dois eventos científicos foi possível obter uma visão sobre o tratamento dado à matéria numa perspectiva internacional.

O trabalho está estruturado em cinco capítulos, iniciando-se com esta breve exposição da pesquisa, sua importância, a questão posta como problemática central, os aspectos metodológicos e as técnicas de pesquisa utilizadas.

No capítulo dois – Concepção sobre elementos essenciais, procura-se demonstrar como conceitos tradicionais sofreram influência do processo de Globalização e da Revolução Tecnológica, com abordagens preliminares e conceituais sobre internet, ciberespaço, teorias sobre controle e regulação da internet e do ciberespaço, bem como os impactos gerados por estas tecnologias.

O capítulo três aborda os aspectos conceituais sobre o cibercrime, seus impactos e prejuízos à sociedade, bem como uma análise sobre direitos fundamentais (liberdade de expressão e privacidade) muitas vezes empregados para acobertar condutas delituosas. É ainda detalhada, uma relevante abordagem sobre o mundo dos *hackers*, grupos, subgrupos, *modus operandi* e os desafios à ordem jurídica proporcionados pela nova criminalidade cibernética.

Com a compreensão do fenômeno esmiuçado na estrutura inicial, no capítulo cinco, a temática é compatibilizada com os aspectos relevantes da Cooperação Penal Internacional e aspectos históricos do ideal de cooperação no direito comunitário europeu e ao cibercrime transnacionais. Esta preocupação pode ser justificada pela dimensão do *modus operandi* dos infratores, pois, as ações danosas podem ter reflexos em mais de um Estado, levando assim a questão para uma problemática vinculada, também, ao Direito Internacional.

No último capítulo, a questão do cibercrime e da cooperação penal internacional é revista com base no instrumento jurídico internacional que tem mostrado os melhores resultados frente à nova criminalidade: a Convenção de Budapeste sobre Cibercrime e os aspectos inerentes à Cooperação Penal Internacional. Merece assim, atenção especial quanto ao processo de sua construção, a partir do Direito Comunitário Europeu e a sua consolidação como Convenção internacional, fazendo uma breve análise possibilidade de ampliação da competência do Tribunal Penal Internacional em face do ciberterrorismo. Finaliza-se o trabalho com uma argüição sobre a necessidade necessidade de ampliação da Convenção e sua importância como instrumento jurídico de caráter mundial.

2 CONCEPÇÃO SOBRE ELEMENTOS ESSENCIAIS

2.1 Soberania: dos Estados Nacionais à nova ordem jurídica internacional

A soberania constitui um dos elementos essenciais do Estado. Seu conceito e características constituem um dos pilares do Estado Moderno, assumindo relevância significativa nas abordagens atuais, notadamente quando sua definição e aspectos tradicionais vêm sendo mitigados pela construção de outros processos e fenômenos muito recentes, como a concepção de globalização, ciberespaço e cooperação internacional.

Sob uma perspectiva histórica, a Antiguidade (até o fim do Império Romano) não conheceu qualquer registro que pudesse se assemelhar à ideia de soberania. Durante a Idade Média, houve intenso conflito pelo estabelecimento de um poder central, supremo, que estivesse acima de todos os outros sob um determinado território. Decorreram assim, inúmeros conflitos entre monarcas e o senhores feudais, externando, pois, embates pelo estabelecimento do poder.

Neste sentido, Matias[1] entende que "o Estado Moderno surgiu graças à desagregação e ao colapso do regime feudal, em um processo no qual o rei foi bem sucedido em submeter todos os senhores à sua autoridade incontestável [...]", sob uma visão interna e externamente "para se emanciparem da Tutela do Santo Império Romano, primeiro e do Papado, depois", como ensina Azambuja.[2] Mas a questão só tomou importância e só veio a consolidar-se sob uma ótica mais doutrinária ao final da Idade Média, notadamente com as ideias de Jean Bodin[3].

Para Dallari[4], a concepção de soberania nesse período era compreendida como sendo "o poder absoluto e perpétuo de uma República, palavra que se usa tanto em relação aos particulares quanto em relação aos que manipulam todos os negócios de estado de uma república." Seguindo este pensamento, a ideia de soberania estaria vinculada ao poder real, do monarca, isto é, um poder de ordem pessoal, inclusive hereditária nos Estados monárquicos.

---

[1] MATIAS, Eduardo Felipe Pérez. **A humanidade e suas fronteiras**: do Estado soberano à sociedade global. São Paulo: Paz e Terra, 2005, p.33.
[2] AZAMBUJA, Darcy. **Teoria geral do Estado**. 41ª ed. São Paulo: Globo, 2001, p.51.
[3] FERREIRA, Luis Pinto. **Teoria Geral do Estado**. 3.ed. São Pulo: Saraiva, 1975. p. 223.
[4] DALLARI, Dalmo de Abreu. **Elementos de teoria geral do Estado**. 15ª ed. São Paulo: Saraiva, 1991, p. 65.

Assevera-se, entretanto, que o reconhecimento da soberania como poder dos monarcas dos Estados na Europa não se efetivou de plano, pois, como afirma Matias[5], somente "a paz de Westfália, celebrada em 1648, encerrou a Guerra dos Trinta Anos, última das guerras de religião a castigar o continente europeu. Nela se firmou a igualdade jurídica entre os Estados, consolidando-se a aceitação do princípio da soberania estatal [...]".[6]

No Século XVIII, os estudos de Rosseau sobre soberania, constantes no "Contrato Social" tiveram grande influência nos ideais de luta da burguesia contra o absolutismo monárquico. Para Rosseau a titularidade do exercício da soberania não estava nas mãos do governante, mas do povo, traduzindo-se nos ideais de soberania popular. Essa concepção viria a ser contraposta na metade do século XIX quando, na Alemanha, ganha corpo à teoria da personalidade jurídica do Estado, como sendo o verdadeiro titular da soberania.

Muitos doutrinadores (Hobbes, Jellinek, Kelsen, Heller, Ranelletti e Reale), procederam aprofundado estudo com o intuito de chegar a um conceito de soberania. Dallari ao abordar a temática assevera que:

> "Procedendo uma síntese de todas as teorias formuladas, o que se verifica é que a noção de soberania está sempre ligada a uma concepção de poder, pois mesmo quando concebida como centro unificador de uma ordem está implícita a idéia de poder de unificação. O que nos parece que realmente diferencia as concepções é uma evolução do sentido eminentemente político para uma noção jurídica de soberania."[7]

Neste sentido seria possível a concepção sobre três aspectos: puramente políticos, puramente jurídicos e uma terceira posição denominada por Dallari[8] de "culturalista". Assim, sob uma dimensão política a soberania expressa a plena eficácia de poder, ou seja, o "poder incontrastável de querer coercitivamente e de fixar as competências."[9] Numa concepção puramente jurídica, tem-se a soberania como "o poder de decidir em última instância sobre a atributividade das normas, vale dizer, sobre a eficácia do direito." Sob o terceiro aspecto Dallari citando Reale diz que soberania seria "o poder de organizar-se juridicamente e de fazer valer dentro de seu território a universalidade de suas decisões nos limites dos fins éticos de convivência."[10]

---

[5] MATIAS, op. cit. n. 1, p.35.
[6] MATIAS entende ainda que a celebração da Paz de Westfália marcou os primórdios da atual sociedade internacional.
[7] DALLARI, op. cit. n. 4, p.67.
[8] DALLARI, op. cit., p.68.
[9] DALLARI, op. cit., p. 68.
[10] DALLARI, op. cit., p. 68.

Em nosso estudo, porém, será relevante considerar a concepção de soberania sob a ótica do direito internacional, que Matias[11] ensina como sendo "a supremacia do poder do Estado sobre seu território e população, e a independência deste em relação a qualquer autoridade exterior", denotando, portanto um caráter interno (autoridade suprema num território) e externo (não há subordinação nem dependência e sim igualdade).

Ao escrever sobre a concepção moderna de soberania, em 1975, Pinto Ferreira[12] teorizou:

> Não se pode compreender o Estado sem a noção de soberania. Uma soberania absoluta evidentemente não existe, pois vários Estados soberanos se interdependem e se autolimitam. Evidentemente, em contrapartida, não se pode pretender a liquidação e a dissolução do dogma da soberania, embora a futura emergência de um Estado mundial exercendo soberania internacional por delegação das várias soberanias, seja decisiva para o mundo e a sobrevivência da humanidade.

Importantes traços eclodem dessa concepção tradicional de soberania. Uma forte vinculação a um poder, restrito às fronteiras territoriais de um Estado; o poder supremo vinculado ao Estado, como entidade jurídica, por delegação de seus nacionais e a ideia de relação de igualdade de poder entre os Estados na comunidade internacional. Vê-se assim, numa ordem interna o poder máximo e na ordem global uma relação paritária, isto é, em equilíbrio.

Serão, concretamente, estes atributos principais, vinculados à ideia de poder, território e relações internacionais que constituirão os grandes desafios dos Estados nacionais em atuar no novo cenário global, com forte influência do processo de globalização (ainda em construção), dos avanços tecnológicos, da nova "ordem mundial"[13] e do surgimento de novas fronteiras (internet e ciberespaço), capazes acelerar o processo de mutação de um novo conceito sobre soberania.

Neste Século XXI a nova formatação está cada vez mais impregnada de conceitos relativos à cooperação internacional, integração econômica, direito comunitário e abdicação de uma fração da soberania em nome de organismos internacionais com caráter

---

[11] MATIAS, op. cit. n. 1, p.74.
[12] FERREIRA, op. cit. n.3x, p.340.
[13] FRANCA FILHO, Marcílio Toscano. **Introdução ao direito comunitário**. São Paulo: Editora Juarez de Oliveira, 2002, p. 13.
Para FRANCA FILHO (op. cit., p.31) as "noções de globalização e nova ordem mundial se confundem no plano político internacional". A nova "ordem mundial" seria compreendida como sendo a "nova forma de distribuição do poder no Globo" no pós guerra-fria a partir de 1989.

supranacional, a exemplo do Tribunal Penal Internacional. Neste raciocínio Franca Filho[14] ratifica que a globalização aponta, sob um ponto de vista institucional, para "a convergência da regulação político-jurídico-econômica entre os países" e num aspecto econômico para "uma crescente perda da Soberania das autoridades responsáveis pelas políticas econômicas nacionais, na ordem globalizada."[15]

Na lição de Borges[16], "A evolução dos sistemas normativos estatais converge, como um tendencial, para sua progressiva unificação [...]. Neste sentido, os blocos regionais de hoje – como o bloco europeu (União Europeia) o sul americano (Mercosul) – são a crisálida dessa meta".

Neste sentido, contrastando a ideia tradicional de soberania em face de uma concepção necessária a se amoldar ao novo cenário global, Borges[17], assevera:

> O fenômeno da globalização, envolvendo e semanticamente denotando ao início a formação de blocos regionais de Estados num espaço comunitário, e tendendo para expansão das organizações comunitárias [...] implica o repensar as relações entre soberania e comunidade. Nas relações interestatais comunitárias, a globalização se manifesta circunstancialmente pela regionalização. [...] O conceito tradicional de soberania (já vimos que não é exagero afirma-lo) está historicamente defasado e mesmo superado.

Os novos parâmetros conexos ao ideal de soberania devem ser compreendidos como uma evolução natural, uma luta pela inserção do novo modelo de Estado na sociedade global, cada vez mais interdependente em relação a outros países, num esforço comum de forma a atender as demandas decorrentes da globalização, notadamente econômica.

Assim, essa nova formatação não pode ser visualizada sob a ótica de perda de poder do Estado provocado pela globalização e pela revolução tecnológica – isto na compreensão de ordem jurídica estatal. Para Matias[18], "trata-se, nesse caso, da repartição de algumas funções do Estado ente instituições internacionais, transnacionais ou supranacionais", cuja visão de Estado com território, povo e governo vêm sendo mitigada, principalmente no que diz respeito ao terceiro elemento que estaria sendo afetado por um novo modelo de governança – governança global e numa ótica mais tecnológica, pelas novas fronteiras decorrentes do surgimento do ciberespaço e da internet.

---

[14] FRANCA FILHO, op. cit. n. 13, p.31.
[15] Em sua obra de referência sobre Direito Comunitário Franca Filho (op. cit. n. 13, p.31.) indica como fator inerente a esta situação o fato de que os países estão se agrupando em blocos econômicos como necessidade de adaptação das economias nacionais às migrações internacionais dos fatores produtivos.
[16] BORGES, José Souto Maior. **Curso de direito comunitário**. São Paulo: Saraiva, 2005, p..67.
[17] BORGES, op. cit., p. 188.
[18] MATIAS, op. cit.n1, p.440.

2.2 A Internet no contexto do mundo globalizado

2.2.1 Aspectos históricos – panorama mundial

A história da internet e de seu emprego como ferramenta de comunicação (entre outras aplicações) é fato recentíssimo. Detalhe importante para se associar a essa compreensão, também, diz respeito às evidências lógicas de que só se pode falar de internet, quando se fala em criação e evolução da informática, dos computadores e seus muitos acessórios indispensáveis. É lógico, então, que para minimizar o caminho a ser explicitado, a abordagem restringir-se-á a relatar um pouco da evolução da internet propriamente dita.

Os primórdios desta inovação tecnológica remontam à criação da ARPANET (Advanced Research Projects Agency Net), que surgiu em 1969, com a finalidade de atender a demandas do Departamento de Defesa dos Estados Unidos (DOD), no auge da Guerra Fria, em resposta ao lançamento do Sputinik, o primeiro satélite espacial soviético. Pode ser considerado, assim, o embrião da maior rede de comunicação do planeta. Nesse período o mundo da informática era dominado por grandes computadores, existentes apenas em avançados centros de pesquisa, notadamente nos Estados Unidos. Os microcomputadores ainda não existiam.

Inicialmente, a pretensão era criar uma rede que pudesse ficar imune a um possível ataque inimigo (ataque soviético aos EUA), e que possibilitasse a interconexão de pontos estratégicos, como centros de pesquisa e tecnologia. Em face da importância estratégica que estava evidente e temendo conseqüências de um ataque nuclear, os Estados Unidos investiram no projeto.

Foi idealizada então uma estrutura de rede desprovida de centro, fazendo quebrar o tradicional modelo de pirâmide, conectado a um computador central. A estrutura proposta permitiria que todos os pontos (nós) tivessem o mesmo status. Inicialmente foram interligados quatro pontos: Universidade da Califórnia (UCLA), o Instituto de Pesquisas de Stanford, e a Universidade de Utah. O nó da UCLA foi implantado em setembro de 1969.

De acordo com Kellen Cristina:

> Quando a ameaça da Guerra Fria passou, a ArphaNet tornou-se tão inútil que os militares já não a consideravam tão importante para mantê-la sob a sua guarda. Foi

> assim permitido o acesso aos cientistas que, mais tarde, cederam à rede para as universidades as quais, sucessivamente, passaram-na para as universidades de outros países, permitindo que pesquisadores domésticos a acessassem [...].[19]

Com o sucesso das primeiras experiências, apenas dois anos após, isto em 1971, já havia duas dúzias de junções de redes locais. Três anos depois, já chegavam a 62 e, em 1981, quando ocorreu o batismo da Internet, eram 200.

Por um período considerável, o acesso à Internet ficou restrito a instituições de ensino e pesquisa. A partir da década de 80, os microcomputadores passaram a custar menos e se tornaram mais fáceis de usar e consequentemente houve uma maior difusão das aplicações de informática, ressaltando-se, porém, que essa utilização estava voltada muito mais para os ambientes das corporações que aplicações domésticas e/ou pessoais.

Segundo Paulo Sérgio Oliveira:

> Já em 1990, a Internet ultrapassou a marca de um milhão de usuários e teve início a utilização comercial da Rede. Empresas pioneiras montam redes próprias de comunicação (como a Compuserve americana) e agora se interligam na Internet e lucram com esta conexão. O envolvimento de dinheiro e a utilização das conexões para vender produtos e serviços abre duas frentes de discussão: a primeira, quem vai arcar com os custos? A segunda, de caráter mais subjetivo: a comercialização distancia a Rede de seus objetivos essenciais?[20]

Concretamente a internet só passou a se popularizar quando Tim Berners-Lee, um físico do Centro de Estudos de Energia Nuclear (CERN), em Genebra, Suíça, propôs uma extensão do *Gopher* utilizando o conceito de *hipertexto* onde partes do texto que estavam "marcadas", ao serem selecionadas através de um clique do mouse, levavam a maiores informações sobre o assunto em questão, estava criada assim a possibilidade do que hoje se convencionou chamar de "navegar". Entretanto, Fernando Vasconcelos[21], entende que "pode-se apontar o ano de 1971, como marco inicial de operacionalização da rede, quando o pesquisador norte americano Ray Tomlinson enviou o primeiro e-mail [...]".

A essência da invenção de Tim Berners-Lee foi o desenvolvimento de um programa denominado *browser*, que fazia a leitura das informações codificadas em linhas de programação e as exibia em uma interface gráfica, como em um computador pessoal. Essa inovação recebeu de Tim Berners-Lee a denominação de *World Wide Web (WWW).*

---

[19] KELLEN Cristina S.P, 1996.
[20] PAULO Sérgio Oliveira, S.P., 1997.
[21] VASCONCELOS, Fernando Antônio de. **Internet: responsabilidade do provedor pelos danos praticados**. Curitiba: Juruá, 2003, p. 33.

Há de se destacar ainda que um poderoso *browser* foi desenvolvido no Centro Nacional de Aplicações em Supercomputação (NCSA): o *Mosaic*. Através desse programa, o usuário da internet poderia acessar informações sem se preocupar com conversão de arquivos ou formatos, possibilitando também acessar outros serviços, tais como o *Gopher, Telnet* (acesso remoto via terminal), FTP (protocolo de transferência de arquivos) ou mesmo enviar *e-mail*. Num passo adiante a empresa *Netscape Com.* lançou uma versão mais poderosa do *Mosaic*: o *Netscape Navigator*, fazendo com que a internet ficasse agora acessível a qualquer usuário de um microcomputador.

Uma pergunta provoca inquietação: quem controla a internet? Ainda que não exista um controle, em termos de propriedade, há controle do ponto de vista da ordenação dos endereços (um controle indireto).

Na Compreensão de Ramonet temos que:

> Actualmente e desde 1988, a rede mundial é administrada pela Internet Corporation for Assigned Names and Numbers (ICANN), um organismo de direito privado sem fins de lucro com sede em Los Angeles, submetido à lei californiana e colocado sob o controle do Departamento de Comércio dos Estados Unidos. A ICANN é a grande controladora da rede. [...]A principal função da ICANN é coordenar os nomes de domínio (Domain Name System, DNS) que ajudam os usuários a navegar pela Internet. Cada computador conectado à Internet possui um endereço único chamado "endereço IP" (de Protocolo Internet). Inicialmente, estes endereços IP são séries de números difíceis de memorizar, mas o DNS permite utilizar em lugar de números letras e palavras mais familiares (o "nome de domínio"). Por exemplo, em lugar de escrever uma série de números, escreve-se www.monde-diplomatique.es. O DNS converte o nome de domínio na série de números que corresponde ao endereço IP, o que permite ao seu computador conectar-se com o lugar procurado. O DNS permite também o bom funcionamento do correio eletrônico. Tudo isso à escala planetária e a uma velocidade ultra rápida.[22]

Indiscutivelmente, a internet é hoje um dos mais poderosos meios de comunicação, de difusão de notícias, de intercâmbio e, sobretudo, terreno fértil para realização de transações comerciais e relacionamentos interpessoais. Isto porque não são poucos os registros de casamentos que foram viabilizados através da net, isto sem aprofundar, no momento, as questões pertinentes ao *e-commerce* que é uma realidade ímpar. Do mesmo modo, ao tempo em que vivenciamos ações destinadas à satisfação de anseios de ordem coletiva e pessoal, há inúmeros registros, conforme abordaremos adiante, de ações criminosas que passaram a ser desencadeadas mediante a internet.

---

[22] RAMONET, Ignacio. **Controlar a internet**. Informação Alternativa, 2005. Disponível em:<http://www.infoalternativa.org/autores/ramonet/ramonet067.htm>. Acesso em: 2 ago.2008.

2.2.2 Aspectos históricos e crescimento da internet no Brasil

A primeira conexão do Brasil com a internet foi feita em 1988, através da LNCC - Laboratório Nacional de Computação Científica (Rio de Janeiro) e BITNET, rede mantida pela Universidade de Maryland, nos EUA[23], por meio de uma conexão de 9.600 bps (bits por segundo)[24]. No mesmo ano a FAPESP - Fundação de Amparo a Pesquisa do Estado de São Paulo estabeleceu conexão com o Laboratório de Física de Altas Energias (Fermilab), em Chivado, EUA. Em 1989, o MCT - Ministério da Ciência e Tecnologia criou a RNP - Rede Nacional de Pesquisa, que construiu o primeiro "*backbone*" nacional.

Havia neste contexto histórico uma grande demanda reprimida, pois o Brasil dispunha de uma política protecionista voltada para os produtos de informática, visando, erroneamente, proteger empresas nacionais que desenvolviam produtos de informática. Este protecionismo impôs ao país uma barreira considerável no acesso a produtos de tecnologia e, consequentemente, atraso na conjugação de conhecimentos que pudessem viabilizar avanço no setor de tecnologia.

Ademais, como se depreende neste processo histórico, a finalidade da internet no Brasil, num primeiro momento, era eminentemente o uso no meio acadêmico e científico, como bem pontifica Takahashi:

> Uma primeira versão de serviços Internet com pontos em 21 estados no País foi implantada pela Rede Nacional de Pesquisa (RNP) de 1991 a 1993, a velocidades baixas. Entre 1995 e 1996, esses serviços foram atualizados para velocidades mais altas. Paralelamente, a partir de junho de 1995, uma decisão do Governo Federal definiu as regras gerais para a disponibilização de serviços Internet para quaisquer interessados no Brasil.[25]

Entre os 21 Estados cuja infraestrutura fora implantada, insere-se, por exemplo, o Estado da Paraíba, cujo ponto de presença foi instalado na *hig-tech* cidade de Campina Grande, dando suporte, por conseguinte, a instalação dos sistemas de rede que passariam a ser utilizados pela Rede Paraibana de Pesquisa - RPP, iniciativa que reuniu a Universidade Federal da Paraíba (UFPB), Fundação Parque Tecnológico da Paraíba (PAQTC), Fundação de

---

[23] STANTON, Michael. **A evolução das redes acadêmicas no Brasil: Parte 1 - da BITNET à Internet. Boletim Bimestral da RNP V.2, n. 6.Rio de Janeiro: RNP, 1998**. Disponível em <http://www.rnp.br/newsgen/9806/inter-br.html>. Acesso em: 10 fev. 2009.

[24] **LINHA DO TEMPO DA INTERNET NO** BRASIL. Disponível em <http://www.internetnobrasil.net/index.php?title=1988>. Acesso em: 10 fev. 2009.

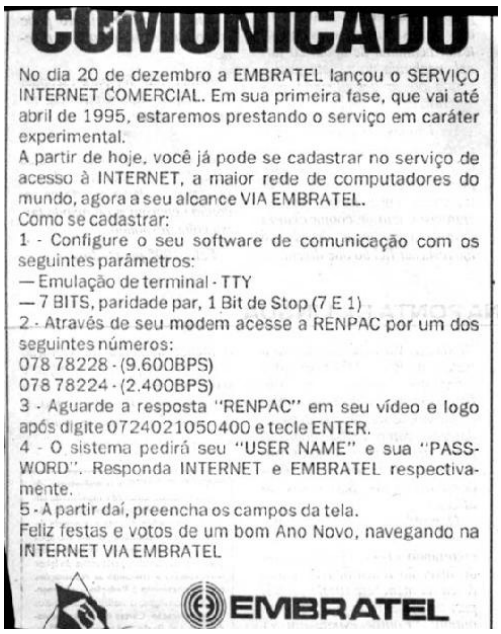
[25] TAKAHASHI, Tadao (Org.) **Sociedade da informação no Brasil: livro verde**. Brasília: Ministério da Ciência e Tecnologia, 2000, p. 133.

Apoio a Pesquisa da Paraíba (FAPESQ) com suporte da RNP/MCT e CNPq. Esta embrionária rede denominada RPP "tem por objetivo implantar, coordenar e disseminar o uso no Estado de uma infra-estrutura de comunicação de dados nos moldes da RNP"[26] congregando instituições de ensino, pesquisa e desenvolvimento.

Em dezembro de 1994, a EMBRATEL (Empresa Brasileira de Telecomunicações), ainda empresa pública, iniciou os primeiros testes comerciais com linhas discadas, escolhendo 5 mil usuários para efetuar os testes em dezembro de 1994.

Na figura abaixo, pode ser visualizada as fáceis instruções para conexão com o serviço:

Figura 1 – Comunicado da EMBRATEL – serviço internet comercial



COMUNICADO

No dia 20 de dezembro a EMBRATEL lançou o SERVIÇO INTERNET COMERCIAL. Em sua primeira fase, que vai até abril de 1995, estaremos prestando o serviço em caráter experimental.
A partir de hoje, você já pode se cadastrar no serviço de acesso à INTERNET, a maior rede de computadores do mundo, agora a seu alcance VIA EMBRATEL.
Como se cadastrar:
1 - Configure o seu software de comunicação com os seguintes parâmetros:
— Emulação de terminal - TTY
— 7 BITS, paridade par, 1 Bit de Stop (7 E 1)
2 - Através de seu modem acesse a RENPAC por um dos seguintes números:
078 78228 - (9.600BPS)
078 78224 - (2.400BPS)
3 - Aguarde a resposta "RENPAC" em seu vídeo e logo após digite 072402105040 0 e tecle ENTER.
4 - O sistema pedirá seu "USER NAME" e sua "PASSWORD". Responda INTERNET e EMBRATEL respectivamente.
5 - A partir daí, preencha os campos da tela.
Feliz festas e votos de um bom Ano Novo, navegando na INTERNET VIA EMBRATEL

EMBRATEL

Fonte: Linha do tempo da internet no Brasil[27]

Alternativamente às conexões viabilizadas no meio acadêmico sob gerência da RNP e pela EMBRATEl, Stanton ao falar da história da internet no Brasil sustenta que:

> A Associação para Comunicações Progressiva (APC) , uma organização internacional de ONGs, incluía o nó Alternex , operado pelo IBASE (Instituto Brasileiro de Análises Sociais e Econômicas) do Rio de Janeiro, e montado com o apoio do Programa das Nações Unidas para o Desenvolvimento (PNUD) em 1989. A Alternex oferecia serviços de *news* e correio eletrônico a indivíduos e organizações sem fins lucrativos. Até 1992 a Alternex/IBASE fazia sua comunicação internacional com IGC

[26] RPP - Rede Paraibana de Pesquisa. **Histórico do ponto de presença da RNP na Paraíba**. Campina Grande, 2008. Disponível em: <http://www.pop-pb.rnp.br/historico.html>. Acesso em: 28 jan. 2009.
[27] **LINHA DO TEMPO DA INTERNET NO BRASIL**. Disponível em <http://www.internetnobrasil.net/index.php?title=1988>. Acesso em: 10 fev. 2009.

> (*Institute for Global Communication* - o ponto de acesso à Internet da APC na California, EUA), usando a tecnologia UUCP sobre ligações discadas.[28]

Em face da necessidade de controle da gestão da internet, em junho de 1995, foi criado, mediante Portaria do Ministro da Ciência e Tecnologia, o Comitê Gestor da Internet, composto por membros dos Ministérios das Comunicações, Sistema Telebrás, Conselho Nacional de Pesquisa e Desenvolvimento Cientifico e Tecnológico, especialistas em redes, comunidades acadêmicas, provedores de serviços, empresas, representantes das Instituições comerciais e econômicas.

O Comitê Gestor tinha como atribuições: fomentar o desenvolvimento de serviços INTERNET no Brasil; recomendar padrões e procedimentos técnicos e operacionais para a INTERNET no Brasil; coordenar a atribuição de endereços INTERNET, o registro de nomes de domínios, e a interconexão de espinhas dorsais; coletar, organizar e disseminar informações sobre os serviços INTERNET.

Neste momento da história da internet (1995) os primeiros serviços privados eram disponibilizados pelos chamados BBSs (*Bulletin Board Systems*), espécies de provedores de acesso a serviços básicos como bate papo, email e serviços de FTP (*file transfer protoco*l – serviço de transferência de arquivos), configurando-se um vertiginoso da Internet no Brasil.

A relevância da Internet já era patente. Além de ser uma forma revolucionária de comunicação e acesso a informações, havia uma demanda reprimida muito grande sob o ponto de vista comercial, pois a EMBRATEL e o Ministério das Comunicações dificultavam as iniciativas dos provedores privados, uma vez que a infraestrutura das conexões de rede não estavam totalmente implantadas, além da indefinição dos custos a serem cobrados.

A partir de 1996 grandes grupos empresariais nacionais como o Grupo Abril, RBS (do Rio Grande do Sul) e Grupo Folha passaram a vender os serviços de assinatura de acesso e de conteúdo. Paralelamente houve uma significativa melhora na infraestrutura e velocidade das conexões.

Em 1997 tivemos a consolidação da Internet brasileira. Novas revistas sobre o assunto foram lançadas, os provedores chegaram a diversas centenas, o conteúdo em língua portuguesa na rede tornou-se significativo. Bancos, empresas, universidades e o governo passaram a manter pontos de presença na grande rede. Estimativas otimistas, mas sem referencial científico, indicavam que o número de usuários no Brasil passou de um milhão.

---

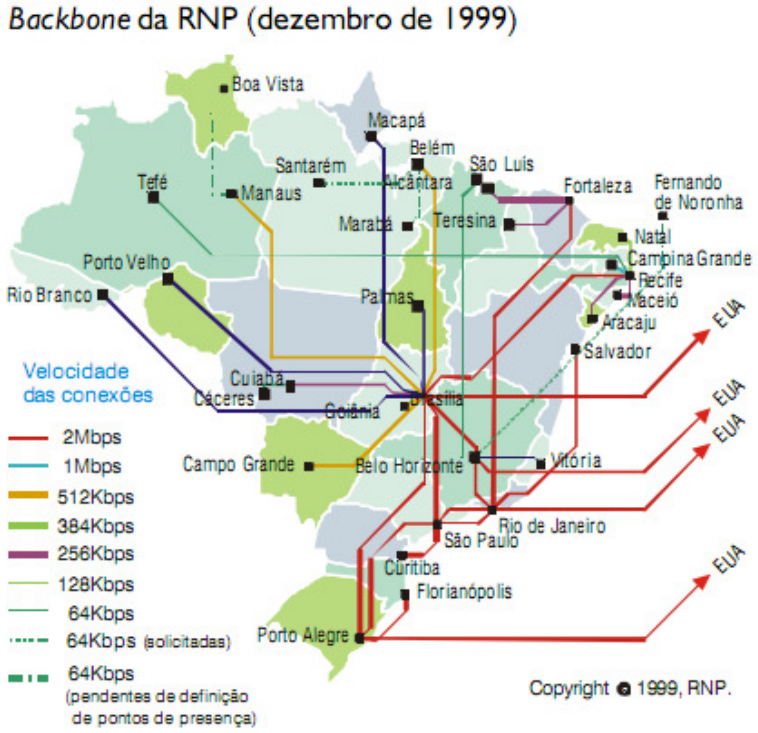
[28] STANTON, op. cit. n.23.

Em 1998 havia uma estimativa de que o número de usuários havia crescido 130% em relação ao ano anterior, segundo estudo do instituto de pesquisa IDC. Desde 1995, com a exploração comercial da Internet no Brasil, o número de usuários cresce a taxas de mais de 100 porcento ao ano. O ano de maior crescimento foi 1996, com 192 porcento. "A analista Monica Benatti, responsável pelo estudo, declarou ao Infonews que, a partir deste ano, o crescimento começa a ser mais lento. A previsão para 1999 é de 40 porcento."[29]

Até o final da década, do século e do milênio, por consequência foram marcados pela consolidação da internet, sobretudo, pelo seu crescimento exponencial a penetração cada vez mais maciça em vários ramos de atividades comerciais, educacionais, de entretenimento e governamentais.

Abaixo temos a figura mostrando a disposição da infraestrutura de rede no Brasil no final do ano de 1999:

Figura 2 – Infraestrutura da rede no final de 1999[30]



Fonte: adaptado de http://www.rnp.br

[29] **História da internet no Brasil**. Disponível em < http://www.internetnobrasil.net/index.php?title=1999>. Acesso em: 10 fev. 2009.
[30] TAKAHASHI, op.cit. n.25, p. 102.

Pode se imaginar nesta linha do tempo, que há dez anos os microcomputadores com acesso à internet no Brasil eram um bem de consumo disponível para um número limitado de lares, isto é, classes média e alta. O acesso também acontecia em locais de trabalho, mas com uso muito limitado devido às restrições naturais decorrentes das relações laborais.

Não é difícil concluir, pois, que havia uma demanda reprimida. Fatores como o alto custo dos microcomputadores, restrições de acesso à internet devido aos problemas ainda existentes no setor de telecomunicações e de provedores de serviço em locais distantes dos grandes centros urbanos. Estes fatores, conjugados ao momento de incerteza econômica (crises internacionais com efeitos no Brasil), configuravam-se como obstáculos ao crescimento e popularização da internet.

Até meados do ano 2000 as dificuldades também atingiam o setor de *e-commerce* em face da desconfiança em relação às compras virtuais e das crises internacionais, a exemplo do *crash* das empresas ponto com, denominado de "estouro da bolha". O número estimado de usuários era de pouco mais de 5 milhões de usuários. Neste cenário, pode se dizer, que a incidência de cibercrimes também era muito restrita, com atuações pontuais de "*defacers*[31]", principalmente. Isto nos induz a pensar numa lógica natural: se o comércio é incipiente, há pouco registro de ações criminosas no setor comercial.

Merece registrar que a "geração internet" é composta hoje por adolescentes na faixa etária de 13 a 15 anos, o que corresponde, aproximadamente, ao período em que os serviços de internet passaram a ser explorados de forma comercial no Brasil. Estes jovens já nasceram e cresceram imersos no uso potencial e comercial de computadores em ambientes de trabalho, nas escolas e residências.

Esse cenário inicial começou a mudar desde 2002. A estabilidade econômica proporcionou oportunidades para consumidores das classes menos favorecidas. De acordo com o site Convergência Digital, do Portal Terra, “medidas de incentivo fiscal concedidas pelo governo à indústria de computadores e a estabilidade econômica e ao crescimento da renda das classes C, D e E, tornaram os PCs um objeto de consumo comum”[32], como outra utilidade necessária a uma residência. Soma-se ainda a este fator a baixa cotação do dólar

---

[31] *Defacers* é a expressão empregada para designar a ação uma forma de ação de *crackers* (uma espécie de “hacker do mal”) que desfiguram páginas de internet deixando mensagens ou até mesmo subtraindo informações de sistemas de banco de dados.

[32] **BRASIL vive o maior "boom" de acessos residenciais à Internet.** São Paulo: Convergência Digital, 2008. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=13021&sid=4>. Acesso em: 2 ago.2008.

frente ao real, o que possibilita menores custos, pois os componentes eletrônicos são cotados na moeda americana.

É necessário lembrar também, que houve uma evolução muito grande na infraestrutura de telecomunicações. As privatizações ocorridas no segundo governo de Fernando Henrique Cardoso não foram capazes de provocar um impacto significativo até o ano 2000. Os efeitos da livre concorrência no setor só puderam ser registrados após 2003. Não é de se estranhar, dessa forma, que o uso de internet discada no Brasil está bem restrito nos dias atuais. A utilização da internet banda-larga tornou-se o padrão de acesso comum ao usuário residencial e comercial, isto a um baixo custo.

Experimenta-se, pois, um momento de inclusão digital sem precedentes, correspondendo a um número estimado de 22,4%[33] da população. A quantidade de usuários brasileiros registra a marca de mais de "40 milhões no último trimestre de 2007, o que equivale a um crescimento de 21,27% sobre o mesmo período de 2006, quando era de 32,9 milhões de pessoas"[34], de acordo com informações do IBOPE, valendo ressaltar que tais números se referem aos acessos residenciais, telecentros, comerciais, *cyber-café* e *lan-houses*. Entre 2000 e 2007, houve um crescimento de 752%, um salto de pouco mais de 5 para mais de 42,6 milhões de usuários[35], conforme números do site *Internet World Stats*, constantes na tabela abaixo:

Tabtela 1 – Número de usuários de internet na América Latina

LATIN AMERICA COUNTRIES / REGIONS	Population (Est. 2007)	Internet Users, Latest Data	% Population (Penetration)	% Users in Table	Use Growth (2000-2007)
Argentina	40,301,927	16,000,000	39.7 %	13.0 %	540.0 %
Bolivia	9,119,152	580,000	6.4 %	0.5 %	383.3 %
Brazil	**190,010,647**	**42,600,000**	**22.4 %**	**34.7 %**	**752.0 %**
Chile	16,284,741	7,035,000	43.2 %	5.7 %	300.3 %
Colombia	44,379,598	10,097,000	22.8 %	8.2 %	1,050.0 %
Costa Rica	4,133,884	1,214,400	29.4 %	1.0 %	385.8 %
Cuba	11,394,043	240,000	2.1 %	0.2 %	300.0 %
Dominican Republic	9,365,818	2,100,000	22.4 %	1.7 %	3,718.

Fonte: *Internet World Stats*[36] (grifo nosso).

[33] **INTERNET** ***user statistics and population stats for the countries and regions that comprise Latin American internet users***. EUA: Internet World Stats, 2008. Disponível em: <http://www.internetworldstats.com/stats10.htm#spanish>. Acesso em: 2 ago.2008.
[34] **BRASIL vive o maior "boom" de acessos residenciais à Internet,** op.cit.n. 32.
[35] **BRASIL vive o maior "boom" de acessos residenciais à Internet**, op.cit.n. 32.
[36] **BRASIL vive o maior "boom" de acessos residenciais à Internet**, op.cit.n. 32.

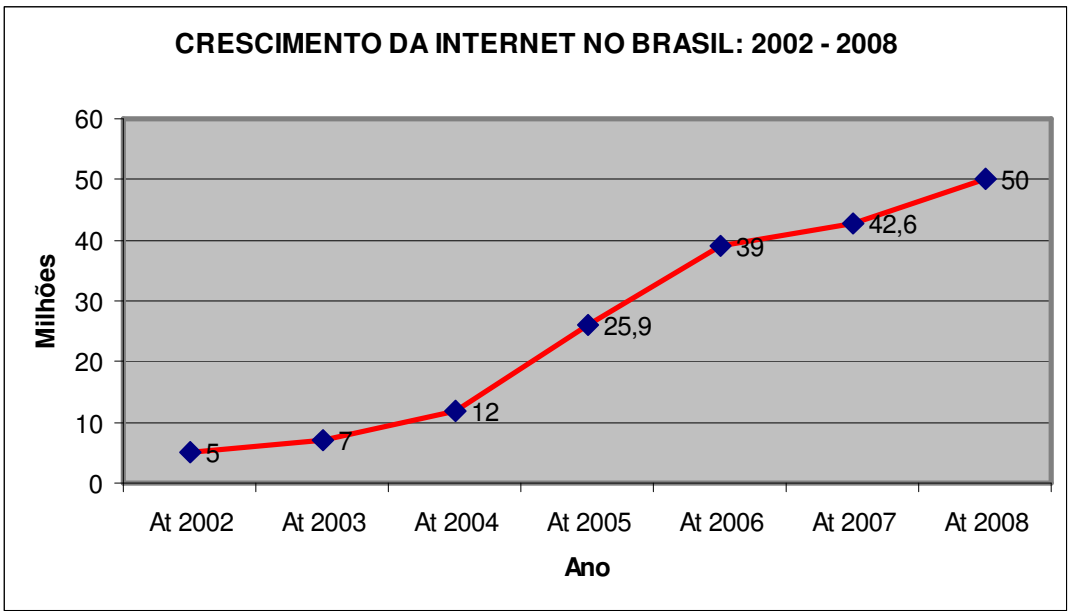
O registro de transações comerciais on-line também cresceu. Estima-se que "o varejo online deve movimentar R$ 8,8 bilhões, subindo 45% em relação a 2007, com um total de 12 milhões de consumidores"[37], que compram eletroeletrônicos, revistas e livros, principalmente. Somam-se ainda a estes números as transações bancárias por "*home banking*" que indicam que "27,3 milhões de pessoas"[38] fazem uso do sistema no Brasil.

Este cenário, com uma pequena amostra a partir do Brasil, denota o grande número de pessoas que fazem uso de internet, evidenciando o que Matias[39] convencionou chamar de "globalização virtual que concentra os extraordinários avanços no processamento e na transmissão da informação", um dos pilares da sociedade da global.

Numa escala mundial, de acordo com a *Internet World Stats*[40], estima-se mais de 1 bilhão e trezentos e cinquenta mil usuários, com destaque para: EUA (215 milhões), China (210 milhões), Japão(87,5 milhões), Índia (60 milhões), Alemanha(53,2 milhões), Brasil(50 milhões), Reino Unido(40,4 milhões), França(34,9 milhões) e Itália(33,1 milhões).

Os números que evidenciam a trajetória histórica de crescimento da internet no Brasil apontam o seguinte:

Gráfico 1 – Crescimento da Internet no Brasil



Fonte: *Internet World Stats* e pesquisa do autor

[37] SANCHEZ, Ligia. **E-commerce deve chegar a R$ 8,8 bilhões no Brasil em 2008**. São Paulo: It Web, 2008. Disponível em: <http://www.itweb.com.br/noticias/index.asp?cod=46185>. Acesso em: 2 ago.2008.
[38] MAIA, Felipe. **Entidades discutem adoção de endereço "b.br" para bancos na web**. São Paulo: Folha On Line, informática, 2008. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u395485.shtml>. Acesso em: 2 ago.2008.
[39] MATIAS, op. cit. n.1, p. 121.
[40] ***INTERNET WORLD STATES***, op.cit.n. 33.

Não seria extraordinário, assim, imaginar que num universo 1,3 bilhões de usuários não exista uma parcela significativa de pessoas e organizações criminosas a desafiar as ações do Estado no ciberespaço, mediante prática de estelionato, espionagem industrial, subtração de informações, dano moral, racismo e também pessoas que "produzem e ou distribuem pornografia usando o computador", como ensina Schell e Martin[41]. Desta forma, concordando com o pensamento de Jean Ziegler[42], "para o crime organizado, a internet é um presente do céu."

2.3 Globalização e Revolução Tecnológica

A compreensão de como se originou, amadureceu e se desenvolve o processo de globalização mundial propicia um embasamento teórico para entender como as novas modalidades de crimes perpetrados por pessoas e organizações criminosas têm prosperado no rastro da Revolução Tecnológica[43]. De modo paralelo, será possível demonstrar como estes fenômenos "pós-modernos"[44] têm afetado a dimensão jurídica inerente à soberania estatal.

Um olhar sobre a dinâmica do que se vivencia induz a uma falsa impressão de que a Globalização, como fenômeno social, é um acontecimento que remonta aos últimos vinte anos.

Esta ideia aproxima-se de fatos históricos recentíssimos, como a queda do Muro de Berlim, em 1989, a desagregação do bloco socialista a partir de 1991 e o consequente fim da guerra fria.

Essa visão contraria a lógica de todo processo histórico. Isto porque a concepção de um mundo globalizado tem vinculação até mesmo com a expansão ultramarina lusitana e ibérica do final do século XV. Num momento posterior, essa concepção de expandir o intercâmbio comercial com outras regiões além-fronteira, serão também influenciadas pelo desenvolvimento experimentado a partir da Revolução Industrial, num processo interligado de

---

[41] CHELL, Bernadete Hlubik; MARTIN, Clemens. ***Cybercrime: A Reference Handbook*.** ABC-CLIO: Santa Bárbara, 2004, p.3.
[42] ZIEGLER, Jean. **Os senhores do crime**. Tradução de Clóvis Marques. Rio de Janeiro: Record, 2003, p. 269.
[43] "Revolução Tecnológica" é a expressão utilizada para designar o processo desenvolvimento e convergência de computadores, suas redes e das telecomunicações.
[44] Ainda que exista muita controvérsia sobre o emprego da terminologia, compreendida como "pós-modernidade".

evolução natural das sociedades, por isso "[...] longe de ser um conceito original ou inédito na história, na sociologia política, na teoria econômica ou mesmo na ciência do direito".[45]

Ainda que o caráter econômico desse processo seja o mais destacado, seus efeitos são estendidos a outras áreas, apresentando um caráter "tecnológico, cultural, político e institucional"[46], afetando, consequentemente, organizações (públicas, privadas e não governamentais) e as pessoas. Neste sentido Paul Hopper[47] defende que a"[...] globalização é mais que simplesmente capitalismo global. Pessoas estão viajando pelo mundo e estabelecendo conexões globais e redes de trabalho por razões variadas, além de financeira e econômica."[48]

Não há consenso doutrinário capaz de propiciar uma definição sobre o termo Globalização ou até mesmo o emprego da terminologia adequada para expressar o processo. Entretanto, Matias[49] entende que "a globalização surge no marco de uma nova era econômica, com características que a diferenciam do movimento anterior de internacionalização da economia, cujo apogeu ocorreu antes da Primeira Guerra Mundial", o que justifica o emprego do termo.

Em face da dificuldade de condensar o pensamento exposto por muitos autores, parece-nos adequado assinalar a definição sintetizada por Matias[50] ao afirmar que a globalização é:

> A aceleração nas trocas de bens, serviços, contratos, informação, viagens internacionais e intercâmbio cultural ou como a maior integração dos países e das pessoas do mundo, causada pela enorme redução dos custos de transporte e comunicação, e pela derrubada das barreiras artificiais ao fluxo de bens, serviços, capital conhecimento e - em menor extensão - pessoas através das fronteiras.

Evidencia-se assim, uma concepção macro em relação à globalização (*latu sensu*) incluindo todos os aspectos não econômicos e uma acepção especificamente voltada para o mercado, isto é, a globalização econômica, embora esta, esteja incluída como uma das faces da primeira.

---

[45] FARIA, José Eduardo. **O direito na economia globalizada**. São Paulo: Malheiros, 1999, p. 60.
[46] MATIAS, op. cit.n.1, p. 106.
[47] HOPPER, Paul. ***Linving with globalization***. New York: Berg Publisher, 2006, p, 4.
[48] Texto original: "[…] *globalization is more than simply global capitalism. People are moving across the globe and stabilishing global connections and networks for a variety of reasons, beyond the financial and economic"*.Tradução nossa.
[49] MATIAS, op. cit.n.1, p. 105.
[50] Idem, n. 41.

Deve-se, portanto, enxergar o fenômeno como um processo em construção voltado para a formação de uma sociedade e de uma economia global, com a "a intensificação da interdependência dos povos, que, embora seja notada de forma marcante no plano econômico, reflete-se também em todos os demais fenômenos mencionados"[51] (globalização econômica, revolução tecnológica, surgimento de uma sociedade civil e de organizações transnacionais, crescente cooperação internacional), que são complementares.

Além de considerarmos o aspecto conceitual da globalização[52], sob uma perspectiva histórica tem que ser destacados importantes marcos históricos, como a expansão ultramarina no final Século XV e Século XVI, experimentada à base da evolução da cartografia sob liderança de Portugal e Espanha. Num momento seguinte, "já nos séculos XVII e XVIII, os fluxos mundiais de comércio e riqueza levaram ao aparecimento de novos pólos de poder na Europa, com o fortalecimento econômico, social e político da burguesia; formação dos Estados nacionais e o advento do mercantilismo e do colonialismo europeu".[53] Tais processos, ainda que não fosse empregado o termo "globalização", podem ser compreendidos nessa dimensão.[54]

Num momento posterior (séculos XVIII e XIX), destaca-se a Revolução Industrial, notadamente com a invenção da máquina a vapor de Watt que possibilitou várias aplicações industriais como o barco a vapor, emprego de máquinas na produção industrial em substituição a grande parte da mão de obra humana e aperfeiçoamento nos meios de transporte com a invenção de locomotivas, o que contribuiu, consequentemente, para o encurtamento de distância, aumento do intercâmbio entre os povos e acumulação de capital, características intrínsecas à evolução do processo de globalização.

Do final do século XIX ao início do século XX, as nações vivenciaram um período de grande expansão econômica. "Os desenvolvimentos técnicos e organizacionais, após a década de 1870, permitiram que uma maior variedade de produtos fosse produzida internamente e fora do país (Inglaterra), dentro dos limites de uma mesma empresa [...]"[55], com avanços significativos da integração mundial de capitais e mercadorias.

---

[51] MATIAS, op. cit. n.45, p. 108.

[52] O aspecto conceitual é relevante por considerar a globalização sob o ponto de visto do processo histórico de evolução da sociedade. Se levarmos em conta determinado período em detrimento de outro mais avançado na linha do tempo teremos consequentemente, concepções diferentes sobre o mesmo objeto de estudo, daí a compreensão da globalização como um processo em construção.

[53] FARIA, op. cit. n.45, p. 60.

[54] O processo de formação dos Estados nacionais têm ligação direta com os debates sobre soberania, isto porque só foi possível consolidar o Estado forte com o fim do poder que antes estava na mão dos senhores feudais, o que dissipava o poder nas mãos de muitos, ainda que existisse um território único.

[55] HIRST, Paul; THOMPSON, Grahame. **Globalização em questão**: a economia internacional e as possibilidades de governabilidade. Tradução Wanda Caldeira Brant. Petrópolis, RJ: Vozes, 1998, p. 41.

Este processo de expansão foi estancado por fatos históricos marcantes, no caso, a I Guerra Mundial, Revolução Russa de 1917 (como contraponto o Comunismo passaria a rivalizar com o capitalismo) e a crise provocada pelo *"crash"* da Bolsa de Nova Iorque, em 1929, culminando com a II Grande Guerra Mundial (uma continuação da I Grande Guerra). Estes fatos históricos provocaram no período uma grande crise, notadamente de caráter econômico e ideológico que só viria a se dissipar quase meio século depois.

No bojo dos horrores decorrentes da II Grande Guerra Mundial, com o seu fim em 1945, o mundo experimentou um período de grandes transformações, principalmente de ordem política, econômica e, sobretudo, ideológica. Assinalou também, o fim da hegemonia mundial da Europa e a ascensão de duas superpotências, os Estados Unidos da América (EUA) e a União das Repúblicas Socialistas Soviéticas (URSS), que travariam no pós-guerra (1945-1989), o período denominado Guerra Fria e a consequente divisão do mundo em duas áreas de influências: uma capitalista, sob liderança dos EUA e outra socialista, sob comando da URSS.

Se sob uma perspectiva a grande depressão provocada pelas I e II grandes Guerras, pela crise econômica na segunda década do século XX e a bipolarização do mundo com os seus desdobramentos foram capazes de retardar o processo de globalização, sob outra ótica, os países, notadamente envolvidos nos conflitos armados tiveram que transpor grandes obstáculos de ordem científica e tecnológica para fornecer a logística necessária à guerra, consequentemente muitas dessas inovações tiveram aplicações civis num segundo momento, o que contribuiu indiretamente para a aceleração do processo de globalização no final do século XX.[56]

Neste sentido Faria entende que:

> Tão ou mais importante foi o impacto da já mencionada conversão da ciência e da tecnologia em fator básico de produção, de competitividade e inovação contínua sobre a ordem econômica mundial. Não é difícil compreender o motivo pelo qual este impacto passou a ser visto como principal mola propulsora do fenômeno da globalização.[57]

Outros fatos político-ideológicos foram marcantes e decisivos para propiciar o cenário adequado à expansão do processo de globalização, sendo dois deles decisivos: a

[56] Um exemplo das aplicações civis de tecnologia desenvolvida para as guerras, por exemplo, temos o notável desenvolvimento da aviação no pós I Guerra Mundial. No pós II Guerra Mundial, com a corrida espacial, houve um notável crescimento da infra-estrutura de telecomunicações, fator decisivo para a ampliação e disponibilização de serviços imprescindíveis à internet.
[57] FARIA, op. cit. n. 45, p. 86.

queda do Muro de Berlim (1989) e a desagregação da União Soviética. O muro era um símbolo significativo da divisão do mundo no pós-guerra em áreas de influência capitalista e comunista (Alemanha Ocidental e Alemanha Oriental) e a sua queda abriu as portas para que a pressão existente sobre os países do Leste Europeu fosse dissipada em forma de movimentos de reivindicação por liberdade e democracia.

