Centro Universitário de Brasília – UNICEUB
Faculdade de Ciências Jurídicas e Sociais – FAJS

ANA CAROLINA MAZONI

CRIMES NA INTERNET E A CONVENÇÃO DE BUDAPESTE

BRASÍLIA
2009

ANA CAROLINA MAZONI

CRIMES NA INTERNET E A CONVENÇÃO DE BUDAPESTE

Monografia apresentada como requisito para conclusão do curso de bacharelado em Direito do Centro Universitário de Brasília.

Orientador: Professor George Leite.

BRASÍLIA

2009

RESUMO

Nas discussões e elaborações legislativas sobre delitos informáticos conclui-se que não há como cogitar solução nacional para eles, devendo o assunto ser debatido em âmbito internacional. Assim, a Convenção de Budapeste, elaborada em 21 de setembro de 2001, visa à produção de uma política criminal comum para fornecer proteção à sociedade contra a criminalidade no espaço virtual. Dessa forma, o presente estudo se propõe a manter o Direito Penal Brasileiro a par destes avanços tecnológicos.

Palavras-chave: Crimes na internet – Crimes informáticos – Convenção de Budapeste – Crimes cibernéticos – Crimes digitais – Criminalidade no espaço virtual.

SUMÁRIO

INTRODUÇÃO

As transformações sociais, econômicas e políticas geraram grandes impactos na sociedade mundial. Com a globalização e as inovações tecnológicas, todos os setores da vida pública e privada foram afetados, gerando a necessidade de se modificar determinadas condutas para se adequar a tal cenário.

É fato que a aproximação do Direito a essas novas mudanças jamais será efetiva, tendo em vista que estas estarão sempre à frente das leis. No que tange principalmente ao Direito Penal, o maior desafio está em encarar que as particularidades ligadas às esses novos acontecimentos se exprimem na formação de grandes vilões: os crimes.

Diante do grande desenvolvimento da tecnologia e das modificações radicais que estas vêm a provocar, o computador e a *internet* seriam os maiores responsáveis pela reflexão a respeito da criação de tipos penais específicos frente à constatação do perigo de utilização que estes estão a causar sobre a população nacional e internacional.

Ao mesmo tempo em que esses mecanismos facilitaram muito a vida das pessoas, eles também estão sendo usados para praticar crimes com amplas conseqüências danosas, devido ao fato de haver ampla liberdade de comunicação e expressão dentro da rede, além da dificuldade de investigação gerada pelo anonimato que esta vem a oferecer.

Para isso, mostra-se fundamental a criminalização destas condutas danosas concomitantemente com a criação de medidas preventivas. Assim, a escolha do tema teve

como princípio norteador o fato de o Brasil ainda não dispor de uma norma especializada em crimes cibernéticos, apesar de tramitar na Comissão de Constituição, Justiça e Cidadania na Câmara dos Deputados, um projeto de lei substitutivo ao PL da Câmara nº 89, de 2003, e PLs do Senado nº 76 e 137, de 2000, versando sobre o referido assunto.

Essa ausência de legislação nacional sobre tais condutas tem gerado uma grande discussão dentro da sociedade moderna. A idéia é estudar uma legislação capaz de transpor de forma célere as fronteiras geográficas dos países, de modo a situar o público brasileiro no cenário internacional, assegurando, claro, o devido respeito aos Direitos Humanos.

Assim, o referido trabalho visa analisar a possível aderência do Brasil na Convenção de Budapeste, propondo orientar e discriminar o que é necessário para que ele se torne um signatário, além de ressaltar quais providências já foram tomadas para que isso ocorra, demonstrando, ainda, quais as razões alegadas pelo governo para não se ter aderido a tal acordo.

Dessa forma, visando debater o tema de forma bastante concisa, porém aprofundada, utilizou-se o método científico, onde foram agrupados os conhecimentos adquiridos com livros doutrinários e jurisprudências à análise dos casos práticos já existentes, possibilitando uma maior abrangência a respeito do assunto. Ademais, através do método dedutivo substancialista, objetivou-se projetar o que ocorre na prática, para o que ocorre no meio jurídico, visando alcançar um equilíbrio no que tange à aplicação de uma legislação capaz de suprir as necessidades do Estado brasileiro.

Sob este ponto, o referido estudo faz uma retrospectiva no tempo, demonstrando como surgiu a *internet* e quais foram os meios utilizados para conseguir remediar e evitar os danos gerados por tal inovação. Depois, chamou-se a atenção para o que vem a ser os crimes digitais e como eles estão presentes na nossa sociedade. E por fim, destacou-se os benefícios do direito comparado para se atingir o propósito aqui estipulado, qual seja, provocar algumas mudanças dentro da legislação brasileira, fazendo o Brasil se tornar um país membro da referida Convenção.

1 EVOLUÇÃO HISTÓRICA DA INTERNET E DA LEGISLAÇÃO REFERENTE AOS CRIMES CIBERNÉTICOS

Remontado às origens da *internet* é claramente visível a contribuição das guerras para toda inovação tecnológica, já que proporcionaram aplicações no desenvolvimento e bem-estar das pessoas[1]. Na Segunda Guerra Mundial, por exemplo, havia necessidade de descobrir meios eficazes para calcular a tabela de artilharia, surgindo então, o primeiro computador eletroeletrônico, o *Automatic Sequence Controlled Calculator* (ASSCC-Calculadora Automática de Sequência Controlada)[2].

No final dos anos 50 durante a guerra fria, com receio de uma guerra atômica, os Estados Unidos da América criaram uma agência, a ARPA (*Advacend Research Projects Agency*) para auxiliar em um possível ataque. Desse modo, esta agência criou uma instituição, a *Rand Corporation*, que tinha como estratégia fracionar as mensagens em pequenos pacotes, tendo cada um a sua própria rota, utilizando-se para tanto diversos meios físicos[3].

Neste sentido, faz-se necessário usar a imaginação para entender tal instituição: a rede teria que ser visualizada como uma máquina de tear, a qual produz várias linhas unidas por nós, sendo cada uma deles um computador, envolvendo dessa forma toda a extensão terrestre. Seguindo essa linha de raciocínio teríamos, em suma, um sistema interligado em rede que funcionaria mesmo se parte dele ficasse fora do ar. Por isso, o

---

[1] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 23.
[2] SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. São Paulo: Revista dos Tribunais, 2003, p. 17.
[3] Ibidem, p. 16.

objetivo da rede descentralizada seria dar opções de rota para os pacotes de dados fracionados. Assim, se algum computador para o qual determinado pacote de dados fosse enviado tiver sido destruído, ele seria direcionado para outra rota, unindo-se depois com os outros pacotes para refazer, na íntegra, a mensagem original[4].

Para que esse sistema pudesse funcionar com eficácia seria necessário criar um protocolo para que todos os computadores conectados à rede pudessem entrar em sintonia, pois se assim não o fosse, as mensagens iriam se perder. Portanto, é importante lembrar que a *internet* somente é viável devido à existência de diversos protocolos de comunicação conectados aos computadores[5].