A desagregação da União das Repúblicas Socialistas Soviéticas - URSS em vários países independentes (do Leste Europeu) veio em seguida. Não era mais possível a manutenção de um regime que buscava a igualdade de todos num tempo de efervescência do capitalismo. Assim, a partir de 1991, ainda que tenha mudado a denominação para Comunidade dos Estados Independentes, a ex-URSS e seus liderados tiveram que buscar novas alternativas a um modelo que não deu certo. "Embora o capitalismo certamente não se achasse na melhor das formas no fim do Breve Século XX, o comunismo do tipo soviético estava inquestionavelmente morto, e era muito improvável que revivesse".[58]

Em sua obra "O mundo é plano: uma breve história do século XXI", Friedman , pontifica:

> A queda do Muro de Berlim, em 9 de novembro de 1989, liberou forças que acabariam libertando todos os povos dominados pelo Império Soviético - mas, na realidade, fez também muito mais que isso: inclinou a balança do poder mundial para o lado dos defensores da governança democrática, consensual, voltada para o livre mercado, em detrimento dos adeptos do governo autoritário, com economia de planejamento centralizado. A Guerra Fria foi um embate entre dois sistemas econômicos - capitalismo e comunismo. Com a queda do Muro, sobrou apenas um sistema, pelo qual todos, de alguma forma, tiveram de se orientar.[59]

Os denominados grandes avanços - no sentido de progresso da humanidade, estão associados ao desenvolvimento científico e a sua consequente aplicação na vida das pessoas, cujos inventos e aperfeiçoamentos são capazes de gerar ou de produzir saltos de qualidade de vida e de retorno econômico. É possível, por isso, asseverar que os fatos mais marcantes do processo de globalização estão interligados, também, com o desenvolvimento e aplicação de novas tecnologias ou processos produtivos.

Desta forma, na lição de Matias:

> São três os grandes paradigmas econômicos da humanidade após a Idade Média. No primeiro, predominaria a agricultura, o hoje chamado setor primário da economia.

---

[58] HOBSBAWM, Eric. **Era dos extremos**: o breve século XX: 1914-1991. Tradução de Marcos Santarrita. São Paulo: Companhia das Letras, 1995, p.553.

[59] FRIEDMAN, Thomas Lauren. **O mundo é plano**: uma breve história do século XXI - Tradução de Cristina Serra e S Duarte. Rio de Janeiro: Objetiva, 2005, p. 62.

> Com a modernização da economia, teríamos alcançado o segundo paradigma, marcado pelo predomínio da indústria, o setor secundário. Hoje, após um processo de informatização, o setor predominante seria o terciário, em que os serviços e a informação estaria no centro da produção econômica.[60]

A compreensão do processo de globalização não pode ser estanque. Todos os acontecimentos de ordem histórica, social, tecnológica e científica estão interligados, numa relação de interdependência variável, conforme o setor para o qual se observe.

Um olhar sobre o processo de globalização hoje vivido, ainda que guarde raízes num passado remoto, é diferente do momento vivido até antes da I Guerra Mundial, pois o avanço científico e tecnológico proporcionado pela criação e aperfeiçoamento do computador e das redes de telecomunicações foram capazes de denominar os fatos registrados (e que ainda estão se aprimorando) no final do Século XX e início do Século XXI da denominada "Revolução Tecnológica".[61]

Enxergando o fenômeno como um acontecimento muito recente, pergunta-se: em que momento e quais acontecimentos da história recente podem ser considerados marcantes para a Revolução Tecnológica? É possível considerar os seguintes fatos marcantes: a criação do primeiro computador eletrônico (1946);[62] lançamento do primeiro satélite para telecomunicações (1960);[63] a criação da internet (1969);[64] a venda em escala comercial dos computadores pessoais (1971) e a criação da WWW ou interface gráfica da internet em 1991 , sendo assim "a profundidade das transformações ocorridas justifica a denominação especial de revolução tecnológica às inovações científicas recentes".[65]

Neste cenário é possível compreender como o processo de globalização se desenvolveu e foi potencializado, motivo pelo qual, tais ideias associam-se ao pensamento de Friedman sobre um “mundo plano” ao externar:

> É inegável que agora um número maior do que nunca de pessoas têm a possibilidade de colaborar e competir em tempo real com um número maior de outras pessoas de um número maior de cantos do globo, num número maior de diferentes áreas e num pé de igualdade maior do que em qualquer momento anterior da história do mundo - graças aos computadores, ao correio eletrônico, às redes, à tecnologia de teleconferência e a novos softwares, mais dinâmicos.[66]

---

[60] MATIAS, op. cit. n. 45, p. 118-119.
[61] Para Matias (op. cit. n. 52) a Revolução Tecnológica decorre da união de aplicações de computadores e das telecomunicações, fazendo surgir as redes de computadores e consequentemente a internet e suas aplicações.
[62] MONTEIRO, Mário A. **Introdução à organização dos computadores**. 3a ed. Rio de Janeiro: LTC Ed., 1996, p.9.
[63] GONÇALVES, Patrícia. **Primeiro satélite de comunicações chegou a órbita há 46 anos**: in Revista Ciência Hoje, versão eletrônica. Disponível em: <http://www.cienciahoje.pt/3889>. Acesso em: 01 jul.2008.
[64] VASCONCELOS, op. cit. n. 21, p. 33.
[65] MATIAS, op. cit. n. 1, p. 19.
[66] FRIEDMAN, op. cit. n. 59, p. 16.

A nova configuração do espaço global, no pós-guerra fria, com suporte dos recursos tecnológicos fez surgir à sociedade da informação. Noutra dimensão, em contraponto aos inúmeros benefícios, houve uma globalização também das ações criminosas com efeitos muito fortes na sociedade, a exemplo dos crimes de internet, ora objeto de estudo, além de outras ações como o terrorismo.

2.4 Ciberespaço: origem, evolução e características

Algumas terminologias apresentam-se associadas à ideia de ciberespaço e muitas vezes empregadas como sinônimas. Cibernética, realidade virtual, internet e *WWW* (*World Wide Web*) ou *Web*, são erroneamente empregados como se tivessem o mesmo significado. Ainda que existam aplicações tecnológicas assemelhadas, a expressão cibernética e ciberespaço bem como as demais têm significado diferentes.

A palavra cibernética deriva do grego "*kubernetes*", com o sentido da palavra piloto, timoneiro, utilizada até mesmo por Platão para qualificar a ação da alma. A doutrina dominante indica que o termo foi utilizado por Norbert Wiener[67] em 1948, onde procurou nominar uma nova ciência que buscava a compreensão dos fenômenos naturais e artificiais através do estudo dos processos de comunicação e controle nos seres vivos, nas máquinas e nos processos de interação social, sendo, portanto, o idealizador da teoria cibernética.

Neste mesmo sentido, com a devida conexão com o novo modelo de sociedade global, Theophilo compreende a cibernética da seguinte forma:

> A cibernética nasceu do estudo comparado das máquinas eletrônicas automáticas sobre os processadores do sistema nervoso dos seres vivos e as suas respectivas conexões nervosas. A simulação deste comportamento pelo computador gerou, na prática, o surgimento da cibernética. Com o desenvolvimento da tecnologia o termo estendeu-se às máquinas que efetuam movimentos diferentes segundo alguma condição interna. Com o advento da eletrônica e a sua grande evolução foi possível a utilização das condições elétricas, magnéticas e óticas, bases dos processadores digitais e da cibernética atuais.[68]

---

[67] O título da obra de Wiener onde é exposta sua teoria cibernética é "*Cybernetics: or control and communication in the animal and the machine*", de 1948.

[68] THEOPHILO JÚNIOR, Roque. **Cibernética Tecnologia e Psicologia**. São Paulo, Academia Brasileira de Psicologia, 2000. Disponível em: <http://www.psicologia.org.br/internacional/ap11.htm>. Acesso em 1 ago.2008.

Desta forma, é possível compreender a associação da cibernética, na atualidade, com os processos de automação, notadamente na indústria, comércio e no setor de serviços, potencializando, desta forma, o emprego de sistemas eletrônicos e digitais em atividades empresariais, num relacionamento entre "todos os campos de estudo,"[69] como ciência da comunicação e do controle. Embora este não seja o sentido que se procure vincular ao presente trabalho, indiscutível a relevância da compreensão da terminologia.

Já a realidade virtual, na lição de Fragoso, é assim posta:

> A Realidade Virtual se apresenta como o mais recente desenvolvimento de uma linhagem de tecnologias de comunicação cuja principal intenção é propiciar ao receptor a ilusão de estar na presença imediata do objeto da representação. Tal enquadramento na linhagem predominante da história dos meios visuais de representação determina que, pelo menos inicialmente, os sistemas de realidade virtual permaneçam atrelados a formas de representação espacial consideradas 'realistas' e 'transparentes' no presente contexto cognitivo e cultural.[70]

Para Hoeschl[71] "A realidade virtual é uma técnica, gerada através de uma série de conceitos, equipamentos e programas, com o fim de formar uma representação de algo que pode ou não existir materialmente [...]." Neste sentido a ideia principal é a intenção de produzir interação humana, numa reprodução tridimensional da realidade que só existe no ambiente imaginário. Esta ideia vincula-se, pois, a uma percepção de simulação de eventos reais, como acontecem em simuladores de voo, projetos arquitetônicos, simuladores de prática de tiro e simulações na área médica.

A Internet é definida por muitos autores como um complexo de redes de computadores, sem que nenhuma esteja subordinada à outra, ou seja, não há um comando central, conforme detalhamento no capítulo específico. Nela estariam inseridas todas as funcionalidades como: páginas WWW ou *Web*, as aplicações de e-mail e também as funcionalidades de transferência e armazenamento de arquivos, denominada de *File Transfer Protocol* (FTP – protocolo de transferência de arquivos). Este complexo se denomina internet e todas as informações a ela inerentes transitam pelo ciberespaço.

---

[69] SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: Editora Revista dos Tribunais, 2003, p. 20.

[70] FRAGOSO, Suely. **Realidade Virtual e Hipermídia - somar ou subtrair?** São Leopoldo: Cyberlegenda nº 9, 2002. Disponível em:<http://www.uff.br/mestcii/sueli1.htm>. Acesso em: 1 set.2008.

[71] HOESCHL, Hugo César. **O ciberespaço e o direito III**. Florianópolis: IJURIS - Instituto de Governo Eletrônico, Inteligência Jurídica e Sistemas, 1997. Disponível em: <http://www.ijuris.org/producaotc/direito_digital/digital/ciber3.htm>. Acesso em: 1 ago.2008.

Muitos autores que se dedicam ao estudo do ciberespaço indicam que o termo foi utilizado pela primeira vez em 1984, por William Gibson, em sua obra de ficção científica intitulada *Neuromancer*. [72]

No início da década de 80 quando Gibson teve as primeiras ideias visionárias sobre o ciberespaço "[...] os computadores pessoais finalmente começaram a atingir um nível de desenvolvimento suficiente para permitir o uso de aplicativos sérios. Surgiram então os primeiros aplicativos de processamento de texto, planilhas, e até mesmo programas de editoração e desenho [...]"[73], ainda que a internet para uso doméstico ainda estivesse distante de se concretizar.

Numa das passagens em seu Neuromancer, Gibson parece antecipar uma visão de ficção científica que viria a se concretizar poucos anos depois com a ação dos *hackers*:

> _ Você é um cowboy do ciberespaço. Os protótipos dos programas que usa para entrar nos bancos industriais de dados foram criados para a Garra Penetrante no assalto ao núcleo computacional de Kirensk. O módulo básico era construído por uma Asa Noturna equipada com um microlight, um piloto, uma matriz e um jóquei. Estávamos desenvolvendo um vírus chamado Toupeira. A série Toupeira foi a primeira geração de programas autênticos de intrusão.[74]

A obra trata de conceitos que foram inclusive empregados pela NASA para desenvolvimento de aplicações em realidade virtual para treinamentos de astronautas. Além de antecipar o emprego de termos como vírus de computador e intrusão, uma das ações perpetradas por grupos *hackers*, terminologias que só viriam a ter uma difusão a cerca de dez anos depois.

Como ensina Rohrmann[75] o ciberespaço surgiu com a "revolução das telecomunicações"[76] que seria equivalente aos termos "mundo online" ou "mundo virtual", como ambiente de comunicação que interliga os dispositivos eletrônicos, permitindo às pessoas a realização de vários atos, muitos dos quais jurídicos.

---

[72] "Neuromancer é um livro de ficção científica que introduziu novos conceitos para a época, como inteligências artificiais avançadas e um cyberespaço quase que "físico", conceitos que mais tardes foram explorados pela trilogia Matrix." Informação disponível em: http://pt.wikipedia.org/wiki/Neuromancer, acessado em 1 ago.2008.

[73] **A década de 80**. Lisboa: Site Ciência Viva. Disponível em: <http://oficina.cienciaviva.pt/~pw020/g3/a%20decada%20de%2080.htm>. Acesso em: 1 ago.2008.

[74] GIBSON, William. **Neurormancer**. Tradução de Abdoule Sam Byd e Lumir Nahodil. São Paulo: Ace Books, 2003, p.31.

[75] ROHRMANN, Carlos Alberto. **Curso de direito virtual**. Belo Horizonte: Del Rey, 2005, p.1.

[76] Para ROHRMANN o espaço virtual seria o resultado da utilização da telecomunicação e da ciência da computação, cujos marcos seriam a invenção do telégrafo, 1835 e o aperfeiçoamento dos computadores.

Na compreensão de Koepsell[77] o ciberespaço "refere-se ao complexo de interruptores e de transações de informações que ocorrem nos interruptores e entre os computadores."[78] Já Vasconcelos[79], numa concepção semelhante, diz que o "o ciberespaço é geralmente conceituado como o conjunto de computadores e serviços que constitui a rede internet." Numa visão mais conexa com o futuro, Silvio[80] afirma que "o ciberespaço é a pátria e terra natal da era da informação - o lugar onde os cidadãos do futuro estão destinados a habitar." Haveria assim, de acordo com Hoeschl[81] "duas formas de ingresso no ciberespaço: a internet e a realidade virtual."

Caracterizariam assim o ambiente denominado ciberespaço: a ausência de fronteiras ou territorialidade difusa, alta incidência de anonimato, a natureza descentralizada, usuários cada vez mais familiarizados tecnicamente e capazes de fugir à regulamentação e grande velocidade do desenvolvimento tecnológico, como ensina Rohrmann.[82]

Duas concepções fundamentais na prática de atos, como fenômenos jurídicos, irão então desafiar a ciência do Direito: a noção de espaço e de tempo. Isto porque "O ciberespaço nos move mais além, para um lugar de luzes virtuais, sem dúvida um lugar que não possui noite, onde o tempo pode ser estruturado e simulado de uma maneira mais flexível", como bem pontifica Kaminski.[83] Este novo parâmetro provocaria assim a "compressão do espaço-tempo", como afirma Carlos e Lemos,[84] e consequentemente, a necessidade de reformulação de algumas bases jurídicas com aplicações específicas para os aspectos tecnológicos decorrentes desse novo espaço global.

2.5 Correntes teóricas sobre a regulação da internet e do ciberespaço

---

[77] KOEPSELL, David R. ***The ontology of cyberspace: philosophy, law, and the future of intellectual property***. Chigaco: Open Court, 2003, p. 12.

[78] Texto original: " *will refer to complex of the switches and information transactions which occur by of those switches within and among computers* " (tradução nossa).

[79] VASCONCELOS, op. cit. n. 21, p33.

[80] ALEXANDRE, Silvio. **O Autor e sua obra. Anexo a Neuromancer**. São Paulo: Aleph, 2 ed., 1991. p. 261. Disponível em: < http://www.scribd.com/doc/2230917/Neuromancer-GIBSON-William>. Acesso em: 1 ago.2008.

[81] HOESCHL, op. cit. n. 71.

[82] ROHRMANN, op. cit. n. 75, p. 22.

[83] KAMINSKI. Omar**. Internet legal**: o direito na tecnologia da informação. Curitiba: Juruá, 2007, p. 41.

[84] CARLOS, Ana Fani Alexsandri; LEMOS, Amália Inês Geraiges (Orgs)**. Dilemas urbanos: novas abordagens sobre a cidade.** 2ª ed. São Paulo: Contexto, 2005, p. 125.

O estabelecimento de controle sobre a internet e ciberespaço comportou, como pode ser observado, uma abordagem inicial sobre a sua infraestrutura, ressaltando, porém, que a gerência sobre a parte física da rede e do registro de nomes de domínio, não alteram o caráter de ambiente sem regulação, sem controle, não subordinado a nenhuma jurisdição, país ou governo, isto no que se refere às informações que transitam na rede, que são expostas e efetivadas.

Quanto aos aspectos que se referem aos marcos regulatórios, Takahashi ao falar sobre a Sociedade da Informação, na qual se insere de forma basilar a internet, escreveu sobre as incertezas do mundo virtual o seguinte:

> Há um hiato de legislação nos novos espaços econômico, social e cultural, criado pela possibilidade, antes inexistente, das mais diversas operações a serem realizadas por meio das redes digitais. Em geral, a falta de regras e princípios claros causa incertezas que prejudicam a gestão dos negócios e os investimentos. No campo ainda imaturo das aplicações das novas tecnologias, esse fato é mais grave e forma uma das maiores barreiras para a difusão do uso das redes eletrônicas, em decorrência do ambiente de indefinições e do adiamento de decisões que gera.[85]

O foco, pois, da abordagem em relação à regulação não deveria ocorrer sobre a infraestrutura, ainda que se deva asseverar a sua necessidade, mas sobre as relações que se estabelecem no ciberespaço. A grande dificuldade de estabelecer regras de regulação da internet e do ciberespaço fez florescer correntes teóricas conflitantes, as quais Rohrmann[86] denomina de: Corrente Libertária, Corrente da Escola de Arquitetura de Rede, Corrente do Direito Internacional e Corrente Tradicionalista.

Os estudos e pesquisas jurídicas sobre estas correntes e os fenômenos correlatos fez florescer um número expressivo de pesquisadores e doutrinadores em escala mundial, notadamente que têm se voltado para o estudo dos cibercrimes.

2.5.2.1 Corrente libertária

A primeira corrente teórica a tratar do "controle" do ciberespaço tem como maior expoente John Perry Barlow, norte americano, poeta, escritor e ativista da internet. As ideias de Barlow prosperaram nos primórdios da expansão comercial da internet, em 1996,

[85] TAKAHASHI, op. cit. n. 25, p.33.
[86] ROHRMANN, op. cit. n. 75, p. 13-33.

quando a rede já contava com vários provedores comerciais e o sentimento de liberdade era a expressão maior da *web*. A visão era a de que as leis do mundo real não teriam validade sobre o ciberespaço, pois este seria "um mundo à parte, mundo esse alheio e indiferente ao direito tradicional"[87].

Esta corrente teórica ganhou impulso maior quando Barlow publicou em 1996 a "*Declaration of independence of cyberspace*" (Declaração de independência do ciberespaço), em contraponto às medidas jurídicas adotadas pelo governo dos EUA com o "*Communications Decency Act – CDA"*[88], um conjunto de regras que objetivavam regular a "indecência" na internet.

A declaração de Barlow tem o seguinte conteúdo:

> DECLARAÇÃO DE INDEPENDÊNCIA DO CIBERESPAÇO
> Por John Perry Barlow
>
> Governos do Mundo Industrial, vocês gigantes aborrecidos de carne e aço, eu venho do espaço cibernético, o novo lar da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. Vocês não são bem vindos entre nós. Vocês não têm a independência que nos une.
>
> Os governos derivam seu justo poder a partir do consenso dos governados. Vocês não solicitaram ou receberam os nossos. Não convidamos vocês. Vocês não vêm do espaço cibernético, o novo lar da Mente.
>
> Não temos governos eleitos, nem mesmo é provável que tenhamos um, então eu me dirijo a vocês sem autoridade maior do que aquela com a qual a liberdade por si só sempre se manifesta.
>
> Eu declaro o espaço social global aquele que estamos construindo para ser naturalmente independente das tiranias que vocês tentam nos impor. Vocês não têm direito moral de nos impor regras, nem ao menos de possuir métodos de coação a que tenhamos real razão para temer.
>
> Vocês não nos conhecem, muito menos conhecem nosso mundo. O espaço cibernético não se limita a suas fronteiras. Não pensem que vocês podem construí-lo, como se fosse um projeto de construção pública. Vocês não podem. Isso é um ato da natureza e cresce por si próprio por meio de nossas ações coletivas. [...][89]

Estas proposições de Barlow passaram a balizar o pensamento dos defensores desta corrente teórica. Influenciaram do mesmo modo, os debates em torno da

---

[87] ROHRMANN, op. cit. n. 75, p. 13.
[88] ROHRMANN, op. cit. n. 75, p. 13.
[89] BARLOW, John Perry. **Declaração de independência do ciberespaço**. Brasília: Ministério da Cultura, 2006. Disponível em: <http://www.cultura.gov.br/site/2006/10/23/declaracao-de-independencia-do-ciberespaco/>. Acesso em: 11 ago.2008.

impossibilidade de "controle" da internet e do ciberespaço "[...] dados o seu caráter internacional e a falta de adequação e eficácia dos mecanismos tradicionais de regulamentação em face das peculiaridades da rede."[90] No Brasil, por exemplo, a influência destas ideias retardaram a adoção de legislação específica para dar tratamento legal às questões de ordem jurídica, como ensina Silva Júnior[91].

O conteúdo doutrinário das ideias libertárias não se limitou à "Declaração de Independência do Ciberespaço" proposta por Barlow. No mesmo ano David R. Johnson, do *Cyberspace Law Institute* e David Post da *Georgetown University Law* nos Estados Unidos, publicaram o artigo "*Law and Borders - The rise of law in cyberspace"* (O Direito e suas fronteiras – o crescimento do direito no ciberespaço) numa das mais conceituadas revistas jurídicas americanas, reforçando assim as ideias da corrente libertária.

Reforçando a tese de problemas de aplicação das leis até então existentes às demandas das relações jurídicas no ciberespaço Johnson e Post[92] teorizaram:

> O ciberespaço radicalmente mina as relações entre a significante legalidade de fenômenos online e localização física. O crescimento das redes globais de computadores está destruindo as ligações entre localização geográfica e: (1) o poder de governos locais para fazer valer o controle sobre o comportamento online; (2) os efeitos do comportamento online sobre as pessoas ou coisas; (3) a legitimidade de esforços de soberanos locais para fazer cumprir as regras aplicáveis aos fenômenos globais; (4) a capacidade de localização física para dar conhecimento das regras que se aplicam. A Net, portanto, subverte radicalmente um sistema de elaboração de normas baseadas em fronteiras entre espaços físicos, pelo menos no que diz respeito à alegação de que o ciberespaço naturalmente deve ser regido por regras definidas territorialmente. (Tradução nossa).[93]

Este pressuposto de inaplicabilidade das leis ao ciberespaço tem como escopo a impossibilidade, em tese, de se estabelecer em que limites territoriais estaria ocorrendo determinado fato sujeito à tutela do Direito. Se um dos pressupostos de aplicação da jurisdição estatal tem por fundamento o ideal de soberania e, estando este, vinculado aos

---

[90] SILVA JÚNIOR, Ronaldo Lemos. **Direito, tecnologia e cultura**. São Paulo: FGV, 2005, p. 94.
[91] SILVA JÚNIIOR, op. cit. n. 90, p.95.
[92] JOHNSON, David R; POST, David. ***Law and Borders - The rise of law in cyberspace***. First Monday, Volume 11, Number 2, 2006. Disponível em:<http://www.firstmonday.org/issues/issue1/law/index.html>. Acesso em: 10 ago.2008.
[93] Texto original em ingles: "*Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically subverts a system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules."*

limites territoriais de um país é de se imaginar, em princípio, que as ideias propostas pelos teóricos da corrente libertária têm fundamento, motivo pelo qual seria experimentado o surgimento "de um novo tipo de direito"[94], com aplicação específica à internet e ao ciberespaço, sendo desnecessário, portanto, a aplicação das regras do direito tradicional.

Decorre assim, que a esse novo mundo o direito tradicional não teria aplicabilidade, na visão de Johnson e Post[95], pois as estruturas de autorregulação do ciberespaço parecem mais adequadas do que as autoridades locais para lidar com as questões jurídicas da *Net*.

Noutro artigo, também publicado em 1996, com o título de "*And how the shall the net be governed*?"(E como a rede será governada?) os mesmo autores referendam a ideia básica que fundamenta a corrente libertária com a aplicação de um Direito Descentralizado, fundado numa "proposta de auto-regulamentação da rede [...] uma proposta libertária porque defende a possibilidade de as normas jurídicas da rede independerem do Estado"[96], ou seja, solução de litígios através da autorregulamentação.

Sintetizando as concepções de cunho teórico de Barlow, Johnson e Post, Rohrmann, assim se pronuncia:

> A corrente libertária tenta resgatar no espaço virtual um mundo completamente separado do mundo real de átomos: acredita-se na utopia que se contrapõe à ideologia do direito tradicional de leis e normas emanadas dos órgãos de representação e de jurisdição estatais competentes.[97]

Neste sentido, a utópica visão de um outro mundo, paralelo, criado pelo ciberespaço, onde as leis dos governos não teriam alcance, é terreno fértil para que seja possível imaginar o pleno exercício da liberdade proporcionado pelas novas tecnologias, num novo mundo, sem fronteiras. Eis o pecado.

2.5.2.2 Corrente da "Escola da Arquitetura da Rede"

A concepção de controle da internet e do ciberespaço foi discutida sob uma ótica do surgimento de um novo direito no ciberespaço, que viria a influenciar fortemente as

---

[94] ROHRMANN, op. cit. n. 75, p. 16.
[95] JOHNSON, David R; POST, David, op.cit. n. 92, p.10.
[96] ROHRMANN, op. cit. n. 75, p. 17.
[97] ROHRMANN, op. cit. n. 75, p. 39.

relações de poder e, consequentemente, a aplicação da lei numa nova fronteira, não sujeita à aplicação do direito tradicional, como pensou Barlow, expoente da escola libertária. Daí, segundo esta visão, a impossibilidade de aplicação das regras tradicionais no ciberespaço, sujeito, portanto, a uma espécie de autorregulação, como fato evidenciador da liberdade plena – utopia.

A corrente da "Escola da Arquitetura da Rede"[98] surgiu a partir das ideias de Lawrence Lessig, professor da *Harvard University Law*, com a publicação do artigo **"***Code and Other Laws of Cyberspace"* (Código e outros direitos do ciberespaço) em 1999, além de outros que tratam da questão da regulação e controle da internet, cujas concepções passaram a nortear os argumentos dos doutrinadores que passaram a seguir esta linha.

O fundamento básico do pensamento de Lassig em "*Code and Other Laws of Cyberspace"* é a de que a relevância da regulação da internet e do ciberespaço não estaria nas leis tradicionais, na regulação imposta pelo Estado, mas pela arquitetura do hardware e dos softwares, ou seja, um controle e regulação além do pretendido pelo Estado, o que seria uma ameaça à liberdade.

Neste sentido, Lassig[99] explica:

> A nossa era é a do ciberespaço. Ela, também, tem um regulador. Esta entidade reguladora, também, ameaça liberdade. Mas somos nós tão obcecados com a ideia de que a liberdade significa "liberdade de governo" que não podemos sequer ver a regulação neste novo espaço. Por isso, não vemos a ameaça à liberdade que esta regulação apresenta. Este código-regulador – é o software e hardware que fazem o ciberespaço como ele é. Este código, ou arquitetura, fixa as condições de como a vida no ciberespaço é experimentada. Ela determina quão fácil é proteger a vida privada, ou como é fácil censurar discursos. Ele determina se o acesso à informação é geral ou se as informações estão zoneadas. Ela afeta aquilo que vê, ou aquilo que é controlado. Em uma série de formas que não se pode começar a ver a menos que um começa a compreender a natureza deste código, o código de regulação do ciberespaço. (tradução nossa).[100]

Enquanto a preocupação da corrente libertária alicerçava-se na "intromissão" do Estado na regulação da internet e do ciberespaço, a corrente da arquitetura da rede

---

[98] Esta terminologia foi adotada por Rohrmann, op.cit. n. 75, p.22.

[99] LESSIG, Lawrence. ***Code and Other Laws of Cyberspace***. Harvard Magazine, 2000. Disponível em: <http://harvardmagazine.com/2000/01/code-is-law.html>. Acesso em: 11 ago.2008.

[100] Texto original: "*Ours is the age of cyberspace. It, too, has a regulator. This regulator, too, threatens liberty. But so obsessed are we with the idea that liberty means "freedom from government" that we don't even see the regulation in this new space. We therefore don't see the threat to liberty that this regulation presents. This regulator is code--the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. It affects who sees what, or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates."*(Tradução nossa).

evidencia um temor de controle, mas não o controle ou regulação exercido pelo Estado, mas pelo comércio, por grupos empresariais e financeiros que, em face do poder econômico sobre grandes sites poderiam exercer um controle paralelo.

Esta regulação através do "código" pode ocorrer, por exemplo, mediante a instalação de filtros de conteúdo. Então o "controle" não se daria mediante lei, mas por alteração nos códigos de sistema capazes de alterar o resultado de uma pesquisa num sistema de buscas, por exemplo, limitando assim a liberdade do usuário em ter uma informação mais real possível.

O exemplo mais evidente que pode ser citado sobre o controle do Estado sobre o que transita na rede, como evidencia Lores[101], é o caso da China, onde há uma estimativa de "[...] 30 mil o número de censores que ficam vigiando os principais fóruns e debates on-line [...].O governo consegue monitorar praticamente todo o tráfego que entra no país." Ou seja, além do controle ou regulação exercido mediante imposições de leis severas, há ainda o controle sobre o que se lê, sobre o que se escreve e sobre o que se procura. Palavras como "Tibet" são monitoradas constantemente, em face dos conflitos separatistas decorrentes dessa porção territorial chinesa, o que seria para o país uma grande ameaça.

Desta forma, há uma evidente dificuldade em exercer a regulação da rede, em muitos aspectos, notadamente quanto ao seu conteúdo, mediante edição de uma lei, por exemplo, limitando o acesso de conteúdos pornográficos. Em face das características da própria internet e das informações que transitam pelo ciberespaço, um indivíduo a partir de um país que proíba acesso a conteúdo de cunho sexual, pode acessar outro onde não exista limitações. Nesta dimensão, a limitação, controle ou regulação exercido com base no "código" surtiria o efeito pretendido de limitar a liberdade do usuário.

Sob uma ótica voltada para a área privada, pode ser citado como exemplo o caso da empresa Norte Americana Google, em face dos conflitos registrados em agosto de 2008 entre a Rússia e a Geórgia. A Google foi acusada de "ter apagado de seu serviço de mapas dados da Geórgia pouco depois do início do conflito no Cáucaso. O site diz que, na realidade, nunca teve informação suficiente sobre a região."[102]O resultado da omissão das informações é a impossibilidade do usuário ter acesso visual sobre a área geográfica de uma região do planeta, sem que exista uma justificativa plausível, a não ser a de estabelecer

---

[101] LORES, Raul Juste. **Internet na China é monitorada por 30 mil pessoas**. São Paulo: Folha On line, 2008. Disponível em:<http://www1.folha.uol.com.br/folha/informatica/ult124u431438.shtml>. Acesso em: 12 ago.2008.

[102] EFE. **Google nega ter apagado Geórgia do serviço de mapas**. São Paulo: Folha On Line, 2008. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u433098.shtml>. Acesso em: 13 ago.2008.

controle, mediante manipulação do "código", sobre o conteúdo acessado, limitando assim a liberdade das pessoas.

Como ensina Rohrmann:

> Esses exemplos de mecanismos de filtragem podem ser considerados como formas de manipular a arquitetura da rede a fim de favorecer um ou outro interesse comercial. Há casos em que governos valem-se de programas de filtros para barrar o acesso de seus nacionais a determinados sites, como em algumas ditaduras que impedem a disseminação de certas noticiais e de opiniões contrárias aos seus interesses, em um claro exercício de censura prévia ao conteúdo da rede.[103]

Neste sentido, podemos compreender a síntese do pensamento dos defensores dessa corrente doutrinária sobre o controle da internet e do ciberespaço na busca pela intervenção/regulação dos Estados para que estes "determinem o programa da rede e, dessa forma, possam, efetivamente, regular o que ocorre no espaço virtual para o bem de todos"[104], o que evitaria que o mercado determine um controle maior ou alheio à vontade dos governos, limitando assim a liberdade das pessoas.

2.5.2.3 Corrente do Direito Internacional

O ideal de uma sociedade global, como defendido por Martins[105], tem forte conexão com proposta de instrumentos jurídicos de direito internacional a regular as ações humanas que se efetivam através da internet e do ciberespaço, com consequentes reflexos no ordenamento jurídico, tanto no âmbito do direito público, a exemplo do fenômeno do cibercrime e da jurisdição, quanto do direito privado, notadamente na esfera de transações econômicas viabilizadas através da grande rede, ou seja, o comércio eletrônico.

Nesta seara, as transações comerciais eletrônicas representaram para o Brasil uma movimentação da ordem de R$ 8,2 bilhões[106], sem possibilidades de dimensionar a incidência de condutas que poderiam necessitar uma regulação no âmbito do direito público.

Para Kobayashi e Ribstein[107] quanto aos aspectos da governança da internet:

---

[103] ROHRMANN, op. cit. n. 75, p. 26.
[104] ROHRMANN, op. cit. n. 75, p. 26.
[105] MATIAS, op. cit. n. 1, p. 107.
[106] MOREIRA, Daniela. **Comércio eletrônico cresce 30% em 2008**. Revista Eletrônica Info, 2008. Disponìvel em: <http://info.abril.com.br/aberto/infonews/012009/08012009-33.shl>. Acesso em: 20 jan.2009.

> O comércio eletrônico oferece tanto oportunidades como desafios para os mercados. Custos de transação reduzidos e mais rápida disseminação da informação oferecem o potencial de consumo mais eficiente. Ao mesmo tempo, no entanto, novos mercados e novas tecnologias podem criar percebidas lacunas jurídicas e aparente oportunidades de nova regulamentação. (Tradução nossa).[108]

O debate posto sobre a governança da internet, como visto quando da análise da corrente libertária e da corrente de arquitetura de rede, com a pregação, respectivamente de uma estrutura que tangencia a anarquia e uma vinculação efetiva à intervenção estatal, contrapõem-se ao cerne do que propõem os defensores desta corrente teórica, com a defesa do exercício da democracia transnacional na rede, mas sob os olhos do Estado, a fim de que abusos não sejam tolerados.

Comungando com o pensamento de Rohrman, a mentalização do ciberespaço como um ambiente internacional é mais realista e possibilita a aplicação de leis nacionais, caso seja necessário, a casos que se verifiquem nos limites territoriais de determinado Estado. Viabilizaria, do mesmo modo, em matéria criminal, a possibilidade de harmonização desta mesma lei nacional a um instrumento jurídico internacional de forma a punir condutas delituosas que se efetivem além-fronteiras.

Quanto aos aspectos comerciais, os conflitos de interesses "podem levar a implicações complexas para sua regulamentação"[109], embora o tema já esteja sendo trabalhado pela no âmbito da OMC (Organização Mundial do Comércio) com o *Trade-Related Aspects of Intellectual Property Rights* – TRIPS (relacionado a direitos de propriedade intelectual), bem com no âmbito da UNCITRAL – *United Nations Commision on International Trade Law* (Comissão das Nações Unidas para direito do comércio internacional).

Ademais, neste mesmo sentido Vasconcelos e Brito defendem que "qualquer modelo nacional de regulamentação, por via de lei ou de qualquer outra forma, tem que ter em vista as iniciativas que se desenvolvem em outros países estabelecendo normas de cooperação

---

[107] KOBAYASHI, Bruce H.;RIBSTEIN, Larry E. **Multijurisdictional regulation of the internet**. In: THIERER, Adam D.; CREWS, Clyde Wayne. **Who Rules the Net?:Internet Governance and Jurisdiction**. Washington: Cato Institute, 2003, p. 159.

[108] Texto original: "*Eletronic commerce provides both opportunities and chalenges for markets. Reduced transaction costs and more rapid dissemination of information offer the potential for more efficient consumer markets. A the same time, however, new markets and technologies can create perceived regulatory gaps and apparent opportunities for new regulation."* (Tradução nossa).

[109] ROHRMANN, op. cit. n. 75, p. 28.

e intercâmbio de informações,"[110] motivo pelo qual a corrente do direito internacional, concordando com Rohrmann, oferece significativa contribuição "para melhor regulamentação das transações eletrônicas, especialmente no que concerne à padronização de certas relações que extrapolam uma única jurisdição."[111]

2.5.2.3 Corrente Tradicionalista

No contexto da análise proposta, qual seja, a de analisar as correntes doutrinárias que tratam da regulação e controle da internet e do ciberespaço, esta é a que se apresenta com mais ênfase e a quem vem sendo aplicada aos conflitos jurídicos decorrentes das relações que se estabelecem na nova fronteira do direito.

A aplicação de leis nacionais a inúmeros casos concretos, por exemplo, tem fundamentado o entendimento de aplicação das leis ao mundo virtual, embora esta dúvida tenha pairado por um período considerável, o que fez emergir, por conseguinte, questionamentos sobre essa viabilidade.

Neste sentido, merece realçar o entendimento de Vasconcelos e Brito que asseveram:

> O que é preciso ter em mente é que a chamada Terceira Revolução Industrial, também conhecida como Revolução Tecnológica (Revolução digital) modificou a estrutura da sociedade. A informática e a Internet funcionaram como catalisadores dessas mudanças estruturais e o Direito precisa se posicionar quanto a necessidade de regulamentar ou não essas novas relações jurídicas virtuais. E caso se posicione no sentido de regulamentação, é preciso saber se: Pode um Estado nacional regulamentar relações jurídicas em uma rede que opera globalmente?[112]

De se observar que a indagação a merecer resposta, não está vinculada à aplicabilidade ou não do ordenamento jurídico tradicional às relações jurídicas operadas na grande rede. Este questionamento passa a ter como elemento nuclear a dimensão de aplicabilidade de tais leis, ou seja, tem-se um fenômeno (a grande rede e a sociedade nela conectada) em escala global, com problemas de igual ordem, à guisa de solução com

---

[110] BRITO, Dante Ponte de.; VASCONCELOS, Fernando Antônio de. **O direito e a economia na era digital**. Prim@ Facie, João Pessoa, a.5. n. 9, jul./dez. 2006. Disponível em:<http://www.josuelima.net/ppgcj/gerencia/docs/26062007124707.pdf>. Acesso em: 18 jan.2009, p. 88.
[111] ROHRMANN, op. cit. n. 75, p. 32.
[112] BRITO, Dante Ponte de.; VASCONCELOS, op. cit. n. 110, p. 85.

instrumentos jurídicos nacionais, inadequados, pois, para solução de conflitos nesta dimensão transfronteiriça restam ineficazes.

Assim, a negação de aplicação das leis nacionais a muitos episódios de ordem publica ou privada, é matéria vencida, exceto nos Estados que ainda não se adequaram a esta realidade ou cujos sistemas de justiça criminal se apresentem inoperantes para tratar com o fenômeno.

Por outro prisma, merece destacar que o ideal de regulação e controle, apresenta-se mais coerente sob uma ótica de tutela legal, ou seja, de proteção ou de regulação de temas que podem ocasionar danos à sociedade, entenda-se neste caso, práticas ilícitas como subtração e dados pessoais, crimes contra a honra, violação de direitos autorais e proteção às relações de consumo.

Esta concepção é diametralmente oposta ao modelo de "controle e regulação" considerado por muitos países, que segundo Goes Jr:

> [...] estão quase que completamente ligados a uma tentativa de controle político ou ideológico como é o caso do Afeganistão, da China e mesmo dos Estados Unidos, com o esforço de dar à rede um padrão adequado à cultura e à moral nacional. Tais países se sentem ameaçados com o modelo quase anárquico que a Internet propõe. Entretanto, a tentativa de se estabelecer fronteiras na rede parece ser uma iniciativa fadada ao fracasso o que indica, mais uma vez, que o caminho tem que passar pela regulamentação internacional de certos aspectos da Internet.[113]

É patente vislumbrar a necessidade de adequações a muitas regras jurídicas já existentes. Outros institutos carecem de novas interpretações e alguns deles já sofreram modificações, notadamente no âmbito do Direito Penal, no que se refere aos delitos de pedofilia através da internet, com a criminalização de condutas antes lícitas, ainda que imorais.

Decorre assim, que cada vez mais se apresenta como atual a expressão "onde está o homem, está a sociedade; onde está a sociedade, está o direito"[114], ao considerarmos que tais avanços de ordem tecnológica provocaram impactos consideráveis nas relações sociais e consequentemente nas relações jurídicas.

Finaliza-se por fim esta abordagem, considerando a possibilidade de conjugação de pontos importantes considerados pela corrente do direito internacional e da corrente tradicionalista, comungando com o pensamento de Rohrmann, ao arrematar que:

---

[113] GOIS JR, José Caldas. **O Direito na Era das Redes: a liberdade e o delito no ciberespaço**. Bauru: EDIPRO, 2001, p. 46.

[114] "*Ubi homo ibi societas, ubi societas ibi jus*", expressão atribuída a Ulpiano, jurisconsulto romano.

> A corrente tradicionalista não nega eventuais dificuldades que podem ser encontradas em casos específicos que envolvem o espaço virtual *(notadamente os aspectos que envolvem o direito internacional)*, especialmente no tocante a pontos como produção de provas e combate à fraude e à criminalidade. Todavia, deve-se lembrar que, em relação a este último ponto, há dificuldades muito grandes também quando se fala em combate à criminalidade que ocorre, por exemplo, nos grandes centros urbanos, a despeito de todo o aparelho policial disponível nas mãos do Estado.[115] (Grifo nosso).

2.6 Impactos das novas tecnologias telemáticas e a sociedade da informação

O ponto de partida da abordagem proposta indica, preliminarmente, a necessidade de elucidação das terminologias utilizadas no escopo do subcapítulo, a saber: compreensão do termo telemática, seus aspectos históricos e impactos na sociedade. Há, do mesmo modo, a pertinência das tratativas voltadas a esclarecer o emprego da terminologia sociedade da informação e a influência da telemática nesta.

A telemática pode ser compreendida como sendo a área do conhecimento humano que reúne o conjunto de tecnologias e aplicações associadas à eletrônica, informática e telecomunicações. O termo também está associado aos "sistemas de comunicação e sistemas embarcados e que se caracteriza pelo estudo das técnicas para geração, tratamento e transmissão da informação."[116]

Sob a ótica do processo histórico, computadores e os sistemas de comunicações encontram raízes na Babilônia e no antigo Egito, por volta de 3.000 a.C., tendo como precursores o ábaco e os papiros egípcios, respectivamente. Houve consequentemente, uma evolução gradativa, cuja história está ligada à evolução dos computadores e dos sistemas de comunicação e de telecomunicação.

A simbiose das duas grandes estruturas fez surgir a telemática. Embora não se possa ter com precisão um fato histórico, pode se dizer que o surgimento da internet, com o lançamento da ARPANET fez surgir, consequentemente, a telemática, quando dois computadores são conectados através de um sistema de rede, isto em 1969.

De acordo com Goel:

---

[115] Rohrmann, p. 34.
[116] ALBERTO, Carlos; *Et al*. **Telecomunicações, informática e telemática**.São Paulo, 2008. Disponível em:<http://www.scribd.com/doc/6184626/Telematica-e-Telemetria>. Acesso em: 28 jan.2009.

> O termo telemática foi cunhado em 1978 por Simon Nora e Alain Minc, em seu relatório intitulado L'Informatisation de la société. Este relatório foi encomendado pelo presidente francês Valéry Giscard d'Estaing, em 1976 [...]. No seu relatório Simon Nora e Alain Minc comparavam as perspectivas da telemática com a eletricidade: 'Hoje, qualquer consumidor de eletricidade pode obter instantaneamente a energia elétrica que ele precisa, sem se preocupar de onde vem ou o quanto ela custa. Há todos os motivos para acreditar que o mesmo será verdade no futuro da telemática'.[117]

Hoje, o dia a dia das pessoas e das organizações está ligado fortemente a aplicações de telemática. Desde o simples fato de efetuar um saque num caixa eletrônico, efetuar ligações ou mandar uma mensagem através do telefone celular ou ler as notícias num portal local, são exemplos da combinação dos recursos de informática com as telecomunicações. Tais recursos tecnológicos são utilidades imprescindíveis às organizações públicas e privadas, bem como à sociedade civil, tanto quanto foi a energia elétrica na metade do século XX.

Neste sentido, os recentes desenvolvimentos da informática e das telecomunicações têm um importante impacto na sociedade e na economia. A crescente disponibilidade de pequenos e acessíveis computadores pessoais tem ajudado a tornar o mundo sem fronteiras. Enquanto os computadores estão se tornando muito menores e mais econômicos (baixo consumo de energia elétrica), dispositivos móveis (aparelhos celulares, handhelds e *smartphones*) estão cada vez mais portáteis e transformando-se em computadores de bolso, acompanhando o usuário em qualquer lugar.

Ao escrever sobre os impactos das novas tecnologias que tornaram o "mundo plano", Thormas Friedman registra que:

> É uma revolução que não tem nada de trivial. É grande. Permite que o chefe esteja num lugar, e seus subordinados, em outro. [Essas plataformas de *software* de fluxo de trabalho] possibilitam a criação de escritórios virtuais globais - que não ficarão circunscritos nem às paredes de uma sala, nem às fronteiras de um país – e dão acesso a talentos situados em diferentes partes do mundo, que poderão desicumbir-se de tarefas que precisem ser levadas a cabo em tempo real. Quando vimos, estávamos trabalhando 24 horas por dia, sete dias por semana, 365 dias por ano - e tudo isso aconteceu num piscar de olhos, ao longo dos últimos dois ou três anos. [118]

---

[117] GOEL, Asvin. **The history of telematics. Téle-matique, 2008**. Disponível em <http://www.telematique.eu/telematics/history.en.html>. Acesso em: 20.jan.2009.
Texto original em inglês: *The term telematics has been coined 1978 by Simon Nora and Alain Minc in their report titled L'Informatisation de la société. This report was mandated by the French president Valéry Giscard d'Estaing in 1976 [...]. In their report Simon Nora and Alain Minc compare the prospects of telematics with electricity: "Today, any consumer of electricity can instantly obtain the electric power he needs without worrying about where it comes from or how much it costs. There is every reason to believe that the same will be true in the future of telematics".* (Tradução nossa).

[118] FRIEDMAN, op. cit. n. 59, p. 97.

Pontificadas as palavras iniciais, pode-se asseverar que este é o cenário através do qual se desenvolveu e mantém-se em franca construção os valores e caracteres inerentes à denominada sociedade da informação.

Nesta nova dimensão de mundo globalizado, a utilização da expressão sociedade da informação pode suscitar inúmeras dúvidas, inquietude e, consequentemente, insegurança quanto ao conteúdo do domínio que se expõe, impondo-se, pois, motivação para desvencilhar objetivamente seu conteúdo.

Sob um prisma técnico, só seria possível falar em sociedade da informação após a convergência de tecnologias. Esta concepção só viria a se concretizar, efetivamente, com a revolução provocada pelas ideias de Tim Berners-Lee ao projetar a *World Wide Web,* ou seja, a face gráfica da internet. Neste sentido, ter-se-ia como elementos fundamentais para este processo "três fenômenos inter-relacionados, que responderam pela gênese da transformação assistida"[119], quais sejam: a convergência de base tecnológica, a dinâmica da indústria, o crescimento e expansão da internet. Quanto a este último acontecimento, encontra lugar na linha do tempo após 1991, embora o conceito de sociedade da informação tenha raízes na década de 60.

Para Simão Filho o conceito de sociedade da informação deve ser compreendido como:

> [...] um modo de desenvolvimento sócio-econômico em que a aquisição, armazenamento, processamento, valorização, transmissão, distribuição e disseminação de informação conducente à criação de conhecimento e à satisfação das necessidades dos cidadãos e das empresas desempenham um papel central na atividade econômica, na criação de riqueza, da definição da qualidade de vida dos cidadãos e das suas práticas culturais é por demais extensiva. [120]

No Brasil o marco referencial para a sociedade da informação foi o lançamento em 2000, pelo Ministério da Ciência e da Tecnologia, do livro intitulado "O livro verde da sociedade da informação no Brasil, o que já demonstrava a preocupação do governo em estabelecer diretrizes que pudessem nortear a formulação de uma estratégia adequada para inserir a produção científica brasileira na Sociedade da Informação.

O escopo do trabalho compreendido, constante no referido livro, dá suporte a três grandes elementos: criação de infraestrutura de redes no país para fomentar o

---

[119] BARRETO JÚNIOR, Irineu Francisco. **Atualidade do conceito de sociedade da informação para a pesquisa jurídica**. *In* PAESANI, Liliana Minardi (Coord). **O direito na sociedade da informação**. São Paulo: Atlas, 2007, p.64.

[120] SIMÃO FILHO, Adalberto. **Sociedade da informação e seu lineamento jurídico**. *In In* PAESANI, Liliana Minardi (Coord). **O direito na sociedade da informação**. São Paulo: Atlas, 2007, p.12.

desenvolvimento de serviços; melhoria na infraestrutura de comunicações e informações (adequação da velocidade de interação com outros países) e os aspectos regulatórios relativos ao proposto, de forma a inserir o Brasil no contexto do cenário internacional.

Poder-se-ia questionar: que repercussões de ordem jurídica o estudo do impacto dessas novas tecnologias podem proporcionar? Como tais fenômenos vêm delineando novos desafios à Ciência do Direito?

Ora, cientes de que essa Revolução Tecnológica produziu efeitos sem precedentes na sociedade é de se esperar que tais fenômenos e suas implicações fossem viabilizadas como elementos riquíssimos para o estudo científico, como ensina Barreto Júnior ao afirmar:

> Neste aspecto, reside o foco das transformações que a sociedade da informação provocou e tende a provocar no exercício dos direitos fundamentais, especialmente dos direitos políticos, já que, a atuação dos meios de comunicação interfere decisivamente nos processos de sociabilidade com o advento da modernidade e da contemporaneidade.[121]

Podem ser elencadas, entretanto, repercussões de ordem social e jurídica que se manifestam em todos os ramos do direito como os registrados na seara trabalhista - com desemprego estrutural; por um prisma revela avanços, como no processamento e tramitação de processos a exemplo da penhora *on line*, entre outros. No ramo do direito empresarial, comercial e do consumidor, com a efetivação cada vez mais crescente do comércio eletrônico.

Neste diapasão Takahashi ao escrever sobre a dimensão proporcionada pela sociedade da informação, analisando-a como fenômeno global e sob uma ótica social, político-econômica, assevera:

> A sociedade da informação não é um modismo. Representa uma profunda mudança na organização da sociedade e da economia, havendo quem a considere um novo paradigma técnico-econômico. É um fenômeno global, com elevado potencial transformador das atividades sociais e econômicas [...]. É também acentuada sua dimensão político-econômica, decorrente da contribuição da infra-estrutura de informações para que as regiões sejam mais ou menos atraentes em relação aos negócios e empreendimentos. Sua importância assemelha-se à de uma boa estrada de rodagem para o sucesso econômico das localidades. Tem ainda marcante dimensão social, em virtude do seu elevado potencial de promover a integração, ao reduzir as distâncias entre pessoas e aumentar o seu nível de informação.[122]

No presente estudo, interessa os aspectos e repercussões de ordem jurídicas vinculados às condutas delituosas que são perpetradas na internet, quer como objeto fim quer

[121] BARRETO JÚNIOR, op. cit. n. 119, p. 67.
[122] TAKAHASHI, op. cit. n. 25, p.30.

como instrumento meio, veja-se o exemplo dos delitos de furto, crimes contra a honra e outros que serão estudados no capítulo específico.

2.7 Internet, ciberespaço e as novas fronteiras jurídicas

O estudo dos fenômenos jurídicos, especificamente os que estão relacionados à teoria jurídica do crime, conduzem a conceitos tradicionais conexos ao pensamento de território, soberania e jurisdição. Numa visão mais detalhada, de cunho doutrinário que se volta para o exercício da jurisdição criminal, surgirão vocábulos como sujeito ativo, sujeito passivo, consumação e tentativa, entre outros elementos que permeiam toda vida acadêmica de profissionais de direito.

A construção doutrinária de institutos, teorias e concepções que fundamentam as terminologias acima especificadas têm um lugar na história bem mais distante que os acontecimentos que têm norteado a Revolução Tecnológica e a Globalização, enquanto processos em construção.

A compreensão do fenômeno da Globalização,[123] que não é um processo novo, indica o conceito de internacionalização das relações entre as pessoas, entre os Estados e organizações públicas e privadas. Entre as pessoas a interação alcançou um processo de intercâmbio sem precedentes e sem fronteiras. De modo igual essa revolução proporcionada pela Revolução Tecnológica foi capaz de potencializar as ações empresariais, tornando assim, empreendimentos regionais em empresas voltadas para o mercado mundial, isto é, transnacionais.

Mas a ideia exposta, a princípio, de evidenciar o caráter econômico, deve ser amenizada em face dos impactos provocados pelo processo de integração cultural, social e político. Na compreensão de Friedman[124] a Globalização propiciou a "criação de um campo de jogo global, mediado pela web, que viabiliza diversas modalidades de colaboração (isto é, o compartilhamento de conhecimento e trabalho) em tempo real, independente de geografia, distância, ou num futuro próximo até mesmo de idioma."

---

[123] PAESANI, Liliana Minardi (Coord). **O Direito na sociedade da informação**. São Paulo: Atlas, 2007, p. 5. PAESANI entende que esse "processo tem raízes no passado, mas só alcançou a intensidade inédita com a Revolução Tecnológica", isto é, o casamento entre a informática e as telecomunicações.

[124] FRIEDMAN, op. cit. n. 59, p. 357.

Num sentido geral as principais características elencadas por autores que se dedicam ao estudo do fenômeno, a exemplo de Barbosa[125] a homogeneização dos grandes centros urbanos, a expansão das grandes empresas para outras regiões, o uso massificado da tecnologia - revolução tecnológica (informática, telecomunicações - internet), a divisão do mundo em áreas de influências ou blocos econômicos comerciais, a formação de uma cultura mista entre as culturas locais e as de outros locais, formando uma cultura de massa universal.

Estes fenômenos encontraram suporte nas novas tecnologias, nas aplicações da informática, nos impactos proporcionados pela internet e no surgimento de novas fronteiras decorrentes das relações que se estabelecem no ciberespaço, configurando assim um redesenho dos conceitos sobre soberania, fronteiras, território e no próprio direito.

Para ilustrar essa contradição, vejamos o pensamento de Ferri, ao tratar da aplicabilidade da lei penal com relação ao território em sua obra sobre "Princípios de Direito Criminal":

> Para os crimes cometidos no território do Estado, que é a base física da sua soberania política e jurídica, a lei aplica-se contra cidadãos e contra estrangeiros, exceto nos casos de prerrogativas pessoais [...] Por território do Estado, por sua exclusiva soberania, não é aplicável nenhuma lei penal estrangeira, nem exeqüível sentença penal estrangeira [...].[126]

Estas assertivas expostas por Ferri encontram consonância com a configuração do Estado nacional e todas as suas características. Entretanto, novos desafios impostos pelo Pós-Guerra Fria e pelos eventos que se seguiram, indicam muito mais uma gradativa redução do poder do Estado, enquanto titular da soberania e da condução da política econômica, hoje, integrada ao contexto internacional, na nova ordem multipolar com zonas de influência e conjugação de Estados em blocos econômicos. É este o contexto a ser descortinado em face da necessidade de situar o estudo sobre o cibercrime no espaço "territorial" que lhe é peculiar, qual seja: o ciberespaço.

Nesta linha de pensamento, aduz-se que não há fronteiras para o ciberespaço. O usuário de um computador pode estar fisicamente num lugar, mas praticar atos no ciberespaço, mediante a internet, com a produção de efeitos noutro, a milhares de quilômetros de distância e de forma instantânea, sendo irrelevante considerar ser dia num ponto "A" e

---

[125] BARBOSA, Alexandre de Freitas (Coord)**. O Mundo Globalizado**: Política, Sociedade e Economia. Contexto: São Paulo, 2006, p.13.

[126] FERRI, Enrico. **Princípios de direito criminal: o criminoso e o crime**. Tradução de Luiz Lemos D´Oliveira. Campinas: Russell Editores, 2003, p 144-146.

noite num ponto "B". Haveria assim, a "compressão do espaço-tempo", como afirma Carlos e Lemos.[127]

Noutra lição relevante, Pinheiro arremata:

> Até onde um ordenamento jurídico tem alcance? O problema não está apenas no âmbito da internet, mas em toda sociedade globalizada e convergente, na qual muitas vezes não é possível determinar qual o território em que aconteceram as relações jurídicas, os fatos e seus efeitos, sendo difícil determinar que norma aplicar utilizando os parâmetros tradicionais.[128]

No contexto do que foi posto inicialmente, como atributos característicos da internet, ou seja, liberdade de expressão, privacidade e amplitude (escala global), reside também as questões mais complexas do direito, ou seja, como compatibilizar os benefícios proporcionados com a possibilidade efetiva de práticas criminosas, que agregam os mesmos pressupostos, que ocorrem em escala mundial provocando prejuízo da ordem de bilhões de dólares. Entretanto, alerta Savona[129] que "Uma parte substancial dos cibercrimes é de caráter transnacional, mas algumas podem acontecer a um nível meramente nacional."[130]

Desta forma, há embate jurídico em duas frentes: uma em relação às práticas de cibercrimes especificamente dentro do território de um Estado, portanto, sujeito às leis e soberania do país e noutro ponto os cibercrimes que são praticados em mais de um país, daí a denominação de transnacionais. São justamente os crimes de internet de caráter transnacional os quais inspiram as maiores preocupações no mundo, ainda que existam bons indicadores de possíveis soluções, é de se observar, porém, que numa condição ou em outra o Brasil com suas dimensões continentais está fortemente inserido neste contexto.

---

[127] CARLOS, Ana Fani Alexsandri; LEMOS, Amália Inês Geraiges (Orgs). op. cit. n. 84, p. 125.
[128] PINHEIRO, Patrícia Peck. **Direito digital**. 2ª ed. São Paulo: Saraiva, 2007, p. 38.
[129] SAVONA, Ernesto Ugo. ***Crime And Technology: New Frontiers For Regulation, Law Enforcement And Research*.** Springer:New York, 2005, p.39.
[130] Texto original: " *a substantial portion of cyber-crime is transnational in nature, but some can happen at a purely domestic level*." (Tradução nossa).

3 O CIBERCRIME COMO FENÔMENO JURÍDICO

3.1 Cibercrime: definição, características e elementos essenciais

3.1.1 O ciberespaço e o ambiente dos novos fenômenos criminais

A compreensão dos fenômenos criminais do mundo pós-moderno[131] globalizado, notadamente os relacionados às Tecnologias da Informação e da Comunicação na denominada Sociedade da Informação, impõe que se estabeleça um esboço histórico, ainda que breve, de como toda problemática está relacionada à evolução do processo histórico da humanidade. Não que se pretenda falar sobre a história puramente, a partir do ábaco, do mundo oriental, por exemplo, mas sobre como foram registrados os primeiros fenômenos criminosos relacionados com o ciberespaço.

O ambiente que deve ser considerado é o ciberespaço, mas conexo com o mundo real e os seus efeitos sobre a sociedade, que é o que interessa como objeto de pesquisa. Na verdade, há uma linha muito tênue entre o que é ciberespaço e o que é o mundo real, uma vez que há uma interdependência cada vez maior entre essas tecnologias que convergiram para esse novo mundo – para a denominada Sociedade da Informação ou sociedade global.

Para que seja preciso imaginar que tais condutas tiveram um marco inicial, faz-se imprescindível, num primeiro plano, situar em que momento tais elementos tecnológicos ou seus fundamentos estavam aptos a gerar uma conduta danosa em face de uma ação humana, consequentemente.

Neste sentido, a abordagem que se faz está agregada, consequentemente, aos momentos iniciais que deram suporte às Tecnologias da Informação e da Comunicação, que compreende a própria evolução das telecomunicações, desde seus primórdios aos dias atuais, sendo assim assevera Mello:

---

[131] RULLI JÚNIOR, Antônio. **Jurisdição e sociedade da informação**. *In:* PAESANI, Liliana Minardi (Coord). **O direito na sociedade da informação**. São Paulo: Atlas, 2008. p.83.
Entende Rulli Júnior que o conhecimento e a informação são a chave dessa nova era que aproxima o local e o global.

> Na realidade, quando se observa a comunicação a partir de uma perspectiva histórica, verifica-se que as técnicas se transformaram, mas o conteúdo e significados permaneceram os mesmos. Tal como a história em geral, a história da comunicação exige perspicácia do pesquisador para diagnosticar os processos de gestação dos fenômenos de comunicação, assim como sua utilização pela comunidade.[132]

Ora, se o ciberespaço surgiu com o advento e evolução das telecomunicações, impõe-se, pois, afirmar que há dificuldade doutrinária para congregar os pontos de vista, que ora indicam o seu marco inicial com invenção do telégrafo[133] e as primeiras mensagens enviadas. Noutro prisma há indicativos de que, tal fato, similarmente ao que se tem hoje, só veio ocorrer com a invenção dos computadores e das primeiras mensagens trocadas através das redes, ainda que de forma embrionária. Outra perspectiva pode indicar que o ciberespaço surgiu com o advento da própria internet.

Para Pinheiro:

> Com o ciberespaço, a geografia como a conhecemos (física) desaparece, surge uma nova geografia, algo que não é material, mas ainda assim é real. O ciberespaço é um não lugar, ou um lugar imaginário, que só temos acesso pelo computador, mesmo assim ele está ligado à realidade pelo uso que temos feito dele nos dias atuais, transformando-o em um espaço intermediário entre duas realidades.
> Como já dissemos, o lugar de situação da Internet é o ciberespaço, o espaço virtual, logo, ela não existe em espaço físico, mas nem por isso ela deixa de ser real. Como o Direito deve lidar com esta falta de lugar, de espaço físico da Internet é uma das grandes questões da atualidade.[134]

Qualquer que seja o ponto de vista abraçado, a questão relevante será a abordagem do fenômeno estudado de acordo com a concepção da informática – computadores, a internet e os sistemas de redes, neste contexto de pós-modernidade e de sociedade global.

Um alerta soa, entretanto, como relata Nagpal:

---

[132] MELLO, Caren Sapienza de. **O futuro das relações de trabalho via comunicação nas organizações do Século XXI. 2004**. 94p. Monografia (Especialização em Gestão Estratégica em Comunicação Organizacional e Relações Públicas) – Universidade de São Paulo, São Paulo, 2004. p. 18.

[133] Couto, com base em Rohrmann destaca que: "A invenção do telégrafo, em 1835, por Morse, representa a origem do espaço virtual. Ao longo dos últimos dois séculos, presenciamos diversos marcos que contribuíram para o desenvolvimento do mundo virtual, tais como o telefone, surgido em 1876 e os primeiros computadores, desenvolvidos durante a década de 1940." Este espaço virtual concebido por Couto é o que se denomina de ciberespaço.
COUTO, Thiago Graça. **O direito virtual: Panorama teórico e técnico do *Cyberlaw* e análise prática das conseqüências jurídicas envolvendo o mau uso das redes de compartilhamento Peer-to-Peer**. 2007. 48 p.Monografia (Bacharelado em Ciências Jurídicas) - Universidade Cândido Mendes, Rio de Janeiro, 2007. p.6.

[134] PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal**. Disponível em: http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile /29397/28953>. Acesso em: 04 abr. 2009.

> O conceito de computador utilizados na presente definição não significa apenas o convencional desktop ou laptop. Inclui ainda Assistentes Pessoais Digitais (PDAs), celulares telemóveis ou smartphones, relógios sofisticados, carros e uma série de equipamentos eletrônicos com conexão à internet. [135]

A observação formulada por Nagpal é condizente com o alto grau de conectividade disponível, em que os equipamentos eletroeletrônicos estão se integrando cada vez mais, sendo a conectividade com a internet um fator primordial. O resultado desta convergência tecnológica, como afirma Friedman é que "não há maior força de nivelamento que a ideia de que todo o conhecimento do mundo está disponível para todos, a qualquer momento, em qualquer lugar."[136] Este é o ambiente onde são perpetradas as condutas objeto de estudo.

3.1.2 Definições para os novos fenômenos criminais envolvendo computadores e a internet

O estabelecimento de uma definição uniforme e consensual para as condutas criminosas registradas mediante emprego de computadores, seus acessórios e periféricos, bem como para as que são registradas no ambiente virtual ou fazendo uso deste ambiente como instrumento suscita inúmeras divergências conceituais.

Este dissenso é natural. Justifica-se pela efervescência de institutos jurídicos que estão em processo de mutação, como é o caso do conceito de soberania, funções e responsabilidades do Estado e do ideal de jurisdição como foi abordado. Estaria assim, surgindo um novo ramo do Direito? Há elementos suficientes que possam indicar e fundamentar tal assertiva? São questionamentos que ainda não tem uma resposta, mas com bons indicativos de que sim.

Desta forma, autores interpretam estas novas figuras jurídicas de forma equivocada, ora dando um tratamento demasiadamente técnico, com vié

---

[135] NAGPAL, Rojas. ***Evolution of cybercrimes. Asian School of Cyber Laws***, 2008. Disponível em: < http://cyberattack.in/images/7/74/Evolution_of_Cyber_Crime.pdf>. Acesso em: 20 mar.2008.
[136] FRIEDMAN, op. cit. n. 59, p. 78.
[137] Norbert Wiener é considerado o pai da "Cibernética". Juntamente com outros cientistas, afirmou na década de 40 que o conjunto de problemas centrados no controle e na comunicação, tanto no tecido vivo quanto na máquina, apresentavam uma unidade essencial.
[138] Lee Loevinger realizou pesquisas, de caráter empírico, com a intenção de promover a racionalização do Direito através da aplicação de métodos quantitativos e da automação.
[139] O jurista Mario Losano acentua uma divisão entre abordagens teóricas e empíricas, classificando as primeiras dentro do modelo de Juscibernética e denominando a segunda de Informática Jurídica.

Sintetizando o debate, quanto ao estudo do fenômeno criminal e o seu consequente enquadramento dentro de uma área de estudo específico, será possível encontrar no Brasil, apenas para exemplificar, denominações como: Direito da Informática[141], Informática Jurídica[142], Direito Eletrônico[143], Direito da Internet[144], Direito Virtual[145], Direito Digital,[146]Direito da Sociedade da Informação[147] e Direito do Ciberespaço.[148] A consequência gerada por essa gama de denominações vinculadas à informática, computadores, internet e ciberespaço, tem como resultado, do mesmo modo, mais de uma dezena de denominações para os delitos praticados com suporte aos novos recursos tecnológicos e neste sentido é possível encontrar: delito informático, crime de informática, crime informático, crime eletrônico, crimes de internet, crimes virtuais, crimes digitais, cibercrime, crimes de computador, delito virtual, crimes computacionais, crimes telemáticos, crimes de alta tecnologia, entre outros.

Comungando com este pensamento Aras declara:

> Delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, crimes telemáticos, crimes informacionais, ciberdelitos, cibercrimes... Não há um consenso quanto ao nomen juris genérico dos delitos que ofendem interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de

---

[140] PINTO, Marcio Moreno. **O Direito da internet: o nascimento de um novo ramo jurídico** . Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2245>. Acesso em: 2 abr. 2009.

[141] VEIGA, Adolfo Olsen da. **Apresentação**. In Olivo, Luiz Carlos Cancellier de, **Direito e Internet: a Regulamentação do Ciberespaço**, UFSC, 2000. p. 34.

No mesmo entendimento que a denominação deveria ser Direito da Informática: Paulo Sá Elias, Omar Kaminski e Adelmário de Castro.

[142] LOSANO, Mário. **A Informática Jurídica 20 anos depois**. Revista dos Tribunais, n. 715, maio de 1995, pp. 350-367.

[143] ALMEIDA FILHO, José Carlos Araújo. **Direito Eletrônico ou Direito da Informática?**.Informática Pública vol.7(2):11-18, 2005. Disponível em: <http://www.ip.pbh.gov.br/ANO7_N2_PDF/IP7N2_almeida.pdf>. Acesso em 3 abr.2009.

Almeida Filho sustenta ainda que o "Direito Eletrônico é o conjunto de normas e conceitos doutrinários destinados ao estudo e normatização de toda e qualquer relação em que a informática seja fator primário, gerando direitos e deveres secundários."

[144]PINTO, op. cit. n. 140.

Pinto ao discorrer sobre o Direito da Internet diz que "[...] a importância de se estabelecer um ramo jurídico com diretrizes próprias, produzindo-se reflexões jurídicas abrangentes e sistemáticas, tencionando esclarecer as novas práticas geradas com advento da rede, legitimando-as e conduzindo-as gradativamente a uma possível regulamentação."

[145] A denominação de Direito Virtual é posta por Rohrmann, op. cit. n. 1.

[146] PINHEIRO, op. cit. n. 128, p.29.

[147] SIMÃO FILHO, op. cit. n. 120, p. 28.

[148] CASTRO, Luis Fernando Martins. **Direito da informática e do ciberespaço**. Revista de Derecho Informático. n. 064, novembro 2003. Disponível em: <http://www.alfa-redi.org/rdi-articulo.shtml?x=1270>. Acesso em: 3 abr.2009.

> computadores e equipamentos periféricos (hardwares), redes de computadores e programas de computador (estes denominados softwares).[149]

No âmbito do direito internacional, num estudo intitulado "Desafio de definir o cybercrime e particularidades criminológicas"[150] publicado na revista "*Law and Technology*" da *Masaryk University*, República Tcheca, Zavrsnik[151] relaciona, do mesmo modo, dez denominações para o fenômeno criminal, com as seguintes denominações em inglês: *computer crime* (crime de computador)*, computer-related crime* (crime relacionado ao computador)*, crime in information science* (crime da ciência da informação)*, ICT crime* (crime de TIC – telecomunicações, informática e comunicações)*, internet crime* (crime de internet)*, virtual crime* (crime virtual)*, computer network crime* (crime de redes de computadores)*, information crime* (crime de informação)*, cybercrime* (cibercrime) *e hig tech crime* (crime de alta tecnologia)*.*

Ainda que no direito nacional seja possível encontrar esta prodigiosa gama de denominações, situação não diferente se verifica no âmbito internacional, como se vê. Nos países de língua inglesa o termo *Cyberlaw* é comum para nomear esse ramo do conhecimento jurídico que trata das relações no ciberespaço.

Desta forma, para Chawki:

> Um dos fatores que tornam árdua uma rápida definição de cibercrime é a dificuldade do dilema da jurisdição. Leis em diferentes jurisdições definem termos de maneira diferente, e é importante para a aplicação da lei e dos encarregados de investigar os crimes, bem como os administradores de redes que desejam envolver-se no combate ao cibercrime que são cometidas contra as redes, para se familiarizar com as leis aplicáveis.
> [...]
> Assim, as definições legais de cibercrime em leis nacionais diferem, dependendo do Estado. Talvez devêssemos olhar para as organizações internacionais para fornecer uma definição padrão de cibercrime.[152]

---

[149] ARAS, Vladimir. **Crimes de informática: uma nova criminalidade**. Revista informática jurídica.com. Disponível em: <http://www.informatica-juridica.com/trabajos/artigo_crimesinformticos.asp>. Acesso em: 3 abr. 2009.

[150] Título original em inglês: "*Cybercrime definitional challenges and criminological particularities*".

[151] ZAVRSNIK, Ales. ***Cybercrime definitional challenges and criminological particularities***. Law and Technology, Brno, Tchec Republic, v.2 n. 2, nov.2008. pp.8-10.

[152] CHAWKI, Mohamed. ***A critical look at the regulation of cybercrime: a comparative analysis with suggestions for legal policy***. DROIT-TIC, 11 April 2005. Disponível em: <http://www.crime-research.org/articles/Critical/>. Acesso em: 5 abr.2009.
Texto original em inglês: *One of the factors that make a hard-and-fast definition of cybercrime difficult is the jurisdictional dilemma. Laws in different jurisdictions define terms differently, and it is important for law enforcement officers who investigate crimes, as well as network administrators who want to become involved in prosecuting cybercrime that are committed against networks, to become familiar with the applicable laws. […]Thus, the definition of cybercrime under state law differs, depending on the state. Perhaps we should look to international organizations to provide a standard definition of cybercrime.* (tradução nossa).

Durante a participação em duas conferências que deram suporte a esta pesquisa, a *SPCI 2008 - The First International Conference on Security, Privacy and Confidentiality Issues in Cyberlaw*, realizada na cidade do Cairo, Egito e *CYBERSPACE 2008*, na cidade de Brno, República Tcheca, os pronunciamentos dos conferencistas de diversos países versaram, também, sobre a dificuldade de se chegar a um termo comum às condutas delituosas também se fizeram evidentes. Entretanto, foi possível observar que no âmbito das discussões acadêmicas e das apresentações dos conferencistas o termo mais empregado foi "*cybercrime*", ou seja, cibercrime, que está sendo empregada neste trabalho.

Esta opção pode representar um contraponto forte aos doutrinadores que defendem a denominação de crime ou delito informático, crime eletrônico, crime digital e crime cibernético. Entretanto, a denominação cibercrime, é a que melhor se coaduna aos termos empregados em âmbito internacional, inclusive na Convenção de Budapeste sobre Cibercrime.

O termo geralmente empregado e mais defendido pelos autores brasileiros refere-se a "crime ou delito informático", nestes estariam englobados os crimes praticados mediante emprego de recursos da informática - computadores, impressoras e seus periféricos como instrumentos para tais práticas, incluindo-se nestes os crimes praticados no ambiente virtual – ciberespaço.

Ora, se os recursos de informática são utilizados como meros instrumentos, por exemplo, imagine-se o ato de alguém digitalizar num *scanner* cédulas de R$ 100,00 (cem reais) e passar a fazer uso de tais cédulas falsas. Em termos práticos, não houve nenhuma informação que viesse a transitar pelo ciberespaço. Desta forma, os crimes informáticos não dependem exclusivamente do ciberespaço para serem cometidos. Os cibercrimes seriam, pois, uma espécie daqueles, que são gênero. Pode se dizer até mesmo que o crime informático já existia mesmo antes da popularização da internet, embora seja preciso advertir que os termos internet e ciberespaço também não se confundem.

Comungando com esse pensamento, merece destacar o pensamento de Chawki, ao asseverar que:

> Assim, é necessário afirmar que o cibercrime e o crime informático tem duas áreas distintas. O crime informático é qualquer ação ilegal perpetrado através de transação eletrônica contra a segurança de um sistema de computador ou dados que ele contém, independentemente do fim, enquanto o cibercrime, no sentido estrito do termo, são

> todos os crimes cometidos contra um sistema de computador ligado à rede de telecomunicações.[153]

Que sentido faz hoje ter disponível um computador em casa ou no trabalho sem acesso à grande rede? Este é o principal foco do estudo, ou seja, voltado para a criminalidade que ocorre na grande rede mundial de computadores. Desta forma, reafirma-se, apresenta-se mais pertinente ao estudo a denominação cibercrime em relação às condutas praticadas no ambiente virtual.

3.1.3 Definição jurídica para o cibercrime

O desafio de estabelecer uma definição para um fenômeno que tem produzido inúmeras controvérsias de ordem doutrinária impõe, por consequência, que se busque um suporte jurídico no âmbito do direito internacional para balizar os elementos constitutivos dessa nova criminalidade, pois na visão de Chawki[154] "[...]a falta de definição legal deste termo é uma fonte de confusão, tanto no campo do pensamento, quanto no nível de análise ou de vocabulário escolhido."[155]

Há necessidade, porém, de uma advertência preliminar. Esta se fixa na compreensão de que nem sempre a lei estabelece definições ou conceitos claros para novos fenômenos jurídicos. Observe-se, neste sentido, que no direito brasileiro a definição jurídica de crime encontra parâmetros bem diferentes daqueles estabelecidos pela doutrina, a quem cabe, com maior clareza conceituá-lo.

Neste prisma, é possível encontrar definições no ordenamento jurídico dos Estados Unidos, Reino Unido, Canadá, Austrália, entre outros países, embora os conceitos sejam diferentes, pois são leis que tratam do tema no âmbito do direito nacional. De modo distinto, a União Europeia conseguiu sintetizar medidas protetivas de cunho comunitário e transnacional, com a Convenção sobre o Cibercrime, sendo que muitos países entre os citados já ratificaram a referida Convenção.

---

[153] CHAWKI, Mohamed. ***Essai sur la notion de cybercriminalité***. Disponível em: <http://www.legalbiznext.com/droit/ESSAI-SUR-LA-NOTION-DE>. Acesso em: 5 abr.2009.
[154] CHAWKI, op. cit. n. 153.
[155] Texto Original em francês: "[...]*l'absence de définition légale de ce terme est source de confusions, tant au niveau du domaine de la réflexion, qu'au niveau de l'analyse ou du vocabulaire choisi*." (tradução nossa).

Para Schjolberg "A primeira iniciativa internacional sobre os crimes informáticos na Europa foi a Conferência do Conselho da Europa sobre aspectos criminológicos da criminalidade econômica, em Estrasburgo, em 1976."[156] Seguindo-se, de acordo com Zavrsnik outras discussões no âmbito da OECD[157], em 1983, (*Organization for Economic Cooperation and Development* - Organização para a Cooperação Econômica e Desenvolvimento) que definiu o fenômeno como sendo "[...] qualquer comportamento ilegal, imoral ou não autorizado que envolva a transmissão ou processamento automático de dados."[158]

Num passo adiante, 1990, numa Conferência em Havana, Cuba, a ONU[159] editou o "Manual de Prevenção e Controle dos Crimes por Computador" (*The United Nations Manual on the Prevention and Control Computer-Related Crime*), estabelecendo o seguinte:

> O Manual das Nações Unidas para Prevenção e Controle dos Crimes por Computador define os crimes de computador como sendo: (1) fraude por manipulação do computador; (2) falsificações por computador; (3) danos ou modificações de dados ou programas de computador; (4) acesso não autorizado a sistemas e serviços de computador; (5) reprodução não autorizada de programas legais de computador.

Foram registrados ainda, como passos significativos à construção de um instrumento jurídico de caráter global, ainda que não plenamente efetivados, os seguintes eventos ou ações: Recomendações do Conselho da Europa - 1995; Formação de um Grupo de Trabalho com Peritos em Alta Tecnologia do G-8 - 1998; Conferência de Standford sobre Cooperação Penal para Combate ao Cibercrime e Terrorismo - 1999.

Durante o "Décimo Congresso sobre Prevenção de Delito e Tratamento do Delinqüente, na cidade de Viena, entre os dias 10 e 17 de abril de 2000, a ONU publicou um comunicado à imprensa, relacionando outros tipos de delitos informáticos, praticados por

---

[156] SCHJOLBERG, Stein. ***The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva***. Disponível em: <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>. Acesso em: 6 abr.2009.
Texto original: "*The first international initiative on computer crime in Europe was the Council of Europe Conference on Criminological Aspects of Economic Crime in Strasbourg in 1976*." (Tradução nossa).
[157] ZAVRSNIK, op. cit. n. 151, p. 7.
[158] United Nations - Economic and Social Comission for Asia and Pacific. ***Understanding cybercrime***. Disponível em: <http://www.unescap.org/icstd/policy/publications/Information-Security-for-Economic-and-Social-Development/WHAT-ARE-CYBERCRIME-AND-COMPUTER-RELATED-CRIMES.pdf>. Acesso em: 5 abr.2009.
Texto original: "[...]*any illegal, unethical, or unauthorized behaviour involving the transmission or automatic processing of data*." (Tradução nossa).
[159] *Eighth United Nations Congress on the Prevention Crime and the Treatment of Offenders in Havana in 1990.* (8o Congresso das Nações Unidas para Prevenção do Crime e tratamento de Ameaças).

meio do computador"[160], quais sejam: a) Espionagem industrial; b) Sabotagem de sistemas; c) Sabotagem e vandalismo de dados;d) Captura ou averiguação de senhas secretas; e) Estratagemas; g) Jogos de azar; h) Fraude; i) Lavagem de dinheiro.

Como instrumento jurídico internacional mais importante para o combate ao cibercrime a União Europeia, através do Conselho da Europa, estabeleceu a Convenção sobre o Cibercrime, também Conhecida como Convenção de Budapeste, uma vez que teve lugar na capital da Hungria, em 23 de novembro de 2001.

A Convenção define nos artigos 2 a 10 o cibercrime, estabelecendo conteúdo de matéria penal em quatro diferentes categorias: (1) infrações contra a confidencialidade, a integridade e a disponibilidade de dados e sistemas; (2) As infrações relacionadas com computador; (3) infrações relacionados com conteúdo; (4) delitos relacionados com a violação dos direitos de autor e direitos conexos.

Para corroborar estes pontos importantes, Chawki pontua que o cibercrime "[...] pode ser definido como qualquer ação ilegal associada com a interligação de sistemas de computadores e redes de telecomunicações, onde a ausência de tal interligação impede a prática ilícita desta ação."

Ainda que não possa traduzir da melhor forma as construções conceituais firmadas pelos doutrinadores, o conceito jurídico estabelece, ao menos, parâmetros para que se delimite o que é permitido e o que é proibido. O lícito e o ilícito. A liberdade do cidadão e o poder de coerção do Estado.

3.1.4 Características e classificação dos cibercrimes

A construção de elementos indicadores que possam caracterizar fenômenos na pós-modernidade apresenta-se como enorme desafio, também. Isto porque houve a agregação de características do ciberespaço a velhos crimes e também o surgimento de outras condutas criminosas exclusivamente praticadas com os recursos deste ambiente.

A alteração de fatores delineadores de aspectos tradicionais do direito penal, como o espaço e o tempo, promoveram significativas mudanças no pensamento de como tais condutas podem ser praticadas. Princípios penais como o tempo e o lugar do crime, passam a

[160] FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre a ética informacional**. R. CEJ, Brasília, n. 20, p. 67-73, jan./mar. 2003. p. 71.

carecer de interpretação mais alargada, porque no ciberespaço o "tempo não existe" e não "há fronteiras."

Do mesmo modo, como afirma Pinheiro, mediante simulações da cibernética "[...] passado, futuro e presente podem estar presentes, simultaneamente em um mesmo lugar, em uma tela, essa possibilidade de ir do passado ao futuro em um click faz com que, às vezes, não nos seja possível dizer o que é o presente."[161]

Desta forma, é possível propor características para os cibercrimes com os seguintes elementos:

- Uso da tecnologia como meio ou como fim para cometimento de crimes;
- Uso da internet, de redes de computadores ou de telecomunicações;
- Caráter transnacional: podem ultrapassa as fronteiras de mais de um Estado;
- Incidência sobre pessoas, propriedade, organizações e sobre Estado.

No direito brasileiro Gomes sugere que esta nova criminalidade:

> [...] conta com as mesmas características da informatização global: transnacionalidade – todos os países fazem uso da informatização (qualquer que seja o seu desenvolvimento econômico, social ou cultural); logo, a delinqüência correspondente, ainda que em graus distintos, também está presente em todos os continentes; universalidade – integrantes de vários níveis sociais e econômicos já têm acesso aos produtos informatizados (que estão se popularizando cada vez mais); ubiqüidade – a informatização está presente em todos os setores (públicos e privados) e em todos os lugares.[162]

Numa perspectiva de âmbito internacional Zavrsnik se posiciona:

> Apesar das diferenças nas definições, as características fundamentais do cibercrime são: a complexidade técnica (preenchendo um com um senso de segurança sobre um lado e medo de 'big brother' sobre o outro), um desenvolvimento rápido (ampliando vulnerabilidade e alargar as possibilidades de infração) e criptografia (como medida de proteção e obstáculo para a detecção de perpetradores).
> Novidades na noção de cibercrime incluem as seguintes características:
> (1) um novo cenário (o virtual) para o crime;
> (2) uma dispersão de comportamentos desviantes: isso envolve antigas formas de comportamento desviante, em novas formas (ou seja, furto de dados) e completamente novas formas de criminalidade (isto é, *cracking, hacking*, computador ataques com *worms* e vírus);
> (3) novos métodos para investigar crime (aplicação da lei) e as novas regras de competência e punição (e-competência e e-punição).[163] (grifo nosso).

---

[161] PINHEIRO, op. cit. n. 134.

[162] GOMES, Flávio Luiz. **Crimes informáticos**. Disponível em: <www.direitocriminal.com.br>. Acesso em 26 mar. 2009.

[163] ZAVRSNIK, op. cit. n. 151.

Texto original: "*Despite the differences in definitions, the fundamental characteristics of cybercrime are: technical complexity (filling one with a sense of safety on one hand and fear of "big brother" on the other), rapid development (enlarging vulnerability and extending the possibilities for infringements) and cryptography (as a protection measure and an obstacle for the detection of perpetrators).*

Cada característica acima mencionada irá requerer das pessoas, das organizações e do Estado ações específicas. O reconhecimento de vulnerabilidades expõe a todos, indistintamente, a condição de vítimas da nova criminalidade. O uso das TIC – Tecnologias da Informação e da Comunicação serão cada vez mais presentes em face da tendência de ampliação da inclusão digital, consequentemente requerendo mais cuidados de todos. O caráter transnacional do cibercrime alterou a ideia de princípios de direito inerentes ao Estado, como a soberania, a ideia de lugar e tempo do crime, do mesmo modo, requerendo, por consequência um esforço global voltado à cooperação penal e adoção de instrumentos jurídicos de caráter internacional.

No Brasil, em face da grande dissonância na denominação dos crimes praticados com empregos de recursos da informática e da internet, aqui denominados cibercrimes, como visto, tem como consequência, do mesmo modo, classificações que se apresentam diferentes do que é proposto pela doutrina internacional.

Desta forma Vianna[164] propõe a classificação, que ele denomina de "crimes informáticos" em: crimes informáticos próprios (puros); crimes informáticos impróprios (mistos); crimes informáticos mistos e crimes informáticos mediatos ou indiretos.

Esta denominação conceitua: os crimes informáticos impróprios (ou mistos), como aqueles em que o computador é usado como instrumento para a execução do crime, mas sem ofensa aos dados nele contidos (não há ofensa ao bem jurídico inviolabilidade da informação automatizada), por exemplo os crimes contra a honra previstos no Código Penal Brasileiro e que podem ser praticados mediante envio de email.

Os crimes informáticos próprios (puros) seriam aqueles em que a objetividade jurídica da norma penal é a inviolabilidade das informações automatizadas (dados). Para esta hipótese o exemplo seria a interceptação de informações que transitam numa rede de dados por exemplo. Os "crimes informáticos mistos" seriam os delitos complexos em que com proteção jurídica aos dados e a outro bem jurídico diverso. Já os "crimes informáticos mediatos ou indiretos" seriam os delitos com fim não informáticos, que na verdade utilizam-se de tais recursos para a prática de outros delitos, ou seja o computador seria meio para se

---

Novelties in the notion of cybercrime include the following features:
(1) a new (the virtual) crime scene;
(2) a dispersal of deviant behaviour: this involves old forms of deviant behaviour in new forms (i.e. data theft) and completely new forms of crime (i.e. cracking, hacking, computer attacks with worms and viruses);
(3) new methods for investigating crime (law enforcement) and new rules for jurisdiction and punishment (e-jurisdiction and e-punishment)."

[164] VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003. pp. 13-26.

atingir um fim. Esta classificação proposta por Vianna não encontra paralelo na doutrina internacional predominante.

Isto posto, Wall propõe a divisão dos cibercrimes em quatro categorias:

> (1) Ciber invasão (intrusão) - atravessando fronteiras em outras pessoas da propriedade e / ou causar danos, por exemplo, hacking, desfiguração, vírus.
> (2) Ciber fraudes e furtos - roubar (dinheiro, bens), por exemplo, fraude de cartão de crédito, as violações de propriedade intelectual (também conhecido como "pirataria").
> (3) Ciberpornografia - violar leis sobre obscenidade e decência.
> (4) Ciberviolência - fazendo dano psicológico, a instigação ou danos físicos contra os outros, assim, leis relativas à protecção da pessoa, por exemplo, ódio, perseguição.[165]

Já Lunker[166] propõe uma classificação de tipos comuns para os cibercrimes estabelecendo os seguinte grupos: (1) Contra indivíduos: a) contra a pessoa; b) contra a propriedade de um indivíduo; (2) Contra organizações: governo, empresas privadas, companhias e grupos individuais; (3) Contra a sociedade.

Destaca-se também a posição posta por Goodman e Brenner[167] que estabelecem a seguinte classificação: (1) crimes contra a pessoa; (2) crimes contra a propriedade; (3) crimes contra o Estado e (4) crimes contra a moralidade.

Como a busca por uma classificação que possa contemplar a multiplicidade de entendimentos doutrinários resta infrutífera, cumpre destacar, com mais ênfase, a classificação constante nas disposições da Seção 1[168] (que trata do direito penal material) na Convenção de Budapeste sobre o Cibercrime[169], títulos I a IV, que se apresenta, sob a ótica legal, a mais lúcida:

---

[165] Wall, D.S. ***Crime and the Internet***, London: Routledge, 2001. p. 3-7.
Texto original: *David S. Wall (2001 3-7) subdivides cybercrime into four established legal categories:*
(1) Cyber-trespass - crossing boundaries into other people´s property and/or causing damage, e.g. hacking, defacement, viruses.
(2) Cyber-dececptions and thefts - stealing (money, property), e.g. credit card fraud, intellectual property violations (a.k.a. 'piracy').
(3)Cyber-pornography - breaching laws on obscenity and decency.
(4) Cyber-violence - doing psychological harm to, or inciting physical harm against others, thereby laws relating to the protection of the person, e.g. hate speech, stalking.

[166] LUNKER, Manish. ***Cyber laws: a global perspective***. Disponível em: <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005846.pdf>. Acesso em: 6 abr. 2009.

[167] GOODMAN, Marc D.; BRENNER, Susan W. ***The emerging consensus on criminal conduct in cyberspace*****.** Disponível em: <http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php>. Acesso em: 6 abr.2009.

[168] BEZERRA, Edson Kowas. et al. **O espaço cibernético e seu emprego como agente de instabilidade de uma nação: uma visão sobre a guerra cibernética**. *In*: ICCyber'2004 – I Conferência Internacional de Perícias em Crimes Cibernéticos. Disponível em: <http://angel.acmesecurity.org/~adriano/papers/anais-iccyber-dpf-2004.pdf>. Acesso em: 5 mar. 2009. p.94.

[169] **Convenção de Budapeste sobre o Cibercrime**. Disponível em: <http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf>. Acesso em: 5 abr.2009.

(1) crimes contra o sigilo, integridade e disponibilidade dos dados e sistemas informáticos (acesso ilegítimo, interceptação ilegítima, interferência de dados, interferência de sistemas, uso abusivo de dispositivos);

(2) infrações relacionadas com computadores (falsidade informática, burla informática);

(3) infrações relacionadas com conteúdo dos dados (pornografia infantil) e

(4) infrações relacionadas com as violações do direito autoral e direitos conexos.

Longe da perfeição, esta construção jurídica ao menos indica o estabelecimento de uma classificação com base na Convenção de Budapeste que, somada aos entendimentos doutrinários, é plenamente capaz de dar um suporte lógico para determinar os elementos essenciais ao enfrentamento do cibercrime.

3.2 Impactos do cibercrime na sociedade: riscos e prejuízos no Brasil

As ações delituosas praticadas na internet e também através dela, irradiam-se como um foco luminoso, trazendo desdobramentos em vários aspectos, mas que incidem sobre as pessoas físicas e jurídicas em forma de prejuízos financeiros e consequentemente constituem obstáculo à implementação das políticas voltadas ao desenvolvimento nacional. Tais prejuízos atribuídos a crimes de computador podem ultrapassar US$ 10 bilhões por ano, em parte, por causa da crescente expansão da internet, como bem pontifica Liliana Minardi Paesani[170].

Mas os registros das ações criminosas traduzem-se também em práticas de racismo, furto, ameaça, dano, estelionato, pedofilia, entre outras modalidades de ações *cracker* (quem ainda não possuem tipificação legal) vindo a ensejar a respectiva possibilidade de punição em face de tais ilícitos, como por exemplo, no caso do *cyberterrorismo* (que já possuem tratamento legal na Inglaterra e EUA).[171]

---

[170] PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil.** 2. ed. – São Paulo: Atlas, 2003, p.38.

[171] SCHOUERI, Luís Eduardo.Org. **Internet: o direito na era virtual.** Rio de Janeiro: Forense,2001, p.373.

Desta forma tais práticas constituem entraves ao desenvolvimento nacional, quando empresas (públicas e privadas) sofrem prejuízos financeiros trilionários[172] em escala mundial, daí porque tais práticas constituem um novo desafio à ciência do direito à medida que se faz premente a necessidade de legislação específica e estruturação de instituições do Estado para combater tais delitos.

Para Tatiana Schoor, enfocando a questão no Brasil:

> "Os crimes digitais geraram um prejuízo de R$ 300 milhões a bancos e administradoras de cartões de crédito em 2005 no Brasil, cerca de 150% a mais que no ano anterior quando contabilizou R$ 100 milhões. Para 2006, o valor das perdas deverá ficar em torno de R$ 350 milhões, de acordo com a pesquisa do IPDI (Instituto de Peritos em Tecnologias Digitais e Telecomunicações) - empresa especializada em perícias digitais e apuração de crimes e fraudes no mundo cibernético."[173]

Tais práticas delituosas tornam-se potencialmente mais perigosas quando se associam ao crime organizado, que passa a fazer uso das mais modernas ferramentas computacionais com vistas à empreitada de atividades ilícitas. É temor atual esta propagação, isto é, migração em massa do crime organizado para a grande rede.

Em decorrências desses impactos, paulatinamente alguns conceitos estão em processo de mutação, numa maturação de ideias que se propagam, infelizmente, em descompasso com essa realidade, mas que precisam de enquadramento legal, sob pena de estar se mantendo um clima de insegurança jurídica no meio econômico-social.

Tais condutas, dentre as quais as que foram descritas em tópicos anteriores, ensejam plena responsabilidade penal em face do dano causado, isto na esfera criminal, sem prejuízo, consequentemente, dos possíveis danos de natureza civil que quase sempre caminham *pari passu.*

Embora seja abordada uma temática que se destaca como um dos pontos da vanguarda do direito, sem regulamentação clara em algumas situações, há ilícitos perfeitamente enquadráveis no Código Penal brasileiro e legislação extravagante, quais sejam:

---

[172] A McAfee, em recente relatório intitulado "Economias inseguras: Proteger informação é vital, afirma que os dados roubo e violação de cibercrime pode ter custado às empresas, tanto quanto $ 1 trilhão em perdas a nível mundial, em propriedade intelectual e despesas de reparação dos prejuízos em 2008.
Texto original: "*McAfee, in a recent report entitled, "Unsecured Economies: Protecting Vital Information, states that data theft and breaches from cybercrime may have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing the damage in 2008*."
FRANK, John B. ***$1 Trillion Lost to Cybercrime...Can Hackers Bail US Out?***. Disponível em: <http://pindebit.blogspot.com/2009/02/1-trillion-lost-to-cybercrimecan.html>. Acesso em: 15 abr.2009.

[173] SCHOOR, Tatiana. **Crimes digitais geraram prejuízo de R$ 300 mi em 2005**. Portal Almeida Carmago Advogados. Disponível em: http://www.almeidacamargo.com.br/AlmeidaCamargo/paginas/Informacao.asp?CodNoticia=237&Categoria=6, Acesso em: 14 mar.2008.

aqueles crimes comuns praticados com auxílio da tecnologia. Tais condutas não necessitam de legislação específica, pois já se encontram sob a égide da legislação vigente.

Merece destacar, que a tecnologia não está somente sendo empregada para o desenvolvimento humano. Por isso que há registros de ações danosas nas principais cidades do mundo. E isso se constitui em mais um desafio às instituições que integram o sistema de Justiça Criminal: policiais, integrantes do Ministério Público e do Poder Judiciário.

Analisando os riscos da internet Rocha entende que:

> No Brasil, um bom parâmetro para o mapeamento desta área está exposto na 9ª Pesquisa Nacional de Segurança da Informação, realizada pela Módulo entre os meses de março e agosto. Segundo análise de Fernando Nery, sócio-fundador da empresa, "a pesquisa, em termos técnicos, ratifica os desafios principais enfrentados pelas organizações: A preocupação com vírus, funcionários insatisfeitos e senhas como principais ameaças; O aumento do uso da internet como meio de fraudes e vazamento de informação, acompanhando o desenvolvimento dos negócios eletrônicos; O desafio de conscientizar os executivos, motivar os usuários e capacitar a equipe técnica, assim como demonstrar o retorno sobre o investimento da segurança; A necessidade de realizar análise de riscos e revisar periodicamente a política de segurança; O crescimento dos problemas de segurança a cada ano, acompanhando o crescimento dos ataques, a evolução da tecnologia e o aumento dos investimentos no setor".[174]

Além da ação de empresas privadas que atuam como consultores independentes, auxiliando as empresas a aperfeiçoarem seus sistemas informatizados, o Estado também tem atuado da mesma forma, protegendo-se de um risco potencialmente danoso. Por outro lado, é preciso uma ação firme dos órgãos que compõem o sistema de Justiça Criminal e, ainda que em número bem inferior às práticas delituosas elas vêm acontecendo, com realização de prisões de pessoas envolvidas com a criminalidade cibernética, agindo aplicando golpes, mediante transferências ilegais de dinheiro, clonagem de cartões, pirataria e lavagem de dinheiro, entre outros delitos.

De acordo com o portal do HSBC Bank Brasil S.A:

> O crime virtual cresce a cada ano. Em 2007, a Polícia Federal (PF) realizou 9 grandes operações para combater essa modalidade criminosa. Embora o número represente cerca de 5% do total de operações realizadas no ano, número considerado baixo segundo a própria PF, o resultado das ações e dos trabalhos em conjunto com outras organizações e instituições foi muito positivo. [175]

---

[174] ROCHA, Luis Fernando. **Retrospectiva 2003 – Parte 1**. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cert.br: São Paulo, 2003. Disponível em < http://www.cert.br/docs/reportagens/2003/2003-12-15.html>. Acesso em: 15 fev. 2009.

[175] Portal do HSBC Bank S.A. **Polícia Federal fecha 2007 com 9 operações de combate ao crime virtual**. Disponível em: <http://www.hsbc.com.br/common/seguranca/artigo-seguranca-comb-crime-virtual.shtml.>. Acesso em: 14 mar.2008.

Há de se destacar, portanto, que tais prisões foram precedidas de ampla investigação com monitoramento dos envolvidos e expedição de mandado de prisão pela Justiça, com atuação destaca do Ministério Público Federal.

As condenações têm acontecido, como a decisão as seguir enunciada e divulgada pelo portal do Tribunal Regional da 5ª Região:[176]

> A prática delituosa realizada através da Internet, especificamente na captação de recursos alheios, tem se convertido em uma ação criminal comum, onde centenas de correntistas bancários sofrem, sorrateiramente, com danos ao patrimônio. Esse tipo de crime é cometido pelos chamados "*crackers*" (termo usado para aqueles que praticam a quebra de um sistema de segurança) e que permanecem impunes pela complexidade em coibir os delitos.
> No entanto, na sessão desta quinta-feira (22/11), a Terceira Turma do Tribunal Regional Federal 5ª Região (TRF5) foi apreciada a questão em prol de garantir a ordem do sistema de segurança bancário nacional. Na ocasião, foram julgados dois habeas corpus (HC 2982 e 2980 PE) referentes a dois *crackers* que atuavam em uma quadrilha de âmbito nacional, determinando, por maioria, a manutenção da prisão preventiva dos acusados. A organização operava criando páginas falsas de bancos na *web* e enviando-as por *e-mail* (através de um vírus denominado *trojan horse*) para clientes específicos. Os mesmos eram incentivados a creditar suas informações bancárias nas fraudulentas *home pages*. Daí, os *crackers* capturavam os dados para posteriores transações ilegais."

Evidencia-se desta forma, considerando o conjunto de práticas comerciais, industriais, técnicas e científicas que há um risco permanente de prejuízos bilionários provocados por "*crackers*" e outros cibercriminosos.

Há assim, consequentemente, impactos negativos nos diversos setores econômicos (mesmo com a ação tímida do sistema de Justiça Criminal), isto sem falar nos prejuízos provocados às pessoas físicas (danos nas relações de consumo), como atentado, notadamente aos direitos fundamentais em incontáveis atentados à honra e à imagem das pessoas.

A ação do Estado em tutelar à ordem econômica tem sido no sentido utilizar a legislação disponível (Código Penal, Lei de Lavagem de Dinheiro e Crimes contra a ordem tributária e econômica) e realizar operações, notadamente de inteligência, tendo a Polícia Federal como principal instrumento com auxílio das Polícias estaduais. O Ministério Público como fiscal da lei tem agido com firmeza no patrocínio de ações penais que tem conseguido instruir um conjunto probatório adequado a um julgamento justo, e consequentemente desarticulando a ação de organizações criminosas, ainda que seja patente.

---

[176] Portal do Tribunal Regional Federal 5a Região. **Terceira Turma nega habeas corpus para "crackers".** Disponível em: <http://www.trf5.gov.br/noticias/1044. Acesso em: 13 mar.2008.

Depreende-se dessa construção lógica, caso não ocorra a proteção estatal, o risco de danos aos princípios insculpidos na ordem econômica, na medida em que servem de contrapeso às políticas de desenvolvimento que norteiam as ações do Estado como agente normativo e regulador da atividade econômica.

Neste sentido, é preciso compreender os riscos que o cibercrime impõe ao desenvolvimento, não apenas sob uma ótica puramente econômica, isto é, que se traduz em indicadores, mas, sobretudo, desenvolvimento que se verifica com o bem estar das pessoas, com a redução dos índices de mortes por desnutrição, com o índice de alfabetização entre outros índices que compõem o chamado IDH – índice de desenvolvimento humano, redução da exclusão digital, entre outras variáveis que são abaladas pelos prejuízos reflexos provocados por este fenômeno.

É justamente sobre o resultado do setor produtivo, isto é sobre as riquezas (compreendidas como divisas e valores capazes de gerar riquezas) que tem agido os denominados cibercriminosos (agora de forma organizada, pois houve uma migração de quadrilhas do mundo real para a internet), como verdadeiros piratas digitais, que saqueiam contas alheias, fazem compras ilegais com informações subtraídas sem autorização, promovem danos aos sistemas de informações de grandes corporações, causando prejuízo sem precedentes na história e numa escala transnacional. Este é o resultado de um fenômeno pós-moderno que desafia a ação do Estado e põe em cheque o Direito com ciência.

A consequência lógica desse prejuízo é a geração de obstáculos que poderiam propiciar investimentos por parte do setor privado e também do setor público, com a perda de tempo e de custos altíssimos na implementação de rotinas de segurança. Estes custos decorrentes de prejuízos inviabilizam ou diminuem de forma considerável os investimentos estatais.

A ação do Estado em tutelar o desenvolvimento econômico como parte integrante da ordem econômica vêm se efetivando, com a desarticulação de quadrilhas muito organizadas. O fundamento maior das condenações têm sido a legislação pátria (Código Penal e Leis Especiais), ainda que de forma tímida em face da ameaça que espreita, o Poder Público demonstra poder de reação e a efetividade das normas de direito penal brasileiras, e , neste contexto, a ausência de um instrumento jurídico de caráter internacional que subsidiasse juridicamente este embate, faz-se evidente.

3.3 Liberdade de expressão, privacidade e cibercrime

A liberdade de expressão representa um dos direitos fundamentais que embasam e caracterizam o Estado Democrático de Direito. É assim, considerado um direito humano fundamental, cujas raízes remontam à luta contra o absolutismo monárquico da França do Século XVIII, que com a queda do Império promulgou a Declaração Universal dos Direitos do Homem e do Cidadão, cujos ideais embasados na liberdade, igualdade e fraternidade passaram a nortear todo ordenamento jurídico do ocidente.

Na compreensão de Bonavides,[177] são considerados direitos de primeira geração e por isso são "direitos que valorizam primeiro o homem singular, o homem das liberdades abstratas, o homem da sociedade mecanicista que compõe a chamada sociedade civil" e por isso passaram a ser inseridos nos textos das cartas magnas das democracias constitucionais.