Assim, foram sendo criados programas para colocar em prática tal dispositivo como o NCP (*Network Control Protocol)*, que foi o primeiro da lista, inaugurando este projeto. Depois, cronologicamente surgiram: o ARPANET (*Advanced Research Projects Agency Network*) com a conexão de quatro computadores: Três na Califórnia, nas Universidades de Stanford, Berkeley e na UCLA e um na Universidade de Utah; o Unix, na sua forma monousuária; o TCP (*Transmission Control Protocol*), com o objetivo principal de fragmentar as mensagens em pacotes e reuni-las no destino final, e o IP (*Internet Protocol*), com a função de descobrir a melhor rota para cada pacote de dados até o resultado final[6].

Após alguns anos, a ARPANET passou a ser gerenciada pela NSF (*Nacional Science Foundation*), órgão do governo americano. Desde então, com a missão de aumentar o meio para que pudesse passar mais informações em um período menor de tempo,

---

[4] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 23.
[5] Ibidem.
[6] Ibidem.

criou-se cinco centros de supercomputação, formando a NSFNET (*National Science Foundation Network*). Em 1990, a ARPANET passa a ser dividida em MILNET, com o objetivo de atender aos militares, e NSFNET para uso acadêmico. Já em 1991, a *internet* foi disponibilizada para as pessoas comuns através da brilhante inovação do cientista *Tim Bernes* Lee, que criou a conhecida *World Wide Web*, ou seja, o popular www,  é utilizado diariamente. Nessa época, foi gerado também o protocolo HTTP, que possibilitava o envio de dados criptografados para operações de dados comerciais pela *internet*. Era uma forma bastante simples para linguagem padrão geral, conhecida, também, como SGML, código usado para fazer os documentos legíveis em todas as plataformas e programas componentes da www[7].

É importante salientar que a *internet* não é a *World Wide Web*, uma vez que, devido ao seu desenvolvimento e amplidão, ela significa o veículo pelo qual o correio eletrônico, os servidores FTP[8], a www, o *Usenet*[9] e outros serviços trafegam. Portanto, a www ficou conhecida por deixar a **face** da *internet* acessível e interessante. Muitos a definem como uma interface, já que é a principal responsável por sua popularização. Junto com o progresso dos navegadores[10], propôs aos usuários a utilização da imagem, som e movimento nos textos[11].

O seu funcionamento é muito simples: passa necessariamente por quatro fases, obedecendo ao protocolo de transferência de hipertexto, o HTTP. Assim, a primeira

---

[7] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 23.
[8] Protocolo de transferência de arquivos: protocolo da Internet usado para transferir arquivos de um computador para outro.
[9] Rede para distribuição de novos itens e mensagens.
[10] Também conhecidos por *browser*. Programa de computador utilizado para visualização e procura de texto, imagens, gráficos e etc. das páginas alojadas nos servidores que compõem a Internet.
[11] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 08.

fase é marcada pela conexão, onde o usuário tenta relacionar-se com o servidor endereçado. Na segunda fase é definido o tipo de servidor selecionado, através do que se chama requerimento. Depois vem a fase da resposta, a qual há a transação de informações entre o usuário e o servidor. Por fim, há o fechamento, onde a conexão é realizada[12].

Em suma, para Gustavo Testa Corrêa:

> A www é um conjunto de padrões e tecnologias que possibilitam a utilização da *Internet* por meio dos programas navegadores, que por sua vez tiram todas as vantagens desse conjunto de padrões e tecnologias pela utilização do hipertexto e suas relações com a multimídia, como som e imagem, proporcionando ao usuário maior facilidade na sua utilização, e também a obtenção de melhores resultados[13].

Então a www é uma conjunção de informações relativas à rede, utilizando-se uma espécie de padrão universal de protocolo, permitindo o acesso de qualquer computador conectado à rede, tendo como missão difundir todo conhecimento nela presente, através de um gigantesco sistema de hipertexto, fazendo sua relação dentro de uma base única de dados. Assim, surgiu o que conhecemos por *internet*, que é o meio de comunicação pelo qual as pessoas têm a possibilidade de pesquisar e aprender sobre diversos temas, além de poder se relacionar umas com as outras em diversos lugares[14].

Entretanto, em face desse crescente relacionamento entre os indivíduos de todas as partes do mundo, cada vez mais próximos e comunicados, surgiu um problema de

---

[12] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 14.
[13] Ibidem, p. 11.
[14] Ibidem.

grande repercussão, decorrente da possibilidade de as pessoas utilizarem a *internet* para cometer crimes[15].

Durante a evolução tecnológica para encontrar um mecanismo eficaz que pudesse facilitar a busca de um equipamento para solucionar os cálculos matemáticos, não houve evidências de que o ser humano pudesse agir de forma a querer lesionar ou colocar em perigo de lesão algum bem jurídico no manuseio desses equipamentos. Por isso, cabe salientar que tais máquinas não foram utilizadas como objetos para qualquer prática delitiva, tendo em vista que elas eram exclusivamente manuseadas por pesquisadores que queriam tão somente a inovação tecnológica das mesmas e alcançar soluções rápidas e confiáveis que proporcionassem uma facilidade maior a eles[16].

Os problemas advindos da utilização errônea e equivocada de tais equipamentos, desvirtuando o objetivo inicial dos mesmos, iniciaram-se quando estes começaram a ser utilizados pela população em geral, saindo da esfera de utilização exclusiva da pesquisa para uso do homem comum[17].

Neste sentido, na década de sessenta é que foram detectados os primeiros casos de conduta criminosa, com o manuseio de dados, sabotagem, espionagem e abuso ilegal de sistemas de computadores, como observa Luciana Boiteux[18]. Por isso, pelo fato de a *internet* fazer parte do desenvolvimento do mundo globalizado, seria necessária uma legislação no Brasil capaz de suprir as necessidades atuais referentes a esses crimes

---

[15] SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. São Paulo: Revista dos Tribunais, 2003, p. 19
[16] Ibidem.
[17] Ibidem.
[18] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 156.

cibernéticos, uma vez que os ordenamentos jurídicos são espacial e temporalmente limitados na sua esfera de eficácia[19].

Através de algumas investigações a respeito do assunto, empregando utilmente métodos criminológicos conduzidos até a metade dos anos setenta, conseguiu-se concluir que a maioria dos crimes cometidos por meio de computadores permanecia não detectada ou até mesmo não divulgada, o que demonstrou para a população em geral o ponto fraco da tal sociedade da informação, gerando grandes debates acerca da necessidade de se priorizar a segurança e de se tentar controlar esses tipos de condutas consideradas lesivas ao meio social[20].

Desta forma, inoportunamente, quando surgiu a difusão das atividades cibernéticas, os estados nacionais não estavam organizados juridicamente para suportar tal fato. Assim, uma vez que estavam diante de um mundo real e não de um mundo paralelo a este, houve a necessidade de se rever alguns aspectos diante de todo este avanço da tecnologia, tendo em vista que qualquer embate nas relações interpessoais equivalia, igualmente, a uma reação no Direito. Neste sentido, os países necessitavam, urgentemente, fazer uma nova formulação de suas normas jurídicas, para que estas pudessem se adequar à nova realidade, munindo-se de um tratamento jurídico igualitário para o uso da documentação tradicional e da digital[21].

---

[19] SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. São Paulo: Revista dos Tribunais, 2003, p. 19.

[20] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 152.

[21] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 23.

Além do mais, essa reformulação terá que ser radical, já que todas as áreas do Direito terão que se adequar a essa transformação. Seguindo essa linha de raciocínio, seria contraditório que a verificação da necessidade de se adequar a esse novo mundo, fosse dificultado pelo atraso das normas jurídicas[22].