No âmbito do direito internacional, encontra-se insculpido no artigo 19, da Declaração Universal dos Direitos Humanos, no Pacto Internacional dos Direitos Civis e Políticos e no artigo 10 da Convenção Europeia dos Direitos Humanos, além de sua introdução como direito fundamental em muitas Constituições, a exemplo da Constituição da República Federativa do Brasil, embora, seja preciso esclarecer, que a liberdade de expressão não é um direito absoluto em muitos países, o que evidencia a procura por um equilíbrio entre o exercício da liberdade de se expressar com a ordem interna do Estado.

Se há respeito à liberdade de expressão, o que dizer então do direito à privacidade no Século XXI, quando cada vez mais a sociedade se sente dependente de bancos de dados que armazenam uma infinidade de informações de caráter pessoal, quer no âmbito do governo, quer nas relações comerciais comuns do dia-a-dia?

A privacidade integra assim como a liberdade de expressão, a esfera de elementares direitos sem os quais a vida do ser humano estaria sufocada pelo não poder se expressar e constrangida pela invasão do refúgio do ser humano que é o direito à sua privacidade, em casa, no trabalho, nas correspondências, em suas informações pessoais e na internet.

Assim, a proteção ao direito à privacidade encontra proteção, em âmbito internacional, no artigo 12, da Declaração Universal dos Direitos Humanos, de 1948, no

---

[177] BONAVIDES, Paulo. **Curso de Direito Constitucional**. 21 ed. Malheiros: São Paulo, 2007, p. 563.

artigo 17, do Pacto Internacional dos Direitos Civis e Políticos e no artigo 8º, da Convenção Europeia de Direitos Humanos, de 1950.

Nos EUA, berço da democracia ocidental, em face dos avanços tecnológicos e dos novos desafios propiciados pela internet e pelo ciberespaço Urofsky[178] diz que:

> Congresso tem tentado proteger informações sobre privacidade através de uma série de estatutos, incluindo as *Electronics Communications Privacy Act*, mas o problema é que a quantidade de informação disponível está a crescer a um ritmo exponencial, muito mais rapidamente do que os meios de controlar e regular o acesso.[179].

Mas é com esta visão, de respeito ao direito à privacidade, como direito humano fundamental que a Suprema Corte dos Estados Unidos ao julgar o caso Schmerber vs. Califórnia (384 US 757,767), em 1966 já decidia com base na Quarta Emenda à Constituição Americana que " A principal função da Quarta Emenda é o de proteger a privacidade e dignidade pessoal contra a intrusão injustificada por parte do Estado"[180], como relatam Solove, Rotenberg e Schwartz[181].

Desta forma Vianna[182] ensina que o direito à privacidade deve ser concebido num tríplice direito, quais sejam:

> [...] direito de não ser monitorado, direito de não ser registrado e direito de não ser reconhecido (direito de não ter registros pessoais publicados) - transcende, pois, nas sociedades informacionais, os limites de mero direito de interesse privado para se tornar um dos fundamentos do Estado Democrático de Direito.

Mas as questões que envolvem a liberdade de expressão e a privacidade tomaram um novo impulso, quando estas liberdades passaram a ser exercidas plenamente na internet e ciberespaço, tendo como pressupostos essenciais da grande rede o caráter de não estar submetido a nenhum controle e o seu caráter mundial. Consequentemente, logo, passaram a ocorrer registros de uso distorcidos de seu grande potencial, que se evidencia

---

[178] UROFSKY, Melvin. ***Individual freedom and the Bill Of Rights. U.S. Departament of State´s Bureau of International Information Program, Chapter 6, Washington D.C, 2003***. Disponível em: http://usinfo.state.gov/products/pubs/rightsof/privacy.htm. Acesso em: 13 mar.2008

[179] Texto original: "*Congress has attempted to protect informational privacy through a number of statutes, including the Electronics Communications Privacy Act, but the problem is that the amount of information available is growing at an exponential rate, far faster than the means to control and regulate access*." (Tradução nossa).

[180] Texto original: "*the overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the state*." (Tradução nossa).

[181] SOLOVE, Daniel J.,ROTENBERG, Marc and SCHWARTZ, Paul. ***Privacy, information and technology***. Aspen Publisher, New York, 2006, p.58.

[182] VIANNA, Túlio**. Transparência pública, opacidade privada**: O Direito como instrumento de limitação do poder na sociedade de controle. Revan: Rio de Janeiro, 2007, p.116.

mediante inúmeros relatos e casos de condutas criminosas praticadas sob o falso argumento de estarem exercendo a liberdade de expressão ou protegidas pelo direito à privacidade.

Em face da amplitude da grande rede e do grande número de usuários, com tendência de crescimento vertiginoso em países em desenvolvimento, há uma propensão cada vez maior para que condutas ilícitas possam prosperar como cibercrime e especificamente incidem sobre a privacidade como: disseminação de *spyware, web bug*, engenharia social, *cookies, phising* e outros códigos maliciosos. As condutas ligadas ao direito de liberdade de expressão são registradas como abusos, crimes contra a honra, racismo, ameaça, violação ao direito à privacidade, entre outras condutas que levaram a União Européia a adotar o Protocolo Adicional à Convenção de Budapeste, visando combater o racismo e a xenofobia na rede, como será exposto no último capítulo.

Tomando como exemplo as práticas de pedofilia infanto-juvenil na internet, as práticas abusivas praticadas sob o argumento de exercício do direito à liberdade de expressão ou de privacidade, traduzem-se em casos de exploração sexual envolvendo crianças e adolescentes, mediante disseminação de fotos, vídeos, textos, imagens e figuras de conteúdo pornográfico. Ressaltando-se ainda, que com o advento de tecnologias como a *web cam* (câmeras para internet), tais condutas são praticadas em tempo real e disseminadas de forma exponencial em sites de vídeos e de relacionamento, a exemplo do *Orkut* (da Google), *MySpace e Facebook*, com destaque para o primeiro em países como o Brasil e a Índia.

3.4 Atividade hacker

3.4.1 Compreendendo o mundo dos *hackers*

A palavra *hacker* deriva do verbo *to hack*, da língua inglesa, que em sentido estrito tem o significado de "cortar, tossir, entalhar, golpear", mas com a adaptação para substantivo passou a significar alguém com habilidade manual para entalhar madeira, conforme entendimento de Medeiros[183].

[183] MEDEIROS, Assis. **Hackers entre a ética e a criminalização**. Florianópolis:Visual Books, 2002, p. 37

A difusão do termo *hacker*, como aquela pessoa que é responsável pela prática de danos na internet é mais conhecida que o fundamento real que deu origem a terminologia. Há na verdade, impropriedade no emprego do vocábulo, que se desvirtuou de seu sentido originário, que esteve associado a professores e estudantes do *Massachussetts Institute of Technology* (MIT), que detinham conhecimentos muito aprofundados sobre informática, eletrônica e redes de computadores e os empregavam em estudos e pesquisas para desenvolvimento tecnológico. A impropriedade no uso errôneo do termo *hacke*r pode ser imputado à grande impressa sensacionalista que passou a massificar essa impressão.

Desta forma Assis Medeiros esclarece que:

> Foi a ainda em meados da década de 80 que a grande imprensa começou a dar espaço de destaque para os **hackers**. Neste sentido, podemos dizer que a mídia de massa como um todo (TV, rádio, jornais e revistas) é uma das principais responsáveis pela deturpação do termo clássico **hacker**. Foram os jornalistas que começaram a usar o termo **hacker** para designar alguém que usa o seu conhecimento com intuito criminoso. (grifos do autor).[184]

De fato, podemos dizer que há impropriedade no emprego da terminologia, mas este é o sentido pelo qual o vocábulo passou a ser difundido, e é o que passou a ser empregado para efeitos de caracterização geral de atitudes danosas praticadas na Web, embora sejam obrigados a fazer um detalhamento explicitando as diferenças existentes entre os personagens que compartilham o espaço virtual da grande rede.

A evolução da cultura *hacker* acompanhou o desenvolvimento da própria informática. Desta forma, Medeiros[185] entende que a primeira geração nasceu no MIT e foi responsável pelo aprimoramento de computadores, a segunda geração de *hackers* surgiu nos anos 70 e lutavam pela democratização da informática ao criticarem o monopólio da IBM, com o fim de massificar a cultura da informática.

A terceira geração de *hackers*, de acordo com Levy, citado por Medeiros[186] "é formada pelos programadores responsáveis pelos jogos de computador", caracterizando-se ainda pelo uso dos *Bulletim Board System* (BBS), que se constituía uma forma de comunicação entre os *hackers*.

A década de 90 fez florescer a quarta geração *hacker*, caracterizada principalmente pela explosão do uso em massa e comercial das redes telemáticas (no caso a internet), impulsionado mais ainda pela nova roupagem gráfica e interativa proporcionada

---

[184] MEDEIROS, op. cit. n. 183.
[185] MEDEIRO, op. cit. n. 183, p. 29-32.
[186] MEDEIROS, op. cit. n. 183, p.32.

pelo uso de *browsers* (navegadores) como o *Mosaic* e o *Netscape Navigator*. Um pouco mais adiante travou-se uma verdadeira guerra cibernética entre a *Netscape* e a *Microsoft*, que visava dominar o comércio de *browsers* para internet.

A revolução tecnológica que se vivenciou fez surgir uma cibercultura e um mundo virtual tão real quanto a vida que se compartilhou. Fez florescer novos personagens, atores sociais que passaram a utilizar a rede de diversas formas, e a partir de então, passaram a receber uma denominação peculiar no *underground* (espécie de submundo da internet), são eles: os *hackers, ckarckers, warez, phreakers e os script kiddies.*

O contexto atual indica não apenas ações isoladas com motivações de cunho ideológico. O crime organizado migrou para o ciberespaço e vem recrutando especialistas em alta tecnologia para prática de condutas criminosas como o *pihsing* e consequente clonagem de cartões e saques em contas bancárias. Tem se valido de investimentos e canais de leilão para promoverem a lavagem de dinheiro, branqueamento de capitais, espionagem, ciberterrorismo e guerra digital.

3.4.2 Grupos e subgrupos

3.4.2.1 *Hacker*

Os *hackers* estão no topo da hierarquia do conhecimento em informática, principalmente "em segurança da informação, sistemas operacionais, linguagem de programação e redes, dominando os melhores métodos de invasão", consoante lição de Mangueira[187].

Conforme visto há erro de denominação quanto ao verdadeiro sentido da palavra hacker, que em termos práticos têm as ações correspondentes a de um *cracker*. Isto quer dizer que ao invés de atribuírem ataques a *sites*, banco de dados, subtração de senhas a grupos *hackers*, na verdade deveriam associar tais condutas danosas aos *crackers*.

[187]MANGUEIRA, Hugo Alexandre Espínola. **Criminalidade cibernética:** estudo dos *hackers* e das implicações legais de seus ataques através da Internet. João Pessoa, 2002, p. 53.

Existiriam assim, alguns fatores essenciais que podem ser diferenciados a partir da chamada ética hacker, a qual estaria associada a alguns princípios. Estes princípios, de acordo com Hell[188] seriam:

> 1) O Conhecimento adquirido deve ser utilizado apenas para benefício da aquisição de mais conhecimentos;
> 2) Todo hacker deve preservar os dados do sistema invadido, jamais deverá corromper, deletar ou alterar esses dados;
> 3) O conhecimento adquirido só deverá ser compartilhado com aqueles que assim o fizerem (E merecerem);
> 4) Um hacker sempre buscará invadir mais e mais sistemas, e sempre resguardar as senhas para futuros acessos;
> 5) Um hacker sempre manterá sigilo da sua existência, jamais se revelará a quem quer que seja. (Somente aos membros do grupo).

Entretanto, ao se fazer uma pesquisa no *site* Google (http://www.google.com.br) e colocar como parâmetro para busca o termo "ética hacker" serão encontradas 44.100 referências no Brasil que se reportam à terminologia "ética hacker".

Ao acessar o endereço na internet http://www.forum-invaders.com.br/phpBB/viewtopic.php?f=55&t=8554911&p=311898, Martins[189] descreve não somente a cinco mandamentos da ética *hacker*, mas a 21:

> 1- Descobriu algo novo, OLHE!
> 2- NÃO APAGUE, pense no que seria melhor; ter acesso a um provedor ou detoná-lo?
> 3- NÃO MODIFIQUE NADA, ao menos que queira que saibam que esteve lá.
> 4- Nunca tente um su root direto! Isso fica logado.
> 5- Não fique dando telnet ou pegando mail usando acesso dos outros!
> 6- Nunca subestime um sysop.
> 7- Escolha horas entre 24:30 as 6:00.
> 8- Uma vez lá dentro tente dominar o lugar, é claro, com cautela.
> 9- Não confie em ninguém.
> 10- Se pegar a senha do root de algum provedor e não souber o que fazer MATE-SE!
> 11- Não teste vírus no seu próprio HD.
> 12- É bom preparar muito bem uma estratégia antes de atacar.
> 13- Use os computadores de sua universidade (é mais seguro).
> 14- Não fique distribuindo informações para ninguém ou dados sobre o que vc pegou.
> 15- NÃO OBEDEÇA REGRAS. Claro que estas tem que ser cumpridas.
> 16- Não tenha pena de ninguém.
> 17- Vc usa o MS-DOze ou o Windoze? Não conte pra ninguém...
> 18- Vc usa o algum UNIX ou LINUX? Esteja certo que esta bem seguro...
> 19- Não crie laços afetivos com a vítima.
> 20- Aprenda o máximo que puder com quem sabe mais! Não se meta a besta direto
> ÚLTIMO: Não se submeta a nenhum sistema hierárquico.

---

[188]HELL, Lord. **A consciência hacker – uma visão objetiva**. Rio de Janeiro: Book Express, 2000, p. 5.
[189]MARTINS, Paulo Roberto. **Mandamentos Hackers**. 2003. Disponível em:<http://www.forum-invaders.com.br/phpBB/viewtopic.php?f=55&t=8554911&p=311898>. Acesso em: 2 ago.2008.

As informações acima transcritas tornaram-se de “domínio público” e encontram-se repetidas em muitos *sites* que versam sobre hacker.

3.4.2.2 *Cracker*

A diferença entre um *hacker* e um *cracker* é basicamente de ordem ideológica. *Cracker* seria uma espécie de *hacker* com disposição para provocar um dano, subtrair informações, invadir um computador, desfigurar a página principal de uma instituição ou até mesmo prestar serviços ao crime organizado. Enquadram-se nesta categoria os "pichadores" de *sites*, conhecidos também como *defacers* que invadem e desfiguram páginas na internet. A terminologia também está associada a pessoas muito habilidosas que “craqueiam” os programas de computador; isto é, retiram travas digitais, descobrem senhas e alteram suas características com o fim de fazer uso de softwares sem pagar pela licença.

Há registros de que o Brasil vem ocupando local de destaque mundial, principalmente pelo fato de possuir grupos de *crackers* muito organizados e ativos. Os grupos *cracker* são os potenciais sujeitos ativos de inúmeras atividades delituosas que são viabilizadas através da internet, daí o risco de cooptação pelo crime organizado.

3.4.2.3 *Lamer*

O termo *lamer* é empregado para designar aqueles indivíduos que estão iniciando no submundo *cracker*. Possuem conhecimentos iniciais sobre técnicas de violação de sistemas, mas são alvo de *hackers* e *crackers*.

Os iniciantes têm acesso às informações sobre violação de sistemas através de literatura especializada ou na própria internet, que é o mais comum, justamente por apresentar muitos *sites* que estimulam o início de atividades *crackers* e também mostram, numa espécie de guia, as principais técnicas de invasão.

3.4.2.4 *Phreaker*

Os *phreakers* são indivíduos que possuem habilidades para violar sistemas de telefonia fixa e/ou móvel. Através da exploração de falhas no sistema, procuram formas de viabilizar a realização de ligações gratuitas, burlando assim o sistema.

É preciso registrar ainda, que a ação dos *phreakers* submete a privacidade dos usuários, principalmente através da clonagem de telefones e escuta clandestina de conversas que transitam na rede de telefonia.

Para Mangueira "A ação dos *phreakers* tem como consequência, ainda, a adulteração no rastreamento de suas ações, uma vez que ele fica "invisível" aos equipamentos das concessionárias e o pagamento pelos usuários inocentes das ligações realizadas"[190].

No caso de clonagem de telefone celular, o *phreaker* fazendo uso de um scanner de frequência ou um receptor de rádio de alta freqüência, consegue identificar o número da linha e o número de série do aparelho, usando-os no clone. Isso também pode ocorrer quando alguém leva o aparelho celular para conserto, pois ao abrir o aparelho, o técnico também tem acesso a esses números, podendo se apoderar deles.

3.4.2.5 Cyberpunk

Para Alex Lamikiz "*cyberpunk* é alguém que sabe usar a tecnologia para criar seu próprio material audiovisual e editar sua própria MTV em seu Macintosh. Indivíduos que usam sua inteligência não para ganhar dinheiro para uma grande empresa, mas para enriquecer sua vida e suas relações humanas".[191]

Suas ações não têm uma motivação específica, agindo assim por pura diversão, muito embora além de violarem os sistemas possam causar danos ou pixações.

3.4.2.6 *Wannabe*

São os indivíduos que estão iniciando as práticas de violações de sistemas,

[190] MANGUEIRA, op. cit. n. 187, p. 58.
[191] LAMIKIZ, **Alex. Afinal o que é cybercultura**. Disponível em: < http://listas.cev.org.br/arquivos/html/cevcomp/2003-09/msg00000.html>. Acesso em: 23 abr. 2009.

fazendo uso para tanto, de programas já prontos que conseguem na internet para invadir sistemas ou descobrir senhas.

3.4.3 Motivações para prática de cibercrime

Questão intrigante que nos parece relevante diz respeito aos motivos pelos quais um indivíduo é levado a perder muito tempo de sua vida fazendo uso de um computador para violar sistemas e consequentemente cometer um cibercrime.

Em setembro de 2003, a revista Época em reportagem da jornalista Luciana Vicária[192] dedicou grande espaço nas suas páginas ao entrevistar Kevin Mitnik um dos maiores *hackers* de todos os tempos:

> Cultuado na internet como o maior hacker de todos os tempos, o americano **Kevin Mitnick**, de 40 anos, tornou-se celebridade aos 17 ao invadir o sistema do Comando de Defesa Aérea dos Estados Unidos. Antes de completar 18 anos já estampava páginas de jornais e revistas com uma habilidade incomum e inédita para a época: destrinchar complexos programas de computador. A brincadeira tomou proporções perigosas quando desafiou gigantes da tecnologia como Motorola, Nokia, Novell e Sun Microsystem. Em 1993 ele foi caçado pela polícia e, dois anos depois, preso pelo FBI, acusado de causar prejuízos superiores a US$ 80 milhões. Condenado, amargou cinco anos na prisão e ficou mais três em liberdade condicional, proibido de chegar perto de computadores. Nem assim perdeu a fama de fora-da-lei mais admirado da rede mundial. Pela primeira vez no Brasil, Mitnick será a estrela da IT Conference, encontro que reunirá mais de 800 profissionais de tecnologia entre os dias 17 e 19, em Salvador. Em entrevista exclusiva a ÉPOCA, ele descreve o prazer de voltar à web e explica como atuam os hackers do novo milênio. (grifo nosso).

Mais adiante, na referida entrevista surge a seguinte abordagem:

> **ÉPOCA** - *Qual era sua motivação?*
> **Mitnick** - O desafio intelectual, a busca pelo conhecimento e a aventura de estar num lugar onde não deveria estar. Comecei aos 17 anos e só parei quando fui preso. Mas eu não era o hacker temido como pintam por aí, um fora-da-lei que cria e espalha vírus. Eu era simplesmente um jovem curioso que buscava desafios em sistemas de segurança. Eu procurava brechas, e não informações. Jamais invadi um sistema para obter vantagens financeiras e até hoje não vi uma prova legal contra mim. (grifos do autor).[193]

Como se vê, ainda que tenha parado de praticar atividades delituosas, Mitnick

---

[192] VICÁRIA, Luciana. **Kevin Mitnick - Hacker regenerado**. São Paulo: Revista Época On Line, Edição nº 278, 15/09/2003. Disponível em: <http://revistaepoca.globo.com/Epoca/0,6993,EPT600936-1666,00.html>. Acesso em: 1 ago.2008.
[193] VICÁRIA, op. cit. n. 190.

transformou-se numa espécie de ícone para o mundo *underground* (submundo na internet), servindo de inspiração para que outros jovens procurem realizar as ações que ele fez. Mas não temos como comparar as atividades de Mitnick, com as ações dos atuais *crackers*, pois viveram momentos diferentes da internet.

Em estudo sobre a ação dos *hackers*, Mangueira[194] enumera doze motivações que levam as pessoas a praticarem condutas danosas na internet, as quais foram simplificadas na tabela abaixo:

Tabela 2 - Motivação e objetivos das violações de sistema

MOTIVAÇÃO	SUJEITO ATIVO	OBJETIVO
Espionagem industrial	*Crackers*	Obter informações, destruir planos ou projetos rivais de empresas rivais ou tornar serviços inoperantes
Ciberterrorismo	*Crackers*	Tem por objetivo um ideal (ex: guerra religiosa), aproveitam-se de falhas de segurança nos sistemas do governo, desestabilizando ou obtendo informações sigilosas. Ex. Ações da Al-Qaeda.
Ideologia	*Crackers*	Fortalecimento da guerra ideológica entre países ricos x países pobres e o crescente sentimento de ódio aos EUA e Inglaterra e ainda conflitos localizados no oriente (Palestinos x Judeus, Iraque x EUA) e na Oceania e Ásia. Maiores alvos: EUA e aliados.
Benefício comercial	*Crackers*	Descobrir os gostos e tendências dos internautas com vistas a oferecer produtos e serviços. A ação se dá mediante instalação de programas espiões.
Violação de privacidade	*Crackers*	Visa fazer incursões em computadores alheios, principalmente usuários domésticos.
Benefício escuso – furto, dano moral, estelionato	*Crakers e Phreakres*	Visa alguma vantagem financeira ou de qualquer ordem, como fazer ligações gratuitas em telefones, transferências eletrônicas ilícitas, compras com cartões de crédito clonados.
Descuido involuntário	*Wannabe*	Não tem um fim específico. Ocorre devido a um descuido na manipulação de um programa de invasão, por exemplo.
Vingança	*Crackers, cyberpunks, phreakers e lammers*	Vingança devido a uma demissão ou por ter perdido um contrato, invadem os computadores rivais buscando vingança.
Busca de reconhecimento	*Hackers, crackers cyberpunks,*	Busca reconhecimento ou aceitação em determinados grupos ou procuram notoriedade ao invadirem sites

[194] MANGUEIRA, op. cit. n. 187, p. 67-70.

	wannabes e lammers	famosos
Aprimoramento de conhecimento técnico	*Hacker*	Procura com as invasões o aperfeiçoamento de suas técnicas ou mesmo desenvolver novas formas de invasão de sistemas, algumas vezes ajudando a corrigi-las.
Vontade de desafiar	*Hackers,crackers, phreakres, wannabes*	Tenta a notoriedade ou reconhecimento com a invasão de sistemas seguros. O sentimento se assemelha aos de grafiteiros e pixadores.
Índole destruidora	*Crackers*	Objetiva invadir sistemas e destruir, alterar ou subtrair informações importantes.
Furto de dados	*Crackers*	Venda de informações no mercado negro a grupos do crime organizado
Subtração de identidade	*Crackers*	Acesso ilegal a sistemas. Clonagem de identidade. Clonagem de cartão.

Fonte: Pesquisa do autor, com base em informações de Mangueira.

É preciso compreender que a visão romântica ou ideológica que se tinha vem sendo substituída por ações motivadas por questões que envolvem grandes importâncias em dinheiro.

Desta forma, noticiou o portal terra:

> Descobrir dados sigilosos e invadir redes deixou de ser uma atividade praticada em busca de conhecimento, como os crackers do período "romântico", ou reconhecimento e fama para os mais modernos.
> Hoje, os bandidos virtuais transformaram o crime em "organizações" estruturadas. O processo é divido entre vários "funcionários", dispostos em cargos distintos, e a atribuição de funções pode ser comparada àquela praticada por uma outra irmandade de criminosos famosa: a máfia.
> A comercialização dos dados se tornou um excelente negócio [...] e, ao contrário do que se pensa, há sempre uma certa demanda: clientes dispostos a pagar por informações roubadas.[195]

3.4.4 *Modus operandi hacker*: principais formas de práticas de cibercrimes e outras ações danosas

Ciente de que motivações não faltam para que ocorram incidentes de violações

[195] PORTAL TERRA. **Roubar dados virou crime organizado**. Disponível em: <http://www.computadorbr.com/informatica-3/roubar-dados-virou-crime-organizado.html>. Acesso em: 23 abr.2009.

de sistemas, há do mesmo modo, interesse das instituições em proteger-se dos riscos proporcionados pelo simples fato de estar conectado à rede.

De acordo com Martins[196] "Existem muitos tipos de ataques a sistemas, e muitos modos de agrupá-los em categorias." Desta forma pode-se agrupar os ataques em três categorias: negação de serviços (indisponibilidade de serviço), subtração de informações e a invasão.

A Indisponibilidade de serviço (*Denial of Service* ou negação de serviço) é o tipo de ataque que impede que os usuários de um determinado serviço o utilizem. Geralmente esse tipo de ataque é muito difícil de ser evitado, pois ao aceitarem serviços do universo externo (como por exemplo, correio eletrônico, chamadas telefônicas, pacotes, etc.), existe a possibilidade de ataque aos mesmos. Felizmente este tipo de ataque não é muito popular, pois pode ser facilmente monitorado e o causador do mesmo ser identificado.

No que se refere à subtração de informação, existe a possibilidade um *cracker* poder acessar as informações sem necessariamente estar *on line* nos computadores que as contém. Normalmente este tipo de ataque visa serviços da internet que disponibilizam informações, ao induzi-los a disponibilizar mais informação do que planejado ou então disponibilizar a mesma para uma pessoa não autorizada.

A subtração de informação não necessita ser ativa ou particularmente técnica. Pois uma pessoa que deseja descobrir informação pessoal de alguém pode simplesmente ligar e perguntar fazendo-se passar por alguém conhecido: este é um tipo de roubo de informação ativo. Similarmente, se alguém quiser coletar informação eletrônica pode buscá-la ativamente fazendo-se passar por uma máquina ou um usuário com acesso válido, ou passivamente monitorando a rede e esperando pela mesma.

O tipo mais comum de ataque é a invasão. Na invasão, os *crackers* têm a possibilidade de utilizar os recursos computacionais do site invadido, como se fossem usuários legítimos. Os invasores têm dezenas de maneiras de obter acesso, que variam desde a chamada "engenharia social" até a simples adivinhação de usuários e senhas.

Como forma de aprofundar o estudo, uma vez evidenciadas as motivações hacker, relaciona-se, agora, as principais formas de ação (*modus operandi*) empregadas para viabilizar os ataques, quais sejam: *spoofing, mail bomb, trojan horse, sniffing, ping of death, Denial of Service (DoS),* vírus de computador*,* engenharia social, *spyware* e *worm*.

---

[196] MARTINS, José Carlos Cordeiro. **Gestão de projetos de segurança da informação**. Rio de Janeiro: Brasport, 2003, p. 217.

3.4.4.1 *Spoofing*

É a técnica de se fazer passar por outro computador da rede para conseguir acesso a um sistema. Há muitas variantes, como o *spoofing* de IP. Para executá-lo, o invasor usa um programa que altera o cabeçalho dos pacotes IP de modo que pareçam estar vindo de outra máquina. Por exemplo: o computador "A" com IP de número 10.1.2.5 comunica-se com outro "B" de número de IP 10.1.2.7. Um cracker fazendo uso de um computador "C" com número de IP 10.1.29.45, consegue burlar a segurança do sistema e faz-se passar por uma das máquinas ("A" ou "B") tendo acesso a uma delas e podendo acessar inclusive outras máquinas conectadas na rede. Os dois tipos de ataque por *spoofing,* bastante conhecidos são - *IP Spoofing* e DNS *Spoofing*.

3.4.4.2 *Mail bomb*

É a técnica de encher um computador com mensagens eletrônicas (geralmente servidores de e-mal). Em geral, o *cracker* usa um *script* (programa) para gerar um fluxo contínuo de mensagem e abarrotar a caixa postal de alguém. A sobrecarga tende a provocar negação de serviço no servidor de e-mail, deixando-o inacessível.

3.4.4.3 *Trojan horse (cavalo-de-tróia)*

O cavalo-de-tróia (*trojan*) é um programa usado para abrir um determinado acesso em seu computador. Com o programa instalado em sua máquina, ele abre essa porta e dá informações suas quando você está conectada à pessoa que lhe mandou o *trojan*. Sempre que o internauta se conectar à *web* o *cracker* que lhe enviou o *trojan* irá saber, e vai passar a monitorar e a ter controle sobre sua máquina.

Estes tipos de programas são enviados principalmente através de arquivos infectados com extensões *.exe*, .com e *.bat*, e quando o usuário faz funcionar a aplicação o *trojan* se instala. Ressalte-se que os golpes estão cada vez mais ousados e o simples fato de

abrir o email e receber um arquivo de texto ou uma foto, pode configurar sério risco de contaminação.

3.4.4.5 *Sniffing*

É um tipo de programa que captura pacotes de dados que transitam na internet, como senhas, logins, número de cartões de crédito. Constitui-se assim numa interceptação das informações que estão transitando na *web*.

3.4.4.6 *Ping of death*

Consiste na remessa de um pacote de informações para um servidor, maior que o permitido, alterando a funcionamento do computador e fazendo-o parar.

3.4.4.7 *Denial of Service (DoS)*

Neste tipo de ataque não há subtração de informação, mas inúmeras requisições que sobrecarregam o tráfego de uma rede, fazendo com que um servidor e seus serviços fiquem “fora do ar”.

3.4.4.8 Vírus de computador

A disseminação de vírus ocorre através de arquivos infectados. Os vírus são pequenos programas que executam as mais diversas rotinas, como: apagar arquivos, travar o computador, inviabilizar o funcionamento de certos programas entre outros.

Os prejuízos devido à infectação por vírus são enormes. “O vírus SirCam causou prejuízos acima de US$ 1 bilhão”, conforme Mangueira.[197]

3.4.4.9 Engenharia Social

É a técnica empregada para descobrir informações sobre um sistema. Não chega a ser um ataque propriamente dito, pois não há invasão, mas a coleta de informações sobre o sistema, numa espécie de atos preparatórios para realização de ataques. Exemplo: ligar para um setor de informática e pedir a senha do servidor, alegando ser um funcionário da empresa.

3.4.4.10 *Spyware*

São programas (*Broadquest*) que são utilizados por empresas para descobrir hábitos, preferências e tendências do usuário, fazendo registro dessas informações e remetendo-as às empresas destino. Constituem uma flagrante violação de privacidade. Vasconcelos[198] cita como exemplo o programa “coelho malvado” fornecido pela empresa Mattel.

Para Mangueira[199], programas como o *gator* e o *cydoor*, além do tradutor *Babylon* seriam programas *spyware*.

3.4.4.11 *Worms*

São programas similares aos vírus, com a diferença de que conseguem realizar cópias de si mesmos ou de algumas de suas partes (e alguns apenas fazem isso). Os *worms* não necessitam infectar outros arquivos para se multiplicar e normalmente se espalham

[197] MANGUEIRA, op. cit. n. 187, p.83.
[198] VASCONCELOS, op. cit. n. 21, p. 38.
[199] MANGUEIRA, op. cit. n. 187, p. 85.

usando recursos da rede (o e-mail é o seu principal canal de distribuição atualmente). Podem provocar travamento do sistema entre outros danos.

3.4.4.12 *Pishing*

Os cavalos de tróia são a técnica preferida no *pishing*, onde o cracker procurar "pescar", obter informações, principalmente dados bancários da vítima que está com o computador infectado, uma vez que o cavalo de tróia possibilita o controle da máquina do usuário.

Tem sido muito comum o registro de pessoas reclamando que tiveram informações bancárias alteradas (saques indevidos) ou usuários de redes de relacionamento que tiveram perfis clonados ou até mesmo subtraídos.

3.4.4.13 *BotNet*

Uma série de ameaças impensáveis tem surgido na rede, tornando o ciberespaço um ambiente potencialmente inseguro. Ataques como o que sofreu a Estônia em 2007, pode ter sido vítima, também, de ataque em massa de computadores conectados a uma BotNet.

De acordo com a Wikipédia:

> Botnet é uma coleção de softwares robôs, ou bots (diminutivo de robots - robôs em inglês), que são executados automaticamente e de forma autônoma. O termo é freqüentemente associado com software malicioso, mas ele também pode referir-se à rede de computadores usando computação distribuída software.
> Embora o termo "botnet" pode ser usado para se referir a qualquer grupo de bots, como o IRC bots, esta palavra é geralmente usada para referir-se a uma coleção de computadores infectados (chamados de computadores zumbis) executando o software, geralmente instalados através worms, cavalos de Tróia, ou backdoors, sob um comando e de controlo das infra-estruturas.

3.5 Cibercrime: jurisdição, competência, desafio à ordem jurídica e ação do estado

3.5.1 Elementos essenciais à compreensão da jurisdição e da competência jurídica do Estado em face do cibercrime

A abordagem sobre as temáticas jurisdição e competência em relação ao cibercrime mostra-se pertinente em face do caráter transnacional do fenômeno, cujas implicações transcendem o estudo puro e simples dos vocábulos, bem como a abordagem tradicional emprestada aos termos nas cátedras universitárias de Direito Constitucional, Direito Penal, Direito Processual e Direito Internacional.

A concepção terminológica também remete a revisão temática sobre os aspectos inerentes a soberania, como constante nas linhas iniciais deste trabalho. Ademais, as expressões soberania, jurisdição, competência e território, quando analisadas sob a dimensão do cibecrime, do ciberespaço e da internet assumem feição cujos delineamentos jurídicos para tratar a questão ainda se encontram em construção, embora, seja possível sopesar os indicadores destas novas tendências a constituírem um desafio ao Estado pós-moderno.

Num primeiro plano, convém salientar que a palavra jurisdição deriva do latim *"júris"* (direito) e "*dicere"* (dizer). Merece, entretanto, sob o ponto de vista da Ciência do Direito, a compreensão de que o termo significa o poder que tem o Estado para fazer a aplicação de suas leis, de seu ordenamento jurídico aos conflitos que emergem da própria convivência em sociedade, resguardando, pois a autoridade da lei e consequentemente a paz social.

Neste sentido Padilha ensina que:

> O Estado tem o dever de resolver as questões para restabelecimento da convivência pacífica. Pouco importa a qualificação da jurisdição como um poder, um poder-dever, etc. Ninguém de sã consciência poderá afirmar possível uma sociedade como a nossa sem atividade jurisdicional. Nesse sentido, sendo ela necessária, é um dever do Estado suprir essa necessidade, sob pena de sua própria desintegração.[200]

No estudo dos institutos jurídicos, dentre as funções do Estado, a jurisdição encontra grande dissenso doutrinário quanto a sua conceituação. Para Lima[201] as teorias mais

---

[200] PADILHA, Luiz R. Nuñes. **Chiovenda, jurisdição voluntária e processo penal**. UFRGS. Rio Grande do SUl, 1996. Disponível em<http://www.direito.ufrgs.br/pessoais/padilla/Trabalhos%20Publicados/CHIOVEND.htm>. Acesso em: 18 fev. 2009.

[201] LIMA, Wesley de. **Uma nova abordagem da jurisdição no Processo Civil contemporâneo**. In: Âmbito Jurídico, Rio Grande, 59, 30/11/2008 [Internet]. Disponível em:

proeminentes são sintetizadas pelas concepções de Chiovenda e Carnelutti, sendo esta tese referendada por Canotilho, para quem o "problema da distinção material das várias funções do Estado (legislação, administração e jurisdição), [...] há muito considerado como uma das questões mais discutidas e relativamente infrutuosas da dogmática jurídica."[202]

Ao escrever sobre a temática Chiovenda teoriza que a jurisdição é:

> Função do Estado que tem por escopo a atuação da vontade concreta da lei por meio da substituição, pela atividade de órgãos públicos, da atividade de particulares ou de outros órgãos públicos, já no afirmar a existência da vontade da lei, já no torná-la, praticamente, efetiva. [...] [203]

Já Carnelutti sustenta que a "jurisdição é uma função de busca da justa composição da lide."[204] Esta composição pode acontecer de forma harmônica, o que enseja a ideia de uma jurisdição voluntária. Pode ocorrer, ainda, mediante intervenção de um terceiro, que não o Estado, configurando-se no que a doutrina denomina de Arbitragem. Na lição de Fredie Didier "exercício de jurisdição por autoridade não-estatal"[205], sendo no Brasil regulada pela Lei 9.307 de 23 de setembro de 1996.[206]

Ainda que a ausência de um consenso possa inserir-se num contexto nebuloso, inegável, porém, que a jurisdição, compreendida sob tríplice aspecto de poder, função e atividade é uma forma de exercício da soberania estatal, o que remete, obrigatoriamente aos elementos essenciais do Estado e consequentemente a ideia de território, fronteiras, ou seja, espaço geográfica onde esse poder jurisdicional é exercido, mas que "pela sua própria natureza, tem um aspecto internacional."[207]

---

http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=5290. Acesso em 22/03/2009.

[202] CANOTILHO, José Joaquim Gomes. **Direito Constitucional**. 6a Ed. Livraria Almedina: Coimbra, 1993. p. 708.

[203] *Apud* LIMA, Wesley de. **Uma nova abordagem da jurisdição no Processo Civil contemporâneo**. In: Âmbito Jurídico, Rio Grande, 59, 30/11/2008 [Internet]. Disponível em http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=5290. Acesso em 22/03/2009.

[204] *Apud* Lima, op. cit. n. 200.

[205] DIDIER JR, Fredie. **Curso de Direito Processual Civil**. 9. ed. Bahia: JusPodivm, 2008, p. 68.

[206] Merece destacar as disposições gerais da Lei que regula a arbitragem no Brasil, que enuncia em seus artigos 1º e 2º, o seguinte:

Art. 1º As pessoas capazes de contratar poderão valer-se da arbitragem para dirimir litígios relativos a direitos patrimoniais disponíveis.

Art. 2º A arbitragem poderá ser de direito ou de eqüidade, a critério das partes.

§ 1º Poderão as partes escolher, livremente, as regras de direito que serão aplicadas na arbitragem, desde que não haja violação aos bons costumes e à ordem pública.

§ 2º Poderão, também, as partes convencionar que a arbitragem se realize com base nos princípios gerais de direito, nos usos e costumes e nas regras internacionais de comércio.

[207] BERMAN, Frank. ***Theoretical approaches to the assertion of jurisdiction - Jurisdiction: the state***. In: CAPPS, Patrick; EVANS, Malcolm; KONSTADINIDIS, Strato V. ***Asserting jurisdiction: international and European legal perspectives***. Oxford: Hart Publishing, 2003. p. 3.

É esta concepção de jurisdição que irá interessar para efeito de estudo, que se mescla, consequentemente, com as práticas danosas do cibercrime, uma vez que a pretensão do exercício da jurisdição em determinada conduta ilícita pode encontrar limites no exercício jurisdicional de outro Estado, tanto em matéria de ordem pública quanto as que envolvam interesses privados, gerando, por consequência impasses para aplicação do direito e qual direito.

Se a jurisdição delimita a ação do Estado para o exercício da função jurisdicional, para Silva a competência judicial é:

> [...] uma parcela da jurisdição, indicadora da área geográfica em que o juiz irá atuar, da matéria e das pessoas que examinará. É a competência que dá ao juiz o poder de julgar. Atribuída em lei (ou seja, a lei fixa quais as causas que determinado juiz, em determinada vara, poderá julgar), a competência determina os limites dentro dos quais pode legalmente julgar. Quando o juiz não tem tal poder, é considerado incompetente, e os atos assim praticados podem ser declarados nulos. Quando um juiz assume a titularidade de uma vara criminal, por exemplo, não poderá julgar uma ação de divórcio, que é de competência das varas de família.[208]

A exposição do conceito de competência, como visto, afasta de plano outras abordagens que se pretenda ofertar, pois, além dessa conotação vinculada ao exercício da jurisdição, ou seja, do Estado juiz, há, contudo, outras feições inerentes à competência, sobretudo àquelas previstas na Constituição da República Federativa do Brasil, que a doutrina empresta a terminologia de "repartição de competências na Constituição Federal".

Registre-se, porém, que essa repartição de competência *latu sensu* indica, sobretudo, a repartição de atribuições que estão mais conexas com o exercício da função executiva e legislativa do Estado, no caso do Brasil - Estado federal. Logo, tal distribuição de encargos prevista na Constituição indicará as competências da União, dos estados-membros e dos municípios. Esta indicação de atribuição é relevante no sentido de que enquanto o Estado-Juiz aplica a lei, há de se ter em mente, porém, a realização de outras funções essenciais como o papel desempenhado pelas organizações policiais (Poder Executivo) e do Ministério Público no exercício de atividade essencial à justiça.

Corroborando o entendimento que enseja grande dificuldade de fixar tais atribuições Ferraz teoriza:

Texto original: *But the nature of these powers shoud also be recalled, at the very out set.* Tradução nossa.
[208] SILVA, De Plácido e. **Vocabulário Jurídico**. Rio de Janeiro: Forense, 11ª. ed., 1994. Disponível em <http://pt.wikipedia.org/wiki/Competência_judicial>. Acesso em: 10 mar. 2009.

> Nenhum Estado federal pode existir sem uma Constituição escrita e rígida, que fixe a distribuição de competências entre a União e as unidades federadas. Não há nada mais delicado, na elaboração constitucional federativa, do que o estabelecimento das competências das entidades de poder que compõem a federação. Essa distribuição - chave da estrutura federal - está sujeita ao princípio de que há um mínimo irredutível de competências da União e do estado-membro.[209]

Pois bem, neste norte, vislumbra-se a jurisdição e a competência como elementos essenciais a serem sopesados em contraponto às condutas delituosas que envolvem o cibercrime, o ciberespaço e a nova perspectiva de cooperação internacional, uma vez que numa perspectiva do direito nacional, há ainda que de forma difusa, instrumentos jurídicos capazes de aplicação aos referidos registro de condutas ilícitas viabilizadas com emprego ou através da internet, sendo esta empregada como fim em si ou como instrumento para prática de crimes.

Num panorama constitucional, uma série de dispositivos irá nortear, como princípios, a aplicação da legislação, notadamente na seara penal. Sob a ótica do direito objetivo e subjetivo, há, respectivamente, disposições claras no próprio Código Penal e no Código de Processo Penal que vem sendo aplicadas pelos órgãos do Poder Judiciário.

Estabelece-se desta forma, a incidência dos princípios que regem a lei penal no espaço. Seriam eles capazes de aplicação em relação ao cibercrime outras condutas danosas perpetradas no ciberepaço? É resposta mais prudente indica que, em parte, há tutela jurisdicional para tais condutas.

Esta resposta é parcial, como bem pontifica Cruz, em face do "caráter extraterritorial apresentado pelas condutas praticadas com o auxílio da informática."[210] Há de se considerar ainda que tais práticas delituosas consubstanciam-se em delitos transfronteiriços ou transnacionais, de modo a impingir novos desafios a princípios e aplicação da lei penal no tempo e no espaço. De acordo com o magistério de Chawki "os cibercrimes têm mais um caráter internacional, embora as informações por si mesmas são regidas pelo direito nacional."[211]

Vê-se, pois, que tais condutas apesar de apresentarem um caráter mundial, em face do alcance da própria rede (Internet) e das novas fronteiras propiciadas têm registro

---

[209] FERRAZ, Anna Cândida da Cunha. **União, Estado e Município na Constituição Federal: competências e limites**. Cadernos Fundap: São Paulo, ano 8, n° 15, págs. 42-47, abr./1998, p. 43.
[210] CRUZ, Daniella da Rocha. **Criminalidade informática: tipificação penal das condutas ilícitas realizadas com cartões de crédito**. Rio de Janeiro: Forense, 2006. p. 2.
[211] CHAWKI, op. cit. n. 153, p. 4.
Tradução do original em francês: "*les infractions informatiques ont le plus souvent un caractère international, alors que les informations en elles-mêmes sont des données régies par le droit national.*" (Tradução nossa).

considerável no âmbito nacional, consequentemente, sujeitando os infratores ao disposto na legislação penal nacional.

3.5.2 Aplicação de leis penais nacionais e os cibercrimes

Como decorrência do princípio da soberania, a lei penal tem vigência no espaço territorial do Estado, como regra. Na lição de Bitencourt "pode ocorrer, em certos casos, para um combate eficaz à criminalidade, a necessidade de que os efeitos da lei penal ultrapassem os limites territoriais para regular fatos ocorridos além de sua soberania."[212] Ou ainda, uma infração penal pode violar bens jurídicos e, por consequência a ordem jurídica, em dois ou mais Estados.

Tomando por base a legislação penal brasileira, portanto, inegável reconhecer que o Estado através de seus órgãos policiais, notadamente a Polícia Federal, o Ministério Público e o Poder Judiciário têm agido firmemente nos últimos cinco anos.

A abordagem sobre a legislação nacional, não desconfigura o reconhecimento do caráter transnacional no cibercrime, o que se pretende, entretanto, é demonstrar a efetividade da legislação nacional quanto aos delitos que aqui forem cometidos. Este indicativo afasta consequentemente, a ideia de que as leis nacionais são como um todo ineficazes.

Decorre, pois, a necessidade de explanação dos princípios que regulam a aplicação da lei penal no espaço, com base na legislação nacional. Estes princípios de acordo com o magistério de Bitencourt[213] são: princípio da territorialidade; princípio real, de defesa ou de proteção; princípio da nacionalidade ou da personalidade; princípio da representação ou da bandeira e princípio da universalidade ou cosmopolita.

A legislação penal brasileira estabelece como regra geral, para aplicação da lei penal no espaço, o princípio da territorialidade, com suporte previsto no art. 5º, *caput,* do Código Penal Brasileiro, de forma que se aplica a lei brasileira, como regra, aos fatos puníveis que forem registrados em nosso território, independente da nacionalidade do infrator, da vítima e do bem jurídico violado.

---

[212] BITENCOURT, Cezar Roberto. **Tratado de direito penal, volume 1: parte geral**. 13ª ed. São Paulo: Saraiva, 2008. p. 175.
[213] BITENCOURT, op. cit. n. 209, p. 175-176.

O segundo princípio denominado pela doutrina de princípio real, de defesa ou de proteção, possibilita a ampliação da jurisdição penal do Estado cujo bem jurídico foi lesado, com fundamento na nacionalidade deste bem, é o que se infere do disposto no art. 7º, inciso I, do Código Penal Brasileiro.

Ao analisar este princípio Bitencourt pondera que:

> Em tempos de "economia global", os interesses nacionais têm sido violados, desrespeitados e, às vezes, até ultrajados no estrangeiro, com grande freqüência. Por isso, esse princípio adquire grande importância na seara do Direito Penal no espaço, ante a necessidade de o Estado, cada vez mais, proteger seus interesses além fronteiras.[214]

Já o princípio da nacionalidade ou da personalidade, tem respaldo no art. 7º, inciso I, do Código Penal Brasileiro e indica a exigência que o Estado impõe acerca do comportamento de seus nacionais noutros países, impedindo a impunidade de seus nacionais em face de crimes cometidos noutros Estados, que não tenham abrangência em face do princípio da territorialidade, pois, não sendo cometido o crime em nosso território, nem existindo lei penal que o puna no Estado onde o delito foi cometido, poderia restar impune tal conduta lesiva a interesses de terceiros. No que diz respeito ao princípio da representação ou da bandeira, ensina a doutrina tratar-se de princípio subsidiário, para aplicar a lei penal do Estado em que tiver sido registrada a embarcação ou aeronave, encontrando amparo legal no art. 7, inciso II, do Código Penal Brasileiro.

De acordo com Bitencourt o princípio da universalidade ou cosmopolita "é característico da cooperação penal internacional, porque permite a punição, por todos os Estados de todos os crimes que forem objeto de tratados e convenções internacionais." Com base no art. 7º, incido II, alínea "a", do Código Penal Brasileiro, a lei penal é aplicada a todos os fatos sujeitos a punição sem considerar o lugar onde houve a infração penal, a nacionalidade do infrator ou do bem jurídico violado.

Esta é uma previsão constante no ordenamento jurídico de muitos Estados modernos, cuja preocupação é estabelecer como ensina Paiva, "mecanismos materiais e processuais impostos com a finalidade principal de reprimir de forma eficiente os crimes contra a humanidade praticados em contornos internacionais."[215]

Mais adiante alerta Paiva:

---

[214] BITENCOURT, op. cit. n. 209, p. 176.

[215] PAIVA, Bruno Teixeira de. **Ampliação da competência do Tribunal Penal Internacional para o julgamento de crimes ambientais transfronteiriços**. 2008. 112p. Dissertação. (Mestrado em Ciências Jurídicas) - Universidade Federal da Paraíba, João Pessoa, 2008. p. 63.

> Entretanto, a imposição de penas por cometimento de crimes internacionais pouco se tem efetivado através de jurisdições nacionais, em virtude de haver gravíssimas falhas na aplicação harmonizada do direito penal internacional. [...] Há casos ainda em que a possibilidade de pena por crimes internacionais através de jurisdições internas é praticamente nula. Isto acontece quando os mecanismos de persecução para o implemento da responsabilidade penal internacional do indivíduo estão além da capacidade de interferência do poder estatal envolvido, ou mesmo, para sua efetivação, põem-se em risco a própria plenitude do poder constituído.[216]

Dificuldades imanentes ao cibercrime e ao ciberespaço, então, poderiam ser enunciadas como pontos cruciais a desafiar o pós-moderno ordenamento jurídico, não apenas do Brasil mais de outras nações.

Estes obstáculos podem ser sintetizados nas seguintes questões:

1. Abuso no exercício de liberdades humanas fundamentais como a liberdade de expressão e privacidade, de forma a mascarar o cometimento de crimes e outras condutas ilícitas;

2. A "natureza oculta"[217] da internet e ainda sem conhecimento adequado de muitas pessoas faz com que estas sejam vítimas, desconhecendo muitas vezes esta situação ou ainda, pratiquem condutas que desconheçam que seja ilegal;

3. Ausência de registros confiáveis (banco de dados) de condutas danosas e crimes, ainda que muitas empresas, ONGs e governos se encarreguem desse esforço;

4. A "[...] natureza global do cibercrime pode resultar que vítimas e infratores estejam localizados em países diferentes, com diferentes leis [...]"[218], tornando difícil uma ação policial e a consequente prestação jurisdicional[219];

5. Necessidade de "harmonização das leis nacionais no tocante à tipificação das condutas relacionadas aos dados e sistemas informáticos [cibercrimes] e o implemento da cooperação internacional"[220];

6. Necessidade de instrumentos jurídicos de cooperação penal internacional de forma a facilitar a cooperação da investigação policial e do trabalho da justiça.

---

[216] PAIVA, op. cit. n. 212, p. 63.

[217] O´BRIEN, Martin; YAR, Majid. ***Criminology: the key concepts***. New York: Taylor & Francis, 2008. p.54. Texto original: "*hidden nature*", tradução nossa.

[218]Texto original: "[...] *the global character of cybercrime may result in offenders and victms being located in different countries, with differente law* […]". (Tradução nossa).

[219] No mesmo sentido Chawki (op. cit. n. 153) defende que "[...] esta situação não é satisfatória, uma vez que mergulha Internet em uma rede de múltiplas normas, gerando insegurança jurídica."
Texto original: "[...] *cette situation est insatisfaisante, car elle plonge les internautes (8) dans un réseau de normes multiples, source d'insécurité juridique (9)"*. (Tradução nossa).

[220]DELGADO, Vladimir Chaves. **Cooperação internacional em matéria penal na convenção sobre o cibercrime**. 2007. 315p. Dissertação. (Mestrado em Direito das Relações Internacionais) - Centro Universitário de Brasília. Brasília, 2007. p. 33.

3.5.3 A ação do Estado frente ao cibercrime: atuação dos órgãos policiais e da justiça brasileira

A construção de um roteiro teórico para que se estabeleça uma clara compreensão de como ocorre o enfrentamento do cibercrime no Brasil impõe, de plano, o registro das práticas criminosas em contraponto com o Sistema de Justiça Criminal. Cumpre salientar que na visão de Lemgruber, o Sistema de Justiça Criminal é integrado pelas "[...] Polícias, Ministério Público, Justiça e Sistema Penitenciário [...]"[221].

Numa dimensão pormenorizada, a decomposição de cada elemento do sistema (formando subsistemas) deve ser mentalizada da seguinte forma: Polícias – Civil, Militar e Federal, respectivamente, com atribuições previstas no art. 144, §§ 1º, 4º e 5º, Constituição Federal do Brasil); Ministério Público – Federal, Estadual e do Distrito Federal e dos Territórios (art. 128, inciso I, "a" e II); Justiça – Justiça Federal e Justiça Estadual ; Sistema Penitenciário – Federal e Estadual. Ressalte-se, entretanto, para efeito de desenvolvimento da pesquisa, serão consideradas as ações viabilizadas pela Polícia Federal, sem, no entanto, deixar de registrar em ponto específico, como são feitos os atendimentos ao cidadão, independente das ações e operações que competiram à Polícia Federal.

3.5.3.1 Atuação da Polícia Federal no combate ao cibercrime

A Polícia Federal tem sua competência estabelecida no art. 144, § 1º, da Constituição Federal, que assim define suas atribuições legais:

> § 1º A polícia federal, instituída por lei como órgão permanente, organizado e mantido pela União e estruturado em carreira, destina-se a:
>
> I - apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como **outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei;**

[221] LEMGRUBER, Julita. **Verdades e mentiras sobre o sistema de justiça criminal**. R. CEJ, Brasília, n. 15, p. 12-29, set./dez. 2001. Disponível em:<http://www2.cjf.jus.br/ojs2/index.php/cej/article/viewPDFInterstitial/427/608>. Acesso em: 10 mar.2009.

> II - prevenir e reprimir o tráfico ilícito de entorpecentes e drogas afins, o contrabando e o descaminho, sem prejuízo da ação fazendária e de outros órgãos públicos nas respectivas áreas de competência;
> III - exercer as funções de polícia marítima, aeroportuária e de fronteiras;
> IV - exercer, com exclusividade, as funções de polícia judiciária da União. (Grifo nosso).[222]

Dentre as ações destacadas, insere-se, mormente, as práticas delituosas que se disseminam quer internamente no país, com repercussões que vão além dos limites dos Estados-membros, quer nos delitos com caráter transnacional e vinculados a criminalidade organizada, sobretudo, como é o caso do cibercrime, cujas características pressupõem o emprego mais especializado e uniforme.

Antes da expansão comercial da internet, que só veio ocorrer no Brasil em 1996, a rede só era utilizada com caráter acadêmico, o que nos leva a concluir pela inexistência, em tese, de condutas ilícitas. Com a abertura e disponibilização comercial dos serviços as primeiras práticas delituosas ou condutas que configuravam ilicitude passaram a ocorrer.

De acordo com França o primeiro "[...] crime cibernético registrado no Brasil aconteceu em São Paulo, em 1996. As ocorrências surgiram na mesma proporção em que à rede crescia."[223] Registra também Sobral que estas primeiras condutas criminosas estavam relacionadas a "pedofilia"[224].

Neste sentido já teorizava Carvalho:

> Sendo perguntado, por exemplo, se a INTERNET é um meio novo de execuções de crimes "velhos" ou é, por si mesma, uma geradora de novos delitos, terei o atrevimento de dizer que as duas partes da pergunta se completam para a resposta: há crimes novos, contemporâneos da formação da rede mundial de computadores, mas estão acontecendo, pela "net", delitos já de muito tempo conhecidos da sociedade, só que agora perpetrados com o requinte do "bit".[225]

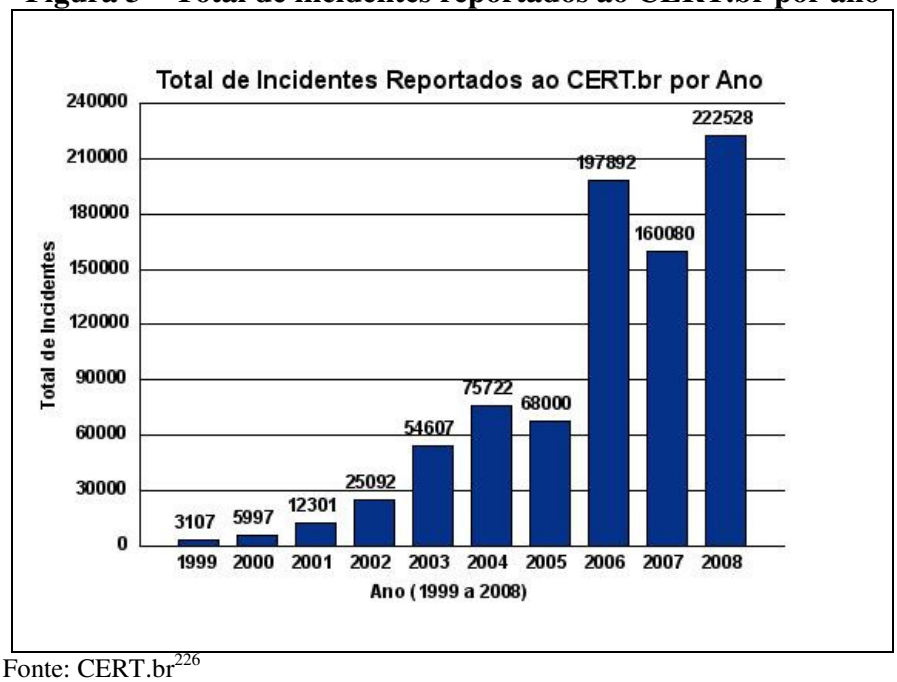
Há grande dificuldade em sistematizar informações confiáveis em face da grande complexidade estrutural, bem como em decorrência da falta de infraestrutura estatal. Mas, de acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança

---

[222] BRASIL. **Constituição da República Federativa do Brasil**. Disponível em: <http://www.planalto.gov.br/constiuição.htm> . Acesso em: 15 abr. 2009.
[223] FRANÇA, Ronaldo. **Deixem meu PC em paz**. Revista Veja, São Paulo, nov.2004. Edição 1980. Disponível em: <http://veja.abril.com.br/171104/p_160.html>. Acesso em: 13 mar.2009.
[224] SOBRAL, Carlos Eduardo Miguel. **Repressão a crimes cibernéticos. Brasília, Departamento de Polícia Federal**. Disponível em: <http://www.febraban.org.br/LerArquivo.asp?Tabela=Home_Arquivos&codigo=id_arquivo&campo1=arquivo&campo2=QtdeAcessos&id_codigo=560&campo3=arquivos/>. Acesso em: 13 mar.2009.
[225] CARVALHO, Ivan Lira de. **Crimes na Internet. Há como puni-los**. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2081>. Acesso em: 22 mar. 2009.

no Brasil - CERT os números de registros de incidentes no período de 1999, ano a ano, até 2008 são os seguintes:

Figura 3 – Total de incidentes reportados ao CERT.br por ano

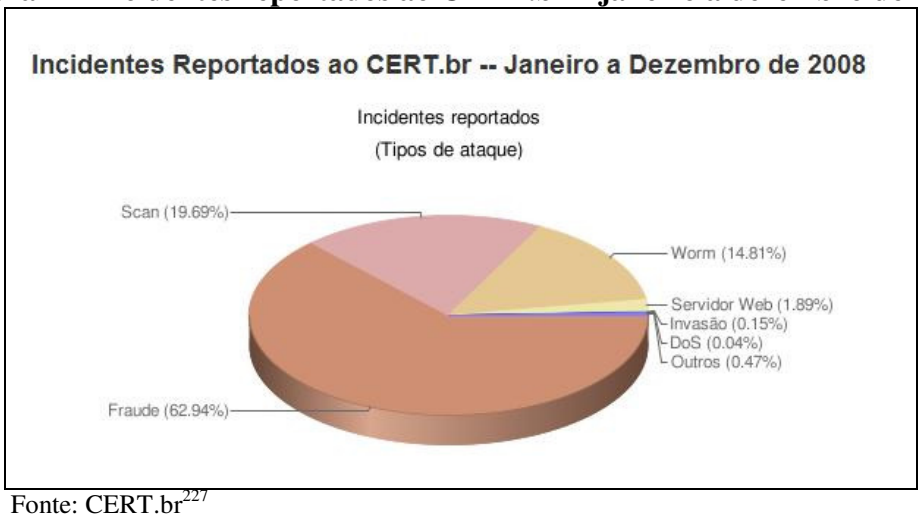


Fonte: CERT.br[226]

Noutro apanhado que demonstram os tipos de incidentes registrados, o levantamento feito pelo CERT mostra que mais de 60% das ações envolvem fraudes na internet, embora estejam registradas ações *scan, worms*, invasão e *DoS,* senão observe:

[226] CERT.br. **Núcleo de Informação e Coordenação do Ponto br, 2008**. Disponível em: http://www.cert.br/stats/incidentes/2008-jan-dec/tipos-ataque.html Acesso em: 22 mar.2009.

Figura 4 – Incidentes reportados ao CERT.br – janeiro a dezembro de 2008



Fonte: CERT.br[227]

Como se vê, os registros de situações demonstram números em escala ascendente (exceto em 2007) onde os cenários e os atores estão em atividade, neste novo ambiente desafiador. Dentre os sujeitos ativos de tais práticas, incluem-se *hackers, crackers, defacers,* pedófilos, fraudadores, estelionatários, entre outros indivíduos a desafiar a ordem jurídica.

Com estes cenários sombrios, seguiu-se a ação do Estado. Passaram a ser desencadeados, pois, os primeiros passos no sentido de dotar a Polícia Federal de um corpo técnico capaz de enfrentar o problema à altura.

A contratação de peritos com formação em ciências da computação, informática e tecnologia da informação, mediante concurso público foram as primeiras medidas desencadeadas após 2001, a fim de dotar a Polícia Judiciária da União de um setor de perícia de crimes cibernéticos e isto só veio a acontecer no âmbito do Departamento de Polícia Federal em 2003, com a criação do SEPFIN – Serviço de Perícias de Informática.

Ressalte-se, porém, que ações de Estado não poderiam restringir-se a capacitação da polícia científica, mas também, de fazer uso de instrumentos jurídicos utilizados para o enfrentamento da nova criminalidade. Neste embate passaram a ser utilizados o Código Penal Brasileiro com fundamentação, notadamente, das condutas típicas concernentes às práticas de furto, crimes contra a honra e dano, apenas para exemplificar.

Outros instrumentos jurídicos de âmbito do direito interno indicam a utilização da Lei n° 7.716/89 (que trata dos crimes de preconceito de raça ou de cor) com as alterações introduzidas pela Lei n° 9.459 (13/05/1997), em especial o seu artigo 20 (praticar, induzir ou

[227] CERT.br, op. cit. n. 222.

incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional / por intermédio dos meios de comunicação social ou publicação de qualquer natureza); Lei n° 9.609/98 (que trata da propriedade intelectual e pirataria de software número); Lei n° 9.610/98 (que estabelece o delito de pirataria de software doméstico ou corporativo) e ainda a Lei n° 8.137/90 (que tipifica os crimes contra a ordem tributária e econômica) e por fim as disposições constantes no Estatuto da Criança e do Adolescente, notadamente os artigos 240, 241-A a 241-E, que passaram a tipificar condutas relativas à pedofilia e pornografia na internet, conforme alterações introduzidas pela Lei n° 11.829/2008.[228]

De acordo com o portal institucional da Polícia Federal, em link onde constam a catalogação das operações realizadas a partir de 2003, especificamente sobre o cibercrime temos os seguintes números:

Tabela 3 – Operações da Polícia Federal – combate ao cibercrime, período 2003-2008

Ano	Operações
2003	1
2004	1
2005	5
2006	9
2007	6
2008	8
Total	30

Fonte: portal institucional da Polícia Federal, com adaptações do autor

Outra informação espantosa emerge quando é efetuado a comparação da quantidade de usuários de internet, registro de incidentes e a quantidade de operações, resultando nos seguintes números:

Tabela 4 – Comparativo: Operações da Polícia Federal, registro de incidentes e número de usuários no Brasil

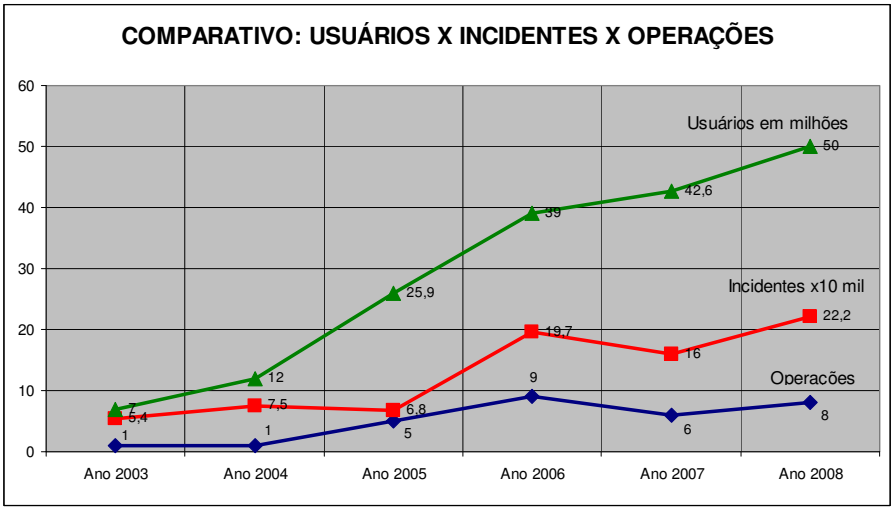
Anos	Operações	Incidentes x10 mil	Usuários – milhões
2003	1	5,4	7
2004	1	7,5	12
2005	5	6,8	25,9
2006	9	19,7	39
2007	6	16	42,6
2008	8	22,2	50

Fonte: portal institucional da Polícia Federal, *Internet World Stats e* CERT.br, com adaptações do autor

[228] A Lei nº 11.829, de 25 de novembro de 2008, alterou Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.

Graficamente obtém-se o seguinte resultado:

Gráfico 2 – Gráfico comparativo: número de usuários (milhões), registro de incidentes (x10 mil) e operações da Polícia Federal



Fonte: Site da Polícia Federal, *Internet World Stats e* CERT.br, com ajustes do autor

Uma avaliação preliminar das informações condensadas acima indica claramente uma forte tendência de aumento no número de usuários, consequentemente implicando num incremento considerável no registro de incidentes, como se apreende, também, da tendência a este item relativa.

Os índices estatísticos são expostos, assim, como um desafio à polícia brasileira, valendo ressaltar que além do combate ao cibercrime feito pela Polícia Federal, com possibilidade de ampliação da unidade especializada para todas as capitais brasileiras, sedes de superintendências regionais. Ressalte-se ainda que já existem unidades especializadas (delegacias) da Polícia Civil em 11 Estados: Distrito Federal, Espírito Santo, Goiás, Minas Gerais, Pará, Paraná, Pernambuco, Rio de Janeiro e São Paulo.

3.5.3.2 Atuação do Poder Judiciário e do Ministério Público brasileiro no combate ao cibercrime

O Poder Judiciário tem suas atribuições definidas pela Constituição da República Federativa do Brasil (primeira instância), nos artigo 109. Já o Ministério Público tem a delimitação de suas atividades no artigo 129, também da Carta Republicana. Tanto o

Poder Judiciário quanto o Ministério Público se desdobram em Poder Judiciário Federal e Ministério Público da União, inserindo-se aqui o Ministério Público Federal. No âmbito das unidades federadas tem-se o Poder Judiciário Estadual e o Ministério Público Estadual.

Considerando que as práticas delituosas perpetradas com emprego de alta tecnologia são enquadradas, para efeitos de punição, como delitos comuns, podem suscitar dúvidas quanto à competência se, da Justiça Federal ou da Justiça Estadual (comum), conforme o bem jurídico violado ou alguma circunstância especial.

Esta explanação inicial tem o objetivo de situar as competências e consequentes responsabilidades do Poder e Órgão encarregado de efetivar, em nome do Estado, a *persecutio criminis*, neste caso, em relação aos cibercrimes.

Mas estariam o Poder Judiciário e o Ministério Público aptos e inseridos nesse contexto de pós-modernidade de forma a proceder a prestação jurisdicional aos cidadãos e empresas vítimas de cibercrimes?

É de se afirmar positivamente. Da mesma forma que os recursos tecnológicos se infiltraram nas mais diversas atividades humanas, não foi diferente na prestação da atividade jurisdicional do Estado, através do Parquet e dos órgãos do Poder Judiciário. Na verdade, o uso da tecnologia possibilitou a difusão de informações constantes em processo com mais agilidade, facilidade e consequentemente possibilitando capacitação de forma a prestar serviços adequados à sociedade.

Neste sentido Efing e Freitas, dizem que:

> O acesso à internet, em conjugação com a informatização do Judiciário, proporcionou uma revolução em todo o sistema de elaboração e comunicação de atos processuais, tanto pelo usuário interno dos serviços Judiciários (juízes e servidores), quanto pelos seus usuários externos (pares, advogados), que passaram a ter acesso a várias informações de difícil obtenção anteriormente. A utilização da internet passou a ser indispensável por aqueles usuários que se conscientizaram de sua importância.[229]

Como pode ser observado na abordagem anterior, nos últimos cinco anos houve um incremento significativo na repressão aos cibercrimes, notadamente pela viabilização de operações da Polícia Federal. Deve-se, entretanto, lembrar, que tais operações tiveram uma participação efetiva tanto do Poder Judiciário como do Ministério Público, notadamente o Ministério Público Federal, ainda que tais participações tenham um cunho mais reservado.

---

[229] EFING, Antônio Carlos; FREITAS, Cinthia Obladen de Almendra. **Direito e Questões Tecnológicas - Aplicados no Desenvolvimento Social**. Curitiba: Juruá, 2008, p. 44.

Um questionamento pode pairar sobre a mente a partir desta explanação. Qual seja: a relação entre as operações e a efetiva participação do Poder Judiciário e do *Parquet*. O norte inicial para esclarecer esta questão está relacionada sobre a forma como o cibercrime vem sendo registrado no Brasil.

Tais práticas, pois, não se efetivam, quase sempre, num único estado federado. Decorre assim a transferência de jurisdição, por consequência, para o plano de competência da Polícia Federal, com base no art. 144, §1º, inciso I[230], da Constituição da República Federativa do Brasil. Merece reforçar que, não raro, tais práticas delituosas abrangem a jurisdição de outros países, embora estas questões não afastem a competência das polícias estaduais nos casos registrados no âmbito dos estados-membros.

Com base em sua Lei Orgânica (Lei Orgânica do Ministério Público da União – Lei Complementar nº 75/93), notadamente em seu art. 6º, e mais com suporte do pressuposto constitucional de zelar pela garantia da lei, da ordem e "[...] do regime democrático e dos interesses sociais e individuais indisponíveis[...][231]" o *Parquet* Federal mantém verdadeira cruzada contra o cibercrime no Brasil, notadamente nos casos de Pedofilia e Pornografia viabilizadas na internet e independente disso, requer assim, a "[...] implementação, pelo Ministério Público Federal, de uma política de atuação e capacitação voltada para a efetiva repressão dos crimes cibernéticos."[232]

Neste sentido, merece ser colacionada uma das conclusões do Relatório do Grupo de Trabalho sobre crimes cibernéticos do Ministério Público Federal:

> A partir da experiência do Grupo de Combate aos Crimes Cibernéticos da PR/SP, foi constatado que, com o aumento do número de casos investigados, alguns juízes federais demonstraram a pouca disposição em conduzir os processos de quebra de sigilo. Há decisões isoladas que delegam ao MPF a tarefa de obter diretamente das empresas os dados sobre os endereços de IPs e seus usuários, ou que, após a determinação judicial da quebra, encaminham os autos para que o MPF elabore e expeça os ofícios diretamente.
>
> De igual modo, a experiência da equipe de delegados e agentes da Polícia Federal existente em Brasília, e que trabalha com o resultados das quebras de sigilo feitas pela CPI da Pedofilia, evidenciou que os mandados de busca e apreensão e outras diligências não eram cumpridos adequadamente pelas delegacias dos diversos

---

[230] O art. 144, §1º, inciso I, assim enuncia ao tratar da competência da Polícia Federal: "apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei;" (grifo nosso).

[231] Art. 127, caput, da Constituição da República Federativa do Brasil, que trata do Ministério Público como função essencial à justiça.

[232] **Relatório do Grupo de Trabalho sobre crimes cibernéticos – Ministério Público Federal**, 2008. Disponível em: < http://2ccr.pgr.mpf.gov.br/docs_institucional/eventos/viii-encontro/ata_grupo_sobre_crimes_ciberneticos.pdf>. Acesso em: 1 mar.2009.

> estados, por desconhecimento das particularidades da investigação dos delitos cibernéticos.[233]

Tais conclusões evidenciam, apesar dos resultados obtidos de forma satisfatória, que há resistências e obstáculos no trabalho desempenhado pelo Ministério Público Federal no cumprimento de suas atribuições legais e constitucionais.

Quanto às demandas que aportam ao Poder Judiciário de primeira instância, estes têm incidência tanto na esfera da Justiça Federal quanto da Justiça Comum dos Estados-membros, havendo pequenas diferenças que se fixam com base na competência, notadamente seguindo a regra estabelecida no art. 109, da Constituição Federal, que trata da competência dos juízes federais, estabelecendo-se a competência dos juízes estaduais de forma residual, ou seja, nos casos concretos, não sendo competência da Justiça Federal, caberá aos juízes estaduais decidirem as lides.

Ressalte-se, entretanto, que na nova sistemática de persecução criminal voltada para o embate contra o cibercrime, não há um estamento do Estado que se sobressaia, pois, ainda que as operações da Polícia Federal tenham sido exitosas, coube ao Ministério Público e, notadamente, ao Poder Judiciário determinar passos fundamentais no curso da investigação, principalmente a quebra de sigilo telemático que permite fazer o rastreamento dos endereços "IP" (*internet protocol* ou endereço de protocolo internet, ou seja, um número que permite identificar um computador fisicamente no ciberespaço) e o monitoramento físico dos envolvidos com autorização da justiça, isto com suporte na Lei n° 9.296/96.[234]

Em face da grande demanda de ações tramitando na justiça, há relevante registro a ser feito com base em matéria do portal IDG Now, ao afirmar que "o número de decisões judiciais envolvendo crimes eletrônicos saltou de 400, em 2002, para mais de 17 mil atualmente"[235], isto em novembro de 2008 e arremata com a seguinte informação:

> Na falta de uma legislação específica para combater os crimes digitais, os tribunais brasileiros vem "combatendo a criminalidade cibernética com a aplicação do Código Penal, do Código Civil e de legislações específicas como a Lei n. 9.296 – que trata das interceptações de comunicação em sistemas de telefonia, informática e telemática

---

[233] BRASIL. Ministério Público Federal. Grupo de trabalho – crime cibernético, resultados e conclusões. Disponível em: < http://2ccr.pgr.mpf.gov.br/docs_institucional/eventos/viii-encontro/ata_grupo_sobre_crimes_ciberneticos.pdf>. Acesso em: 16 abr.2009.

[234] O art. 1º, da n° 9.296/96 – "A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça."

[235] IDG NOW! Internet e legislação. **Crimes eletrônicos geral 17 mil decisões no Brasil, em 6 anos**. Disponível em: <http://idgnow.uol.com.br/internet/2008/11/25/crimes-eletronicos-geram-17-mil-decisoes-judiciais-no-brasil-em-6-anos/>. Acesso em: 2 mar.2009.

> – e a Lei n. 9.609 – que dispõe sobre a proteção da propriedade intelectual de programas de computador", informa uma reportagem do STJ.
> De acordo com o levantamento, grande parte dos magistrados, advogados e consultores jurídicos considera que 95% dos delitos cometidos eletronicamente já estão tipificados no Código Penal brasileiro por caracterizar crimes comuns praticados por meio da internet. Os outros 5% para os quais faltaria enquadramento jurídico abrangem transgressões que só existem no mundo virtual, como a distribuição de pragas virtuais.[236]

Neste sentido, caberia formular o seguinte questionamento: quais os resultados ou que decisões judiciais foram tomadas em face das mais de trinta operações da Polícia Federal e das centenas de pessoas presas?

Não sendo objeto do presente estudo, ainda assim foi possível rastrear e se chegar a algumas condenações em face das referidas operações, como se observa na amostragem:

Tabela 5 – Operações da Polícia Federal e julgamento em 1ª instância

Ano	Operação
2006	Control+Alt+Del "A Polícia Federal desencadeou na manhã do dia 7 de dezembro a Operação Control+Alt+Del para prender uma quadrilha envolvida com o roubo de senhas bancárias através da Internet. Foram cumpridos mandados de prisão e de busca e apreensão nos estados do Pará, Maranhão, Piauí, Goiás e São Paulo. Ao todo 215 policiais federais participaram da ação."
2006	Scan "A Operação Scan aconteceu no dia 14 de fevereiro e prendeu 55 integrantes de uma quadrilha especializada em desviar dinheiro de contas bancárias através de transferências e pagamentos realizados pela Internet. Ao todo 330 policiais realizam mandados de prisão e de busca e apreensão nos estados da Paraíba, Rio Grande do Norte, Ceará, Pernambuco, Bahia, São Paulo e Paraná. As investigações iniciaram em maio de 2005, e estima-se que o grupo tenha desviado mais de 10 milhões de reais."

Fonte: Portal institucional da Polícia Federal com adaptação do autor

No caso da operação "Control+Alt+Del", em relação aos principais acusados, o processo tramitou na Justiça Federal do Estado do Pará e as sei primeiras condenações, em primeira instância, aconteceram em fevereiro de 2008, com aplicação de "penas que variam

[236] IDG NOW!, op. cit. n. 230.

entre 06 e 12 anos de prisão, pelos crimes de formação de quadrilha, furto qualificado e quebra de sigilo."[237]Há ainda sete ações tramitando contra cerca de 50 envolvidos na mesma Seção Judiciária Federal.

Quanto ao segundo caso as condenações, em primeira instância, aconteceram em abril de 2009, Justiça Federal do Estado da Paraíba, Seção Judiciária da cidade de Campina Grande, cujas penas variaram de 3 a 9 anos de reclusão, alguns com regime de cumprimento de pena no "semiaberto".

As condenações tiveram por base denúncia do Ministério Público Federal fundamentada nos crimes de furto qualificado, formação de quadrilha, interceptação telemática ilegal e violação de sigilo bancário, merecendo realçar o seguinte, quanto às práticas delituosas perpetradas pelos envolvidos:

> A quadrilha era formada por programadores, usuários, aliciadores e laranjas, que transferiam dinheiro e realizavam saques de contas da Caixa Econômica e Banco do Brasil. De acordo com os autos do processo, com base nos interrogatórios dos réus e testemunhas, "somente em uma agência do Banco do Brasil em Campina Grande (Agência Borborema), ocorreram 287 transferências ilícitas, recebidas em contas de clientes daquela agência, no período entre novembro de 2004 e fevereiro de 2006, no qual a quadrilha estava atuando livremente. O volume total de transferências ilícitas somente para as contas dessa agência chegou ao elevado valor de R$ 355.555,92 (trezentos e cinquenta e cinco mil, quinhentos e cinquenta e cinco reais e noventa e dois centavos).[238]

Conclusão preliminar em tais julgamentos permite inferir que nos casos em que os delitos são perpetrados em território nacional, não tem ocorrido obstáculos à ação do Estado, uma vez que as ações da Polícia Federal tem demonstrado isso, com reforço do Ministério Público Federal e o consequente julgamento à cargo do Poder Judiciário.

Ressalte-se, porém, que a ausência de um instrumento jurídico internacional, para fins de cooperação penal e estabelecimento de regras e procedimentos tem dificultado muito a ação dos órgãos estatais, como foi possível verificar nos casos de solicitação de quebra de sigilo da CPI da Pedofilia em desfavor da Google Inc. mantenedora do site de relacionamentos Orkut.

A empresa Google que mantém uma subsidiária no Brasil, resistiu em fornecer as informações confidenciais constantes em 3.261 álbuns privados do Orkut que podem reunir

---

[237] Consultor Jurídico. **Quadrilha virtual: seis acusados de fraudes bancárias na internet são condenados**. São Paulo, 2008. Disponível em: <http://www.conjur.com.br/2008-fev-12/seis_acusados_fraudes_bancarias_sao_condenados>. Acesso em: 2 mar.2009.

[238] Justiça Federal - Seção Judiciária da Paraíba. **Juiz federal condena hackers envolvidos na Operação Scan**. João Pessoa, 2009. Disponível em: <http://www.jfpb.jus.br/site/det_noticias.asp?chave=179>. Acesso em: 3 abr.2009.

conteúdos e imagens de pornografia infantil, mas com a instalação da Comissão que tem poderes judiciais a Google decidiu colaborar. Noutras tentativas anteriores Procuradores da República tiveram o acesso negado ao conteúdo constantes nos álbuns, sob o argumento de que pelo fato da Google ser uma empresa americana, com base de dados nos Estados Unidos, estaria sujeita à jurisdição das leis norte-americanas, que asseguram a liberdade de expressão e não às leis brasileiras, ainda que os supostos crimes de *cyber* pornografia infantil tivessem registro no Brasil.

Desta forma, há embate jurídico em duas frentes: uma em relação às práticas de cibercrimes especificamente dentro do território de um Estado, portanto, sujeito às leis e soberania do país e noutro ponto as condutas criminosas que são praticadas em mais de um país, daí a denominação de transnacionais. São justamente os crimes de internet de caráter transnacional os quais inspiram as maiores preocupações no mundo, ainda que existam bons indicadores de possíveis soluções, de se observar, porém, que numa condição ou em outra o Brasil com suas dimensões continentais está fortemente inserido neste contexto, sendo assim um desafio, sobretudo, pela dificuldade de atuação da polícia, de Promotores Públicos e de Juízes.

5 COOPERAÇÃO PENAL INTERNACIONAL E A CONVENÇÃO DE BUDAPESTE SOBRE CIBERCRIME

5.1 Cooperação penal internacional na pós-modernidade

5.1.1 A construção dos ideais de cooperação e de uma justiça penal internacional

O estabelecimento de um liame lógico para compreender o desenvolvimento do processo de cooperação entre os povos não é novo. Não será necessário se reportar aos tempos imemoriais em que o homem manifestou suas emoções e comunicou-se mediante pinturas rupestres que a História da humanidade tem registrado.

Atente-se, porém, que a abordagem desse processo situado na pós-modernidade, do mundo globalizado e das avançadas tecnologias é fenômeno recentíssimo, que mantém conexão óbvia com o processo de globalização, daí porque, este referencial histórico está relacionado ao colapso do sistema comunista da extinta URSS.

Antes que se estabelecesse a construção de um processo de penalização de graves crimes contra a humanidade, os antecedentes históricos irão identificar claramente dificuldades de efetivação de punição por tais condutas pelos Estados nacionais ou mesmo de reprimi-las. Decorreu assim, a necessidade de busca por um ideal de justiça supranacional, que pudesse promover um processo e um julgamento justo, com a isenção e credibilidade que não foi possível experimentar nos Tribunais Penais da Primeira e da Segunda Guerra Mundial.

No entendimento de Souza:

> As primeiras respostas estatais aos crimes praticados fora de seus territórios surgiram com os códigos francês e alemão do século XIX, como observado pod Donnediee de Vabres. Nessa época, a necessidade não passava de um abrandamento do princípio da territorialidade da lei penal.[239]

[239] SOUZA, Solange Mendes de. **Cooperação jurídica penal no MERCOSUL: novas possibilidades**. Rio de Janeiro: Renovar, 2001. p.111.

As tentativas de criar uma jurisdição penal internacional terão como marco[240] efetivo o período de depressão do pós 1ª Guerra Mundial, com o estabelecimento do Tratado de Versalhes - previsão de Tribunais Ad hoc (art 227, composto por 5 membros indicados pelos EUA Grã-Bretanha, França, Itália e Japão) para o julgamento do ex-Kaiser da Alemanha. Seguiu-se a formação de um Comitê Consultivo de Juristas em 1920, que apresentou proposta à Liga das Nações, sendo que não foi aceita, ainda que vários organismos internacionais como a União Interparlamentar e *International Law Association* tenha trabalhado em outros projetos.

Estas primeiras iniciativas demonstraram a necessidade de um organismo internacional de jurisdição penal sendo dificultada pelo sentimento de valorização muito forte da chamada soberania nacional, que inviabilizava as pretensões de um órgão supranacional para julgamento sobre crimes de guerra.

Compreendendo que a eclosão da 2ª Guerra Mundial decorreu das questões não satisfatoriamente equacionadas no pós 1ª Guerra Mundial, Paiva pontua o seguinte:

> Entretanto, o verdadeiro marco de reconhecimento de uma jurisdição penal internacional retroage aos eventos chocantes experimentados pela humanidade no curso da Segunda Guerra Mundial, impostos pelos regimes políticos nacional-socialista alemão e fascista italiano. De fato, na resta dúvida de que, concretamente, as definições acerca de uma Jurisdição Penal Internacional forma construídas a partir do contexto geopolítico emanado do final do conflito internacional de 1945.[241]

Na esteira desse contexto, o fim do segundo grande conflito mundial desencadeou os processos penais para julgamento dos crimes de guerra - Tribunais para Nuremberg e Tóquio, que representou mais uma resposta (dos vencedores) aos hororrores do nazismo na Europa e das invasões japonesas na Ásia, com a prática de genocídio. Foi uma demonstração clara de estabalecer órgãos com jurisdições não-nacionais para processar e punir crimes de dimensão e alcance internacional, ainda que tenha o registro de parcialidade, com a imposição da vontade dos vencedores sobre os vencidos.

Entre o fim dos horrores da 2ª Guerra Mundial e a efetiva retomada das iniciativas referente a uma jurisdição penal internacional transcorreram aproximadamente meio século. Isto representa o período de nebulosidade nas relações de cooperação entre as

---

[240] DELGADO pontua que: "A cooperação penal internacional não é um fenômeno recente. A sua manifestação mais remota nos remete ao longíquo tratado de paz, celebrado em 1280 a. C. entre Ramsés II, Faraó do Egito e Hatussilli III, Rei dos Hititas, sendo considerado o mais antigo tratado de extradição da humanidade. É evidente que não possuía as características que atualmente apresenta, tanto é assim que previa-se a extradição de criminoso político e não de criminoso comum."
DELGADO, op.cit. 217, p. 35-36.

[241] PAIVA, op. cit. n. 212, p. 65-66.

nações como fruto da guerra-fria que dividiu o mundo muito mais que tão somente entre bloco socialista e bloco capitalista.

Numa detalhada análise sobre o surgimento da justiça penal internacional Bazelaire e Cretin se pronunciam:

> Na realidade, os ultrajes repetidos cometidos contra o homem ao longo de todo século XX não puderam deixar indiferentes os juristas, que se mobilizaram e ainda se mobilizam a fim de impedir a proliferação dos comportamentos gravemente prejudiciais à dignidade da pessoa humana.[242]

O estabelecimento de uma nova "ordem mundial", no pós guerra-fria provocou uma onda de otimismo e consequentemente um rearranjo nas forças geopolíticas do mundo. Estes fatos tiveram como consequências: (1) a redução da desconfiança e suspeição que haviam impedido relações amigáveis e cooperação entre o bloco ocidental e o bloco oriental; (2) Os Estados que sucederam a URSS (Rússia e membros da CEI) passaram a aceitar e respeitar alguns princípios básicos do direito internacional; (3) Grau de acordo inédito nas visões dos cinco membros permanentes do Conselho de Segurança da ONU, uma convergência nas visões, tornando o cumprimento de suas funções mais efetivo.

Essa nova dimesão de mundo com a geopolítica multipolar não teve um início tranquilo. A divisão de Estados com múltiplas etnias, gerou desordens, colapsos e fragmentação, resultando conflitos armados com muitas mortes e derramamento de sangue. Cita-se como exemplo a ex-Iugoslávia que após ser dividida em 1991, deu origem República da Croácia, República da Bósnia e Herzegovina, República da Sérvia (a província autônoma do Kosovo encontra-se atualmente sob tutela internacional), República de Montenegro, República da Eslovénia e República da Macedónia.

A decorrência lógica de tais atrocidades foi a instalação pelo Conselho de Segurança da ONU do Tribunal Militar Internarcional para a ex-Iugoslávia (Crimes de Guerra e Crimes contra a Humanidade) e para Ruanda, com competência para processar e julgar genocídios praticados nestes dois Estados. O risco de se criar um tribunal Ad hoc para cada conflito num determinado país, como Camboja, Serra Leoa e Timor Leste, levou a ONU a agilizar os trabalhos de criação de um Tribunal Penal Permanente.

Os trabalhos que antecederam a criação de uma corte internacional penal permanente tiveram a Conferência de Roma (1998), marcada por intensos debates e incertezas. Negociações preparatórias indicavam um grande número de posições conflitantes

---

[242] BAZELAIRE, Jean Paul; CRETIN, Thierry; tradução de Luciana Pinto Venâncio. **A justiça penal internacional, seu futuro: de Nuremberg a Haia**. Barueri: Manole, 2004. p. 13.

entre os diversos Estados, bem como devido a complexidade das questões referentes à soberania. A construção de um acordo enfrentava dificuldades técnicas e jurídico-políticas. Os obstáculos técnicos estavam relacionados ao desenvolvimento de um sistema eficaz de justiça penal internacional, que fosse compatível com os diversos sistemas jurídicos do mundo (dificuldades relativas à complexidade de investigação, instrução e cooperação entre os Estados).

As dificuldades de ordem jurídico-políticas estavam relacionadas à definição de crimes e ao exercício da jurisdição, ainda que houvesse um consenso geral quanto à inclusão dos crimes de genocídio, crimes de guerra e crimes contra à humanidade. Empecilhos quanto à delimitação de jurisdição do Tribunal - que Estados deveriam aceitar a jurisdição da Corte? Seria uma jurisdição universal (não era preciso o Estado aceitar a jurisdição, pois seria automática) ou não? Houve muitas divergências em relação a esta questão, notadamente pelos EUA que foram infelixíveis.

Dissertando sobre tais divergências, Boiteux pontua:

> Os esforços da comunidade internacional por meio das Nações Unidas, para aprovar o Estatut foram enormes, assim como os obstáculos que tiveram de ser superados pelos representantes dos países que uniram suas forças e firmaram compromisso para conseguir chegar ao texto final, em especial diante da resistência à criação do TPI por parte de quatro fortes países: EUA, Índia, China e Israel.[243]

Registre-se ainda que as ONGs exerceram forte pressão e loby para que fossem aprovadas as disposições referentes a um Tribunal mais forte, com jurisdição automática, promotor indepedente, jurisdição sobre conflitos internos armados e com preocupação em relação às questões de gênero.

Para Paiva:

> A existência de uma corte penal internacional de caráter permanente traz aporte para a consolidação de um rígido sistema jurídico internacional, necessário para evitar a impunidade dos responsáveis por sérias violações aos direitos humanos e impedir a reiteração de atos no futuro.[244]

Em 17 de julho de 1998, em Roma, na Itália foi celebrado o Estatuto de Roma, estabelecendo o Tribunal Penal Internacional, com jurisdição automática, Promotor independente, jurisdição sobre conflitos armados internos, não subordinação ao Conselho de

---

[243] BOITEUX, Luciana. **Os princípios penais no Estatuto do Tribunal Penal Internacional à luz do direito brasileiro.** *In*:JAPIASSU, Carlos Eduardo Adriano (Coord.). **Direito penal internacional estrangeiro e comparado**. Rio de Janeiro: Lúmen Júris, 2007. p.91.
[244] PAIVA, op. cit. n. 212, p.80.

Segurança da ONU, autoridade para emitir decisões sobre jurisdição e admissibilidade e competência para julgamento de delitos mais graves contra a humanidade. A Corte foi instalada em 2002, em Haia, Capital dos Países Baixos, iniciando oficialmente suas atividades em 11 de março de 2003.[245]

5.1.2 O exemplo do direito comunitário europeu

A formação dos ideais de um direito comunitário agrega-se aos momentos históricos da segunda metade do século XX, notadamente pelas grandes dificuldades que passou a vivenciar a Europa no pós 2ª Guerra Mundial. Como o próprio termo designa, a terminologia e expressão "comunitária" pressupõe a existência de um direito comum a vários Estados, sem que o todo pertença a qualquer deles.

O saldo trágico do pós-guerra teve a marca da ascensão e posteriormente queda de ideologias totalitárias, que foram capazes de proporcionar atrocidades contra a humanidade sem precedentes históricos. Mas o esforço e a união voluntária dos povos europeus passou a ser o grande esforço coletivo, a inspirar um ideal que consistiu, sobretudo, em suplantar os conflitos do passado e em alicerçar o futuro de forma conjunta.

Para Borges,

> O direito comunitário não é originariamente constituído por um sistema de normas jurídico-positivas oriundas de uma única fonte de produção normativa, como se elas decorressem, desde sempre e exclusivamente, dos órgãos da própria comunidade. Ele é, na sua origem e formação, ponto de intersessão entre (a) normas de direito nacional (intra-estatal), (b) normas fundadas no direito internacional, como os Tratados de Maastricht, Amsterdam, Nice (União Europeia) [...] (MERSCOSUL), e (c) normas de direito internacional privado comum, não-estatais, mas convencionais. [...] em nome da integração, a soberania estatal se retrai no âmbito comunitário. Sem que dela entretanto os Estados-membros da comunidade abram mão.[246]

Deste modo, concretiza-se na pós-modernidade como forte resposta em face dos riscos e oportunidades proporcionados pela globalização econômica e pela revolução da informação, numa clara mensagem de que a força dos povos está na diferença que cada um

---

[245] Wikipédia, a enciclopédia livre. **Estatuto de Roma.** Disponível em: <http://pt.wikipedia.org/wiki/Estatuto_de_Roma>. Acesso em 9 abr.2009.
[246] BORGES, José Souto Maior. **Curso de direito comunitário**. São Paulo: Saraiva, 2005, p.32.

pode assegurar, muito mais que a imposição de uma vontade única e prevalecente, num passo a passo didático para as demais nações do mundo.

Neste sentido, em menos de meio século a Europa partiu de seu caráter multiétnico para a formação de uma União a congregar todos os povos signatários de seus instrumentos jurídicos, que passaram pela cooperação, pela integração regional até chegar ao seu estágio atual.

Desta forma Franca Filho estabelece lúcida distinção entre coperação internacional e integração regional:

> Na verdade, a cooperação é uma das primeiras formas de aproximação entre Estados e, ao contrário da integração, apresenta laços institucionais bastante incipientes. [...] cujas decisões se dão no plano da coordenação intergovernamental (igualdade entre os Estados), e, quando muito alcançam objetivos de segurança, de ajuda mútua financeira ou de eliminação de protecionismo. Na esfera da integração, por outro lado, os Estados se agrupam não para garimpar vantagens uns dos outros, mas para unir forças e competir melhor, frente a terceiros países. [...] Assim, fazem surgir as entidades supranacionais ou supra-estatais, órgãos autônomos cuja principal característica é a independência em relação aos Estados partes do espaço integrado para a adoção de medidas políticas específicas.[247]

No caso da formação da União Europeia podem ser observadas as seguintes fases[248]: em 9 de Maio de 1950: renasce a Europa e já em 1951 é estabelecido o Tratado de Paris que criou a Comunidade Europeia do Carvão e do Aço (CECA). Em 25 de Março de 1957: criada a Comunidade Econômica Europeia, com o advento do Tratado de e Tratado Constitutivo da Comunidade Europeia da Energia Atómica (Euratom). Em 20 de Julho 1965 através do Tratado de Fusão estabeleceu-se um Conselho único e uma Comissão única na União Europeia.

A primeira ampliação da Comunidade Europeia passa a congregar em 1 de Janeiro de 1973, a Dinamarca, Irlanda e o Reino Unido. Aos 10 dias de Junho de 1979 ocorrem as primeiras eleições diretas do Parlamento Europeu por sufrágio universal. e 1 de Novembro de 1993: a União Europeia, com a assinatura do Tratado de Maastricht (que também estabeleceu a unidade econômica e monetária), tendo por elementos essenciais três bases.

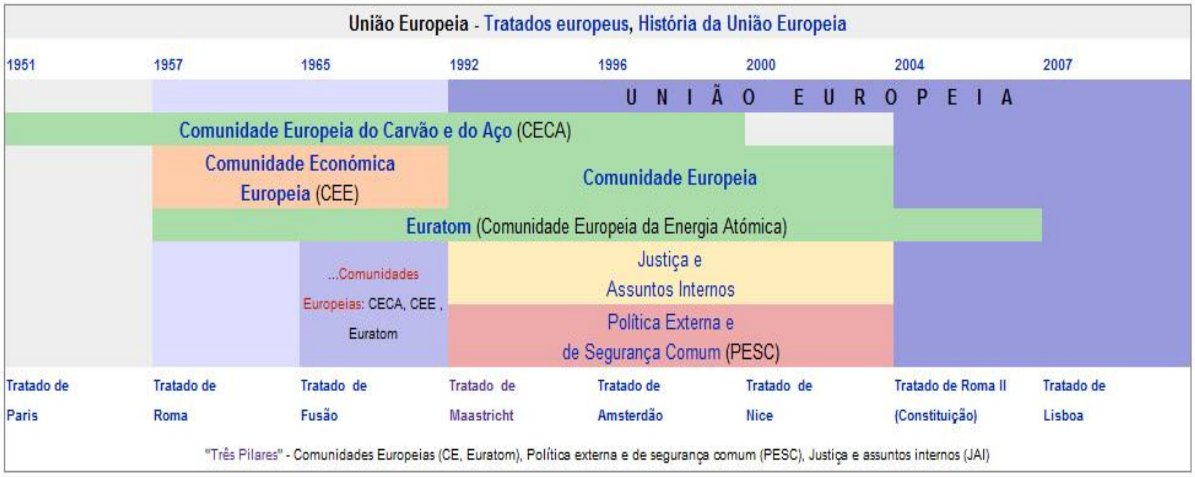
A figura a seguir ilustra como ocorreu essa evolução:

---

[247] FRANCA FILHO, op. cit. n. 13, p. 39-40.

[248] União Européia. **Wikipédia, a enciclopédia livre.** Disponível em: http://pt.wikipedia.org/wiki/Uni%C3%A3o_Europ%C3%A9ia Acesso em: 8 abr.2009.

Figura 5 – Evolução da União Europeia



Fonte: Wikipedia[249]

Num enfoque mais específico, é possível vislumbrar o estabelecimento dos pilares da União Europeia, no Tratado de Maastricht, sobre três bases[250]:

> 1.º pilar: as Comunidades europeias, herdeiras da Comunidade Europeia do Carvão e do Aço, da CEE e do tratado Euratom. Retomam o Tratado de Roma revisto pelo Acto único. Compõe-se de um pilar supranacional relativo às políticas integradas (Política agrícola comum, união alfandegária, Mercado interno, euro, etc.). Para as matérias relevantes deste pilar, os Estados membros transferiram uma parte relativamente importante das suas competências e soberania para a União Europeia.
> 2.º pilar: a Política Externa e de Segurança Comum (PESC). Cooperação intergovernamental, em matéria de assuntos externos e de segurança.
> 3.º pilar: a **Cooperação policial e judiciária em matéria penal**.[251] (grifo nosso).

Com enfoque dirigido à questão do enfrentamento da criminalidade organizada, que, por motivos óbvios constitui óbice ao desenvolvimento, uma vez que impacta as economias nacionais, reduzindo, por consequência, investimentos do Estado em áreas estratégicas. Interessa, pois, o aprofundamento do "Terceiro Pilar", base da União Europeia, que se volta, especificamente à cooperação policial e judiciária em matéria penal.

O ideal de estabelecer espaços de liberdade, segurança e justiça, fez-se necessária a instituição, no âmbito da União Europeia, da cooperação policial e judiciária em matéria penal, com o objetivo precípuo de garantir um nível de proteção satisfatório aos seus cidadãos. A fixação destas regras indicam ainda, a necessidade de uma cooperação rápida e

---

[249] Disponível em: <http://pt.wikipedia.org/wiki/Pilares_da_Uni%C3%A3o_Europeia>. Acesso em 4 abr. 2009.
[250] Em 13 de Dezembro de 2007, em Lisboa, Portugal, os dirigentes da União Europeia assinaram o Tratado de Lisboa, que finalizou vários anos de negociações sobre questões institucionais. O Tratado modificou, sem os substituir, os tratados da União Europeia e da Comunidade Europeia, conferindo, entretanto, à União Europeia personalidade jurídica própria para assinar acordos internacionais de nível comunitário.
[251] Pilares da União Européia. **Wikipédia, a enciclopédia livre.** Disponível em: <http://pt.wikipedia.org/wiki/Pilares_da_Uni%C3%A3o_Europeia>. Acesso em: 8 abr.2009.

eficiente tanto da polícia, quanto das instituições judiciárias, tendo por fundamento o disposto no art. 29, do Tratado da União Europeia. Este dispositivo, constante do Terceiro Pilar da UE (Título VI) destina-se a "a prevenir, mas também a lutar contra o racismo e a xenofobia, por um lado, e a criminalidade organizada, nomeadamente o terrorismo, o tráfico dos seres humanos, os crimes contra crianças, bem como os tráficos de droga e de armas, a corrupção ou a fraude, por outro."[252]

Neste sentido, fixam-se laços de cooperação comum entre: os serviços nacionais de polícia, serviço nacionais aduaneiros e Autoridades judiciárias nacionais e se efetivam em termos práticos e operacionais com as atividades desempenhadas pela Eurojust[253], Europol[254] e Rede Judiciária Europeia em Matéria Penal[255]. Estas atividades

---

[252] Europa Glossário. **Cooperação policial e judiciária em matéria penal**. Disponível em: <http://europa.eu/scadplus/glossary/police_judicial_cooperation_pt.htm>. Acesso em: 9 abr.2009.

[253] A Eurojust foi "Instituída por uma decisão do Conselho de 2002, a Eurojust é o órgão responsável por reforçar a luta contra as formas graves de criminalidade, através de uma cooperação judiciária mais estreita na União Europeia. Esta entidade de concertação dos ministérios públicos nacionais da União é composta por 27 representantes nacionais: juízes, procuradores e agentes da polícia destacados por cada Estado-Membro. Pode cumprir as respectivas tarefas através de um ou vários membros nacionais ou enquanto colégio. Além disso, cada Estado-Membro pode designar um ou vários correspondentes nacionais, que podem também constituir um ponto de contacto da rede judiciária europeia. A Eurojust é competente no que diz respeito às investigações e aos procedimentos penais no domínio das formas graves de criminalidade, nomeadamente organizada ou transfronteiriça. Os objectivos prosseguidos são o incentivo da coordenação entre as autoridades competentes dos diferentes Estados-Membros, bem como o apoio na prestação de auxílio judiciário mútuo em matéria penal no plano internacional e a execução dos pedidos de extradição ou do mandado de captura europeu.A Eurojust contribui igualmente para as investigações criminais dos Estados-Membros, com base nas análises efectuadas pela Europol. As competências dos dois órgãos sobrepõem-se, abrangendo os seguintes domínios: criminalidade informática, fraude e corrupção, branqueamento dos produtos do crime, crimes contra o ambiente e participação numa organização criminosa."
Europa Glossário. Eurojust. Disponível em: <http://europa.eu/scadplus/glossary/eurojust_pt.htm>. Acesso em: 9 abr.2009.

[254] A"Europol é um órgão de cooperação entre os serviços policiais e aduaneiros dos Estados-Membros. A ideia de criar um Serviço Europeu de Polícia foi evocada a partir do Conselho Europeu do Luxemburgo (Junho de 1991). Previsto pelo Tratado de Maastricht, o Serviço iniciou as suas actividades em Janeiro de 1994, com a designação de «Unidade Droga Europol» (UDE). A Convenção que cria a Europol foi assinada em Julho de 1995 e entrou em vigor em 1 de Outubro de 1998. A Europol é competente em matéria de combate à criminalidade e ao terrorismo, mas não é uma polícia europeia propriamente dita. Trata-se de um instrumento ao serviço dos Estados-Membros destinado a permitir-lhes enfrentar melhor os fenómenos criminosos. Concretamente, a acção da Europol consiste, por um lado, em facilitar a transmissão de informações entre os serviços nacionais e, por outro, em lhes fornecer investigações de âmbito criminal. A Europol participa nas equipas comuns de investigação formadas pelos serviços dos diferentes Estados-Membros, facultando-lhes no local as informações de que necessitam."
Europa Glossário. Europol. Disponível em: < http://europa.eu/scadplus/glossary/europol_pt.htm>. Acesso em: 9 abr.2009.