Neste sentido, faz-se necessário questionar se aos crimes cibernéticos seriam aplicadas novas figuras jurídicas ou se seriam utilizadas aquelas normas já existentes nas legislações de todo o mundo, cada um, claro, com sua devida peculiaridade[23].

Portanto, diante desse questionamento, fica evidente a necessidade da normatização dessas condutas, tendo em vista a velocidade com que elas se desenvolvem sem compatibilização jurídica. Assim, é imprescindível estabelecer uma proporção direta entre essas condutas criminosas e os ordenamentos jurídicos[24].

Nesta ocasião foram criadas as primeiras comissões européias voltadas para análise da delinquência informática, tendo como destaque a atuação da Associação Internacional de Direito Penal (AIDP), que foi pioneira na reunião de especialistas para o estudo do tema[25].

Segundo Demócrito Reinaldo Filho[26], com o surgimento da *internet* adveio a evidente idéia de que uma moderna sociedade estava se construindo: uma sociedade em que

---

[22] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 156.
[23] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 207.
[24] BOITEUX, op.cit., p. 156.
[25] Ibidem.
[26] Apud CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 14.

o poder da comunicação passou a representar um papel considerável e muito mais importante que qualquer outra forma de poder.

2 CRIMES DIGITAIS

Embora não se esteja nem perto de assistir ao fim do papel impresso, como queriam alguns profetas do apocalipse digital logo no início da febre "ponto.com", a verdade é que se caminha a passos largos para um novo limiar, que revolucionará ainda mais o mundo da informação no meio eletrônico[27].

Esta breve introdução tem o cunho de demonstrar algumas das implicações originadas pela chegada da era digital[28].

Atualmente, as pessoas e as grandes empresas estão altamente dependentes desse sistema de informação, tendo em vista que proporciona eficiência e eficácia diante dos outros meios de comunicação. O problema, entretanto, é que essa dependência as torna vulneráveis ao estrago, à perda e ao extravio de informações que porventura elas tenham vindo a armazenar dentro dos computadores[29].

Primeiramente, é essencial que se faça uma retrospectiva dentro do Direito Penal para compreender analogamente o que viria a ser um crime cibernético. Assim, verifica-se que a doutrina clássica define como sendo uma ação típica, antijurídica e culpável[30].

---

[27] GUEIROS JÚNIOR, Nehemias.. Internet Legal: O direito na tecnologia da informação. **Convergência das mídias:** Mundo Jurídico quer acompanhar. 1. ed. São Paulo: Saraiva, 2003, p. 137.
[28] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 1.
[29] Ibidem.
[30] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 206.

Para que esse conceito seja aplicado aos crimes cibernéticos, necessário é que se possa ampliar o seu campo de abrangência, adicionando o fato de serem estes praticados contra ou pelo emprego de sistemas informatizados[31].

Os crimes digitais são aqueles que estabelecem relação com as informações guardadas em arquivo ou que estão sendo trocadas pelos computadores, sendo elas acessadas ilicitamente e usadas para ameaçar ou fraudar[32].

Gustavo Testa Corrêa, citando Neil Barret, afirma que "a era da informática não afeta apenas as nossas empresas ou correio eletrônico, mas também toda a infra-estrutura nacional como a economia"[33].

Devido ao anonimato, a *internet* é um lugar propenso ao cometimento de delitos, pois oferece aos infratores maior segurança devido ao fato de não serem descobertos com tanta facilidade como seriam se estivessem agindo no campo da realidade não virtual[34].

Surge, porém, uma questão bastante interessante em torno deste assunto: esclarecer se a *internet* seria utilizada como meio e como fim para determinada conduta delituosa ou se, somente como meio. Neste sentido, há o crime de informática puro e o crime de informática impuro ou misto. No primeiro caso, tem-se o sistema de informática compreendido como meio e também como fim, almejado pelo criminoso virtual. O segundo,

---

[31] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 206.
[32] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 43.
[33] Apud CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 43.
[34] CORREA, op. cit., p. 44.

por sua vez, seria somente a utilização de tal sistema como meio, ou seja, como veículo para a prática de um delito que já está devidamente definido na legislação penal vigente[35].

Como exemplo de crime impuro pode-se citar a pornografia que, de acordo com um estudo realizado pela Universidade de Carnegie-Mellon, ficou constatado que mais de 80% das fotografias enviadas pela *internet* têm cunho pornográfico. Mas, ainda assim, esse número é irrisório, uma vez que a Rede é o veículo perfeito para a ação de comerciantes fraudulentos, pedófilos, piratas de *software*, traficantes de informação terrorista, *hackers* e muito mais[36].

Já em relação ao crime puro, tem-se que, da mesma maneira que um indivíduo na vida real pode sofrer ou causar algum ato ilícito, outro indivíduo navegando pela *Internet* é perfeitamente vulnerável à ação de *hackers* e vírus de computadores quando seus agentes infringem algumas normas estabelecidas por alguns sistemas de segurança das empresas ligadas à rede, remetendo também mensagens eletrônicas ameaçando a todos que estão a sua volta[37].

Assim, cabe ressaltar que no caso dos crimes informáticos puros, a infração a determinado bem jurídico não está prevista em lei, tendo sido atribuída, nestes casos, a impunidade por ausência de regulamentação específica na área de direito penal, dando vazão à atuação dos agentes criminosos[38].

---

[35] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais**.** São Paulo: Edipro, 2001, p. 206 e 207.
[36] Ibidem.
[37] Ibidem, p. 208.
[38] Ibidem.

Quanto aos crimes mistos, os infratores cometem delitos previstos na legislação nacional, porém os cometem utilizando a *internet*. Nestes casos, portanto, não há que se falar em novos tipos penais, pois os bens que porventura forem violados já estão devidamente tutelados pelo Código Penal e por Leis Penais Especiais[39].

Assim, fica evidente que tais inovações tecnológicas apenas acrescentaram um novo *modus operandi*, ou seja, um novo meio para a execução do crime. Entretanto, seja como for, a previsão constante na lei não fala no emprego da *internet* como uma nova possibilidade para a obtenção do resultado final do crime[40].

Por isso, neste sentido faz-se necessário remeter-se ao princípio da reserva legal disposto no artigo 1º, do Código Penal Brasileiro, qual seja, "não há crime sem lei anterior que o defina" e "não há pena sem prévia cominação legal", para afirmar a impossibilidade do emprego da analogia *malem partem* e fazer algumas observações acerca do tema[41].

Dessa forma, cabe salientar a discordância em relação ao que foi dito pelo Ministro do Supremo Tribunal Federal, Sepúlveda Pertence: "invenção da pólvora, não reclamou a definição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo"[42]. A *internet* em nada pode ser comparada com a pólvora, uma vez que não há nenhuma ligação direta entre ela e qualquer instrumento de alta periculosidade, como entre o computador e a arma de fogo. Para haver a morte, é

---

[39] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 23.
[40] Ibidem.
[41] Ibidem.
[42] SUPERIOR TRIBUNAL DE JUSTIÇA. 1ª Turma. HC nº 76.689. Ementa:[...]Relator: Sepúlveda Pertence. DJU 6.11.1998, p. 3.

imprescindível que haja um instrumento vulnerante capaz de ferir alguém e matá-lo. Em relação ao computador, não se pode fazer a mesma afirmação, já que a *internet* não está intimamente ligada com nenhum tipo de crime, principalmente com o de homicídio.