[255] "A Rede Judiciária Europeia (RJE) em matéria penal é um instrumento destinado a facilitar o auxílio judiciário mútuo no quadro da luta contra a criminalidade transnacional. O seu fundamento reside numa Acção Comum adoptada pelo Conselho em 29 de Junho de 1998.A rede judiciária é composta por pontos de contacto que ficam à disposição das autoridades judiciárias locais e das autoridades judiciárias dos outros Estados-Membros para lhes permitir estabelecer contactos recíprocos directos. Estes pontos de contacto fornecem igualmente as informações jurídicas e práticas necessárias para ajudar as autoridades em causa a estabelecer, de forma eficaz, um pedido de cooperação judiciária."
Europa Glossário. Eurojust. Disponível em: <http://europa.eu/scadplus/glossary/eurojust_pt.htm>. Acesso em: 9 abr.2009.

implicam ainda, no âmbito jurídico, da "aproximação das disposições de direito penal dos Estados-Membros, bem como a criação de mecanismos de reconhecimento mútuo das decisões judiciais em matéria penal."[256]

Depreende-se assim, no âmbito do direito comunitário europeu vigente, como principal instrumento jurídico a tutelar os cidadãos europeus das mais variadas formas de criminalidade: contra a criminalidade organizada, contra o branqueamento de capitais, contra as drogas, fraudes, contra o racismo e a xenofobia,terrorismo e também do cibercrime.

Num estudo sobre crime organizado, no qual se insere o cibercrime, Domingues pontifica com propriedade:

> Os esforços até então coligidos pelos Estados nacionais tanto no âmbito interno, quanto no âmbito internacional, não lograram suficientemente capazes de conter a criminalidade econômica organizada transnacional – que tende a chegar ao nível da supranacionalidade – advinda de um mundo economicamente globalizado, posto que, como foi visto anteriormente, os Estados encontram-se limitados à suas próprias bases conceituais e institucionais, que não conseguem abranger toda a extensão desta nova forma de criminalidade.[257]

Assim, o amadurecimento dessas relações jurídicas foram naturais para os trabalhos desenvolvidos no âmbito da União Europeia que culminaram com o estabelecimento da Convenção do Conselho da Europa sobre o Cibercrime[258], também conhecida como Convenção de Budapeste (ETS 185), datada de 23 de novembro de 2001, acrescida de seu Protocolo contra Crime de Racismo e Xenofobia (ETS 189), como instrumentos jurídicos próprios do direito comunitário europeu que servem como guia a balizar o combate a estes delitos cibernéticos na sociedade global.

5.2 A União Europeia e a construção da Convenção de Budapeste

O esfoço da União Europeia para constituição de um instrumento jurídico hábil a combater o cibercrime tem como precursores os trabalhos desenvolvidos pela OCDE e pelo

---

[256] Idem Idem.

[257] DOMINGUES, Antonio Carlos Iranlei Toscano Moura. **O Tribunal Penal Internacional e o combate à criminalidade econômica organizada transnacional.** Dissertação apresentada ao Programa de Pós-Graduação – CCJ – UFPB: Mestrado em Direito Econômico. João Pessoa – PB, 2007. p.82.

[258] "A Convenção do Conselho da Europa sobre o Cibercrime é o resultado de 4 quatro) anos de trabalho do "Comitê de Peritos em Crimes no Ciberespaço (PC-CY)", estabelecido pelo Comitê de Ministros do Conselho da Europa, em 4 de fevereiro de 1997.
DELGADO, op.cit. 217, p. 153.

G8, e também, de outros estudos viabilizados pelas Nações Unidaes e pelo Conselho da Europa. A Convenção de Budapeste resultou assim, como fruto destes estudos e recomendações que se fizeram prementes, principalmente a partir da construção do ideal de cooperação em matéria penal que já amadurecido neste espaço comunitário.

Estes trabalhos desenvolvidos pela OCDE foram muito significativos uma vez que contribuíram para a implementação de novas medidas, ainda nos idos de 1982 quando em Paris "[...] decidiu sobre a nomeação de uma comissão de peritos para discutir a cibercriminalidade e a necessidade de mudança nos Códigos Penais."[259]

No caso do G8 estas atividades iniciais datam de 1998 com a criação de um grupo de especialistas para atuar no combate ao crime organizado transnacional, principalmente com o objetivo de assegurar que nenhum criminoso recebesse refúgio em qualquer lugar do mundo.

Reforçando este ideal, bem antes, a Interpol se firma como primeira organização internacional a enfrentar os crimes cibernéticos e discutir os aspectos legais quando em 1979 realizou uma conferência em Paris, firmando a preocupação de que "A natureza da criminalidade informática é internacional, devido ao constante aumento das comunicações por telefone, etc satélites, entre os diferentes países. As organizações internacionais, como a Interpol, deveria dar mais atenção a este aspecto."

Entretanto a primeira iniciativa internacional para debater o cibercrime na Europa foi do Conselho da Europa numa conferência especial sobre aspectos criminológicos da criminalidade econômica em Estrasburgo, em 1976, quando vários cibercrimes foram descritos e introduzidos.[260]Soma-se a esta, outras iniciativas abordadas em 1985 e em 1989 com a definição de uma lista que incluia uma série de cibercrimes como falsificação de computador, danos aos dados em computadores ou programas de computador, sabotagem, acesso não autorizados, a intercepção não autorizada e a reprodução não autorizada de programas de computador (pirataria de softwares).

A emergente preocupação levou os líderes europeus a reunir-se um evento especial, a Cimeira de Tampere, em 1999, com o objetivo de estabelecer definições,

---

[259] SCHJOLBERG, op. cit. n. 156.
Texto original: "[…]decided on appointing an expert committee to discuss computer-related crime and the need for changes in the Penal Codes."
[260] SCHJOLBERG, op. cit. n. 156.
Texto original: "*The first international initiative on computer crime in Europe was the Council of Europe Conference on Criminological Aspects of Economic Crime in Strasbourg in 1976. Several categories of computer crime were introduced.*"

incriminações e sanções comuns relacionadas aos "crimes de alta tecnologia", como relata Chawki.[261]

Fixaram-se nessa linha uma série de recomendações no âmbito do Conselho da União Europeia. Desta forma temos as Recomendações do Comitê de Ministros Nº R (85) que relacionava à aplicação prática da Convenção Europeia sobre Auxílio Judiciário Mútuo em Matéria Penal quanto às cartas rogatórias para a intercepção de telecomunicações. Do mesmo modo as Recomendaões de Nº R (88) sobre as medidas destinadas a combater a pirataria no domínio do direito de autor e dos direitos conexos; N.º R (87) que disciplina a utilização de dados de caráter pessoal na área policial; N.º R (95) relativa à proteger os dados de carácter pessoal no setor das telecomunicações e a Recomendação N.º R (89) sobre a criminalidade informática que estabelece diretrizes para os legisladores nacionais referente à definição de certos cibercrimes.

No vácuo destes acontecimentos seguiram-se ainda: a Recomendação Nº R (95) relativa a problemas processuais penais relacionados com as tecnologias da informação; Resolução n.º 1 adoptada pelos Ministros Europeus da Justiça na sua 21ª Conferência (Praga, 10 e 11 de Junho de 1997), que estabelecia ao Comitê de Ministros apoio para o trabalho desenvolvido pelo Comitê Europeu para os Problemas Criminais (CDPC) em face da criminalidade, objetivando aproximar as legislações penais nacionais, permitindo a utilização de meios de investigação eficazes.

Merece destaque a Resolução n.º 3, adotada na 23ª Conferência dos Ministros Europeus da Justiça (Londres, 8 e 9 de Junho de 2000), que incentivava as partes intervenientes nas negociações a seguir esforços para viabilizar soluções coerentes. Permitia cooperação para que o maior número possível de Estados participassem do encontro que viria a culminar com a Convenção de Budapeste. Houve também o reforço no sentido de efetivar um mecanismo ágil e eficaz para a cooperação penal internacional, com enfoque para os cibercrimes.

Tendo igualmente em conta um plano de ação adotado pelos Chefes de Estado e de Governo do Conselho da Europa, por ocasião da sua Segunda Cimeira (Estrasburgo, 10 e 11 de Outubro de 1997), para procurar respostas comuns face ao desenvolvimento das novas tecnologias da informação, com base nas normas e princípios do Comitê de Ministros do Conselho da Europa que estabeleceu neste mesmo ano um comitê de peritos intitulado

[261] CHAWKI, op. cit. n. 152.

"Comité de Peritos sobre a criminalidade no ciberespaço (PC-CY)"[262], a assumindo as negociações sobre um projeto de convenção internacional sobre a cibercriminalidade. Estes trabalhos perduraram por aproximadamente quatro anos, merecendo destacar que entre abril de 1997 e dezembro de 2000, o PC-CY realizou 10 reuniões plenárias e 15 reuniões do seu grupo aberto de redação. Tendo os trabalhos sido finalizados em abril de 2001.

De acordo com Delgado:

> Além dos Estados-membros do Conselho da Europa, também os Estados Unidos, Canadá, Japão e África do Sul contribuíram com o referido Comitê para a elaboração da Convenção sobre o Cibercrime, tendo sido convidados a participar do rocesso de sua elaboração na qualidade de "observadores externos". O seu texto final, juntamente com o respectivo "Relatório Explicativo", foram submetidos à aprovação e adoção pelo Comitê de Ministros do Conselho da Europa, em sua 109ª Sessão, a 8 de novembro de 2001, e a Convenção foi aberta à assinatura pelos Estados-membros do Conselho da Europa e os não-membros, mas que também participaram do seu processo de elaboração, na cidade de Budapeste, a 23 de novembro de 2001.[263]

Desde sua adoção em 23 de novembro de 2001, em Budapeste, Hungria, um total de 46 Estados já assinaram a Convenção sobre Cibercrime (Convenção de Budapeste), sendo que deste total, até 16 de abril de 2009, 28 nações já a ratificaram, incluindo países que não integram a União Europeia: Canadá, Costa Rica, República Dominicana, Japão, México, Filipinas África do Sul e com destaque os Estados Unidos, berço da internet (a Convenção foi ratificada em 2006 e entrou em vigor em 1 de janeiro de 2007).

Destaque-se ainda, quanto aos aspectos essenciais da Convenção, que em 1 de março de 2006, passou a vigorar o Protocolo Adicional à Convenção de Budapeste, que visa criminalizar condutas de cunho racista e xenófobo, através de ameaças, insultos e condutas congêneres, praticadas através da internat e redes de computadores.

Nesta dimensão a Convenção de Budapeste sobre Cibercrime é o primeiro tratado internacional que busca abordar a cibercriminalidade e harmonizar as legislações nacionais, melhorar técnicas e aumentar a cooperação entre as nações. Representa ainda uma nova era na cooperação penal entre as nações, oferecendo uma regulamentação supranacional "a fim de efetivamente combater infrações relacionadas aos cibercrimes facilitando a

---

[262] Convention on Cybercrime (ETS No 185). **Explanatory Report**. Disponível em:<http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm>. Acesso em: 11 abr.2009.
[263] DELGADO, op. cit. n. 253, p.154.

detecção, investigação e repressão de tais delitos, tanto a em âmbito nacional quanto internacional, e fornecendo mecanismos de rápida e confiável cooperação internacional."[264]

5.3 Tratamento legal do cibercrime na Convenção de Budapeste

Como se depreende de todo contexto formado, isto é, ainda que os principais fundamentos tecnológicos que embasam o funcionamento das novas tecnologias encontrem raízes num momento anterior à década de 90, foi apenas com a popularização da internet que os conceitos tradicionais entraram num processo de mutação. Um novo componente iria possibilitar que espaço e tempo passassem a ter novos contornos, numa supressão de escalas, de forma fazer com que sejam indiferentes os conceitos de território e lugar do crime.

Se tradicionais conceitos foram revistos, da mesma forma a sociedade passou a sofrer os efeitos da prática de condutas que durante muito tempo permeavam o ideário humano como se ficção científica fosse.

Os novos fenômenos assim denominados de cibercrime, têm um novo território – o ciberespaço, mas seus efeitos se materializam na vida humana sob muitas formas, o que requereu, pois a construção de novos instrumentos jurídicos que pudesse fazer frente ao fenômeno em escala global, solução apenas viabilizada mediante a cooperação penal internacional.

Não interessa desta forma, que se estabeleçam leis rígidas, mas com amplitude limitada, e, é isto que os dotrinadores tem compreendido, pois, não há possibilidade jurídica de que tais instrumentos tenham alcance além das fronteiras que própria noção de soberania irá limitar, pois:

> As novas tecnologias existentes irão desafiar os conceitos jurídicos. Informação e comunicação fluir mais facilmente em todo o mundo. Fronteiras não são mais limites para este fluxo. Os criminosos estão cada vez mais localizadas em locais diferentes do que os seus actos produzir os seus efeitos. No entanto, as leis são geralmente confinado a um território específico. Assim, soluções para os problemas devem ser abordados pela legislação internacional, que requeiram a adopção de adequados instrumentos jurídicos internacionais. A presente Convenção visa enfrentar este

[264] CHAWKI, Mohamed. WAHAB, Mohamed S. Abdel. ***Identity Theft in Cyberspace: Issues and Solutions***. Lex Electronica, vol.11 n°1 (Printemps / Spring 2006). Disponível em: <hhttp://www.lex-electronica.org/docs/articles_54.pdf>. Acesso em: 11 abr.2009.

> desafio, com o devido respeito aos direitos humanos na nova sociedade da informação.[265]

Neste sentido, o tratamento legal do cibercrime na Convenção de Budapeste foi fruto de amplo debate, cuja formulação requereu anos de maturação e emprego de toda experiência proporcionada pela vivência no direito comunitário europeu.

Desta forma, o próprio preâmbulo da Convenção de Budapeste, estabelece:

> Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e confiável; [...]de modo a tornar mais eficazes as investigações e as acções penais relativas a infracções penais relacionadas com sistemas e dados informáticos, bem como permitir a recolha de provas em forma electrónica de uma infracção penal;[266]

Assim, a Convenção de Budapeste sobre o Cibercrime significa avanço formidável no combate à criminalidade cibernética, só possível, em escala global, mediante a cooperação dos Estados, através de suas instâncias policiais e judiciais, sem que seja preciso esquecer que há medidas que podem ser tomadas no âmbito do direito nacional no Estados, pois nem todas as condutas delituosas são transfronteiriças.

5.3.1 A Convenção e sua estrutura normativa

A Convenção de Budapeste sobre o Cibercrime está estruturada em em quatro Capítulos, assim compreendido como linhas centrais a estruturar o instrumento jurídico. Por questões de ordem metodológica e para melhor compreensão de sua estrutura, faz-se necessário a apresentação de seus elementos essenciais.

---

[265] CONVENTION ON CYBERCRIME, op. cit. n. 253.
Texto original: *The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge, with due respect to human rights in the new Information Society.* (Tradução nossa).

[266] CONVENTION ON CYBERCRIME, op. cit. n. 253.

O Capítulo I, trata de terminologias, constando apenas um artigo.

O Capítulo II estabelece medidas a tomar a nível nacional, com o fixação de aspectos referentes ao direito penal material, processual e competência, assim estabelecida:

> Secção 1 – Direito penal material
> Título 1 – Infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos
> Título 2 – Infracções relacionada com computadores
> Título 3 – Infracções relacionadas com o conteúdo
> Título 4 – Infracções relacionadas com a violação do direito de autor e direitos conexos
> Título 5 – Outras formas de Responsabilidade e Sanções
> Secção 2 – Direito Processual
> Título 1 – Disposições comuns
> Título 2 – Conservação expedita de dados informáticos armazenados
> Título 3 – Injunção
> Título 4 – Busca e Apreensão de dados informáticos armazenados
> Título 5 – Recolha em tempo real de dados informáticos
> Secção 3 – Competência[267](com destaques do autor)

O Capítulo III, da Convenção apresenta-se como o mais significativo ao presente estudo, uma vez que trata da cooperação internacional, compondo este, duas seções, com os seguintes dispositivos:

> **Secção 1 – Princípios gerais**
> Título 1 – Princípios gerais relativos à cooperação internacional
> Título 2 – Princípios relativos à extradição
> Título 3 – Princípios Gerais relativos ao auxílio mútuo
> Título 4 – Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis
> **Secção 2 – Disposições específicas**
> Título 1 – Auxílio mútuo em matéria de medidas provisórias
> Título 2 – Auxílio mútuo relativamente a poderes de investigação
> Título 3 - Rede 24/7 (grifo nosso)[268]

No capítulo IV, são expostas as disposições finais, com destaque para os artigos que tratam da adesão à Convenção, da aplicação territorial e de seus efeitos.

A Convenção tem como escopo principal, numa visão geral a sintetizar o seu cerne: (1) harmonizar o direito penal interno (de cada país) e harmoniza-lo com as previsões relativas ao cibercrime; (2) prover o direito processual penal interno de poderes necessários para a investigação e repressão de delitos como bem como outros crimes cometidos por meio de um sistema de computador ou obtenção de provas em relação ao que está em formato eletrônico e (3) a criação de uma rápido e eficaz regime de cooperação internacional.

---

[267] CONVENÇÃO DE BUDAPESTE, op. cit. n. 253.
[268] CONVENÇÃO DE BUDAPESTE, op. cit. n. 253.

É preciso fazer o registro de que o texto original da Convenção, traduzido do inglês para o português, não representa com exatidão o sentido e expressão de termos utilizados nas Tecnologias da Informação e da Comunicação, ou mesmo, puramente no quotidiano da informática. Por exemplo, no artigo 1º, que trata das definições, o texto em original em inglês prevê a definição de "*computer system*", já o texto traduzido para português e disponível indica a expressão "sistema informático", que obviamente tem um sentido muito mais amplo que "*computer system*" (sistema de computador). Independente de tais distorções, o aprofundamento dos pontos mais relavantes da Convenção serão abordados e, sempre que possível, os ajustes e comentários serão externados.

5.3.1.1 Definições essenciais

O art. 1º, da Convenção de Budapeste estabelece a definição para quatro itens: sistema informático, dados informáticos, fornecedor de serviço e dados de tráfego. Sistema informático é definido como "qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles" desenvolve ou executa o tratamento automático de dados.

No ponto seguinte, alínea "b", do artigo 1o, esclarece o próprio instrumento jurídico a definição para "dados informáticos", como sendo "qualquer representação de factos, de informações ou de conceitos, incluindo um programa" que possibilite um sistema informático executar uma função. Nos termos da Convenção, alínea "c", é fixada a definição para "fornecedor de serviço" que seria a entidade de caráter público ou privado que possibilite a utilização de seus serviços de forma a viabilizar comunicação através de um sistema informático e ainda "qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores desse serviço.

De acordo com o disposto na alínea "d", tráfego de dados significa:

> [...] todos os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Desta forma, são definidos, em síntese o sistema, ou seja, o conjunto de equipamentos empregados para atividades na área de informática, incluindo computador, impressoras e scanners. O conjunto de equipamentos, da forma como descrita, não representa risco potencial, pois sem acesso à rede internacional de computadores seu alcance fica restrito ao lar de seu proprietário. Outro ponto chave definido, diz respeito aos softwares utilizados, bem como o produto da utilização do sistema, que pode, por exemplo ser um texto digitado ou até mesmo um programa de computador, ou seja, esse conjunto de informações armazenadas no "sistema informático" irão constituir os dados informáticos.

Quanto a definição das entidades públicas ou privadas que fornecem ou disponibilizam o serviço de provedor, ou seja, a pessoa que irá possibilitar a conexão do interessado à rede mundial de computadores ou ainda a pessoa que armazena tais informações – espécie de provedor de conteúdo.

Ao tratar de "dados de tráfego", a Convenção quer indicar todas as informações que transitam na rede, de forma que se possa estabelecer uma lista de parâmetros que são essenciais para identificação da origem e do destinatário, consequentemente, seus possíveis remetentes e destinatários, uma vez que se prioriza os aspectos referentes a origem, destino, trajeto, hora, data, tamanho e duração ou tipo do serviço.

As redes de computadores surgiram com a necessidade humana de compartilhar informações que, a princípio, estavam isoladas em computadores. Esse compartilhamento de informações é viabilizado quando dois computadores ou mais são conectados, fazendo com que exista uma interação entre eles.

Neste sentido, Mangueira[269] assevera que "A interligação de computadores possibilita o compartilhamento de arquivos, periféricos (impressoras, leitoras de discos óticos e disquetes, discos rígidos, *plotters*, etc.) e conexões com outras redes (é aqui que reside o perigo!), como a internet."

O grande segredo da internet é a capacidade de colocar em conexão diferentes redes de computadores, fazendo com que haja uma interação global. Essa conectividade só é possível graças à existência de um protocolo de global de informações, o que torna possível diferentes redes e sistemas se comunicarem entre si.

Essa linguagem universal é conhecida como TCP/IP (*Transmission Control Protocol/Internet Protocol*), que foi desenvolvido na década de 70. Dessa forma, conforme ensina Mangueira:

---

[269] MANGUEIRA, op. cit. n. 187, p.30.

> O TCP/IP envia informações divididas em pacotes e possui camadas (níveis) com funções bem específicas, para o nível físico, para o transporte, para a rede interna (internet) e para a aplicação. Ao transferir uma mensagem de uma aplicação de uma máquina a uma outra aplicação localizada em uma outra máquina, o protocolo transmite a mensagem do nível de aplicação até o nível físico, daí a mensagem é transmitida pela rede até o outro computador, que transporta a mensagem da camada física até a aplicação.[270]

Podemos dizer então, que cada computador que esteja conectado à *web* possui um endereço IP (Protocolo de Internet). Protocolo IP "é o protocolo da Internet, que permite a interconexão de diferentes redes para transmissão de pacotes de dados."[271] Cada computador que esteja conectado a uma rede com acesso à internet possui um endereço IP, e isto funciona como se fosse uma impressão digital, que torna determinada máquina única na rede, o que facilita, por conseguinte, o rastreamento e localização de computadores que foram utilizados por pessoas que estejam conectadas à rede para praticar crimes.

5.3.2 Diretivas ao direito nacional

A Convenção de Budapeste sobre o Cibercrime, quanto ao estabelecimento de medidas a serem tomadas no âmbito do direito de cada Estado, ou seja, no direito nacional, fixa em seu Capítulo II medidas a serem tomadas em três eixos centrais: primeiro sobre aspectos referentes ao direito material, com definição de infrações e necessidade de harmonização das condutas descritas com o direito interno; como segundo pilar trata do direito processual, ou seja, a adoção de medidas para delinear poderes e instrumentos para fins de investigação ou procedimento penal (busca e apreensão, coleta de provas e interceptação de telecomunicações) e como terceiro ponto os aspectos referentes à questão da competência em relação às infrações descritas nos artigos 2º a 11 da Convenção.

Reforçando este entendimento Schjolberg pontua quanto as disposições do Capítulo II:

> Capítulo 2 inclui medidas a serem tomadas a nível nacional e abrange o direito penal material, direito processual e da jurisdição. Direito penal material contém a definição

[270] MANGUEIRA, op. cit. n. 187, p.32.
[271] MARTINS, op. cit. n. 193, p. 103.

> dos delitos contra a confidencialidade, a integridade e a disponibilidade de dados e sistemas, crimes relacionados ao computador e crimes relacionados com falsificação e fraude, infrações relacionadas com a pornografia infantil e os crimes relacionados às violações de direitos do autor e direitos conexos. Disposições da lei processual penal é aplicável em qualquer delito cometido por meio de um sistema de computador e para a coleta de provas referente aos crimes. As disposições contêm medidas de preservação do computador e do dados armazenados, a produção, pesquisa e apreensão de dados informáticos armazenados e sua coleta em tempo real.[272] (tradução nossa).

O delineamento das ações previstas são imprescindíveis uma vez que o Estado assine e ratifique a Convenção, não pode haver incongruências ou questões dissonantes entre o que está posto no instrumento jurídico internacional assinado e ratificado, e o direito nacional. Constitui assim, um dos principais fatores positivos relatados pelos doutrinadores internacionais quanto à harmonização do direito interno e do direito posto pela Convenção.

5.3.2.1 Previsão de delitos e medidas a serem adotadas no âmbito do direito material

5.3.2.1.1 Crimes contra à integridade, confidencialidade e disponibilidade dos sistemas e dados informáticos

Recomendação para que no direito interno, do país signatário da Convenção, sejam estabelecidas condutas delituosas para os atos de acesso ilegítimo intencional (total ou parcial com violação de medidas de segurança, cujo objetivo seja a obtenção de dados informáticos ou outra intenção ilícita); interceptação ilegítima de dados informáticos; interferência em dados; interferência em sistemas e uso abusivo de dispositivos.

In casu para os atos de acesso ilegítimo, interferência de dados informáticos, interferência em sistemas e uso abusivo de dispositivos estariam compatíveis com a ideia de elaboração de novas tipificações penais, visto que a descrição das condutas presentes na

---

[272] SCHJOLBERG, op. cit. n. 156.
Texto original: *Chapter 2 includes measures to be taken at the national level and covers substantive criminal law, procedural law and jurisdiction. Substantive criminal law contains of offences against the confidentiality, integrity and availability of computer data and systems, 51 computer-related offences such as computer-related forgery and fraud, offences related to child pornography, and offences related to infringements of copyright and related rights. Provisions of procedural law shall apply on any criminal offence committed by means of a computer system, and to the collection on evidence in electronic form of a criminal offence. The provisions contain expedited preservation of stored computer data, production order, search and seizure of stored computer data, real-time collection of computer data.*

Convenção não encontram tipos penais semelhantes em nosso ordenamento jurídico penal. Há entretanto, previsão para acesso não autorizado em relação à administração pública, consideranto tal prática violação de sigilo funcional, conforme estabelecido no art. 325, §1º, incisos I e II, da Lei n º. 9.983/2000.[273]

Por outro prisma, quanto à conduta de interceptação ilegítima de dados informáticos, há disposições presentes a partir do próprio texto constitucional que dispõe em seu art. 5º, inciso XII, sobre a inviolabilidade do "[...] sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas [...]" a própria Carta Magna excetua as hipóteses de ordem judicial, para fins de investigação criminal ou instrução processual penal.

A partir da tutela prevista na própria Constituição Federal, há previsão de punição para essa conduta presente na Lei 9.296/96[274], que regulamenta o art.5o, inciso XII, trata da definição do crime de inteceptação não autorizada de comunicação informática ou telemática de dados.

5.3.2.1.2 Infrações penais relacionadas com computadores

A Convenção do Conselho da Europa sobre Cibercrime dispõe em seu Título 2, das infrações relacionadas a computadores. Especificamente as condutas de falsidade e burla informática. Esta duas hipóteses previstas na Convenção já encontram regulamentação penal no ordenamento jurídico penal brasileiro, pois a Lei n º 9.983/2000[275], inseriu os artigos 313-

[273] O art. 325, §1º, incisos I e II, da Lei n º. 9.983/2000, assim estabelece: "I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública" e de quem "II – se utiliza, indevidamente, do acesso restrito", ambos sancionados com penas de detenção de 6 meses a 2 anos, ou multa;"

[274] A Lei 9.296/96, em seu art. 10, considera crime, punível com reclusão de 2 a 4 anos e multa o ato de "realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei."

[275] O Código Penal Brasileiro dispõe da seguinte forma:

"Inserção de dados falsos em sistema de informações (Incluído pela Lei nº 9.983, de 2000)
Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000))
Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)

Modificação ou alteração não autorizada de sistema de informações (Incluído pela Lei nº 9.983, de 2000)
Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000)

A e 313-B, estabelecendo punição para as condutas de "inserção de dados falsos em sistema de informações" e "modificação ou alteração não autorizada de sistema de informações".

Há ainda disposições de ordem penal constantes no Código Eleitoral, ou seja, no art. 72 da Lei n. 9.504/97[276], que cuida das infrações relacionadas com acesso indevido ao sistema de voto eletrônico ou dano aos equipamentos utilizados na votação, que em nosso caso realiza-se através de urnas eletrônicas.

5.3.2.1.3 Infrações penais relacionadas com o conteúdo

O art. 9º, da Convenção de Budapeste sobre Cibercrime, trata especialmente da conduta das infrações relacionadas com a pornografia infantil na internet. Estas condutas durante os três últimos anos provocaram uma espécie de comoção social no Brasil, em face dos comportamentos mais perversos, contendo cenas de sexo explícito com crianças e adolescentes. O alerta surgiu quando a empresa Google Inc. passou a disponibilizar no Brasil o site de relacionamentos Orkut. O que seria um espaço para estreitamento de laços sociais, rapidamente converteu-se num espaço para práticas de disseminação de cenas de sexo explícito envolvento menores e maiores de 18 anos, o que gerou a instalação de uma Comissão Parlamentar de Inquérito (CPI) no Senado Federal.

A pressão social, bem como a grande repercussão internacional que os fatos geraram potencializaram a tramitação de projeto legislativos, culminando com rápida aprovação no parlamento e sanção presidencial da Lei nº 11.829/2008, que alterou a Lei nº 8.069/1990 - Estatuto da Criança e do Adolescente, objetivando aprimorar "o combate à

Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)
Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado. (Incluído pela Lei nº 9.983, de 2000)."

[276]Assim estabelece o Código Eleitoral:

"**Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:**
I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;
II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;
III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes."

produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet."[277]

Como se depreende das disposições acima fixadas, passados sete anos da Convenção de Budapeste, o Brasil estipulou em sua legislação nacional, a punição para condutas de pornografia infantil, inclusive na internet, mas ressalte-se, que a edição dessa medida legislativa não decorreu de adesão à Convenção, mas da pressão exercida pela sociedade e pelos debates parlamentares com o advento da CPI da pedofilia.

5.3.2.1.4 Infrações penais relacionadas com a violação do direito de autor e direitos conexos

Um dos aspectos mais significativos do impacto da internet na sociedade, relaciona-se com o direito autoral. Em duas conferências que subsidiaram o presente estudo - SPCI 2008 (*1st International Conference on Security, Privacy and Confidentiality Issues in Cyberlaw*), Cairo, Capital do Egito e Cyberspace 2008 (*6th Internatinal Conference Cyberspace 2008*), na cidade de Brno, República Tcheca, a temática foi abordada com ênfase por especialistas da Índia e da União Europeia.

No direito brasileiro duas leis regulam a matéria relacionada aos direitos autorais e direitos conexos, a Lei nº 9.609/98, que dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País e a Lei nº 10.695/2003, que alterou as disposições constantes no Código Penal Brasileiro, referente aos direitos autorais e direitos conexos. As duas legislações contemplam a previsão de providências constantes na Convenção de Budapeste e, em aderindo à Convenção, em termos de direito material, a legislação brasileira não careceria de ajustes.

5.3.2.1.5 Outras formas de responsabilidade criminal e sanções

No título 5, art. 11o, a Convenção de Budapeste sobre Cibecrime dispõe sobre as medidas necessárias para responsabilizar e punir a forma tentada dos delitos que nela estão

[277] Brasil. **Lei 11.829/2008**, disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm>. Acesso em: 15 abr.2009.

dispostos, bem como as práticas que forem perpetradas mediante cumplicidade, cujas disposições de ordem penal, encontram-se estabelecidas no art.14 e no art. 29, do Código Penal Brasileiro e, neste caso, também não seriam necessários ajustes.

Merece observação o disposto no art. 12º, que se refere a responsabilidade penal da pessoa jurídica em face de crime praticados, ainda que individualmente (desde que a pessoa exerça poder de direção), e de forma omissiva, quando tenha negligenciado a supervisão e o controle de atividades exercidas por seus empregados.

Quanto às sanções e medidas, previstas no art.13, o instrumento jurídico internacional de combate ao cibercrime prevê que os Estados signatários tomem medidas "necessárias para assegurar que as infracções penais verificadas em aplicação dos Artigos 2º a 11º sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo penas privativas da liberdade."[278] Prevê, inclusive, a necessidade de imposição de sanções pecuniárias quando se tratar de pessoa jurídica.

5.3.2.2 Medidas a serem adotadas no âmbito do direito processual

5.3.2.2.1 Alcance e condições das medidas de ordem processual a serem tomadas

O art. 14, da Convenção de Budapeste especifica como medida a ser tomada pela parte signatária da Convenção, que seja determinado no direito interno a instituição de poderes e procedimentos previstos, a fim de facilitar a investigação e os procedimentos penais, notadamente, às condutas previstas nos seus artigos 2o ao 11o, respectivamente, bem como regular a coleta de provas, embora o próprio dispositivo faça previsão de que o Estado que adotar a Convenção possa estabelecer limitações, mediante ressalvas.

O art. 15, estabelece o seguinte:

> "Artigo 15º - Condições e salvaguardas
> 1. Cada Parte assegurará que o estabelecimento, a entrada em vigor e a aplicação dos poderes e procedimentos previstos na presente Secção são sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma protecção adequada dos direitos do Homem e das liberdades, designadamente estabelecidas em conformidade com as obrigações decorrentes da aplicação da Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos (1950), do Pacto Internacional das

[278] CONVENTION ON CYBERCRIME, op. cit. n. 253

> Nações Unidas sobre os Direitos Civis e Políticos, (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos Direitos do Homem e que deve integrar o princípio da proporcionalidade.
> 2. Quando for apropriado, tendo em conta a natureza do poder ou do procedimento em questão, as referidas condições e salvaguardas incluirão, designadamente, um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a limitação do âmbito de aplicação e a duração do poder ou procedimento em causa.
> 3. Na medida em que seja do interesse público, em particular da boa administração da justiça, cada Parte examinará o efeito dos poderes e dos procedimentos da presente Secção sobre os direitos, responsabilidades e interesses legítimos de terceiros."[279]

Como se vê, há uma preocupação clara para que, mesmo com a adoção da Convenção pelo Estado interessado e que tenha sua adesão aprovada pelo Conselho de Ministros da União Europeia, não ocorram violações a direitos e garantias já consubstanciados pelo direito nacional, além de tratados e convenções internacionais.

Uma das previsões que se apresenta como relevante, indica a necessidade do controle judicial das medidas a serem adotadas, embora seja possível fazê-la por outras formas de controle independente, o que não se apresenta como aconselhável. Este controle, em termos de legislação nacional, já tem previsão na própria Constituição Federal, que dispõe em eu art. 5o, inciso XII, sobre a necessidade de autorização judicial nos casos de interceptação de comunicações de dados.

5.3.2.2.2 Conservação expedita de dados informáticos armazenados

Os registros de acesso à internet são viabilizados por provedores de acesso, que possibilitam a conexão entre o usuário e a internet (acesso às informações de outras redes), funcionando como intermediário e recebendo pela prestação desse tipo de serviço. Consequentemente, é de se esperar que as informações referentes aos acessos fiquem registradas, mas, ao menos no Brasil, não há legislação específica que obrigue os provedores de acesso ou mesmo provedores de conteúdo[280] a manterem arquivos que viabilizem tal procedimento.

---

[279] CONVENTION ON CYBERCRIME, op. cit. n. 253

[280] Provedores de conteúdo são empresas que mantém difusão/exploração de serviços como de notícias, sites de relacionamentos, revistas e jornais.
Neste sentido o Termo de Cooperação Mútua firmado entre a Comissão Parlamentar de Inquérito do Senado Federal – CPI da Pedofilia, Ministério Público Federal e outras instituições prevê o seguinte:
"b) de acesso: qualquer entidade, publica ou privada, que faculte aos usuários dos seus serviços a possibilidade de conexão a Internet mediante atribuição de endereço IP;

A rigor, uma das argumentações a serem postas poderia vincular-se ao próprio exercício do direito à privacidade que, em tese, poderia estar sendo aviltada em face desse tipo de procedimento. Outra questão que pode ser suscitada indica a necessidade de armazenamento de grande quantidade de informações, o que poderia demandar, por consequência, custos para viabilizar tais registros.

Quanto aos aspectos constantes na Convenção de Budapeste, o art. 16, prevê que os países signatários adotem medidas de ordem legislativa (produção de leis, se ainda não as tiver) para que se exija a conservação expedita (segura/confiável) de dados informáticos específicos, notadamente referente ao tráfego de dados, que possam ser alterados ou perdidos. Estas informações, na verdade, seriam os registro de acesso no provedor de serviços ou de conteúdo, de forma a viabilizar data, hora, identificação de quem acessou através do número IP e qual o conteúdo acessado, o que é perfeitamente possível, sob o ponto de vista técnico.

Outra diretiva proposta, indica a necessidade ajuste legal de forma a constar que a pessoa mantenedora do serviço de provedor de conteúdo ou de acesso mantenha os registros de acesso por um período de 90 (noventa dias), com possibilidade de renovação desse prazo. Do mesmo modo, a previsão legal deve estabelecer a obrigação de sigilo sobre a execução dos referidos procedimentos durante o período previsto pelo seu direito interno.

Ressalte-se ainda, que a adoção de tais medidas estariam sujeitas à previsão do disposto no art. 14 e 15, bem como que devam ser operacionalizadas com agilidade, conforme prevê o art. 17, da Convenção.

No Brasil, após os escândalos que vieram a público com as investigações promovidas pela CPI da Pedofilia - Comissão Parlamentar de Inquérito do Senado Federal, com apoio do Ministério Público Federal e da Polícia Federal e participação de vários órgãos e entidades da sociedade civil, houve a celebração de um Termo de Mútua Cooperação entre os órgãos governamentais, empresas de telecomunicações mantenedoras de serviços e organizações da sociedade civil. Do mesmo modo, já havia um Termo de Ajustamento de Conduta celebrado entre a empresa Americana Google Inc. (mantenedora do site de relacionamento Orkut e principal alvo das investigações) e o Ministério Público Federal.[281]

---

c) de conteúdo ou interativo: qualquer entidade que processe ou armazene dados informaticos registrados, inseridos, excluidos ou alterados, de forma ativa, por usuários."
Comissão Parlamentar de Inquérito - Pedofilia. **Termo de Cooperação Mútua**. Disponível em: <http://www.prsp.mpf.gov.br/cidadania/dhumInt/Termo%20de%20Coopera%E7%E3o%20-%20Safernet%20e%20PRSP.pdf>. Acesso em: 12 abr. 2009.

[281] No caso do Termo de Ajustamento de Conduta firmado entre o Ministério Público Federal e a Google Inc. o prazo para guarda das informações era de 180 dias. Informação disponível em: <http://www.prsp.mpf.gov.br/TACgoogle.pdf>. Acesso em: 17 abr.2009.

Um dos itens previstos é a preservação dos registro pelo prazo de noventa dias, com possibilidade de renovação por igual período.[282]

5.3.2.2.3 Injunção[283] - Obrigações impostas

Uma das grandes dificuldades de se combater os cibercrimes refere-se a questão da localização física do infrator. Isto porque no ciberespaço, a questão territorial contém uma dimensão diferente da real. Uma página de internet pode se encontrar armazenada num servidor num determinado país e ser violada à distância, mediante uso de um provedor, por exermplo, de um terceiro país. Do mesmo modo pode acontecer noutros delitos.

Assim, o art. 18, da Convenção de Budapeste estabelece como obrigação dos Estados partes a adoção de medidas legislativas (prodição de leis) para que empresas mantenham registros de localização física de seus usuários. Isto na prática, corresponde a fornecer endereço e demais informações pessoais do assinante. Estas informações são diferentes das informações que transitam na rede e que possivelmente sejam registros de acesso dos assinantes.

Há previsão também da obrigação de fornecimento sobre "Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base

---

[282] De acordo com o Termo de Cooperação Mútua, tem-se o seguinte:
"CLÁUSULA SÉTIMA - Da Preservação de Dados Relativos ao Conteúdo da Comunicação
As empresas fornecedoras de serviços de conteúdo ou interatividade preservarão os dados relativos ao conteúdo da comunicação, até então armazenados em seus servidores, referente a determinado(s) usuário(s), mediante requerimento da autoridade policial ou de membro do Ministério Público, de que conste o número do inquérito policial ou procedimento, independentemente de autorização judicial, observado o disposto no inciso I da CLÁUSULA DÉCIMA deste TERMO.
Parágrafo primeiro. A transferência dos dados preservados a autoridade solicitante somente será feita mediante autorização judicial.
Parágrafo segundo. As empresas signatárias preservarão os dados a que se refere esta cláusula até a intimação da decisão judicial que autorizar a sua transferência à autoridade solicitante, ou pelo prazo máximo de noventa dias, prorrogável uma única vez, por igual período, findo o qual deverão destruir o respectivo conteúdo.
Parágrafo terceiro. A preservação dos dados futuros somente será feita mediante prévia autorização judicial."

Comissão Parlamentar de Inquérito - Pedofilia. Termo de Cooperação Mútua. Disponível em: <http://www.prsp.mpf.gov.br/cidadania/dhumInt/Termo%20de%20Coopera%E7%E3o%20-%20Safernet%20e%20PRSP.pdf>. Acesso em: 12 abr. 2009.

[283] Alguns termos utilizados na versão traduzida da Convenção de Budapeste em Português (Portugal) apresentam-se de forma não muito usual ou corrente nos círculos jurídicos brasileiros, merecendo, portanto, alguns esclarecimentos, quando necessário.
O termo **injunção**, de acordo com Priberam, Dicionário de Português *on line*, significa:
1. Ato de injungir, imposição. 2. Obrigação imposta.
Dicionário Priberam da Língua Portuguesa. Disponível em:
<http://www.priberam.pt/dlpo/definir_resultados.aspx>. Acesso em: 15 abr.2009.

num contrato ou acordo de serviços."[284] É o que dispõe o art. 18, item 3, alínea "c", da Convenção de Budapeste.

5.3.2.2.4 Busca e apreensão de dados informáticos armazenados

A abordagem sobre a busca e apreensão constante na Convenção de Budapeste, encontra pertinência ao direito processual penal, comportando, por isso, uma explanação de ordem constitucional, notadamente quanto à observância dos direitos fundamentais insertos no art. 5o, incisos X e XI, que se referem à tutela da intimidade, da vida privada e da honra da pessoa; bem como da proteção ao domicílio.

Por este prisma, Barros pontua:

> Em primeiro lugar, trata-se da proteção casa do indivíduo, cuja inviolabilidade só pode ser excepcionada nas situações previstas na Constituição. Para esse fim, o termo casa deve considerado de forma ampla, tal como definido no artigo 150 §§ 3.º e 5.º, do Código Penal, compreendendo qualquer local que sirva de abrigo, residência ou moradia ou aquele não aberto ao público onde o indivíduo exerce profissão ou atividade.
> De outro lado, a Constituição, no artigo 5.º, X, proclama serem invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação. Sem enfrentar a discussão conceitual, que se estabelece entre as expressões intimidade e vida privada, importa salientar que o indivíduo não pode ter sua vida devassada indevidamente.
> Assim, mesmo no curso de busca domiciliar, legalmente autorizada, deve-se preservar a intimidade e a privacidade, não se divulgando fatos que não tenham relação com a diligência.

Registre-se, entretanto, que a percepção sobre os respeito aos direitos fundamentais não podem ser compreendidos de forma absoluta. Comporta, portanto, limitações que o próprio texto constitucional estabelece ao fixar o poder-dever estatal de punir, obedecido, sobretudo, o princípio da legalidade.

Na Convenção do Conselho da Europa sobre Cibercrime o art. 19 determina que os Estados signatários deverão adotar medidas legislativas para habilitar autoridades competentes na realização de busca e apreensão em sistemas informáticos, bem como em dados que neles se encontrem armazenados. Do mesmo modo obriga provedores de acesso e de conteúdo, a manter os referidos dados protegidos.

---

[284] CONVENTION ON CYBERCRIME, op. cit. n. 253.

Dentre as medidas constantes no art. 19, item 3, da Convenção são fixadas medidas com as seguintes prerrogativas:

> a) Apreender ou obter de forma semelhante um sistema informático ou uma parte deste ou um suporte de armazenamento informático;
> b) Realizar e conservar uma cópia desses dados informáticos;
> c) Preservar a integridade dos dados informáticos pertinentes armazenados; e
> d) Tornar inacessíveis ou eliminar esses dados do sistema informático acedido.[285]

Reforçando a tese de necessidade da cooperação internacional e da busca e apreensão visando combater a criminalidade organizada transnacional, posta-se à colação, importante decisão do Superior Tribunal de Justiça, que assim se pronunciou:

> [...] 12. A aplicação da Lei 9.613/98 é inquestionável, face o juízo rogante investigar supostos crimes de lavagem de dinheiro, razão pela qual o Brasil, ao editar o Decreto n.º 5.015, de 12 de março de 2004, tornou-se subscritor da Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo), a qual expressamente prevê, em seu art. 18, a realização de diligências de busca ou apreensão e se perfaz suficiente à denotar cooperação entre Brasil e Bélgica.
> 13. A Lei Complementar 105/2001 apenas serviu como supedâneo do acórdão ora embargado para a decretação da quebra do sigilo bancário do interessado por estar configurado, em tese, crime de lavagem de dinheiro (art. 1°, § 4°, VIII, do aludido diploma legal).
> 14. A questão que gravita em torno do envolvimento do interessado na atividade criminosa descrita no pedido do juízo rogante diz respeito ao meritum causae e extrapola a competência deste sodalício, na linde do disposto no art. 9º da Resolução n.º 9, de 04 de maio de 2005, deste STJ (Precedentes: AgRg na CR 2.497 - US, Relator Ministro BARROS MONTEIRO, Corte Especial, DJ de 10 de dezembro de 2007 e AgRg na CR 733 - EX, Relator Ministro CESAR ASFOR ROCHA, Corte Especial, DJ de 10 de abril de 2006).
> 15. A soberania nacional ou a ordem pública não restaram afetadas, porquanto a novel ordem de cooperação jurídica internacional, encartada na Convenção de Palermo, prevê a possibilidade da concessão de exequatur em medidas de caráter executório, em seus arts 12, partes 6 e 7; e 13, parte 2.
> 15. Impugnação afastada e acolhimento dos embargos de declaração apenas para sanar as omissões apontadas, sem condenação em custas e honorários advocatícios a título de sucumbência, ex vi do art. 1°, parágrafo único, da Resolução/STJ n° 0905/2005. [286]

A sujeição da jurisdição nacional aos tratados e convenções internacionais, decorre da própria opção legislativa quando estabelece como princípio fundamental da República Federativa do Brasil a cooperação entre os povos, visando o progresso da humanidade. A consequência lógica, desse princípio, é o estreitamento dos laços entre os Estados, visando o fortalecimento das ações do Estado em face da criminalidade organizada

[285] CONVENTION ON CYBERCRIME, op. cit. n. 253
[286] BRASIL. Superior Tribunal de Justiça. **EDcl na CR .438/BE**, Rel. Ministro LUIZ FUX, CORTE ESPECIAL, julgado em 01/08/2008, DJe 20/10/2008. Disponível em: < http://br.vlex.com/vid/43535078>. Acesso em: 15 abr.2009.

transnacional, que se evidencia também, em face do próprio processo de globalização em condutas ilícitas que atenta contra a ordem jurídica e a paz social em forma de cibercrimes.

Neste sentido, outra importante decisão do Superior Tribunal de Justiça, assim esclarece quanto a situação de busca e apreensão em tratados e convenções internacionais:

> Deveras, a Convenção das Nações Unidas contra o Crime Organizado Transnacional (Decreto 5.015/2004) também inclui a cooperação judiciária para 'efetuar buscas, apreensões e embargos', 'fornecer informações, elementos de prova e pareceres de peritos', 'fornecer originais ou cópias certificadas de documentos e processos pertinentes, incluindo documentos administrativos, bancários, financeiros ou comerciais e documentos de empresas', 'identificar ou localizar os produtos do crime, bens, instrumentos ou outros elementos para fins probatórios', 'prestar qualquer outro tipo de assistência compatível com o direito interno do Estado Parte requerido' (art. 18, parágrafo 3, letras a até i). Parágrafo 8 do art. 18 da Convenção ressalta que: 'Os Estados Partes não poderão invocar o sigilo bancário para recusar a cooperação judiciária prevista no presente Artigo'.[287]

5.3.2.2.5 Coleta em tempo real de dados e conteúdos informáticos

Os artigos 20 e 21 , da Convenção de Budapeste, em sua versão em idioma Português (Portugal) faz alusão a "Recolha em tempo real de dados informáticos" e "Intercepção de dados relativos ao conteúdo", o que permissa venia, no primeiro caso, para a leitura jurídica que se faz no Brasil, soa o tanto quanto estranho. Daí, parece mais apropriado falar em "Coleta em tempo real de dados informáticos", quanto à primeira providência e a segunda não comporta observações.

A pretensão do dispositivo faz sentido, uma vez que muitas condutas requerem intervenção imediata para que determinada prova seja coligida, captada ou seja, coletada e num sentido mais jurídico apreendida, tanto quanto às informações que se referem ao tráfego, quanto ao conteúdo. A exigência que se faz com os dispostivos é que ocorram inserções no ordenamento jurídico de legislação que faça a previsão destas medidas.

Um questionamento pode suscitar o imaginário do usuário brasileiro e de outros países, que utilizam serviços disponibilizados por empresas Norte Americanas: uma vez que o s EUA são signatários da Convenção de Budapeste, cuja convenção passou a vigorar a partir de 1 de janeiro de 2007, serviços como o *hotmail, msn, yahoo mail, gmail,*

---

[287] SUPERIOR TRIBUNAL DE JUSTIÇA. **Julgados especiais**. Disponível em: < http://www.jusbrasil.com.br/jurisprudencia/1454634/carta-rogatoria-cr-438-be-2005-0015196-0-stj>. Acesso em 15 abr.2009.

Orkut, entre outros, que são mantidos por empresas situadas nos EUA poderiam sofrer investigação mesmo se encontrando fora dos Estados Unidos? A afirmação é que sim, pois estas empresas sujeitam-se à jurisdição americana que é signatária da Convenção de Budapeste, logo, obrigada estaria a cooperar com possíveis investigações, mesmo que os usuários se encontrem noutro país, uma vez que os computadores empregados como servidores lá estão baseados fisicamente.

Registre-se que no bojo das investigações da Comissão Parlamentar de Inquérito e do Termo de Cooperação que foi celebrado com o Ministério Público Federal, empresas de Telecomunicações e ONGs essas medidas não foram previstas, embora seja plenamente passível de execução. Entretanto, para efeitos da Convenção de Budapeste, estas medidas estão sujeitas às restrições e salvaguardas previstas nos artigos 14 e 15.

5.3.2.3 Competência na Convenção de Budapeste

Em decorrência da própria noção de soberania, estabelece-se o ideal de jurisdição, sendo a competência instituto correlato, ou seja, no interesse público esta faz o Estado titular de competências. A soberania delimita assim, a área de jurisdição de um Estado, fixando, por consequência a sua competência para indicar o foro adequado que deva apreciar e julgar um pleito ou questão.

Para Rezek:

> A generalidade da jurisdição significa que o estado exerce no seu domínio territorial todas as **competências** de ordem legislativa, administrativa e **jurisdicional**. A exclusividade significa que, no exercício de tais **competências**, o estado local não enfrenta a concorrência de qualquer outra soberania. Só ele pode, assim, tomar medidas restritivas contra pessoas, detentor que é do **monopólio do uso legítimo da força pública**.[288] (grifo do autor).

Isto posto, no contexto do direito interncional público, instância onde se efetivam os tratados e convenções, compreende-se a competência como sendo "[...] o conjunto de poderes funcionais conferido a um órgão para a realização das atribuições (ou

[288] REZEK, José Francisco. **Direito Internacional Público**. Belo Horizonte: PUC Minas, 2005. p. 153.

de uma parte das atribuições) da entidade a que pertence [...]"[289], podendo ser interna ou externa. Ou ainda pode a compreendida como sendo a limitação do exercício do poder Jurisdicional. Trata, por isso, das regras que apontam quais situações que serão julgadas pelos órgãos do Poder Judiciário. É, portanto, a "medida e o limite da jurisdição [...]."[290]

Com a exposição desse panorama, os conceitos tradicionais de soberania, e por consequência, jurisdição e competência são mitigados pela nova formatação de cooperação entre os Estados, que em nome de um ideal maior – integração regional, abrem mão de parte de seus poderes tradicionalmente vinculados.