Uma pessoa pode vir a auxiliar alguém a cometer suicídio por meio de um computador sem ter que lhe oferecer uma corda para a realização de tal feito. Apenas utilizando a *internet*, através de uma *web cam*, por exemplo, é possível induzir alguém a se matar sem que se esteja fisicamente presente ao lado da pessoa. Por isso, é inconcebível a comparação feita pelo Ministro em relação ao referido tema[43].

Seguindo esta linha de raciocínio, é *mister* que haja uma legislação específica tratando dos crimes informáticos impuros de forma mais concisa e eficaz, tendo em vista que não se pode dar o mesmo peso a um crime de estelionato cometido na vida real a um cometido na virtual[44].

Uma solução ideal para a previsão legislativa concreta desses crimes seria adicionar uma espécie de qualificação para cada delito previamente descrito no Código Penal Brasileiro. Neste viés, para a cominação da pena, o fato de o indivíduo ter cometido determinado crime por meio da *internet* será levado em consideração como agravante, qualificadora ou causa de aumento de pena[45].

Assim, ficaria equilibrado o cometimento de tais crimes em relação àqueles nos quais não se utiliza este veículo de comunicação para chegar ao resultado final do delito. Não seria justo processar e julgar uma pessoa que cometeu o crime de peculato no mundo

---

[43] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 10.
[44] Ibidem.
[45] Ibidem.

material da mesma forma que uma pessoa que o cometeu no mundo digital, tendo em vista que a *internet* abre um leque maior de opções para executá-lo, uma vez que a prática de tal delito pode gerar efeitos em locais distantes e diferentes entre si, dificultando a localização do agente[46].

Devido a isso, o referido tema torna-se controverso, já que alguns doutrinadores acreditam que havendo legislação vigente que trate de determinados crimes, seria desnecessário criar outras leis que abordassem o mesmo conteúdo[47].

O problema, entretanto, é que os profissionais do Direito não percebem que as leis atuais não estabelecem corretamente as condutas delituosas ora em questão. Assim, é utópico acreditar que o sistema penal atual consiga suprir as necessidades de punição pelo Estado aos crimes informáticos impuros. Que dirá, então, em relação aos crimes cibernéticos puros[48].

As atuais leis podem ser empregadas em tais casos, porém, elas teriam que passar por algumas mudanças com a adição de alguns pontos, que utilizados conjuntamente com o que já está previsto, atingiriam de maneira mais eficaz o seu objetivo[49].

O grande desafio é compreender e acompanhar as inovações, uma vez que na base de cada estudo que venha a ser realizado é de extrema importância que se garanta a

---

[46] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 157.

[47] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 208.

[48] PINHEIRO, Patrícia Peck. **Direito Digital**. 2. ed. São Paulo: Saraiva, 2007, p. 25.

[49] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 59.

pacificação social, o desenvolvimento sustentável das novas relações que irão surgir e, principalmente a manutenção do próprio Estado Democrático de Direito[50].

Aos operadores do direito é dada a difícil tarefa de pesquisar e descobrir respostas sensatas e inteligentes, capazes de suprir as necessidades advindas dessa nova era tecnológica, dando ensejo a uma coexistência pacífica entre os indivíduos e esse novo mundo que surge[51].

Em resumo, é claramente visível que uma fraude eletrônica é uma prática totalmente diferente do fato de enviar um *e-mail* contendo pornografia infantil[52]. Entretanto, pelo fato de ambos terem sido cometidos através do computador, são classificados equivocadamente, por alguns doutrinadores, como crimes informáticos em geral, sem que haja distinção em relação a crimes puros e impuros. E analisando sob o aspecto da distância e da velocidade fornecidas a ambos pelo espaço cibernético, é completamente compreensível que tais doutrinadores as agrupem dentro de uma mesma classificação, tendo em vista que não restam suspeitas de que essas condutas delituosas promovem por si só, um aumento de sua potencialidade lesiva ao bem jurídico protegido quando praticadas através da *internet*, pouco importando se essas condutas já existiam ou não dentro do ordenamento jurídico. Essa idéia, contudo, apesar de compreensível, não possui qualquer fundamento e tem que ser modificada.

---

[50] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 159.

[51] PINHEIRO, Patrícia Peck. **Direito Digital**. 2. ed. São Paulo: Saraiva, 2007, p. 35.

[52] Ibidem, p. 156.

3 POLÍTICAS CRIMINAIS DE PREVENÇÃO E REPRESSÃO DOS CRIMES DIGITAIS

A lei é, foi, e sempre será de extrema importância para a precaução e punição dos delitos, tanto no mundo real como no mundo virtual[53].

Para Hans Kelsen:

> O Direito é uma ordem normativa da conduta humana, ou seja, um sistema de normas que regulam o comportamento humano. Como o termo 'norma' se quer significar que algo deve ser ou acontecer, especialmente que um homem se deve conduzir de determinada maneira. É este o sentido que possuem determinados atos humanos que intencionalmente se dirigem à conduta de outrem[54].

É por meio da lei que o imoral e as condutas ilícitas conseguem ser evitadas, permitindo que a sociedade e o Estado conviverem com maiores garantias e proteção relação à violência existente. Entretanto, mesmo assim é muito difícil assegurar que todos venham a cumpri-la[55].

A inovação tecnológica já virou uma realidade. Porém, tendo em vista que o ordenamento jurídico vigente não vem acompanhando tal inovação, é possível que se venha a deparar, dentro da legislação brasileira[56], com algumas lacunas[57], as quais o Direito tem a obrigação de preencher, mediante um esforço sério e concentrado para pesquisar e compreender sua real necessidade e abrangência. Nos casos de omissão da lei, é aplicado o princípio da auto regulamentação. Esse princípio, se é que pode se chamar dessa maneira,

---

[53] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 58.
[54] Apud CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 58.
[55] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 159.
[56] CORRÊA, op. cit., p. 58.
[57] Quando a lei silencia ou nem sucintamente se refere ao caso em concreto, cuja hipótese deveria prever.

parte da premissa de que ninguém melhor do que o próprio interessado para saber quais são as lacunas que o Direito deve preencher[58].

Analisando tal situação, fica evidente a grande contradição que se está vivendo hoje em dia dentro do Direito Brasileiro. Enquanto as inovações tecnológicas se sucedem com rapidez estonteante, está se aplicando, ao que parece, um instituto denominado autotutela, que é encarada como precária e aleatória, pois somente foi utilizada nas fases primitivas da civilização dos povos, onde não havia o Estado para impor a sua vontade acima da vontade de particulares[59]. É necessário, primeiramente, aceitar que a tecnologia avançou mais do que a legislação poderia alcançar, pois a partir da criação da *internet*, se evidenciou o surgimento de novos conceitos sobre valores antigos, como o surgimento dos crimes cibernéticos.

Para Patrícia Peck Pinheiro:

> [...] a auto regulamentação permite maior adequação do direito à realidade social, assim com maior dinâmica e flexibilidade para que ele possa perdurar no tempo e manter-se eficaz. O princípio que norteia a auto regulamentação é o de legislar sem muita burocracia, observando a Constituição e as leis vigentes[60].