Arrematando esta ideia, Miranda pontifica:

> [...] os tratados internacionais livremente formulados e reconhecidos pelos Estados não implicam uma afronta à sua soberania, na medida em que a vontade soberana do Estado se faz presente na formulação e/ou no momento de sua assinatura. O Estado assumiria, desta forma, suas obrigações internacionais de forma voluntária, submetendo-se ao Direito Internacional em função da sua vontade soberana própria. No entanto, o exercício dessa vontade soberana está sujeito às determinações constitucionais de cada país, de um lado, e à aprovação/referendo dos acordos e tratados internacionais por parte do Parlamento nacional, de outro.[291]

Desta forma, o art. 22 da Convenção de Budapeste estabelece a necessidade de que parte dos Estados adotem medidas para que as regras de competência sejam tratadas no direito interno em relação às infrações constantes nos artigos 2º a 11, da Convenção, quando esta for cometidas nos seguintes locais:

> a) No seu território; ou
> b) A bordo de um navio arvorando o pavilhão dessa Parte;
> c) A bordo de uma aeronave matriculada nessa Parte e segundo as suas Leis; ou
> d) Por um dos seus cidadãos nacionais, se a infracção for punível criminalmente onde foi cometida ou se a infracção não for da competência territorial de nenhum Estado.

As regras gerais para aplicação da competência, no ordenamento jurídico brasileiro são fixadas pelo Código Penal e pelo Código de Processo Penal. Ressalte-se ainda, que a Constituição Federal nos artigos 92 a 126 trata do Poder Judiciário brasileiro, por conseguinte, deliena-lhe sua competência.

---

[289] ALBUQUERQUE, Antonio. **Direito internacional público: resumo**. Lisboa: Universidad Lusófona, 2007.
[290] CAPEZ, Fernando**. Curso de processo penal**. 6a ed. São Paulo: Saraiva, 2001. p. 181.
[291] MIRANDA, Napoleão. **Globalização, soberania nacional e direito internacional**. R. CEJ, Brasília, n. 27, out./dez. 2004. p.86. Disponível em: < http://www.cjf.jus.br/revista/numero27/artigo11.pdf>. Acesso em 16 abr.2009.

Os artigos 5º, 6º e 7º do Código Penal brasileiro cuidam das regras sobre territorialidade, lugar do crime e extraterritorialidade. A regra geral é a prevista no art. 5º, que trata do princípio da territorialidade[292] (territorialidade temperada ou moderada, uma vez que faz ressalva aos tratados e convenções de qual o país seja signatário), aplicando-se ao crime cometido no Brasil, a lei penal brasileira.

Quanto ao lugar do crime o Brasil adotou a teoria mista, pura, unitária ou da ubiquidade, conforme dispõe o art. 6º[293], decorrendo que o *locus commissi delict* "[...] tanto pode ser o da ação como o do resultado, ou ainda o lugar do bem jurídico atingido.

Assim, as disposições constantes no art. 7º[294], do Código Penal brasileiro são exceções à regra geral, ou seja, sujeição à lei nacional ainda que o delito seja cometido no estrangeiro.

Ademais, no âmbito processual penal a competência *ratione loci* é estatuída pelo art 70, do Código de Processo Penal e "[...] será, de regra, determinada pelo lugar em que

---

[292] Para Bitencourt estariam ainda a regular a aplicação da lei penal no espaço o princípio real, de defesa ou de proteção; princípio da nacionalidade ou da personalidade; princípio da universalidade ou cosmopolita; princípio da representação ou da bandeira. Estes princípios constituem exceção à regra geral.

[293] O Código Penal brasileiro diz no art.6º:
"Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado."

[294] O Código Penal brasileiro estabelece no art.6º:
Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:
I - os crimes:
a) contra a vida ou a liberdade do Presidente da República;
b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público;
c) contra a administração pública, por quem está a seu serviço;
d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil;
II - os crimes:
a) que, por tratado ou convenção, o Brasil se obrigou a reprimir;
b) praticados por brasileiro;
c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados.
§ 1º - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro.
§ 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições:
a) entrar o agente no território nacional;
b) ser o fato punível também no país em que foi praticado;
c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição;
d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena;
e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.
§ 3º - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior:
a) não foi pedida ou foi negada a extradição;
b) houve requisição do Ministro da Justiça.

se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução."[295]

Isto posto, em face do disciplinamento constante no direito brasileiro, as previsões constantes no art. 22, da Convenção de Budapeste já estariam atendidas, caso a República Federativa do Brasil venha a aderir a este importante instrumento jurídico de direito internacional.

5.3.3 Aspectos inerentes à cooperação penal internacional na Convenção de Budapeste

A sociedade do Século XXI estará cada vez mais dependente das tecnologias da informação e da comunicação, estará cada vez mais conectada à internet, on line no ciberespaço. As relações sociais e comerciais que se estabelecem estarão cada vez mais presentes, gerando, por consequência divisas financeiras, produção de conhecimento e de interação entre as pessoas. Estas mudanças, consequentemente, também tem modificado a dimensão jurídica dos instrumentos utilizados para regular estas situações novas.

Neste sentido, merece registro trecho da minuta do relatório explicativo, da Convenção, que estabelece:

> As novas tecnologias representam um desafio face aos conceitos jurídicos existentes. O fluxo de informações e das comunicações, a nível mundial, é agora substancialmente mais fácil. As fronteiras já não constituem um limite para este fluxo. Cada vez mais, os autores dos crimes encontram-se em locais diferentes daqueles em que os seus actos produzem efeitos. No entanto, as legislações nacionais estão geralmente confinadas a um território específico. Assim sendo, impõe-se que as soluções para problemas que se colocam sejam abordadas por uma legislação internacional, pelo que se requer a adopção de instrumentos jurídicos de âmbito internacional. A presente Convenção propõe-se responder a este desafio, atribuindo o devido respeito aos direitos do Homem no seio da nova Sociedade da Informação.[296]

---

[295] República Federativa do Brasil. Código de Processo Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689Compilado.htm>. Acesso em: 15 abr.2009.
O Código de Processo Penal quanto à questão da competência ainda estabelece nos parágrafos do art. 70:
"§ 1º - Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.
§ 2º - Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.
§ 3º - Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção."

[296] CONSELHO DE MINISTROS DA UNIÃO EUROPÉIA. **Minuta do relatório explicativo**. Disponível em: <https://www.safernet.org.br/drupal/sites/default/files/Relatorio-explicativo-convencao-cibercrime.pdf>. Acesso em: 15 abr.2009.

As práticas danosas à sociedade se revestem das mais variadas formas. Da prática de spam, pedofilia na internet ao ciberterrorismo. Muitas delas já com tratamento legal em muitos países, outras nem tanto. Igualmente ao caráter transversal da internet, as práticas criminosas, do mesmo modo, irradiam-se pelas mais variadas atividades humanas, nas quais exista um computador conectado à internet.

Do mesmo modo que a internet tem possibilidato a partilha de conhecimento em escala global, também tem proporcionado a dispersão de atividades ligadas ao crime organizado, que tem migrado para aproveitar as novas fronteiras estabelecidas pela internet – novas "oportunidades".[297]

Este novo cenário para o cibercrime apresenta características particulares em cada país. Por exemplo, em países como Israel, Estados Unidos e Reino Unido, tem-se uma forte preocupação com questões relativas ao ciberterrorismo. Na Índia e China há preocupações sobre violação de direitos autorais e pirataria. Desta forma, cada Estado apresenta uma particularidade, mas a questão central não é preocupação de um único Estado exclusivamente, pois o problema envolve e coloca em risco a todos.

A resposta mais proeminente para combater o cibercrime, sob uma ótica jurídica, sem dúvidas, aponta para a Convenção de Budapeste sobre o Cibercrime. Representa um esforço múltiplo, que transcende o interesse de um Estado em particular. A convenção é fruto do esforço da União Europeia, conjugados com interesses e necessidades de outros países a exemplo dos Estados Unidos e Japão que resolveram estabelecer num instrumento jurídico internacional os ideais de cooperação penal internacional para combater o cibercrime.

5.3.3.1 Princípios gerais

Os redatores da Convenção de Budapeste incluiram um capítulo específico para tratar das questões relativas à cooperação interncional, no caso, o "Capítulo III". Estabelece assim, de início, três princípio gerais: primeiro, no art. 23, "Princípios gerais relativos à cooperação internacional"; no art. 24, "Princípios relativos à extradição" e nos

[297] Neste sentido Williams entende que "[...] os grupos do crime organizado utilizam a Internet para comunicações (normalmente codificadas) e para qualquer outro propósito quando consideram que seja útil e lucrativo."
WILLIAMS, Phil. **Crime Organizado e Cibercrime: Sinergias, Tendências e Reações**. *In* **Questões globais: coibição do crime internacional**. Publicação do Departamento de Estado dos Estados Unidos. Agosto de 2001, Vol. 6, n.2. p.23.

artigos 25 e 26, trata “Princípios Gerais relativos ao auxílio mútuo” e prestação de “Informações espontâneas”, cabendo, logo, comentários específicos para cada item, em face da complexidade e relevância que cada um deles enseja.

5.3.3.1.1 Princípios gerais relativos à cooperação internacional

A Convenção fixa no art. 23, três princípios gerais que nortearão a cooperação internacional. Como primeiro ponto relevante indica que as partes signatárias do instrumento jurídico internacional cooperarão da forma mais ampla possível aplicando “[...] instrumentos internacionais pertinentes sobre a cooperação internacional em matéria penal, de acordos celebrados com base nas legislações uniformes ou reciprocas, e do seu direito nacional [...].” A ideia desta disposição é viabilizar, com agilidade, a prestação de informações, coleta de provas e outras ações no combate ao cibercrime, com esforço comum, em nível internacional.

Como segundo suporte, direciona a atenção do esforço conjunto para as infrações previstas na Convenção como delito ou crime informático, no caso, cibercrimes, incluindo-se, neste rol, a coleta de provas em relação a tais práticas criminosas que atentes contra os sistemas ou os dados, conforme previsto no art. 14, parágrafo 2, alíneas “a” e “b” (que está relacionada às infrações previstas nos artigos 2º ao 11, da Convenção).

O terceiro parâmetro irá indicar que a previsão de aplicação dos instrumentos jurídicos internacionais de cooperação internacional em matéria penal não excluem ou anulam disposições constantes em outros tratados e convenções de que o Estado signatário seja parte, notadamente os de assistência jurídica mútua e de extradição, bem como as disposições constantes no direito nacional que regulem aspectos específicos da cooperação internacional.

5.3.3.1.2 Princípios relativos à extradição

A utilização do instituto jurídico denominado extradição não é recente em termos de cooperação jurídica internacional. A globalização de muitas atividades humanas, notadamente do comércio que ganhou novos contornos com a internet, o que se reveste de inúmeras conquistas (difusão do conhecimento, por exemplo), mas também trouxe, nesta

esteira, a expansão da criminalidade, notadamente a cibernética, cujos prejuízos, apenas de ordem financeira, atingiu a cifra de 1 trilhão de dólares em 2008, segundo relatório da McAfee.[298]

Pontuar um conceito para a extradição, faz-se imprescindível, assim para Rezek:

> É a entrega, por um Estado a outro, e a pedido deste, de pessoa que em seu território deva responder a processo penal ou cumprir pena. Cuida-se de uma relação executiva, com envolvimento judiciário de ambos os lados: o governo requerente da extradição só toma essa iniciativa em razão da existência do processo penal – findo ou em curso – ante sua Justiça; e o governo do Estado requerido [...] não goza, em geral, de uma prerrogativa de decidir sobre o atendimento do pedido senão depois de um pronunciamento da Justiça local.[299]

Desta forma, estabelece-se a extradição como instrumento de cooperação jurídica internacional, num esforço que envolve o Poder Executivo e Judiciário dos Estados, objetivando evitar que criminosos fiquem impunes à justiça à medida que empreendam fuga e passem a esconder-se, vivendo clandestinamente (até mesmo cometendo outros delitos) fora do território onde praticaram os crimes ou ainda, no caso dos cibercrimes, mesmo os cometa à distância.

Na Convenção de Budapeste a extradição é tratada no art. 25 e seus itens de 1 a 7. Quanto à sua aplicação, entre as partes, de acordo com o item 1, nas infrações previstas nos artigos 2o ao 11o, é necessário que a infração seja punida pela legislação dos dois Estados. Exige-se ainda que a pena máxima, seja privativa de liberdade, de pelo menos um ano, se as penas forem diferentes será aplicada a prevista no tratado ou acordo (que não a Convenção de Budapeste). Desta forma, a determinação se a prática delituosa acarretará ou não a extradição dependerá do período máximo da pena aplicada à infração, que é o foco do pedido de extradição.

A Convenção cuida ainda, de forma especial, da aplicação da extradição em relação aos delitos previstos no item 1, do art. 24, determinando que tais infrações sejam passíveis de extradição em qualquer tratado de extradição existente ou que venha a ser firmado entre as partes.

No item 3, do art.24, a Convenção estabelece que quando uma parte condicionar uma extradição à existência de um tratado não firmado entre as partes, a parte

---

[298] FRANK, John B. ***$1 Trillion Lost to Cybercrime...Can Hackers Bail US Out?***. Disponível em: <http://pindebit.blogspot.com/2009/02/1-trillion-lost-to-cybercrimecan.html>. Acesso em: 15 abr.2009.

[299] REZEK, Francisco. **Direito Internacional Público: curso elementar**."10. ed ver. E atual. – São Paulo: Saraiva, 2005. p. 263.

requerida (que detém a guarda do detido), a Convenção de Budapeste poderá ser considerada como base jurídica para a extradição, a qualquer conduta prevista no art. 24, item I. E em caso de inexistência de condicionamento da extradição em tratado entre as partes, estas ficam obrigadas a incuir em seu ordenamento que as infrações constantes no art. 24, item 1 são passíveis de extradição, como prevê o art. 24, item 4.

O item 5, do art. 24, determina que a parte requerida não está obrigada a efetivar a extradição, se considerar que os termos previstos em tratado ou legislação aplicável não tenham sido satisfeitos. "Trata-se, pois, de mais um exemplo do princípio segundo qual a cooperação internacional deverá ser levada a cabo em conformidade com os termos dos instrumentos internacionais aplicáveis e em vigor entre as partes, os acordos recíprocos existentes ou a legislação adotada em nível nacional."

O item 6 cuida da possibilidade de recusa da extradição de seus nacionais, por parte de determinado Estado. Imagine-se a hipótese de que dois Estados "A" e "B", signatários da Convenção e um deles envie para a outra parte um pedido de extradição, e o Estado requerido negue o pedido alegando que não faz extradição de um nacional ou que o estado requerido também se acha competente no litígio. Qual a solução que prevê a Convenção de Budapeste para esta hipótese? A solução que prevê a Convenção é que o Estado requerente solicite a abertura de um processo criminal para apurar a infração cometida pela pessoa, que pretendia ver extraditada, para que o mesmo não fique impune apenas pelo fato de ser um nacional.

Em face da relevância e pertinência do tema, o Supremo Tribunal Federal do Brasil, tem assim se pronunciado:

> O brasileiro nato, quaisquer que sejam as circunstâncias e a natureza do delito, não pode ser extraditado, pelo Brasil, a pedido de Governo estrangeiro, pois a Constituição da República, em cláusula que não comporta exceção, impede, em caráter absoluto, a efetivação da entrega extradicional daquele que é titular, seja pelo critério do *jus soli*, seja pelo critério do *jus sanguinis*, de nacionalidade brasileira primária ou originária. Esse privilégio constitucional, que beneficia, sem exceção, o brasileiro nato (CF, art. 5º, LI), não se descaracteriza pelo fato de o Estado estrangeiro, por lei própria, haver-lhe reconhecido a condição de titular de nacionalidade originária pertinente a esse mesmo Estado (CF, art. 12, § 4º, II, *a*). Se a extradição não puder ser concedida, por inadmissível, em face de a pessoa reclamada ostentar a condição de brasileira nata, legitimar-se-á a possibilidade de o Estado brasileiro, mediante aplicação extraterritorial de sua própria lei penal (CP, art. 7º, II, *b*, e respectivo § 2º) — e considerando, ainda, o que dispõe o Tratado de Extradição Brasil/Portugal (Artigo IV) —, fazer instaurar, perante órgão judiciário nacional competente (CPP, art. 88), a concernente *persecutio criminis*, em ordem a impedir,

> por razões de caráter ético-jurídico, que práticas delituosas, supostamente cometidas, no exterior, por brasileiros (natos ou naturalizados), fiquem impunes.[300] (grifo nosso).

De acordo com Tuma Júnior[301] o Brasil até dezembro de 2008 tinha 23 tratados bilaterais de extradição, com os seguintes países: Argentina, Austrália, Bélgica, Bolívia, Chile, Colômbia, Equador, Espanha, Estados Unidos da América, França, Itália, Lituânia, México, Paraguai, Portugal, Reino Unido da Grã-Bretanha e Irlanda do Norte, República da Coreia, Romênia, Rússia, Suíça, Ucrânia, Uruguai e Venezuela. Quanto aos tratados multilaterais estão em vigor Mercosul – só Estados Parte –, Mercosul, Bolívia e Chile, além da Convenção das Nações Unidas contra o Crime Organizado Transnacional, conhecida como Convenção de Palermo.

Como se vê, embora a questão da extradição aparente ser um óbice à implementação da Convenção de Budapeste, mas esta, em seu próprio conteúdo, dá solução jurídica ao principal obstáculo, que é a extradição de nacionais. Esta solução é aplicável ao caso brasileiro, uma vez que não permitiria que um cidadão brasileiro cometesse atos criminosos, e valendo-se da condição deixasse de responder por suas condutas.

5.3.3.1.3 Princípios Gerais relativos ao auxílio mútuo

O auxílio mútuo em matéria de direito internacional, como o próprio nome designa, representa ajuda importante na conjugação de forças para combater a cibercriminalidade, o que se consubstancia, na verdade, em ajuda recíproca, como a própria Convençção de Budapeste denota no art. 25.

Prevê assim, neste dispositivo, que os Estados partes (signatários da Convenção), possam colaborar da forma mais ampla possível, principalmente nas investigações e procedimentos que envolvam os crimes relativos aos sistemas e dados informáticos e ainda na fase de coleta de provas da investigação criminal, prevendo também, que caso das disposições constantes nos artigos 27 a 35, da Convenção, estas sejam estabelecidas na legislação nacional (conforme consta nos itens 1 e 2 do art. 25).

---

[300] BRASIL. Supremo Tribunal Federal. **Julgados especiais**. Disponível em: <http://www.stf.jus.br>. Acesso em 20 abr. 2009.

[301] TUMA JÚNIOR, Romeu. **Extradição, extensão, princípios e acordos internacionais**. Revista eletrônica DireitoNet. Disponível em: <http://www.direitonet.com.br/artigos/exibir/4727/Extradicao-conceito-extensao-principios-e-acordos-internacionais>. Acesso em: 15 abr.2009.

A Convenção em seu item 3 estabelece que, em caso de urgência, os pedidos de auxílio múto entre seus signatários possa ser viabilizada por meio da fax ou mensagem eletrônica (e-mail), oferecidas as condições de segurança e autenticidade, com posterior confirmação oficial se o Estado requerido exigir.

Esta preocupação decorre da própria volatilidade das informações constantes em sistemas informáticos, onde a simples execução de um programa ou ação do infrator pode inviabilizar a coleta de provas de forma segura e rápida, o que pode provocar prejuízos à investigação. Daí a necessidade de que tais providências se processem da forma mais célere possível.

Ressalte-se, contudo, que a assitência mútua, conforme disposições do item 4, está sujeita aos termos e condições estabelecidos pelas legislações internas e pelos tratados de assistência mútua que forem aplicáveis, com a previsão, consequente, de salvaguardas (referente aos direitos das pessoas que esteja no território do Estado requerido). Estas disposições do item 4 não serão aplicáveis em caso de existência de indicações expressas em contrário, constantes nas disposições da Convenção, relativas à cooperação internacional.

Outra previsão constante no art. 25, em seu intem 5, refere-se à hipótese de subordinação ao auxílio mútuo à dupla incriminação. Pode acontecer que determinada conduta criminosa, prevista na Convenção, tenha previsão no ordemanento jurídico de dois Estados partes, que pretendam efetivar assistência mútua, mas estas disposições são tratadas no direito interno, de ambas, com denominações terminológicas difentes (por exemplo uma conduta ser descrita no Brasil como "pedofilia infantil na Internet" e em Portugal "exploração sexual infantil na internet"), neste caso, a previsão da Convenção de Budapeste é que as diferenças de ordem técnica não constituam impedimento à prestação da assistência mútua.

Em muitos procedimentos investigativos órgãos policiais produzem muito mais informações do que previamente poderia ser dimensionado. Nestes casos, informações relevantes, mas que não integram o alvo da investigação principal, acabam por originar outro procedimento de investigação.

Ocorre também, com os novos fenômenos criminais, com caráter transnacional, que investigações iniciadas num determinado país, sobre fato específico, possa gerar desdobramentos de registros criminais em outros, que não seja de interesse precípuo, do Estado que iniciou a investigação.

Deste modo, a previsão que faz o art. 26, da Convenção de Budapeste, é possibilitar que, respeitadas as limitações referentes ao direito interno, e sem que seja

formulado pedido prévio, uma parte signatária da Convenção informe a outra parte, da existência de informações que possam ser relevantes noutra investigação da parte destinatária.

Este tipo de procedimento é comum, e já se aplicava mesmo antes da Convenção de Budapeste. Há registros de operações da Polícia Federal brasileira que, nos trabalhos de investigação de determinado crime no Brasil, foi possível remeter informações a países europeus que viabilizaram aprofundamento investigativo.

O ideal de cooperação internacional, visando o combate aos crimes cibernéticos e também ao crime organizado não pode limitar-se às questões e embaraços de ordem burocrática, desde que não possam provocar violação aos direitos fundamentais, o que se presume, notadamente pela exigência de confidencialidade que as investigações ensejam e assim prevê o item 2, do art. 26, da Convenção.

5.3.3.1.4 Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis

O artigo 27, da Convenção de Budapeste, trata dos "Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis." A pretensão do dispositivo, em termos práticos, é viabilizar a cooperação internacional mediante auxílio mútuo, tendo como instrumento a própria Convenção. Esta é a hipótese suscitada caso Estado requerente e Estado requerido não sejam signatário de tratado, convenção ou outro acordo comum.

Desta forma, o art. 27 da Convenção indica que serão aplicáveis o disposto nos seus itens de 1 a 9 deste artigo, que prevêm, sinteticamente: designação de uma ou mais autoridades que se encarreguem de gerenciar as respostas, recebimento e envio de pedidos de auxílios mútuos, bem como sua execução ou transmissão à autoridade competente para sua execução; execução dos pedidos de auxílios mútuos, conforme especificado pela Parte requerente; estabelecimento das condições de recusa, de acordo com o constante no art. 25, item 4; estabelecimento de possibilidade de adiamento para cumprimento de um pedido, para evitar prejuízos a investigações em curso; estabelecimento de procedimento de comunicar à Parte requerente sobre a recepção ou recusa do pedido de auxílío mútuo; fixação de regras de confidencialidade de fatos e objetos constantes nos pedidos de auxílio mútuo; possibilidade de remessa, por parte de autoridades judiciárias (em caso de urgência) da Parte requerente, com

remessa de cópia à autoridade central que gerencia os auxílios mútuos no Estado parte e estabelece ainda a possibilidade de que pedidos de auxílios mútuos possam se processar através da Interpol.

O art. 28, da Convenção de Budapeste encerra a seção I, tratando da confidencialidade e da restrição de utilização. Neste caso, em face do caráter sigiloso que as investigações estão sujeitas, os signatários de um acordo de auxílio mútuo, pode requerer que o caráter confidencia do pedido, devendo a Parte requerida da possibilidade ou não, do cumprimento da solicitação.

5.3.3.2 Disposições específicas

5.3.3.2.1 Auxílio mútuo em matéria de medidas provisórias

Em face da volatilidade de dados constantes em sistemas informáticos, a Convenção prevê em seu art. 29, a instituição de medidas em âmbito internacional equivalentes ao disposto no art. 15. Deste modo, medidas de proteção dos dados, faz-se imprescindíveis, para evitar que ocorram alteração, remoção ou eliminação de dados antes, no curso e após uma investigação. As partes signatárias do auxílio mútuo devem, portanto, ter a capacidade jurídica para proporcionar a preservação confiável no terriório da parte requerida.

Ademais, as disposições do art. 29, ensejam ainda a previsão das informações que devam constar no pedido de auxílio mútuo, como requisitos para requisição de preservação expedita de dados informáticos, bem como medidas que o Estado requerido deva proceder, possibilidades de recusa e instrução em caso de dupla incriminação, bem como as situações relativas aos prazos de conservação dos dados (prazo não inferior a 60 dias) e possibilidade de acesso (inclusive remoto), busca e apreensão.

O art. 30 da Convenção prevê medida equivalente ao disposto no art. 17, mas neste caso, a providência prevista é em âmbito internacional. Desta forma, a minuta do relatório explicativo da Convenção detalha:

> Frequentemente, e mediante solicitação de uma Parte no território da qual foi cometida uma infração, a Parte requerida irá proceder à preservação dos dados de tráfego relativos a uma comunicação transmitida através dos seus computadores, a

> fim de detectar a origem da comunicação e identificar o autor da infracção ou localizar provas decisivas.[302]

Em termos objetivos, um usuário ao fazer uso da internet pode acessar informações simultâneas (várias imagens de cenas de sexo numa única página, por exemplo), que se encontram hospedadas ou armazenadas em diferentes computadores, consequentemente, em diferentes Estados (diferentes jurisdições). Decorre daí, o estabelecimento pela Convenção, de que a "[...] Parte requerida obrigar-se-á a fornecer à parte requerente, nos mais breves prazos, os dados de tráfego suficientes para permitir a identificação do fornecedor de serviços no outro Estado [...]."[303]

Para ilustrar tal questão, importante trazer à colação, julgado do Superior Tribunal de Justiça (Brasil), sobre uma página na internet que, em tese, incitava o consumo de substância entorpecente (*Cannabis sativa,* maconha):

> Como se viu do relatório, o fato foi trazido a lume por meio eletrônico – isto é, de endereço na internet no qual se encotram instruções sobre "como plantar maconha". Confiramos o pronunciamento do Ministério Público paranaense (pronunciando-se pela competência federal):
> 'No entanto, em se tratando de crime praticado por meio eletrônico, é de notório conhecimento a grande dificuldade em se identificar seus autores, vez que muitos domínios utilizados para tais práticas delituosas estão localizados no exterior, como no caso dos autos, dificultando a individualização e identificação de seu responsável. [...]
> Ademais, é impossível se afirmar, a priori , em qual localidade específica do vasto território nacional estaria localizado o computador do qual partiram as informações reputadas incitações ao crime. Portanto, não seria razoável que a autoridade policial do estado do Paraná efetuasse diligências no sentido de localizar, junto a órgãos estrangeiros, informações sobre crime que poderia ter ocorrido em São Paulo, Alagoas, Amazonas, Rio Grande do Sul, etc.
> Também, cabe ressaltar que tal endereço eletrônico, até a presente data, continua em pleno funcionamento, incitando tal prática delituosa por todo o território nacional.
> Por fim, como bem ressaltou a autoridade policial no verso de fls. 40, o fato tem repercussão internacional, eis que o hospedeiro do endereço eletrônico em questão tem sede nos Estados Unidos da América.'
> As informações são, pois, no sentido de hospedeiro fora do âmbito nacional – hipoteticamente, na Califórnia. Malgrado tal acontecimento – se verdadeiro –, o fato repercutiu mesmo foi no território nacional – repitamos: "... em qual localidade específica do vasto território nacional estaria localizado o computador do qual partiram as informações reputadas incitações ao crime. 'Destarte, o meu entendimento é o de que se cuida de ação de incitar restrita ao território nacional, daí não virem à colação os incisos IV e V do art. 109 da Constituição: de um lado, por que não se trata de infração em detrimento de bens, serviços ou interesses da União; de outro, porque a eventual ação de incitar ocorreu internamente.
> Voto pela competência estadual – do Juízo de Direito da Vara de Inquéritos Policiais de Curitiba (o suscitante).[304]

---

[302] CONVENTION ON CYBERCRIME – EXPLANATORY REPORT (ETS NO 185), op. cit. n. 253
[303] CONVENTION ON CYBERCRIME, op. cit. n. 253
[304] BRASIL. Conselho de Justiça Federal. **Incitação pela internet ao plantio de maconha é competência da Justiça Estadual**. Disponível em:

A decisão do Superior Tribunal de Justiça (STJ) decidiu conflito negativo de competência que se instalou entre a justiça comum estadual do Paraná e a justiça federal, tendo o STJ firmado entendimento, neste caso, de que a competência seria da justiça comum estadual.

Como se vê, pessoa não identificada (num Estado A), criou página fazendo apologia às drogas e a hospedou em servidor Norte Americano, cujos atos decorrentes de tal conduta, incidem sobre usuários brasileiros, indistintamente, além de outras pessoas de países diversos que acessaram o referido site.

A convenção possibilitaria (se o Brasil fosse signatário da Convenção de Budapeste) que os EUA prestassem auxílio mútuo no sentido de viabilizar a disponibilização das informações referentes aos dados e ao tráfego, com vistas a identificar o possível ou possíveis infratores.

5.3.3.2.2 Auxílio mútuo relativamente a poderes de investigação

Na hipótese explicitada quanto à apologia ao consumo de drogas, vê-se tratar de conduta transfronteiriça, que tem característica muito comum a outras práticas que a própria Convenção estabelece.

A solução que a Convenção preceitua, para viabilizar as investigações encontra respaldo jurídico no seu art. 31, que estabelece como preceito geral:

> Artigo 31º - Auxílio mútuo relativamente ao acesso a dados informáticos armazenados
> 1. Uma Parte pode pedir a outra Parte para investigar ou aceder de forma semelhante, apreender, ou obter de forma semelhante, e divulgar dados armazenados por meio de sistema informático que se encontre no território dessa outra Parte, incluindo os dados conservados em conformidade com o artigo 29º.
> 2. A Parte requerida dará satisfação ao pedido aplicando os instrumentos internacionais, acordos e legislação referida no artigo 23º, e dando cumprimento às disposições pertinentes do presente Capítulo.
> 3. O pedido deve ser satisfeito o mais rapidamente possível nos casos em que:
> a) Existam motivos para crer que os dados relevantes são especialmente vulneráveis à perda ou modificação; ou

---

<http://www.direito2.com.br/cjf/2006/out/17/incitacao_pela_internet_ao_plantio_de_maconha_e_competencia>. Acesso em: 16 abr.2009.

> b) Os instrumentos, acordos e legislação referida no n.º 2 prevejam uma cooperação rápida.[305]

Outras disposições constantes no art. 32, da Convenção, reforçam os poderes investigativos, quando possibilitam, juridicamente, que os Estados signatários, mediante autorização, tenham acesso remoto e possam coletar (inclusive em tempo real – art. 33, da Convenção) os dados informáticos que estejam armazenados e que sejam de domínio público. Estas medidas aplicam-se tanto às informações de dados de tráfego – art. 33, quanto aos dados informáticos de conteúdo, como fixa o art. 34, da Convenção.

5.3.3.2.3 Rede 24/7

A operacionalização de uma grande estrutura para combater o cibercrime e dar suporte técnico às demandas dos países signatários da Convenção de Budapeste, como medida de cooperação internacional, requer a instalação de um escritório ou rede 24/7[306], que se constitui numa grande central de suporte e apoio, que funciona 24 horas, sede dias por semana.

A previsão legal para a central 24/7 é fixada pela Convenção no art. 35, que estabelece:

> O auxílio incluirá a facilitação, ou se o direito e práticas internas o permitirem, a aplicação directa das seguintes medidas:
> a) A prestação de aconselhamento técnico;
> b) A conservação de dados em conformidade com os artigos 29º e 30º; e
> c) A recolha de provas, informações de carácter jurídico e localização de suspeitos.[307]

Não há registro que o Brasil disponha de uma estrutura pública funcionando nos parâmetros de uma rede 24/7, mas já é disponível uma Central de Combate aos Crimes

[305] CONVENÇÃO DE BUDAPESTE, op. cit. n. 253.
[306] 24 / 7 é uma sigla que significa "24 horas por dia, 7 dias por semana", geralmente se referindo a um serviço disponível sem interrupção. "O primeiro uso conhecido do termo é atribuído ao jogador basquete Jerry Reynolds, que em 1983, descreveu o seu salto baleado como sendo "boas 24 horas por dia, sete dias por semana, 365 dias por ano." Informação disponível em: < http://en.wikipedia.org/wiki/24/7>. Acesso em: 17 abr.2009.
Texto original: "*The first known use of the term is attributed to basketball player Jerry Reynolds, who in 1983 described his jump shot as being "good 24 hours a day, seven days a week, 365 days a year".* (tradução nossa).
[307] CONVENÇÃO DE BUDAPESTE, op. cit. n. 253.

Cibernéticos, no Departamento de Polícia Federal, bem como a manutenção de um serviço de denúncias on line, mantido pela ONG Safernet,[308] que recebe, mantém acompanhamento estatístico e jurídico de denúncias de pedofilia na internet.

5.3.4 Salvaguardas, reservas e Protocolo Adicional à Convenção de Budapeste

Em face da dificuldade de se construir um consenso global, foram estabelecidas na Convenção de Budapeste salvaguardas e reservas, de forma a possibilitar a assinatura e ratificação mais facilitada das partes na Convenção e da adesão de outros Estados, nos termos que ela estabelece.

Deste modo, as salvaguardas são fixadas no art. 15, de Convenção, que preceitua:

> 1. Cada Parte assegurará que o estabelecimento, a entrada em vigor e a aplicação dos poderes e procedimentos previstos na presente Secção são sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma protecção adequada dos direitos do Homem e das liberdades, designadamente estabelecidas em conformidade com as obrigações decorrentes da aplicação da Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos (1950), do Pacto Internacional das Nações Unidas sobre os Direitos Civis e Políticos, (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos Direitos do Homem e que deve integrar o princípio da proporcionalidade.
> 2. Quando for apropriado, tendo em conta a natureza do poder ou do procedimento em questão, as referidas condições e salvaguardas incluirão, designadamente, um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a limitação do âmbito de aplicação e a duração do poder ou procedimento em causa.
> 3. Na medida em que seja do interesse público, em particular da boa administração da justiça, cada Parte examinará o efeito dos poderes e dos procedimentos da presente Secção sobre os direitos, responsabilidades e interesses legítimos de terceiros.[309]

---

[308] "A **SaferNet** Brasil é uma organização não governamental, sem fins lucrativos, que reúne cientistas da computação, professores, pesquisadores e bacharéis em Direito com a missão de defender e promover os Direitos Humanos na Internet. Ela atua recebendo denúncias de crimes cibernéticos no Brasil. É um sítio que congrega as notícias sobre estes crimes, seu combate e as sentenças, disponibilizando publicamente a legislação existente sobre crimes de informática, além de receber denúncias on-line. É voltada basicamente para luta contra a pedofilia e todas as formas de racismo em sítios brasileiros ou feitos por brasileiros ou voltados para o Brasil em qualquer provedor estrangeiro.
Através da Central Nacional de Denúncias de Crimes Cibernéticos, operada em parceria com o Ministério Público Federal, oferece à sociedade brasileira e a comunidade internacional um serviço anônimo de recebimento, processamento, encaminhamento e acompanhamento on-line de denúncias sobre qualquer crime ou violação aos Direitos Humanos praticado através da Internet."
Iformação disponível em: < http://pt.wikipedia.org/wiki/SaferNet>. Acesso em: 17 abr.2009.

[309] CONVENTION ON CYBERCRIME, op. cit. n. 253

Merece registro assim, a menção de que as salvaguardas devem assegurar uma adequada proteção das liberdade e direitos fundamentais, bem como do Pacto Internacional das Nações Unidas sobre Direitos Civis e Políticos. Em face da necessidade de harmonização com o direito nacional, o art. 42 da Convenção prevê a possibilidade do Estado "[...] no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar a sua intenção de fazer uso de reserva."[310]

Em face da necessidade de adequação da Convenção, bem como estabelecer tratamento uniforme de combate aos cibercrimes em todas as suas formas, notadamente as condutas criminosas de racismo e xenofobia que cresceu na rede, em 1 de março de 2006 passou a vigorar o Protocolo Adicional à Convenção, que visa "criminalizar a divulgação de material racista e xenófobo, através de sistemas informáticos, bem como dos comportamentos racistas e xenófobos-motivados, ameaças e insultos."[311]

5.4 Tribunal Penal Internacional e cibercrimes: competência e possibilidades de punição

As Tecnologias da Informação e da Comunicação (TICs) são uma das principais variáveis a caracterizar a Sociedade da Informação, aqui compreendida, na mesma dimensão, como sociedade global ou sociedade da Era da Informação. Estas denominações irão remeter as possíveis análises que se possa fazer, aos aspectos de conectividade global, de zonas de influência econômica multipolar e das demais características que se agregam ao ideal de pós-modernismo.

Este avanço significa, sob uma viés sócio-econômico e cultural, na geração de inúmeras possibilidades para pessoas que antes se encontravam limitadas a uma esfera de desenvolvimento voltado ao seu Estado em si. O novo panorama que se firmou, ao menos em tese, é capaz de propiciar, mais do que em qualquer outro momento da história, oportunidades

---

[310] O art. 42 da Convenção de Budapeste estabelece:
"Artigo 42º - Reservas
Qualquer Estado pode, mediante notificação por escrito dirigida ao Secretário Geral do Conselho da Europa no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar a sua intenção de fazer uso da(s) reserva(s) previstas nos artigos 4º, n.º 2, 6º, n.º 3, 9º, n.º 4, 10º, n.º 3, 11º, n.º 3, 14º, n.º 3, 22º, n.º 2, 29º, n.º 4, e 41, n.º 1.
Nenhuma outra reserva poderá ser formulada."

[311] WIKIPÉDIA. **Convention on Cybercrime**. Disponível em: <http://en.wikipedia.org/wiki/Convention_on_Cybercrime>. Acesso em: 22 abr.2009.

para todos. Para todos aqueles que têm um maior grau de escolaridade e consequente capacitação profissional

No sentido em que caminhou a humanidade, nos últimos vinte anos (tendo a queda do Muro de Berlim como referencial), para esse ideal de liberdade (possibilidades de explorar o mundo pela grande rede) e de desenvolvimento (geração de riquezas), como teorizou Amartya Sen outros riscos passaram a ser mais evidentes. Não mais o risco de uma 3ª Guerra Mundial patrocinada por grandes potências nucleares (EUA x Ex- URSS), mas os riscos e danos possíveis de serem previstos a partir do avanço do cibercrime, como espécie ou sustentáculo das ações que dão suporte ao crime organizado internacional.

A previsão de cenários tão desastrosos foi posta pelo próprio cinema, enquanto expressão da arte, há quase três décadas com o filme WarGames (1983) que expôs, como ficção, o risco de uma guerra nuclear entre as grandes potências da época (EUA x URSS) à partir de uma invasão dos computadores do sistema de defesa Norte Americano por um *hacker*, que viria a desencadearia um alerta global.

Da ficção par a realidade, há ameaças globais que são conexas ao cibercrime como gênero e o ciberterrorismo (neoterrorismo), ciberataques e o racismo e xenofobia *on line* como espécies. O medo do terro em escala transnacional foi ampliado pelos acontecimentos que se registraram com o tenebroso 11 de setembro de 2001, com o ataque ao World Trade Center em Nova Iorque, EUA. Foram reforçadas com outras ações terroristas espalhadas pelo mundo (como o ataque ao metrô de Madrid, em 2004,) cujas imagens são disponibilizadas on line para qualquer cidadão no acessar no *youtube,*[312] como propaganda de guerra ou do terror.

Na presente abordagem em relação ao Tribunal Penal Internacional, far-se-á uma análise quanto aos atos de ciberterrorismo, merecendo, portanto, por questões doutrinárias uma abordagem preliminar sobre terrorismo..

Segundo Feliciano:

> Embora deite raízes na Revolução Francesa e no Terror jacobino, o *terrorismo*, tal como o conhecemos, pode ser considerado um fenômeno moderno, característico do século XX. Mas foi o século XXI a testemunhar o mais letal ataque terrorista de todos os tempos, a saber, a destruição das torres do *World Trade Center*, consumada no fatídico dia 11 de setembro de 2001. Tornou-se, desafortunadamente, um marco negativo na Históriada Humanidade — a ponto de se difundir, desde então, o emprego da expressão ″pós-Onze de Setembro″ para designar fenômenos muito recentes da pós-modernidade. Mas não bastou. Ao ″Onze de Setembro″ seguiram-se outros atentados com igual alarido internacional, como o ″Onze de Março″, no

[312] O *youtube* é um site na internet onde o usuário pode disponibilizar ou assistir vídeos *on line*.

> metropolitano de Madrid (11.03.2004), [...] e os atentados na Inglaterra (Londres, 07.07.2005 e 21.07.2005) e no Egito (Sharm el-Sheik e Naama Bay, 23.07.2005).[313]

Como instrumentos jurídicos que tratam do terrorismo, podem ser exemplificados: a 4ªConvenção de Genebra sobre a proteção de civis em tempo de guerra (12.08.1949, art. 33), as Convenções de Tóquio (1963), Haia (1970) e Montreal (1971). Ações correlatas como a tomada ilícita de aeronaves, a Convenção para prevenir e punir atos de terrorismo configurados em delitos contra pessoas e extorsão conexa (Organização dos Estados Americanos — Washington, 1971), a Convenção européia para a repressão do terrorismo (Comitê de Ministros do Conselho da Europa, 1976) e o Tratado da União Européia que, no Título VI (*"Disposições relativas à cooperação policial e judiciária em matéria penal"*) inclui o terrorismo.

No Brasil, a temática encontra contornos jurídicos que são delineados na Constituição Federal, que considera o terrorismo um crime inafiançável, insuscetível de graça ou anistia (artigo 5º, XLIII, Constituição da República Federativa do Brasil).

No plano infraconstitucional o delito é previsto no art. 20, da Lei 7.170, de 14.12.1983 (Lei de Segurança Nacional), que estabelece:

> Devastar, saquear, extorquir, roubar, seqüestrar, manter em cárcere privadeo, incendiar, depredar, provocar explosão, praticar atentado pessoal ou atos de terrorismo, por inconformismo político ou para obtenção de fundos destinados à manutenção de organizações políticas clandestinas ou subversivas. Pena — reclusão, de 3 (três) a 10 (dez) anos.[314]

Neste sentido, estabelecer uma definição para terrorismo se apresenta como algo desafiador, em face das inúmeras divergências de ordem doutrinária e legal. Entretanto, em face das várias leituras que o termo enseja, pode se chegar a conclusão de que terrorismo[315] pode ser compreendido como a pratica de quaisquer atos ou ameaças de

---

[313] FELICIANO, Guilherme Guimarães. **Terrorismo: contornos jurídicos para o Direito Penal**. Jus Navigandi, Teresina, ano 9, n. 782, 24 ago. 2005. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=7189>. Acesso em: 20 abr. 2009.

[314] BRASIL. Presidência da República, Casa Civil - Subchefia para Assuntos Jurídicos. Lei nº 7.170, de 14 de DEZEMBRO DE 1983. Define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L7170.htm>. Acesso em: 20 abr.2009.

[315] Ruiz e Almeida sustentam que Assembléia Geral da ONU definiu o terrorismo global como: "atos criminosos com o objetivo de ou calculados para provocar um estado de terror no público geral, um grupo de pessoas ou determinados indivíduos por razões políticas, quaisquer que sejam as considerações de cunho político, filosófico, ideológico, racial, étnico, religioso ou outro que possam ser invocadas para justificá-los."
RUIZ, Fernanda; ALMEIDA, D. Freire. **O julgamento de atos de terrorismo pelo Tribunal Penal Internacional**. Disponível em:

violência que tenha como objetivo provocar o terror e pânico na população civil de uma determinada localidade.

Noutra dimensão, com viés voltado para o enfoque que se pretende abordar, o ciberterrorismo, do mesmo modo, enfrenta grande dificuldade conceito uniforme, pois concorrem para divergências de elementos que integram ou possam constituir um embasamento epistemológico satisfatório.

A abordagem mais citada e enunciadora é de Denning, que diz:

> Ciberterrorismo é a convergência de terrorismo e de ciberespaço. É geralmente entendido como ataques e ameaças de atentado contra computadores, redes de informação e dados nele armazenados quando feito para intimidar ou coagir um governo ou de seu povo em prol de causas ou objetivos políticos ou sociais. Além disso, para ser classificado como ciberterrorismo, deve resultar em um ataque, violência contra pessoas ou bens, ou, pelo menos, causar dano suficiente para gerar medo e que levam à morte ou lesão corporal, como explosão, falha em sistema de navegação de aeronaves, contaminação da água, ou grave perdas econômicas seriam exemplos. Graves ataques contra infra-estruturas críticas poderia ser, dependendo de seu impacto também.[316]

Exposto estes contornos e considerando os aspectos inerentes ao sistema de punição legal, de caráter global, muito controverso, notadamente quanto aos aspectos de extradição, processo e punição de nacionais por outros Estados, seria possível vislumbrar competência do Tribunal Penal Internacional para tais atos? Faz-se imprescindível pois, uma abordagem sintética sobre a competência da Corte Internacional Penal.

A competência do Tribunal Penal Internacional é estabelecida pelo art. 5º, do Estatuto de Roma, que assim enuncia:

> Artigo 5.º Crimes da competência do Tribunal
> 1 - A competência do Tribunal restringir-se-á aos crimes mais graves que afectam a comunidade internacional no seu conjunto. Nos termos do presente Estatuto, o Tribunal terá competência para julgar os seguintes crimes:
> a) O crime de genocídio;
> b) Os crimes contra a Humanidade;
> c) Os crimes de guerra;

<http://bdjur.stj.gov.br/jspui/bitstream/2011/18600/2/O_Julgamento_de_Atos_de_Terrorismo.pdf>. Acesso em: 21 abr.2009.

[316] DENNING, D. ***Cyberterrorism, Testimony before the Special Oversight Panel of Terrorism***. Committee on Armed Services, US House of Representatives, 2000. Disponível em: http://www.cs.georgetown.edu/~denning/infosec/cyberter ror.html>. Acesso em: 19 abr.2009.

Texto original: *Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact*. (tradução nossa).

> d) O crime de agressão.
> 2 - O Tribunal poderá exercer a sua competência em relação ao crime de agressão desde que, nos termos dos artigos 121.º e 123.º, seja aprovada uma disposição em que se defina o crime e se enunciem as condições em que o Tribunal terá competência relativamente a este crime. Tal disposição deve ser compatível com as disposições pertinentes da Carta das Nações Unidas.[317]

Logo, o entendimento de que ações terroristas e neoterroristas (ciberterrorismo) poderiam inserir-se no contexto de competência da Corte Internacional Penal, enseja, de plano, esta análise.

Pugnando pela inadmissibilidade de enquadramento legal para atos terroristas (incluindo aqui os que, em tese, sejam executados por meios informáticos ou telemáticos – ciberterrorismo), Marques argui:

> O direito internacinal criminalizou o terrorismo. Nas Convenções de Genebra é considerado como grave violação, devendo todos os Estados reprimi-los em suas legislações internas, contudo não é um crime de competência do Tribunal Penal Internacional (TPI).[318]

Ressalte-se porém, que a interpretação que se deva emprestar à analise de questão dessa magnitude não se limita a um mero olhar ou interpretação literal das competências originárias do Tribunal Penal Internacional, constantes em seu artigo 5º. Esta visão deve ser alargada, de forma a contemplar atos reflexos que atentam contra a humanidade, contra civis inocentes numa guerra que não tem objetivos, líderes e territórios definidos.

Nesta dimensão, compreendendo o ciberterrorismo como um misto do novo terrorismo (extremista) e dos recursos tecnológicos proporcionados pelos computadores e pela internet, surge a terminologia ciberterrismo – instrumento de alta tecnologia dos grupos organizados que estão a preparar novos ataques. A incerteza sobre onde e quando estes ataques ocorrerão provoca em áreas críticas ou países não alinhados um ambiente de tensão permanente.

O examplo mais emblemático - não foram cenas do filma War Games, ocorreu na Estônia, ex república soviética que aliou-se à OTAN, como bem dispõe Teixeira:

> Nas últimas três semanas, a Estônia, um dos três estados bálticos, sofreu três ondas sucessivas de ataques cibernéticos, interrompendo os serviços de internet e

---

317 **Estatuto de Roma do Tribunal Penal Internacional** (TPI). Disponível em: <http://www.fd.uc.pt/CI/CEE/OI/TPI/Estatuto_Tribunal_Penal_Internacional.htm>. Acesso em: 21 abr.2009.

318 MARQUES, Helvetius. **O terrorista e os direitos humanos**. Disponível em: <http://www.juridicas.unam.mx/sisjur/internac/pdf/10-478s.pdf>. Acesso em: 21 abr.2009.

> imobilizando o governo. O país de 1,4 milhão de habitantes e território com área equivalente à do estado do Rio de Janeiro orgulha-se da eficiência de seu estado on-line, sem a burocracia dos papéis, e de ter realizado as primeiras eleições nacionais pela internet. Com seus serviços eletrônicos abalados pelo ciberataque, a Estônia mergulhou num caos equivalente apenas ao de 1991, quando o colapso da União Soviética permitiu a independência do país. Impossibilitadas de ler e-mails, as autoridades tiveram de recorrer aos velhos aparelhos de fax. Sites de notícias saíram do ar e ninguém conseguia acessar os serviços bancários on-line. Nunca antes um estado havia sofrido um assalto cibernético tão sistemático e devastador. As implicações do ataque fizeram soar o alarme na Europa, e a Otan, a aliança militar do Ocidente, da qual a Estônia faz parte, enviou uma equipe de especialistas para tentar erguer uma barreira de defesa tecnológica e ajudar os estonianos a localizar os responsáveis pelo vandalismo eletrônico. Numa reunião na sexta-feira passada em Samara, na Rússia, o presidente da Comissão Européia advertiu que o bloco poderia sair em defesa da Estônia na guerra pela internet.[319]

O saldo pós ataque cibernético, que poderia ter consequências e desdobramentos imensuráveis foi a instalação de um centro de combate ao cibercrime na Estônia, limite da fronteira entre a União Europeia e a Rússia. O que se especula ou se projeta para um futuro de não mais que cinco anos é uma corrida mais concentrada dos países do ocidente e do oriente em treinar seu ciberexércitos conta as ciberameaças, notadamente as ameaças terroristas perpetradas pelo ciberespaço.

Desta forma, compreende-se como possível e desejável o enquadramento de condutas terroristas no rol de competências do Tribunal Penal Internacional. Há duas possibilidades: uma premente e outra a médio prazo (inclusão do crime de terrorismo no rol de competências do TPI em sede de revisão do Estatudo de Roma).

As ações imediatas devem incluir atos terroristas (inclusive os perpetrados pelo ciberespaço - ciberterrorismo) na compreensão de que são delitos contra a humanidade[320], em face de sua ação específica e sistemática contra alvos civis, mais vulneráveis e incapazes de chance de defesa – o ataque ao World Trade Center, atos terroristas contra o metrô de Madrid, ataques contra edificações das Nações Unidas são exemplos clássicos de atos terroristas que atingem com violência e crueldade a humanidade, logo reclamam intervenção de uma

---

[319] TEIXEIRA, Duda. **Uma guerra pela internet: o maior cibertaque da história tira a Estônia da rede. O suspeito é a Rússia.** Disponível em: <http://www.defesanet.com.br/zz/intel_ciberwar.htm>. Acesso em: 21 br.2009.