Perante tal afirmação, surge uma questão importante: até quando, de fato, tal princípio conseguirá se manter eficaz? Talvez até quando o **legislar sem burocracia** não ultrapassar os limites da esfera individual de cada um, pois do contrário, irá se instaurar o caos no mundo globalizado, onde a legislação penal vigente será um retorno ao talião, olho por olho, dente por dente. Com o aumento dos crimes cibernéticos se perderá o controle e não

---

[58] PINHEIRO, Patrícia Peck. **Direito Digital**. 2. ed. São Paulo: Saraiva, 2007, p. 47.
[59] GRINOVER, Ada Pellegrini. **Teoria Geral do Processo**. 22. ed. São Paulo: Malheiros, 2006, p. 27.
[60] PINHEIRO, op. cit., p. 48.

se conseguirá estabelecer um equilíbrio, querendo todos fazer justiça com as suas próprias mãos.

Diante de toda essa situação e com o avanço cada vez maior da tecnologia, não é possível falar somente em medidas de prevenção, tendo em vista que a situação já fugiu ao controle há algum tempo. Claro que essas terão que existir, porém, juntamente com uma política criminal repressiva intensa de combate a referidos delitos[61].

Para alguns doutrinadores como Luciana Boiteux[62], a prevenção seria mais eficaz que a mera previsão legal de tipos especiais, pois em sua opinião o direito penal não serve à finalidade de impedir a prática de delitos. Porém, seguindo essa linha de raciocínio, chegaria a uma conclusão um tanto quanto absurda. Talvez a autora até tenha partido de premissas corretas para fazer tal afirmação, uma vez que de acordo com os princípios da intervenção mínima e da fragmentariedade do Direito Penal, somente as condutas mais gravosas realizadas contra os bens jurídicos mais importantes é que devem ser punidas. Contudo, há de se observar que estes princípios se relacionam somente com uma parcela dos bens jurídicos protegidos pela ordem jurídica, e no caso em tela, os delitos cibernéticos estariam sem sombra de dúvida, dentro deste espectro de abrangência.

Desse modo, no que tange ao objetivo de inibir e desestimular a prática de condutas delituosas cometidas através do uso de computadores, não há mais tempo para aplicar apenas sanções administrativas, com penas de multa e medidas educativas[63]. No momento atual, em que as pessoas já sabem perfeitamente o que podem e o que não podem

---

[61] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 159.

[62] Ibidem.

[63] PINHEIRO, Patrícia Peck. **Direito Digital**. 2. ed. São Paulo: Saraiva, 2007, p. 48.

fazer quando navegam na rede, a sanção deve ser proporcional à conduta praticada[64]. Assim, analisando atentamente os crimes cibernéticos e seus potenciais infratores, será que estes realmente atingem bens jurídicos de menor importância, para poderem ser tratados dessa forma? Será que a sociedade se tornaria mais segura caso as pessoas conseguissem adotar técnicas de prevenção tão eficazes a ponto de deixarem de utilizar o computador? Seria uma hipocrisia acreditar nisso.

Nesse ramo há muita esperteza. Normalmente, o criador de um vírus é o mesmo que vende o anti-vírus e depois é contratado pela empresa vítima do golpe. É muito comum o envolvimento de profissionais de informática em práticas delituosas através de computadores[65]. E se deixar as coisas como estão, pensando apenas em políticas criminais preventivas, essas pessoas irão adquirir cada vez mais poder e todos os demais indivíduos terão que se submeter a elas. A *internet* está virando um mercado negro, onde as pessoas estão querendo se promover a qualquer custo, mesmo que venham a infringir determinadas normas.

Os crimes de informática são de rápida execução[66] e podem ofender pessoas e bens de vários lugares do mundo ao mesmo tempo, sem que se possa descobrir sua autoria[67]. Daí ser necessário não apenas falar em medidas de prevenção, o que será perda de tempo, pois se passará uma sensação de impunidade e de tolerância quanto aos crimes praticados com o uso dos recursos da *internet*[68]. Por certo naqueles casos menos graves (raríssimos, inclusive, devido à própria natureza do ato), onde não seja atingido um bem jurídico

---

[64] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 31.
[65] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 162.
[66] PINHEIRO, Patrícia Peck. **Direito Digital**. 2. ed. São Paulo: Saraiva, 2007, p. 31.
[67] Ibidem, p. 39.
[68] BOITEUX, op.cit., p. 165.

constitucionalmente relevante, não se descarta a possibilidade da utilização de medidas preventivas[69].

E, para exercer o papel de prevenção dos delitos informáticos, o ideal seria chamar o Comitê Gestor Internet do Brasil, que criado pela Portaria Interministerial n. 147, de 31 de maio de 1995, que tem a função de dar efetividade à participação da sociedade nas decisões que giram em torno de questões[70] como a implantação, administração e fruição da *internet*. Tal comitê tem, ainda, como principais atribuições[71] fomentar o desenvolvimento de serviços ligados à *internet* no Brasil; recomendar padrões e procedimentos técnicos e operacionais para a *internet* no País; coordenar a atribuição de endereços na *internet*, o registro de nomes de domínios e a interconexão de espinhas dorsais, além de coletar, organizar e disseminar informações sobre os serviços ligados à *internet*. Assim, não seria nada mal se esse Comitê viesse a auxiliar na política de prevenção criminal, juntamente com a criação de leis específicas para crimes cibernéticos.

Para Gustavo Testa Corrêa:

> O Comitê Gestor Internet do Brasil é o maior exemplo da tendência mundial a tornar a *internet* algo desvinculado do Poder Público, incentivando a participação da sociedade civil na formulação de diretrizes básicas para o desenvolvimento organizado[72].

Resumindo, o Direito Penal não constitui um conjunto fatigante de proteção de bens jurídicos, abrangendo todos eles sem exceção, mas representa um conjunto descontínuo de seleção de ilícitos derivada da necessidade de criminalizá-los ante a

---

[69] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p.165.
[70] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. Ed. São Paulo: Saraiva, 2002, p. 17.
[71] Ibidem.
[72] Ibidem, p. 18.

imprescindibilidade da proteção jurídico-penal, como nos casos dos crimes ora em discussão. Segundo Rogério Grecco, "nem tudo interessa para o direito penal, mas tão somente uma pequena parte, uma limitada parcela de bens que estão sob a sua proteção, mas que sem dúvida, pelo menos em tese, são os mais importantes e necessários ao convívio da sociedade"[73].

[73] GRECCO, Rogério. **Curso de Direito Penal**: parte geral. 11. ed. São Paulo: Impetus, 2009, vol. 1, p. 40.

4 DIREITO COMPARADO

O Direito Comparado oferece a oportunidade de entrar em contato com atividades e iniciativas relevantes e positivas por parte das legislações internacionais, além de possibilitar o acesso a criações inovadoras de vários países, obtendo delas o essencial e fundamental para tentar adaptá-las ao mundo atual[74].

A idéia de abordar referido ramo do direito fundou-se no fato do país ainda não ter abordado pela legislação ora vigente, leis que tratem de crimes digitais. Assim, o objetivo aqui presente está calcado na hipótese do Brasil, espelhando-se em ordenamentos jurídicos internacionais, criar leis que possibilitem abordar tal tema de forma concisa e coerente de acordo com o que é feito em outros lugares do mundo[75].

Alguns países, como Inglaterra e Estados Unidos da América, se destacaram por terem saído na frente na corrida contra o tempo no que diz respeito à criação de leis que se adequem ao contexto atual[76].

Diante do conjunto de transformações na ordem política e econômica mundial que vem acontecendo nas últimas décadas, estes países promoveram algumas mudanças positivas em seus ordenamentos jurídicos[77]. Algumas condutas que antes pareciam inocentes e desprovidas de tipificação penal ganharam notoriedade e passaram a gerar danos quase que irreparáveis para a sociedade. Diante desta situação, foi necessário delinear uma

---

[74] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 632.
[75] Ibidem.
[76] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 64.
[77] Ibidem.

estratégia para combater tais condutas, que prejudiciais à população, não podiam continuar impunes.

No Reino Unido, até meados dos anos 80, o *hacking*[78] não era considerada uma conduta típica, anti-jurídica e culpável. Apenas tinha o caráter de ofensa disciplinar. Porém, a partir do momento em que essa conduta tornou-se uma prática constante dentro das universidades, fez-se necessário a criação de uma lei para poder conter tal situação. O *Computer Misuse Act* (Lei de Abuso por Computadores) definiu três tipos de ofensas criminais: Ofensa que envolve o ganho não autorizado de acesso a um computador, ou a uma parte dele (Essa é a mais geral das especificações); Ofensa que envolve o ganho não autorizado de acesso a um computador ou a uma parte dele, com a intenção de violar a lei posteriormente, e também ofensa que envolve o ganho não autorizado de acesso a um computador, ou a uma parte dele com a intenção de modificar os seus dados, obstando o seu funcionamento ou acesso de usuário autorizado[79].

Já em 1986, nos Estados Unidos, foi promulgada a *Computer Fraud and Abuse Act* (Lei de Fraudes e Abusos por computador), tendo sido considerada a lei mais importante no que tange aos crimes digitais. Ela tipificou várias atividades, objetivando esclarecer ao violador de determinado sistema que sua conduta ia contra as regras da sociedade e assim poderia esta vir a ser punida[80].

Ainda neste mesmo país, foram criadas a *Children´s Internet Protection Act of 2000* (Lei de Proteção a Criança nas Internet- LPCI) e *Communications Decency Act of*

---

[78] Hacking é o crime cometido por uma pessoa, que tendo notório conhecimento em sistemas operacionais (*hacker*) penetra no sistema alheio.
[79] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. Ed. São Paulo: Saraiva, 2002, p. 65 e 66.
[80] Ibidem, p. 64 e 65.

1996 (Lei da Moralização das Comunicações). A primeira, com o objetivo de proteger crianças que acessam a *internet* de materiais prejudiciais na rede, obrigou "a utilização de uma tecnologia que bloqueia ou filtra o acesso, tanto de menores[81] quanto de adultos, a materiais obscenos ou pornografia infantil". A segunda, por sua vez, depois de devidamente aprovada pelo Congresso norte-americano em 1996, como parte de uma lei mais abrangente, denominada "Lei das Telecomunicações" e imediatamente após ter sido sancionada, foi declarada inconstitucional, tendo em vista que violava a Primeira Emenda da Constituição norte-americana que dizia que o Congresso não faria nenhuma lei que pudesse cercear a liberdade de expressão de seus cidadãos[82].

Essa lei relacionada à divulgação de informações pelos meios de comunicação, de autoria do Senador do Estado de Nebraska, James Exon, foi sancionada pelo ex-presidente dos Estados Unidos da América, Bill Clinton. Ela enunciava o controle da propagação de tudo que fosse considerado reprovável. A referida lei se originou de uma reação da sociedade local no que dizia respeito ao atentado ocorrido contra o prédio público em Oklahoma, quando os meios de telecomunicação expuseram à população que na *internet* estava disponível conteúdo que ensinava a confecção de bombas caseiras e até como conduzir campanhas terroristas[83].

Assim, o caso foi a julgamento onde, de um lado estava a União Americana para a Defesa das Liberdades Civis e os provedores, e do outro o governo e sua **Exon Bill** ficando a sua inconstitucionalidade por ferir a liberdade de expressão. Do mesmo modo

---

[81] A LPCI define "menor" como alguém que ainda não completou 17 anos de idade.
[82] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 639.
[83] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 98.

ocorreu com a *America OnLine (AOL)*, que não pôde ser responsabilizada por informações propagadas através de seus sistemas.

Aqui no Brasil, em princípio os crimes cibernéticos foram tratados pela doutrina como um incidente do ramo do direito penal econômico, uma vez que foi dada preferência à proteção de programas de computadores, relativamente ao tempo de realização do seu direito com preterição do de outros, provavelmente por influências exercidas pelas empresas multinacionais, tendo sido editada uma legislação que os colocou sob a defesa das leis de direitos autorais. (Lei 7.646, de 18 de dezembro de 1987)[84] [85].

Depois, aumentou-se a lista das condutas cometidas através do computador, tendo sido editada a Lei 8.137/1990, que preceitua os delitos contra a ordem tributária, a qual no seu art. 2º, define como crime a conduta de "utilizar ou divulgar programas de processamento de dados para fins de sonegação fiscal". Já em 1995, com a Lei 9.100 outros tipos penais foram previstos, como o "acesso indevido a sistema de tratamento automático de dados utilizados pelo serviço eleitoral, com o fim de alterar a apuração ou a contagem dos votos (art. 67, VII), e a alteração de programas de computador para provocar resultado diverso do esperado em sistema de votação eletrônica (art. 67, VIII)[86].

Dessa forma, com a edição da Lei 9.983 de 14 de julho de 2000, que tendo alterado e incluído alguns artigos no Código Penal Brasileiro criou novos institutos como fim de proteger dados e sistemas de informações, por exemplo, conforme consta do art. 313-B,

---

[84] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. Revista Brasileira de Ciências Criminais. São Paulo: Revista dos Tribunais, 2004, p. 173.

[85] Especificamente sobre a proteção da propriedade intelectual de programas de computador, foram editadas em nosso País posteriormente as Leis 9.069/1998 e 9.610/1998.

[86] BOITEUX, op.cit., p. 173.

caput do referido Código, crimes próprios de funcionários públicos que modifiquem ou alterem sistemas informáticos da Administração Pública, punindo também a divulgação de informações sigilosas de bancos de dados oficiais, de acordo com o que dispõe o artigo 153, parágrafo 1-A, do Diploma Penal[87].

A falta de legislação específica que trate de crimes cibernéticos é constatada pela jurisprudência do Supremo Tribunal Federal, no julgamento do HC nº 76.689, cuja ementa é a seguinte:

> CRIME DE COMPUTADOR: PUBLICAÇÃO DE CENA DE SEXO INFATO JUVENIL (E.C.A., ART. 241). MEDIANTE INSERÇÃO EM REDE BBS/INTERNET DE COMPUTADORES, ATRIBUÍDA A MENORES: TIPICIDADE: PROVA PERICIAL NECESSÁRIA À DEMONSTRAÇÃO DA AUTORIA: HC DEFERIDO EM PARTE.
> 1. O tipo cogitado - na modalidade de 'publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente' - ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.
> 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.
> 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial.[88]

Atualmente, diante do acesso ilimitado de pessoas à *internet*, verificou-se além de um aumento de delitos praticados por meio de computadores, uma maior incidência

---

[87] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 154.