[320] Neste mesmo entendimento Ruiz e Andrade teorizam que "[...] em face do caráter internacional apresentado pelo terrorismo, posto que é uma conduta que afeta cidadãos de diferentes países e, em grande parte, tem sua ação realizada em mais de um Estado, acredita-se que, como crime que é, deve ser um delito incluído na competência de uma jurisdição de âmbito internacional e, sobretudo, imparcial, de onde se conclui que tal jurisdição é concretizada e atualmente representada pelo Tribunal Penal Internacional."
RUIZ, Fernanda; ALMEIDA, D. Freira. O julgamento de atos de terrorismo pelo Tribunal Penal Internacional. Disponível em:
<http://bdjur.stj.gov.br/jspui/bitstream/2011/18600/2/O_Julgamento_de_Atos_de_Terrorismo.pdf>. Acesso em: 21 abr.2009.

jurisdição supranacional e de competência do Tribunal Penal Internacional (art. 7º, do Estaturo de Roma).[321]

[321] O Estatuto de Roma estabelece:
Artigo 7.º Crimes contra a Humanidade
1 - Para os efeitos do presente Estatuto, entende-se por «crime contra a Humanidade» qualquer um dos actos seguintes, quando cometido no quadro de um ataque, generalizado ou sistemático, contra qualquer população civil, havendo conhecimento desse ataque:
a) Homicídio;
b) Extermínio;
c) Escravidão;
d) Deportação ou transferência à força de uma população;
e) Prisão ou outra forma de privação da liberdade física grave, em violação das normas fundamentais do direito internacional;
f) Tortura;
g) Violação, escravatura sexual, prostituição forçada, gravidez à força, esterilização à força ou qualquer outra forma de violência no campo sexual de gravidade comparável;
h) Perseguição de um grupo ou colectividade que possa ser identificado, por motivos políticos, raciais, nacionais, étnicos, culturais, religiosos ou de sexo, tal como definido no n.º 3, ou em função de outros critérios universalmente reconhecidos como inaceitáveis em direito internacional, relacionados com qualquer acto referido neste número ou com qualquer crime da competência do Tribunal;
i) Desaparecimento forçado de pessoas;
j) Crime de apartheid;
k) Outros actos desumanos de carácter semelhante que causem intencionalmente grande sofrimento, ferimentos graves ou afectem a saúde mental ou física.
2 - Para efeitos do n.º 1:
a) Por «ataque contra uma população civil» entende-se qualquer conduta que envolva a prática múltipla de actos referidos no n.º 1 contra uma população civil, de acordo com a política de um Estado ou de uma organização de praticar esses actos ou tendo em vista a prossecução dessa política;
b) O «extermínio» compreende a sujeição intencional a condições de vida, tais como a privação do acesso a alimentos ou medicamentos, com vista a causar a destruição de uma parte da população;
c) Por «escravidão» entende-se o exercício, relativamente a uma pessoa, de um poder ou de um conjunto de poderes que traduzam um direito de propriedade sobre uma pessoa, incluindo o exercício desse poder no âmbito do tráfico de pessoas, em particular mulheres e crianças;
d) Por «deportação ou transferência à força de uma população» entende-se a deslocação coactiva de pessoas através da expulsão ou de outro acto coercivo, da zona em que se encontram legalmente, sem qualquer motivo reconhecido em direito internacional;
e) Por «tortura» entende-se o acto por meio do qual uma dor ou sofrimentos graves, físicos ou mentais, são intencionalmente causados a uma pessoa que esteja sob a custódia ou o controlo do arguido; este termo não compreende a dor ou os sofrimentos resultantes unicamente de sanções legais, inerentes a essas sanções ou por elas ocasionadas acidentalmente;
f) Por «gravidez à força» entende-se a privação de liberdade ilegal de uma mulher que foi engravidada à força, com o propósito de alterar a composição étnica de uma população ou de cometer outras violações graves do direito internacional. Esta definição não pode, de modo algum, ser interpretada como afectando as disposições de direito interno relativas à gravidez;
g) Por «perseguição» entende-se a privação intencional e grave de direitos fundamentais em violação do direito internacional por motivos relacionados com a identidade do grupo ou da colectividade em causa;
h) Por «crime de apartheid» entende-se qualquer acto desumano análogo aos referidos no n.º 1, praticado no contexto de um regime institucionalizado de opressão e domínio sistemático de um grupo rácico sobre um ou outros e com a intenção de manter esse regime;
i) Por «desaparecimento forçado de pessoas» entende-se a detenção, a prisão ou o sequestro de pessoas por um Estado ou uma organização política, ou com a autorização, o apoio ou a concordância destes, seguidos de recusa em reconhecer tal estado de privação de liberdade ou a prestar qualquer informação sobre a situação ou localização dessas pessoas, com o propósito de lhes negar a protecção da lei por um longo período de tempo.
3 - Para efeitos do presente Estatuto, entende-se que o termo «sexo» abrange os sexos masculino e feminino, dentro do contexto da sociedade, não lhe devendo ser atribuído qualquer outro significado.

5.5 A ampliação da Convenção de Budapeste: compatibilização dos direitos fundamentais com os termos da Convenção

A força de um instrumento jurídico internacional não subsite apenas às disposições que nele estão contidas. Uma Convenção internacional não tem sentido senão o de propiciar que as nações, irmanadas, possam conjugar esforços no sentido de cooperarem entre si, visando combater um mal que lhes é comum, no caso, o avanço de práticas criminosas que se propagam pela internet e pelo ciberespaço.

Neste sentido, com vistas à maior amplitude possível, há possibilidades que outros Estados juntem-se ao esforço global de combate ao cibercrime. Estas disposições estão contidas na própria Convenção de Budapeste.

Desta forma a Convenção estabelece:

> Artigo 37º - Adesão à Convenção
> 1. Após a entrada em vigor da presente Convenção, o Comité de Ministros do Conselho da Europa pode, depois de ter consultado os Estados contratantes da Convenção e de ter obtido o acordo unânime, convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção. A decisão é tomada pela maioria prevista no artigo 20º, alínea d), dos Estatutos do Conselho da Europa e por unanimidade dos representantes dos Estados contratantes com direito de voto no Comité de Ministros.
> 2. Em relação a qualquer Estado aderente à Convenção, em conformidade com o n.º 1, a Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data do depósito do instrumento de adesão junto do Secretário Geral do Conselho da Europa.

Como se vê, a Convenção está aberta à adesão de outros Estados que não participaram de sua elaboração. Merece ressalva, entretanto, algumas disposições que aparentam obstacular pretensões. Um Estado não pode manifestar o interesse em aderir a Convenção, como se depreende da leitura do dispositivo, terá que ser convidado pelo Comitê de Ministros do Conselho da Europa após a obtenção de acordo unânime e consulta aos demais Estados signatários.

No Brasil há uma pressão muito forte para que o país manifeste interesse em aderir a Convenção, mas como se vê, a manifestação de interesse não é suficiente para que se provoque a adesão e sua inserção no rol de signatários, terá pois, que ser convidado, após a exigência e consulta que o próprio instrumento jurídico prevê.

Para Erdelyi o Ministério das Relações Exteriores do Brasil (Itamaraty):

> [...] ainda não tem posição definida e não descartou totalmente a adesão do Brasil à Convenção de Budapeste – acordo do Conselho Europeu de cooperação e política criminal comum em vigor desde 2004 depois da ratificação com cinco países para o combate aos crimes cibernéticos. [...]
> A ministra Virgínia Bernardes Toniatti, da Coordenação-Geral de Combate aos Ilícitos Transnacionais, do Itamaraty, afirma que a convenção ainda está sob análise e discussão. Segundo Virgínia, do ponto de vista diplomático, não seria bom para o Brasil aderir a uma convenção já que não participou do discussão dos seus termos. 'Nós não participamos das negociações. Não colocamos nossa marca, nossos objetivos e interesses', afirma Virgínia. 'Como pode todos os países terem o mesmo compromisso e não poder fazer reservas no mesmo patamar? Sempre preferimos negociar convenções importantes', conclui a ministra.[322]

A preocupação da Ministra é relevante, uma vez que não é suficiente, primeiro apenas o interesse unilateral do Estado brasileiro, uma vez que a adesão está condicionada a um convite formulado pelo Comitê de Ministros do Conselho da Europa. Segundo ponto, a adesão implica numa série de adequações e estudos preliminares para compatibilizar as leis nacionais em face de institutos contraditórios e não permitidos pela própria Constituição Federal, como é o caso da extradição, embora a Convenção de Budapeste estabeleça a possibilidades de ressalvas pelo Estado parte que ela aderir.

Outra observação diz respeito a um possível conflito entre direitos fundamentais estabelecidos pela Constituição federal, como por exemplo o direito à privacidade e medidas processuais de investigação que podem ser viabilizadas, pois há dispositivos na Convenção que autorizam, por exemplo, no "Artigo 32 - Acesso transfronteiríço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público"[323] e a coleta de informações em tempo real, previstas no art. 33, da Convenção de Budapeste, como medida de auxílio mútuo em cooperação internacional em matéria depenal.

Tais medidas, apenas a título de exemplo, podem implicar também, em confronto, por exemplo com dispositivos constitucionais que tutelam a inviolabilidade das

---

[322] ERDELYI, Maria Fernanda. **Itamaraty ainda estuda adesão à Convenção de Budapeste**. São Paulo: Consultor Jurídico, 2008. Disponível em: <http://s.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste>. Acesso em 22 abr.2009.

[323] O artigo 32, da Convenção de Budapeste, assim enuncia:
Artigo 32º - Acesso transfronteiríço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público
Uma Parte pode, sem autorização de outra Parte:
a) Aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou
b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte,se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático.

comunicações de dados, previstas no art. 5º, XII (cláusula pétrea)[324], cuja violação só pode ser autorizada mediante ordem judicial.

Noutro plano, é inaceitável, do mesmo modo, que o suposto exercício de direitos fundamentais sejam utililizados para mascarar atividades delituosas, como tem se registrado em inúmeras ações policiais já evidenciadas no Brasil, entre vários delitos, como lavagem de dinheiro, formação de quadrilha e prática de atos covardes de pedofilia envolvendo crianças e adolescentes, como ficou demonstrado na Comissão Parlamentar de Inquérito da Pedofilia.

Observe-se assim, que é perfeitamente possível o estabelecimento de salvaguardas e reservas quanto aos principais pontos que possam suscitar controvérias. A adesão à Convenção possibilita este mecanismo de forma a hamonizar as necessidades de implementação de alterações no direito nacional, evitando que ocorram conflitos entre o que se estabelece no plano da cooperação penal internacional e os direitos fundamentais.

Isto posto, é imprescindível que o Brasil seja recepcionado no rol dos Estados signatários da Convenção de Budapeste para fazer frente ao cibercrime com instrumentos jurídicos adequados, uma vez que seu caráter transfronteiriço inviabiliza ações efetivas de forma a proteger os riscos globais.

---

[324] A Constituição da República Federativa do Brasil prevê:
Art. 5º .....
X - são invioláveis a **intimidade, a vida privada**, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
XII - **é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados** e das comunicações telefônicas, salvo, no último caso, por **ordem judicial**, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (grifo nosso).

6 CONCLUSÃO

As transformações de ordem política, econômica, social e ideológica do pós Guerra Fria criaram ambiente propício para que as forças revolucionárias do pós-modernismo alterassem substancialmente o clima de tensão existente no mundo, propiciando o ambiente necessário para que a globalização se efetivasse e com esta ocorresse a revolução tecnológica e o novo zoneamento das áreas de influência, fazendo fortalecer, sobretudo os ideais de solidariedade humano.

Na esteira destes acontecimentos, seguiu-se o avanço da internet e de novas formas de enxergar o mundo e de se relacionar. O surgimento de forças de convergência que transformaram as práticas comerciais, o exercício de direitos e liberdades públicas, além de um novo impulso na área de educação, com reflexos profundos no campo jurídico tem norteado o enfoque do século XXI.

A pesquisa viabilizou, desta forma, a análise com profundidade das questões postas como objetivos, propiciando conclusões sobre questões inquietantes relacionadas com fenômenos da sociedade da informação, onde muitos parâmetros para o mundo jurídico e para o Estado encontram-se em processo de redesenho, mas que não deixam de indicar caminhos para possíveis questões e soluções complexas.

Desta forma foi possível constatar que no estudo e enfrentamento do cibercrime, os conceitos tradicionais como soberania, tempo e lugar do crime e, por conseqüência, da jurisdição e competência tem que ser enxergados sob um novo viés – o da necessidade de integração ao mundo global e da premente dependência de um regime de cooperação penal internacional (pois sofreram em relação à internet e ao ciberespaço modificações nos seus aspectos tradicionais).

Os novos fenômenos criminosos migraram em grande parte, do mundo real para a grande rede. Não que tenham deixado de pertencer ao mundo dos fatos humanos sujeitos às regras do direito. O cibercrime é, pois, ameaça real, com números e índices crescentes como foi demonstrado. Seu desdobramento em múltiplas facetas, tem provocado danos que ultrapassam cifras de bilhões de dólares em escala mundial, com reflexos inequívocos no Brasil, podendo atingir desta forma o equilíbrio da ordem econômica.

As empresas, o governo e a sociedade civil têm sofrido as conseqüências da incidência de tais práticas, que provocando danos financeiros ao Estado, instituições e pessoas, acabam por limitar o poder de investimento, uma vez que serão dispensados grandes

somas financeiras para recompor danos e reforçar a estrutura dos sistemas de informática, em face da necessidade de segurança.

Subtração de identidade, práticas de racismo e xenofobia *on line*, pedofilia na rede, clonagem de cartão, ciberterrorismo e cibertaques, entre outras práticas que atentam contra a integridade, confidencialidade e segurança do tráfego e dos dados de sistemas de computadores, configuram-se em ameaças que requerem um esforço conjunto.

O Brasil mesmo sem dispor de instrumentos jurídicos adequados tem conseguido promover o enfrentamento de grandes ameaças, com a desarticulação de grupos criminosos organizados com alcance nacional e internacional, mediante ações, notadamente, da Polícia e do Ministério Público Federal. Mas estas ações do Estado têm se mostrado apenas como um arrefecimento contra o cibercrime (pois tem acontecido apenas em instâncias federais), uma vez que combater o cibercrime prescinde de investimentos em qualificação de integrantes do sistema de justiça criminal – policiais, promotores públicos e juízes, notadamente no âmbito dos estados federados.

Constatou-se assim, que muitas condutas criminosas encontram tipificação legal e possibilidade de punição no próprio direito penal nacional (como vem ocorrendo) – punição, por exemplo, para os crimes de furto qualificado, dano, racismo, crimes contra a honra, formação de quadrilha, entre outros. Mas outras questões de ordem processual, de investigação policial e procedimentos judiciais, encontram óbices de ordem legal quanto à jurisdição e competência para agir além fronteiras, ambiente onde estas ações cibercriminosas, via de regra, efetivam-se mais intensamente, atingindo mais de uma jurisdição.

Aos grandes desafios da humanidade, somem-se os esforços globais de todas as nações. A cooperação penal internacional, mediante tutela de instrumentos jurídicos específicos, coloca-se neste sentido, como indicador de oportunidade para que todos os países se unam na missão de combater o cibercrime. O exemplo da construção do ideal de cooperação comunitária na União Européia, notadamente na seara de cooperação internacional em matéria penal, impõe-se como exemplo mais efetivo.

Os conflitos de jurisdição entre os países, na questão de combate aos crimes de internet, não se resolvem tão somente com a análise tradicional dos conceitos de soberania, poder estatal e jurisdição, pois esta idéia foi diluída pelo novo direito que se estabelece perante o avanço tecnológico, requerendo assim, a conjugação de esforços de forma cooperada, como prevê a Convenção do Conselho da Europa sobre Cibercrime – a Convenção de Budapeste.

Desta forma, o combate ao cibercrime não é responsabilidade apenas da União Européia, mas de todos os países. É uma necessidade a ampliação de seu principal instrumento jurídico de combate ao cibercrime, uma vez que tem se mostrado como instrumento hábil a viabilizar a cooperação penal internacional, mediante suas disposições que tratam da definição de condutas, do estabelecimento de parâmetros para harmonização e do direito nacional e notadamente das disposições de cooperação, como as medidas de auxílio mútuo exaustivamente analisadas. Não se pode dizer que se trata de uma Convenção perfeita, mas estabelece de forma clara, as ressalvas e reservas possíveis.

Da análise dos aspectos dos instrumentos de cooperação fixados pela Convenção de Budapeste, é possível concluir que se apresenta de forma a propiciar aos Estados partes, poderes para efetivar a busca, apreensão e interceptação de dados de tráfego e de conteúdo, coleta de provas, inclusive em tempo real, medidas de auxílio mútuo, procedimentos quanto à extradição (não admissível no direito brasileiro). Ressalte-se que algumas disposições previstas carecem de análise quanto à compatibilidade com o ordenamento jurídico brasileiro, notadamente de ordem constitucional, enquanto outras medidas já existem no direito pátrio, de forma que, no conjunto, não se vislumbram impedimentos ou óbices para que o Brasil tome parte da Convenção (após formulação de convite como previsto).

Desde a adoção em 23 de novembro de 2001, 46 países já assinaram a Convenção sobre Cibercrime (Convenção de Budapeste), sendo que deste total, até 16 de abril de 2009, 28 nações já haviam ratificado, incluindo países que não integram a União Europeia, quais sejam: Canadá, Costa Rica, República Dominicana, Japão, México, Filipinas, África do Sul e Estados Unidos.

Em face de práticas racistas que estavam a prosperar sem controle na grande rede, em 1 de março de 2006 passou a vigorar o Protocolo Adicional à Convenção, que determina ao seus signatários a criminalização no direito nacional “a divulgação de material racista e xenófobo”, através de sistemas informáticos, bem como dos comportamentos racistas e xenófobos, ameaças e insultos.

Outras condutas que atingem grandes grupamentos humanos, como nos casos de ciberterrorismo (terrorismo cibernético) comporta visão de crime contra a humanidade, sujeitando seus infratores à jurisdição do Tribunal Penal Internacional, como foi visto.

Merece registro que é perfeitamente possível o estabelecimento de salvaguardas e reservas quanto aos principais pontos que possam suscitar controvérias. A adesão à Convenção possibilita este mecanismo de forma a hamonizar as necessidades de

implementação de alterações no direito nacional, evitando que ocorram conflitos entre o que se estabelece no plano da cooperação penal internacional e os direitos fundamentais.

Isto posto, é imprescindível que o Brasil e outras nações sejam convidadas e recepcionadas no rol dos Estados signatários da Convenção de Budapeste para fazer frente ao cibercrime com instrumentos jurídicos adequados, uma vez que seu caráter internacional multilateral viabiliza ações efetivas de forma a proteger a sociedade de riscos globais.

REFERÊNCIAS

A DÉCADA DE 80. **Lisboa: Site Ciência Viva.** Disponível em: <http://oficina.cienciaviva.pt/~pw020/g3/a%20decada%20de%2080.htm> Acesso em: 1 ago.2008.

ALBERTO, Carlos; Et al. **Telecomunicações, informática e telemática**.São Paulo, 2008. Disponível em:<http://www.scribd.com/doc/6184626/Telematica-e-Telemetria> Acesso em: 28 jan.2009.

ALBUQUERQUE, Antonio. **Direito internacional público: resumo**. Lisboa: Universidade Lusófona, 2007.

AFONSO, Carlos Alberto. **Internet: quem governa a infra-estrutura?.** ILDES/FES, 2002, p. 2. Disponível em:<http://64.233.167.104/search?q=cache:hpfKq5Ed3w0J:www.direitoacomunicacao.org.br/novo/index.php%3Foption%3Dcom_docman%26task%3Ddoc_download%26gid%3D190+%22Internet:+quem+governa+a+infra-estrutura%3F%22&hl=pt-BR&ct=clnk&cd=1&gl=br>. Acesso em: 3 ago.2008.

ALEXANDRE, Silvio. **O Autor e sua obra. Anexo a Neuromancer**. São Paulo: Aleph, 2 ed., 1991. p. 261. Disponível em: < http://www.scribd.com/doc/2230917/Neuromancer-GIBSON-William> Acesso em: 1 ago. 2008.

ALMEIDA FILHO, José Carlos Araújo. **Direito Eletrônico ou Direito da Informática?**.Informática Pública vol.7(2):11-18, 2005. Disponível em: <http://www.ip.pbh.gov.br/ANO7_N2_PDF/IP7N2_almeida.pdf> Acesso em 3 abr.2009.

ARAS, Vladimir. **Crimes de informática: uma nova criminalidade**. Revista informática jurídica.com. Disponível em: <http://www.informatica-juridica.com/trabajos/artigo_crimesinformticos.asp> Acesso em: 3 abr. 2009.

AZAMBUJA, Darcy. **Teoria geral do Estado**. 41ª ed. São Paulo: Globo, 2001, p.51.

BARBOSA, Alexandre de Freitas (Coord)**. O Mundo Globalizado**: Política, Sociedade e Economia. Contexto: São Paulo, 2006.

BARLOW, John Perry. **Declaração de independência do ciberespaço**. Brasília: Ministério da Cultura, 2006. Disponível em: <http://www.cultura.gov.br/site/2006/10/23/declaracao-de-independencia-do-ciberespaco/>. Acesso em: 11 ago.2008.

BARRETO JÚNIOR, Irineu Francisco. **Atualidade do conceito de sociedade da informação para a pesquisa jurídica**. In PAESANI, Liliana Minardi (Coord). O direito na sociedade da informação. São Paulo: Atlas, 2007.

BAZELAIRE, Jean Paul; CRETIN, Thierry; tradução de Luciana Pinto Venâncio. **A justiça penal internacional, seu futuro: de Nuremberg a Haia**. Barueri: Manole, 2004. p. 13.

BERMAN, Frank. ***Theoretical approaches to the assertion of jurisdiction - Jurisdiction: the state***. In: CAPPS, Patrick; EVANS, Malcolm; KONSTADINIDIS, Strato V. ***Asserting jurisdiction: international and European legal perspectives***. Oxford: Hart Publishing, 2003.

BEZERRA, Edson Kowas. et al. **O espaço cibernético e seu emprego como agente de instabilidade de uma nação: uma visão sobre a guerra cibernética**. *In*: ICCyber'2004 – I Conferência Internacional de Perícias em Crimes Cibernéticos. Disponível em: <http://angel.acmesecurity.org/~adriano/papers/anais-iccyber-dpf-2004.pdf> Acesso em: 5 mar. 2009

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 21 ed. Malheiros: São Paulo, 2007.

BORGES, José Souto Maior. **Curso de direito comunitário**. São Paulo: Saraiva, 2005, p..67.

BRASIL. Superior Tribunal de Justiça. **EDcl na CR .438/BE**, Rel. Ministro LUIZ FUX, CORTE ESPECIAL, julgado em 01/08/2008, DJe 20/10/2008. Disponível em: < http://br.vlex.com/vid/43535078>. Acesso em: 15 abr.2009.

BRASIL. Conselho de Justiça Federal. **Incitação pela internet ao plantio de maconha é competência da Justiça Estadual**. Disponível em: <http://www.direito2.com.br/cjf/2006/out/17/incitacao_pela_internet_ao_plantio_de_maconha_e_competencia>. Acesso em: 16 abr.2009.

BRASIL. Ministério Público Federal. **Grupo de trabalho – crime cibernético, resultados e conclusões.** Disponível em: < http://2ccr.pgr.mpf.gov.br/docs_institucional/eventos/viii-encontro/ata_grupo_sobre_crimes_ciberneticos.pdf>. Acesso em: 16 abr.2009.

BRASIL. Supremo Tribunal Federal. **Julgados especiais**. Disponível em: <http://www.stf.jus.br>. Acesso em 20 abr. 2009.

BRASIL. Presidência da República, Casa Civil - Subchefia para Assuntos Jurídicos. **Lei nº 7.170, de 14 de DEZEMBRO DE 1983. Define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L7170.htm>. Acesso em: 20 abr.2009.

BRASIL vive o maior "boom" de acessos residenciais à Internet. São Paulo: Convergência Digital, 2008. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=13021&sid=4>. Acesso em: 2 ago.2008.

BRITO, Dante Ponte de.; VASCONCELOS, Fernando Antônio de. **O direito e a economia na era digital.** Prim@ Facie, João Pessoa, a.5. n. 9, jul./dez. 2006. Disponível em:<http://www.josuelima.net/ppgcj/gerencia/docs/26062007124707.pdf> Acesso em: 18 jan.2009.

BRASIL. Superior Tribunal de Justiça. **Julgados especiais**. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/1454634/carta-rogatoria-cr-438-be-2005-0015196-0-stj>. Acesso em 15 abr.2009.

BRASIL. **Lei 11.829/2008**, disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm>. Acesso em: 15 abr.2009.

BRASIL vive o maior "boom" de acessos residenciais à Internet. São Paulo: Convergência Digital, 2008. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=13021&sid=4>. Acesso em: 2 ago.2008.

BOITEUX, Luciana. **Os princípios penais no Estatuto do Tribunal Penal Internacional à luz do direito brasileiro.** *In*:JAPIASSU, Carlos Eduardo Adriano (Coord.). **Direito penal internacional estrangeiro e comparado**. Rio de Janeiro: Lúmen Júris, 2007. p.91.

CARLOS, Ana Fani Alexsandri; LEMOS, Amália Inês Geraiges (Orgs). **Dilemas urbanos: novas abordagens sobre a cidade**. 2ª ed. São Paulo: Contexto, 2005.

CAPEZ, Fernando. **Curso de processo penal.** 6a ed. São Paulo: Saraiva, 2001

CARVALHO, Ivan Lira de. **Crimes na Internet. Há como puni-los**. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2081>. Acesso em: 22 mar. 2009.

CASTRO, Luis Fernando Martins. **Direito da informática e do ciberespaço**. Revista de Derecho Informático. n. 064, novembro 2003. Disponível em: <http://www.alfa-redi.org/rdi-articulo.shtml?x=1270> Acesso em: 3 abr.2009.

DOMINGUES, Antonio Carlos Iranlei Toscano Moura. **O Tribunal Penal Internacional e o combate à criminalidade econômica organizada transnacional.** Dissertação apresentada ao Programa de Pós-Graduação – CCJ – UFPB: Mestrado em Direito Econômico. João Pessoa – PB, 2007. p.82.

CERT.br. **Núcleo de Informação e Coordenação do Ponto br, 2008**. Disponível em: http://www.cert.br/stats/incidentes/2008-jan-dec/tipos-ataque.html Acesso em: 22 mar.2009.

CGI.BR. **Sobre o CGI.br**. Disponível em:<http://www.cgi.br/sobre-cg/index.htm>. Acesso em: 2 ago.2008.

CHAWKI, Mohamed. ***Essai sur la notion de cybercriminalité***. IEHEI, juillet 2006. Disponível em <http://www.iehei.org/bibliotheque/cybercrime.pdf> Acesso em: 05 mar. 2009.

CHAWKI, Mohamed. ***A critical look at the regulation of cybercrime: a comparative analysis with suggestions for legal policy***. DROIT-TIC, 11 April 2005. Disponível em: <http://www.crime-research.org/articles/Critical/. Acesso em: 5 abr.2009.

CHAWKI, Mohamed. WAHAB, Mohamed S. Abdel. ***Identity Theft in Cyberspace: Issues and Solutions.*** Lex Electronica, vol.11 n°1 (Printemps / Spring 2006). Disponível em: <hhttp://www.lex-electronica.org/docs/articles_54.pdf>. Acesso em: 11 abr.2009.

CHELL, Bernadete Hlubik and MARTIN, Clemens. ***Cybercrime: A Reference Handbook*.** ABC-CLIO: Santa Bárbara, 2004.

CONVENÇÃO DE BUDAPESTE SOBRE O CIBERCRIME. Disponível em: <http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf> Acesso em: 5 abr.2009.

CONSELHO DE MINISTROS DA UNIÃO EUROPÉIA. **Minuta do relatório explicativo**. Disponível em: <https://www.safernet.org.br/drupal/sites/default/files/Relatorio-explicativo-convencao-cibercrime.pdf>. Acesso em: 15 abr.2009.

COMISSÃO PARLAMENTAR DE INQUÉRITO - PEDOFILIA. **Termo de Cooperação Mútua.** Disponível em: <http://www.prsp.mpf.gov.br/cidadania/dhumInt/Termo%20de%20Coopera%E7%E3o%20-%20Safernet%20e%20PRSP.pdf>. Acesso em: 12 abr. 2009.

CONSELHO DA EUROPA. **Convenção de Budapeste sobre o Cibercrime**. Disponível em: <http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf>. Acesso em: 12 abr.2009.

COUTO, Thiago Graça. **O direito virtual: Panorama teórico e técnico do *Cyberlaw* e análise prática das conseqüências jurídicas envolvendo o mau uso das redes de compartilhamento Peer-to-Peer**. 2007.

CRUZ, Daniella da Rocha. **Criminalidade informática: tipificação penal das condutas ilícitas realizadas com cartões de crédito**. Rio de Janeiro: Forense, 2006.

DALLARI, Dalmo de Abreu. **Elementos de teoria geral do Estado**. 15ª ed. São Paulo: Saraiva, 1991.

DELGADO, Vladimir Chaves. **Cooperação internacional em matéria penal na convenção sobre o cibercrime**. 2007. 315p. Dissertação. (Mestrado em Direito das Relações Internacionais) - Centro Universitário de Brasília. Brasília, 2007.

DENNING, D. ***Cyberterrorism, Testimony before the Special Oversight Panel of Terrorism*.** Committee on Armed Services, US House of Representatives, 2000. Disponível em: http://www.cs.georgetown.edu/~denning/infosec/cyberter ror.html>. Acesso em: 19 abr.2009.

DICIONÁRIO PRIBERAM DA LÍNGUA PORTUGUESA. Disponível em: <http://www.priberam.pt/dlpo/definir_resultados.aspx>. Acesso em: 15 abr.2009.

DIDIER JR, Fredie. **Curso de Direito Processual Civil**. 9. ed. Bahia: JusPodivm, 2008.

EFE. **Google nega ter apagado Geórgia do serviço de mapas**. São Paulo: Folha On Line, 2008. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u433098.shtml>. Acesso em: 13 ago 2008.

EFING, Antônio Carlos; FREITAS, Cinthia Obladen de Almendra. **Direito e Questões Tecnológicas - Aplicados no Desenvolvimento Social**. Curitiba: Juruá, 2008.

ERDELYI, Maria Fernanda. **Itamaraty ainda estuda adesão à Convenção de Budapeste.** São Paulo: Consultor Jurídico, 2008. Disponível em: <http://s.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste>. Acesso em 22 abr.2009.

ESTATUTO DE ROMA DO TRIBUNAL PENAL INTERNACIONAL (TPI). Disponível em: <http://www.fd.uc.pt/CI/CEE/OI/TPI/Estatuto_Tribunal_Penal_Internacional.htm>. Acesso em: 21 abr.2009.

EUROPA GLOSSÁRIO. **Eurojust**. Disponível em: <http://europa.eu/scadplus/glossary/eurojust_pt.htm>. Acesso em: 9 abr.2009.

EUROPA GLOSSÁRIO. **Cooperação policial e judiciária em matéria penal**. Disponível em: <http://europa.eu/scadplus/glossary/police_judicial_cooperation_pt.htm>. Acesso em: 9 abr.2009.

FARIA, José Eduardo. **O direito na economia globalizada**. São Paulo: Malheiros, 1999.

FRANÇA, Ronaldo. **Deixem meu PC em paz**. Revista Veja, São Paulo, nov.2004. Edição 1980. Disponível em: <http://veja.abril.com.br/171104/p_160.html>. Acesso em: 13 mar.2009.

FELICIANO, Guilherme Guimarães. **Terrorismo: contornos jurídicos para o Direito Penal**. Jus Navigandi, Teresina, ano 9, n. 782, 24 ago. 2005. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=7189>. Acesso em: 20 abr. 2009.

FRANK, John B. ***$1 Trillion Lost to Cybercrime...Can Hackers Bail US Out?.*** Disponível em: <http://pindebit.blogspot.com/2009/02/1-trillion-lost-to-cybercrimecan.html>. Acesso em: 15 abr.2009.

FERRAZ, Anna Cândida da Cunha. **União, Estado e Município na Constituição Federal: competências e limites**. Cadernos Fundap: São Paulo, ano 8, n° 15, págs. 42-47, abr./1998.

FERREIRA, Luis Pinto**. Teoria Geral do Estado**. 3.ed. São Pulo: Saraiva, 1975.

FERRI, Enrico. **Princípios de direito criminal: o criminoso e o crime**. Tradução de Luiz Lemos D´Oliveira. Campinas: Russell Editores, 2003.

FRAGOSO, Suely. **Realidade Virtual e Hipermídia - somar ou subtrair?** São Leopoldo: Cyberlegenda nº 9, 2002. Disponível em:<http://www.uff.br/mestcii/sueli1.htm> Acessado em: 1.9.2008.

FRANCA FILHO, Marcílio Toscano. **Introdução ao direito comunitário**. São Paulo: Editora Juarez de Oliveira, 2002.

FRIEDMAN, Thomas Lauren. **O mundo é plano**: uma breve história do século XXI - Tradução de Cristina Serra e S Duarte. Rio de Janeiro: Objetiva, 2005.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre a ética informacional**. R. CEJ, Brasília, n. 20, p. 67-73, jan./mar. 2003.

GIBSON, William. **Neurormancer**. Tradução de Abdoule Sam Byd e Lumir Nahodil. São Paulo: Ace Books, 2003.

GOEL, Asvin. ***The history of telematics. Téle-matique***, 2008. Disponível em <http://www.telematique.eu/telematics/history.en.html> Acesso em: 20 jan.2009.

GOIS JR, José Caldas. **O Direito na Era das Redes: a liberdade e o delito no ciberespaço**. Bauru: EDIPRO, 2001, p. 46.

GOMES, Flávio Luiz. **Crimes informáticos**. Disponível em: <www.direitocriminal.com.br>. Acesso em 26 mar. 2009.

GONÇALVES, Patrícia. **Primeiro satélite de comunicações chegou a órbita há 46 anos**: in Revista Ciência Hoje, versão eletrônica. Disponível em: <http://www.cienciahoje.pt/3889> acesso em: 01 jul.2008.

GOODMAN, Marc D.; BRENNER, Susan W. ***The emerging consensus on criminal conduct in cyberspace.*** Disponível em: <http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php> Acesso em: 6 abr.2009.

HELL, Lord. **A consciência hacker – uma visão objetiva**. Rio de Janeiro: Book Express, 2000.

HIRST, Paul; THOMPSON, Grahame. **Globalização em questão**: a economia internacional e as possibilidades de governabilidade. Tradução Wanda Caldeira Brant. Petrópolis, RJ: Vozes, 1998.

História da internet no Brasil. Disponível em < http://www.internetnobrasil.net/index.php?title=1999> Acesso em: 10 fev. 2009.

HOBSBAWM, Eric. **Era dos extremos**: o breve século XX: 1914-1991.Tradução de Marcos Santarrita.São Paulo: Companhia das Letras, 1995.

HOESCHL, Hugo César. **O ciberespaço e o direito III**. Florianópolis: IJURIS - Instituto de Governo Eletrônico, Inteligência Jurídica e Sistemas, 1997. Disponível em: <http://www.ijuris.org/producaotc/direito_digital/digital/ciber3.htm> Acesso em: 1 ago.2008.

HOPPER, Paul. ***Linving with globalization***. New York: Berg Publisher, 2006.

ICANN. **A comunidade internacional da Internet trabalha em equipe para promover a estabilidade e a integridade da Internet**. Marina Del Rey, 2008. Disponível em:<http://www.icann.org/tr/portuguese.html>. Acesso em: 03 ago.2008.

IDG NOW! Internet e legislação. **Crimes eletrônicos geral 17 mil decisões no Brasil, em 6 anos**. Disponível em: <http://idgnow.uol.com.br/internet/2008/11/25/crimes-eletronicos-geram-17-mil-decisoes-judiciais-no-brasil-em-6-anos/> Acesso em: 2 mar.2009.

Internet - História da internet. Wikipedia, enciclopédia livre. Disponível em:<http://pt.wikipedia.org/wiki/Internet>. Acesso em: 4 ago.2008.

INTERNET ***user statistics and population stats for the countries and regions that comprise Latin American internet users*****.** EUA: Internet World Stats, 2008. Disponível em: <http://www.internetworldstats.com/stats10.htm#spanish>. Acesso em: 2 ago.2008.

JOHNSON, David R; POST, David. ***Law and Borders - The rise of law in cyberspace***. First Monday, Volume 11, Number 2, 2006. Disponível em:<http://www.firstmonday.org/issues/issue1/law/index.html>. Acesso em: 10 ago.2008.

Justiça Federal - Seção Judiciária da Paraíba. **Juiz federal condena hackers envolvidos na Operação Scan**. João Pessoa, 2009. Disponível em: <http://www.jfpb.jus.br/site/det_noticias.asp?chave=179> Acesso em: 3 abr.2009.

KAMINSKI. Omar**.** Internet legal: o direito na tecnologia da informação. Curitiba: Juruá, 2007.

Kellen Cristina S.P, 1996.

KOEPSELL, David R. ***The ontology of cyberspace: philosophy, law, and the future of intellectual property***. Chigaco: Open Court, 2003.

KOBAYASHI, Bruce H.;RIBSTEIN, Larry E. ***Multijurisdictional regulation of the internet*****.** In: THIERER, Adam D.; CREWS, Clyde Wayne. ***Who Rules the Net?:Internet Governance and Jurisdiction*****.** Washington: Cato Institute, 2003.

LAMIKIZ, Alex. **Afinal o que é cybercultura**. Disponível em: < http://listas.cev.org.br/arquivos/html/cevcomp/2003-09/msg00000.html>. Acesso em: 23 abr. 2009.

LEMGRUBER, Julita. **Verdades e mentiras sobre o sistema de justiça criminal**. R. CEJ, Brasília, n. 15, p. 12-29, set./dez. 2001. Disponível em:<http://www2.cjf.jus.br/ojs2/index.php/cej/article/viewPDFInterstitial/427/608> Acesso em: 10 mar.2009.

LESSIG, Lawrence. ***Code and Other Laws of Cyberspace***. Harvard Magazine, 2000. Disponível em: <http://harvardmagazine.com/2000/01/code-is-law.html>. Acesso em: 11 ago.2008.

LIMA, Wesley de. **Uma nova abordagem da jurisdição no Processo Civil contemporâneo**. In: Âmbito Jurídico, Rio Grande, 59, 30/11/2008 [Internet]. Disponível em: http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id= 5290. Acesso em 22/03/2009.

LINHA DO TEMPO DA INTERNET NO BRASIL. Disponível em <http://www.internetnobrasil.net/index.php?title=1988>. Acesso em: 10 fev. 2009.

LORES, Raul Juste. **Internet na China é monitorada por 30 mil pessoas**. São Paulo: Folha On line, 2008. Disponível em:<http://www1.folha.uol.com.br/folha/informatica/ult124u431438.shtml>. Acesso em: 12 ago.2008.

LOSANO, Mário. **A Informática Jurídica 20 anos depois**. Revista dos Tribunais, n. 715, maio de 1995. pp. 350-367.

LUNKER, Manish. ***Cyber laws: a global perspective***. Disponível em: <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005846.pdf> Acesso em: 6 abr. 2009.

MAIA, Felipe. **Entidades discutem adoção de endereço "b.br" para bancos na web**. São Paulo: Folha On Line, informática, 2008. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u395485.shtml>. Acesso em 2 ago.2008.

MANGUEIRA, Hugo Alexandre Espínola. **Criminalidade cibernética:** estudo dos *hackers* e das implicações legais de seus ataques através da Internet. João Pessoa, 2002.

MARQUES, Helvetius. **O terrorista e os direitos humanos.** Disponível em: <http://www.juridicas.unam.mx/sisjur/internac/pdf/10-478s.pdf>. Acesso em: 21 abr.2009.

MARTINS, José Carlos Cordeiro. **Gestão de projetos de segurança da informação**. Rio de Janeiro: Brasport, 2003, p. 217.

MARTINS, Paulo Roberto. **Mandamentos Hackers**. 2003. Disponível em:<http://www.mapavirtual.com.br/newpaul/mandhacker.html>. Acesso em 2 ago.2008.
MATIAS, Eduardo Felipe Pérez. A humanidade e suas fronteiras: do Estado soberano à sociedade global. São Paulo: Paz e Terra, 2005, p.33.

MEDEIROS, Assis. **Hackers entre a ética e a criminalização**. Florianópolis:Visual Books, 2002.

MELLO, Caren Sapienza de. **O futuro das relações de trabalho via comunicação nas organizações do Século XXI. 2004**. 94p. Monografia (Especialização em Gestão Estratégica em Comunicação Organizacional e Relações Públicas) – Universidade de São Paulo, São Paulo, 2004.

MELLO, Patrícia Campos. **O mundo tem medo da China? Nós também - o maior enigma da economia mundial.** São Paulo:Terceiro Nome, 2005.

MIRANDA, Napoleão. **Globalização, soberania nacional e direito internacional**. R. CEJ, Brasília, n. 27, out./dez. 2004. p.86. Disponível em: < http://www.cjf.jus.br/revista/numero27/artigo11.pdf>. Acesso em 16 abr.2009.

MONTEIRO, Mário A. **Introdução à organização dos computadores**. 3a ed. Rio de Janeiro: LTC Ed., 1996.

MOREIRA, Daniela. **Comércio eletrônico cresce 30% em 2008. Revista Eletrônica Info, 2008**. Disponìvel em: <http://info.abril.com.br/aberto/infonews/012009/08012009-33.shl> Acesso em: 20 jan.2009.

NAGPAL, Rojas. ***Evolution of cybercrimes. Asian School of Cyber Laws, 2008***. Disponível em: < http://cyberattack.in/images/7/74/Evolution_of_Cyber_Crime.pdf> Acesso em: 20 mar.2008.

PAESANI, Liliana Minardi (Coord). **O Direito na sociedade da informação**. São Paulo: Atlas, 2007.

O´BRIEN, Martin; YAR, Majid. ***Criminology: the key concepts***. New York: Taylor & Francis, 2008.

PAIVA, Bruno Teixeira de. **Ampliação da competência do Tribunal Penal Internacional para o julgamento de crimes ambientais transfronteiriços**. 2008. 112p. Dissertação. (Mestrado em Ciências Jurídicas) - Universidade Federal da Paraíba, João Pessoa, 2008.

PADILHA, Luiz R. Nuñes. **Chiovenda, jurisdição voluntária e processo penal**. UFRGS. Rio Grande do SUl, 1996. Disponível em<http://www.direito.ufrgs.br/pessoais/padilla/Trabalhos%20Publicados/CHIOVEND.htm> Acesso em: 18 fev. 2009.

PAULO SÉRGIO OLIVEIRA, S.P., 1997.

PILARES DA UNIÃO EUROPÉIA. Wikipédia, a enciclopédia livre. Disponível em: <http://pt.wikipedia.org/wiki/Pilares_da_Uni%C3%A3o_Europeia>. Acesso em: 8 abr.2009.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal**. Disponível em: http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile /29397/28953> Acesso em: 04 abr. 2009.

PINHEIRO, Patrícia Peck. **Direito digital**. 2ª ed. São Paulo: Saraiva, 2007.

PINTO, Marcio Morena. **O Direito da internet: o nascimento de um novo ramo jurídico** . Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2245>. Acesso em: 2 abr. 2009.

PORTAL TERRA. **Roubar dados virou crime organizado**. Disponível em: <http://www.computadorbr.com/informatica-3/roubar-dados-virou-crime-organizado.html>. Acesso em: 23 abr.2009.

PORTAL DO HSBC BANK S.A. **Polícia Federal fecha 2007 com 9 operações de combate ao crime virtual.** Disponível em: <http://www.hsbc.com.br/common/seguranca/artigo-seguranca-comb-crime-virtual.shtml.> Acesso em: 14 mar.2008.

PORTAL DO TRIBUNAL REGIONAL FEDERAL 5A REGIÃO**. Terceira Turma nega habeas corpus para "crackers"**. Disponível em: <http://www.trf5.gov.br/noticias/1044. Acesso em 13.mar.2008.

RAMONET, Ignacio. **Controlar a internet**. Informação Alternativa, 2005. Disponível em:<http://www.infoalternativa.org/autores/ramonet/ramonet067.htm>. Acesso em: 2 ago.2008.

REED, David. ***A balanced introduction to computer science***. 2nd ed. Omaha: Prentice Hall, 2007.

RELATÓRIO DO GRUPO DE TRABALHO SOBRE CRIMES CIBERNÉTICOS – Ministério Público Federal, 2008. Disponível em: < http://2ccr.pgr.mpf.gov.br/docs_institucional/eventos/viii-encontro/ata_grupo_sobre_crimes_ciberneticos.pdf>. Acesso em: 1 mar.2009.

RPP - **Rede Paraibana de Pesquisa.Histórico do ponto de presença da RNP na Paraíba**. campina Grande, 2008. Disponível em: <http://www.pop-pb.rnp.br/historico.html> Acesso em: 28 jan. 2009.

REZEK, José Francisco. **Direito Internacional Público**. Belo Horizonte: PUC Minas, 2005.

REZEK, Francisco. **Direito Internacional Público: curso elementar**.10. ed ver. E atual. – São Paulo: Saraiva, 2005. p. 263.

ROHRMANN, Carlos Alberto. **Curso de direito virtual**. Belo Horizonte: Del Rey, 2005.

ROCHA, Luis Fernando. **Retrospectiva 2003 – Parte 1. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** Cert.br: São Paulo, 2003. Disponível em < http://www.cert.br/docs/reportagens/2003/2003-12-15.html> Acesso em: 15 fev. 2009.

RUIZ, Fernanda; ALMEIDA, D. Freire. **O julgamento de atos de terrorismo pelo Tribunal Penal Internacional.** Disponível em: <http://bdjur.stj.gov.br/jspui/bitstream/2011/18600/2/O_Julgamento_de_Atos_de_Terrorismo.pdf>. Acesso em: 21 abr.2009.

RULLI JÚNIOR, Antônio. **Jurisdição e sociedade da informação**. *In:* PAESANI, Liliana Minardi (Coord). **O direito na sociedade da informação**. São Paulo: Atlas, 2008.

SANCHEZ, Ligia. **E-commerce deve chegar a R$ 8,8 bilhões no Brasil em 2008**. São Paulo: It Web, 2008. Disponível em: <http://www.itweb.com.br/noticias/index.asp?cod=46185>. Acesso em: 2 ago.2008.

SAVONA, Ernesto Ugo. ***Crime And Technology: New Frontiers For Regulation, Law Enforcement And Research*.** Springer:New York, 2005.

SCHOUERI, Luís Eduardo.Org. **Internet: o direito na era virtual**. Rio de Janeiro: Forense,2001, p.373.

SCHJOLBERG, Stein. **The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva**. Disponível em: <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf> Acesso em: 6 abr.2009.

SCHOOR, Tatiana. **Crimes digitais geraram prejuízo de R$ 300 mi em 2005**. Portal Almeida Carmago Advogados. Disponível em: http://www.almeidacamargo.com.br/AlmeidaCamargo/paginas/Informacao.asp?CodNoticia=237&Categoria=6. Acesso em: 14 mar.2008.

SILVA JÚNIOR, Ronaldo Lemos. **Direito, tecnologia e cultura**. São Paulo: FGV, 2005.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: Editora Revista dos Tribunais, 2003.

SILVA, De Plácido e. **Vocabulário Jurídico**. Rio de Janeiro: Forense, 11ª. ed., 1994. Disponível em <http://pt.wikipedia.org/wiki/Competência_judicial> Acesso em: 10 mar. 2009.

SIMÃO FILHO, Adalberto. **Sociedade da informação e seu lineamento jurídico**. *In* PAESANI, Liliana Minardi (Coord). **O direito na sociedade da informação**. São Paulo: Atlas, 2007.

SOBRAL, Carlos Eduardo Miguel. **Repressão a crimes cibernéticos. Brasília, Departamento de Polícia Federal**. Disponível em: <http://www.febraban.org.br/LerArquivo.asp?Tabela=Home_Arquivos&codigo=id_arquivo&campo1=arquivo&campo2=QtdeAcessos&id_codigo=560&campo3=arquivos/>. Acesso em: 13 mar.2009.

SOLOVE, Daniel J.,ROTENBERG, Marc and SCHWARTZ, Paul. ***Privacy, information and technology***. Aspen Publisher, New York, 2006.

STANTON, Michael. **A evolução das redes acadêmicas no Brasil: Parte 1 - da BITNET à Internet**. Boletim Bimestral da RNP V.2, n. 6.Rio de Janeiro: RNP, 1998. Disponível em <http://www.rnp.br/newsgen/9806/inter-br.html> Acesso em: 10 fev. 2009.

TAKAHASHI, Tadao (Org.) **Sociedade da informação no Brasil : livro verde.** Brasília: Ministério da Ciência e Tecnologia, 2000.

TEIXEIRA, Duda. **Uma guerra pela internet: o maior cibertaque da história tira a Estônia da rede.** O suspeito é a Rússia. Disponível em: <http://www.defesanet.com.br/zz/intel_ciberwar.htm>. Acesso em: 21 br.2009.

THEOPHILO JÚNIOR, Roque. **Cibernética Tecnologia e Psicologia**. São Paulo, Academia Brasileira de Psicologia, 2000. Disponível em: <http://www.psicologia.org.br/internacional/ap11.htm> Acesso em: 1.8.2008.

United Nations - Economic and Social Comission for Asia and Pacific. **Understanding cybercrime**. Disponível em: <http://www.unescap.org/icstd/policy/publications/Information-Security-for-Economic-and-Social-Development/WHAT-ARE-CYBERCRIME-AND-COMPUTER-RELATED-CRIMES.pdf> Acesso em: 5 abr.2009.

UROFSKY, Melvin. ***Individual freedom and the Bill Of Rights. U.S. Departament of State´s Bureau of International Information Program, Chapter 6, Washington D.C*, 2003**. Disponível em: http://usinfo.state.gov/products/pubs/rightsof/privacy.htm.

UNIÃO EUROPÉIA. Wikipédia, a enciclopédia livre. Disponível em: http://pt.wikipedia.org/wiki/Uni%C3%A3o_Europ%C3%A9ia Acesso em: 8 abr.2009.

VASCONCELOS, Fernando Antônio de. **Internet: responsabilidade do provedor pelos danos praticados**. Curitiba: Juruá, 2003.

VEIGA, Adolfo Olsen da. **Apresentação**. *In* Olivo, Luiz Carlos Cancellier de, **Direito e Internet: a Regulamentação do Ciberespaço**, UFSC, 2000.

VIANNA, Túlio**. Transparência pública, opacidade privada**: O Direito como instrumento de limitação do poder na sociedade de controle. Revan: Rio de Janeiro, 2007.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003. pp. 13-26.

VICÁRIA, Luciana. **Kevin Mitnick - Hacker regenerado**. São Paulo: Revista Época On Line, Edição nº 278, 15/09/2003. Disponível em: <http://revistaepoca.globo.com/Epoca/0,6993,EPT600936-1666,00.html> Acesso em: 1 ago.2008.

ZAVRSNIK, Ales. ***Cybercrime definitional challenges and criminological particularities***. Law and Technology, Brno, Tchec Republic, v.2 n. 2, nov.2008. pp.8-10.

ZIEGLER, Jean. **Os senhores do crime**. Tradução de Clóvis Marques. Rio de Janeiro: Record, 2003.

WALL, D.S. **Crime and the Internet**, London: Routledge, 2001. pp. 3-7.

WIKIPÉDIA. A enciclopédia livre. **Estatuto de Roma**. Disponível em: <http://pt.wikipedia.org/wiki/Estatuto_de_Roma>. Acesso em 9 abr.2009.

WIKIPÉDIA. **Convention on Cybercrime**. Disponível em: <http://en.wikipedia.org/wiki/Convention_on_Cybercrime>. Acesso em: 22 abr.2009.

WILLIAMS, Phil. **Crime Organizado e Cibercrime: Sinergias, Tendências e Reações**. In Questões globais: coibição do crime internacional. Publicação do Departamento de Estado dos Estados Unidos. Agosto de 2001, Vol. 6, n.2. p.23.

GLOSSÁRIO

Parquet- Ministério Público

Persecutio criminis – Persecução criminal

Backbone – Espeinha dorsal da internet

Cookies – Arquivos temporário armazenados na memória do computador.

CNPq – Conselho Nacional de Pesquisa Científica.

Cyber-café - Ambiente comercial para uso de internet paga.

E-commerce **-** Comércio eletrônico

Hig-tech – Alta tecnologia

Home pages – Página de um site.

IBOPE **–** Instituto Brasileiro de Opinião Pública e Estatística

IBM – Industrial Business Machine. Empresa de tecnologia.

Infonews **–** Notícias de informática.

Lan-houses **-** Ambiente comercial para uso de internet paga.

Logado – O mesmo que conectado.

Mail – Correio.

Modus operandi – Modo de operação.

MS-DOze – Apelido do MS-DOS, sistema operacional da Microsoft.

Pari passu [lat.] 1. a passo igual; simultaneamente.

PCs **-** Computador pessoal

Phising – Técnica cracker de captura ou subtração de informações.

RNP/MCT – Rede Nacional de Pesquisa/ Ministério da Ciência e Tecnologia.

Spyware – Programa espião.

Root – O mesmo que rota ou raiz de um sistema operacional.

Sysop – Sistema operacional.

Telnet - Programa para conexão de internet.

Web bug – Bug ou pane da internet.

Loby – Pressao de um grupo para obtenção de vantagens.

ANEXOS

Convenção de Budapeste

Protocolo adicional