[88] SUPERIOR TRIBUNAL DE JUSTIÇA. 1ª Turma. HC nº 76.689. Ementa:[...]Relator: Sepúlveda Pertence. Brasília, DF, 28 set. 98. DJU 6.11.1998, p. 3.

de determinadas condutas delituosas[89]. Neste sentido, algumas propostas foram feitas para a regulamentação de tais condutas. Como destaque tem-se o atual projeto de lei do Senador Eduardo Azeredo do PMDB-MG, que substitui os projetos de lei da Câmara 137/2000, 76/2000 e 89/2003[90].

O atual projeto referente aos crimes cibernéticos, de autoria do Senador Eduardo Azeredo, em trâmite perante a Câmara dos Deputados, está sendo considerado inconstitucional, uma vez que não há o equilíbrio entre a repressão penal às condutas mais graves e a garantia e o respeito aos direitos humanos, à liberdade de expressão e de circulação e principalmente no que se refere ao mais democrático e livre espaço de comunicação mundial[91].

A intenção do político era reunir projetos anteriores e transformá-los em uma lei única que pudesse alterar em alguns pontos o Código Penal Brasileiro. Esse substitutivo, aprovado pela Comissão de Constituição e Justiça e votado pelo plenário do Senado está na Câmara dos Deputados, e passará por algumas comissões para depois ser votado em plenário, mas não tem data prevista para a apreciação dos parlamentares[92].

É um trâmite longo, tendo assim, tempo suficiente para analisar e verificar a procedência de cada fundamento a ser utilizado, havendo a possibilidade de impedir que esse projeto vire lei. Para tanto, faz-se necessário entender qual o conteúdo de tal projeto que

---

[89] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. Revista Brasileira de Ciências Criminais. São Paulo: Revista dos Tribunais, 2004, p. 173.

[90] It Web. Projeto de lei para crimes na internet passa no Senado. São Paulo, 10 jul. 09. Disponível em: <http://www.itweb.com.br/noticias/index.asp?cod=49540>. Acesso em: 4 out. 09.

[91] Folha Online. Críticos comparam lei sobre internet ao AI-5. São Paulo, 11 mai. 09. Disponível em: <http://www.tudoagora.com.br/noticia/18768/Criticos-comparam-lei-sobre-internet-ao-AI-5.html>. Acesso em: 4 out. 09.

[92] Ibidem.

dentre outras coisas, pretende liquidar com o avanço das redes de conexão abertas (Wi-Fi) e ainda, ordenar que todos os provedores de acesso à Internet denunciem seus usuários, colocando-os em uma situação constrangedora. Dessa forma, se o projeto for aprovado, dezenas de atividades criativas poderão ser consideradas criminosas de acordo com seu artigo 285-B. Assim, instaurar-se-ia uma séria ameaça à diversidade da rede e às possibilidades recombinantes, além do medo e da vigilância[93].

Este projeto de lei cria o provedor que delata, infringindo assim, um princípio maior, que seria o direito a privacidade previsto no artigo 5, inciso X, da Constituição Federal: "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". Em suma, se tal projeto virar lei, instaurar-se-ia um estado de polícia, onde a vigilância seria diária[94].

Outro problema do referido projeto é a proibição de que se "obtenha dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida". A pena varia de 2 a 4 anos, mais multa. O objetivo, evidentemente, é impedir a pirataria. Porém, seria totalmente fora do normal ter a necessidade de provar que está autorizado a carregar qualquer informação colhida na *internet*[95].

---

[93] It Web. Projeto de lei para crimes na internet passa no Senado. São Paulo, 10 jul. 09. Disponível em: <http://www.itweb.com.br/noticias/index.asp?cod=49540>. Acesso em: 4 out. 09.

[94] MARTINS, Paulo Mário. **Críticas ao Projeto de lei de Crimes Digitais dão tom â audiência esvaziada.** Disponível em: <http://www.safernet.org.br/site/noticias/cr%C3%ADticas-ao-projeto-lei-crimes-digitais-d%C3%A3-tom-audi%C3%AAncia-esvaziada>. Acesso em: 03 out. 09.

[95] Ibidem.

A rede é, fundamentalmente, uma máquina de cópias. *A priori*, muitas pessoas defendiam a idéia de que o conteúdo disponibilizado pela *Internet* não possuía direito algum. Acreditava-se que toda e qualquer informação veiculada por ela era de domínio público e devido a este fato, poderia reproduzi-la sem prévia autorização do autor.

Atualmente, essa questão já está sedimentada:

> O Google está digitalizando milhares de livros fora de catálogo. Muitos deles têm o detentor do copyright desconhecido. Se o dono aparecer, eles tiram da lista. Em caso contrário, fica público. No Brasil, se o substituto do senador Azeredo for aprovado, esta que será a maior biblioteca pública do mundo será ilegal[96].

O projeto de lei poderá virar letra morta assim que entrar em vigor e gerará um problema de grande dimensão, uma vez que alguns farão o que enuncia o referido texto e outros não, arguindo que é inconstitucional. E como já não bastasse o país ter muitas leis consideradas ineficazes e inconstitucionais em vigor, vem mais uma para aumentar este grupo e paralisar o sistema.

O senador não foi feliz em redigir tal projeto que teria tudo para trazer ao Brasil uma legislação decente a respeito do referido tema: Visando proteger os interesses de empresas estrangeiras da indústria do entretenimento, não se preocupa em proteger os cidadãos brasileiros, vítimas de crimes na rede[97].

A *internet* deveria ter somente uma utilidade: disseminar informação e facilitar as relações interpessoais. Não seria justo os inocentes pagarem pelos culpados. O

---

[96] MAIA, Felipe. Críticos comparam lei sobre internet ao AI-5 e anunciam protesto em SP. **Folha Online,** São Paulo, 11 mai. 09. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u562920.shtml>. Acesso em: 1 out. 09.

[97] Ibidem.

direito à informação na rede não pode ser tornado ilegal. A matéria gera críticas de diferentes setores da sociedade civil, por supostamente ter o potencial de promover a criminalização em massa de usuários de internet. O senador nega as acusações[98].

Ao todo, o projeto prevê a criação de treze novos crimes, com penas que variam de um a três anos de prisão. O texto abrange crime de estelionato e falsificação de dados eletrônicos ou documentos, criação ou divulgação de arquivos com material pornográfico envolvendo crianças e adolescentes, roubo de senhas de usuários do comércio eletrônico e divulgação de imagens privadas[99].

O projeto provocou reações no País inteiro. Em várias cidades foram realizadas manifestações contrárias, onde se argumentava que o propósito do senador era criminalizar práticas cotidianas na *internet* e tornar suspeitas as redes P2P[100], tornando a fiscalização DRM[101] mais forte e intensa, gerando uma espécie de impedimento ao livre uso de aparelhos digitais e também ao direito à liberdade de expressão[102]. Tais manifestos, inclusive, foram chamados de "Ato Conta o AI-5 Digital"[103].

Os críticos do projeto consideram o texto demasiadamente amplo e, por isso mesmo vago, ao tratar resumidamente de crimes importantes que mereceriam uma consideração maior. O projeto indica, por exemplo, que o fato dos usuários de *internet* que

---

[98] FELITTI, Guilherme. **Crime digital:** compare as principais leis mundiais com o projeto de lei. Disponível em: <http://www.safernet.org.br/site/noticias/crime-digital-compare-principais-leis-mundiais-com-projeto-brasileiro>. Acesso em: 03 out. 09.

[99] MAIA, Felipe. Críticos comparam lei sobre internet ao AI-5 e anunciam protesto em SP. **Folha Online,** São Paulo, 11 mai. 09. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u562920.shtml>. Acesso em: 1 out. 09.

[100] Peer-to-peer: Conexão sem fio, similar à Wi-fi, que possibilita a troca de arquivos on-line.

[101] Sistema que limita o número de cópias possíveis de um arquivo.

[102] Uol. Senado aprova projeto de lei que tipifica crimes cometidos na Internet. Disponível em: <http://tecnologia.uol.com.br/ultnot/2008/07/10/ult4213u492.jhtm>. Acesso em 03 out. 09.

[103] MAIA, op. cit.

baixam e trocarem, uns com os outros, arquivos (músicas, textos e vídeos) sem autorização do titular é crime, comparando tal conduta com a pirataria. O que seria contraditório, pois praticar tal conduta é totalmente diferente do referido crime[104].

Um exemplo significativo da dificuldade de repressão ao uso da *internet* para fins ilícitos ou imorais ocorreu no Estado da Bahia, onde o Ministério Público ofereceu denúncia contra determinado provedor de *internet* que era utilizado para a divulgação de pornografia infantil por um de seus clientes, tendo em vista o disposto no Estatuto da Criança e do Adolescente[105]. A denúncia foi recebida e ensejou mandado de busca e apreensão do computador utilizado para a disseminação do referido material, como também, para a apreensão de todos os demais computadores do provedor em questão[106].

Mas, no caso, era claramente visível o cometimento do crime previsto no artigo 241 do Estatuto da Criança e do Adolescente, que preceitua que fotografar ou publicar cena de sexo explícito ou pornografia envolvendo criança ou adolescente tipifica crime de reclusão. Porém, não se pode atribuir tal infração à empresa provedora de *internet*, uma vez que um provedor de serviço à rede é apenas o intermediário entre o usuário e a conexão. Neste caso, há que se considerar, portanto, o que preceitua a Constituição Federal no artigo 5, inciso XII[107]: "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".

---

[104] BOCCHINI, Bruno. **Práticas cotidianas na Internet podem virar crime, avalia professor.** Disponível em: <http://www.ecosdanoticia.com.br/index.php?option=com_content&task=view&id=6299&Itemid=84>. Acesso em 1 out. 09.

[105] KAMINSKI, Omar. **Internet Legal:** O direito na tecnologia da informação. 1. ed. Curitiba: Juruá, 2003, p. 19.

[106] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 99.

[107] Ibidem, p. 100.

Consoante o que decidiu o Superior Tribunal de Justiça, em acórdão recente, somente poderá haver quebra de sigilo para fins de investigação criminal ou instrução criminal e somente com autorização judicial. Eis o seu teor:

> CONSTITUCIONAL. PROCESSUAL PENAL. HABEAS-CORPUS. SIGILO DE DADOS. QUEBRA. BUSCA E APREENSÃO. INDÍCIOS DE CRIME. INVESTIGAÇÃO CRIMINAL. LEGALIDADE. CF, ART. 5º, XII. LEIS 9.034/95 E 9.296/96.
> - Embora a Carta Magna, no capítulo das franquias democráticas ponha em destaque o direito à privacidade, contém expressa ressalva para admitir a quebra do sigilo para fins de investigação criminal ou instrução processual penal (art. 5º, XII), por ordem judicial.
> - A jurisprudência pretoriana é unissonante na afirmação de que o direito ao sigilo bancário, bem como ao sigilo de dados, a despeito de sua magnitude constitucional, não é um direito absoluto, cedendo espaço quando presente em maior dimensão o interesse público.
> - A legislação integrativa do - canon - constitucional autoriza, em sede de persecução criminal, mediante autorização judicial, "o acesso a dados, documentos e informações fiscais, bancários, financeiras e eleitorais" (Lei nº 9.034/95, art. 2º, III), bem como " a interceptação do fluxo de comunicações em sistema de informática e telemática" (Lei nº 9.296/96, art. 1º, parágrafo único).
> - Habeas-corpus denegado[108].

Todos os crimes virtuais têm sua jurisdição, assim como os crimes reais. A diferença está no que diz respeito ao fato da *internet* residir em um grande número de jurisdições diferentes, já que ela é mutável[109].

Por todo exposto, parece bastante claras as imperfeições que condenam o projeto.

---

[108] SUPERIOR TRIBUNAL DE JUSTIÇA. 6ª Turma. HC nº 15.026, Ementa: [...] Relator: Vicente Leal. Brasília, DF, 24 set. 02. DJ 04.11.2002, p. 266.

[109] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 170.

5 TRATADOS E CONVENÇÕES

5.1 Convenção de Budapeste

Muito se vem discutindo a respeito da dificuldade de definir o tempo e o lugar de determinada conduta criminosa uma vez que na *web* não há fronteiras que impeçam os criminosos de realizar qualquer delito[110].

Devido a este aspecto é que se questiona a respeito da efetiva obrigação de determinado país de responder por determinado delito, e qual seria a competência referente ao poder de polícia nestes casos[111].

Nos Estados Unidos da América, quando fica evidente que um crime ultrapassou as fronteiras daqueles países, a competência passa a ser federal, sendo cada delito investigado por órgãos secretos como o *FB* e *Air Force OSI* . Já na União Européia a situação é um pouco diferente: Um país, juntamente com outros, combatem tais delitos através de acordos, os quais dispõem a possibilidade de todos os países-membros terem permissão de investigar crimes ocorridos fora de sua jurisdição[112].

Tendo os crimes cibernéticos alta complexidade, devido ao fato de estarem relacionados com o local em que se consumam, e, por consequência de constituir de várias jurisdições distintas afetando países diferentes, é imprescindível que sejam investigados e identificados.

---

[110] PINHEIRO, Patrícia Peck. **Direito Digital**. 2. ed. São Paulo: Saraiva, 2007, p. 46.

[111] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 181.

[112] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. Ed. São Paulo: Saraiva, 2002, p. 72.

No mundo da *internet* não é fácil localizar o lugar onde o agente está interagindo. Assim, para Patrícia Peck Pinheiro[113], "Muitos sites têm terminação '.com', sem o sufixo de país (por exemplo, sem o '.br' em seguida) o que teoricamente significa que estão localizados nos Estados Unidos. Só que vários deles apenas estão registrados nos Estados Unidos e não têm nenhuma existência física nesse país. Uma tendência mundial é assumir definitivamente o endereço eletrônico como localização da origem ou efeito do ato. Assim, se uma empresa brasileira registra um site como '.com', em vez de '.com.br', pode ter de se sujeitar às leis de diversos países no caso de questões jurídicas internacionais".

O pequeno número de casos submetidos ao crivo policial e aos tribunais faz com que a habilidade técnica para solucionar tal problema deixe a desejar, pois como demonstrado anteriormente, a tendência é o aumento qualitativo e quantitativo de tais ilícitos[114].

Alguns especialistas sustentam que tratados ou convenções internacionais poderiam solucionar o problema. E talvez, eles tenham razão, tendo em vista que sendo a *Internet* um meio de comunicação que ultrapassa limites e fronteiras de qualquer país, seria pouco provável que somente leis nacionais de cada Estado conseguissem definir como, quando, onde e qual legislação seria responsável por determinada conduta delituosa de um indivíduo. Assim, nas discussões e elaborações legislativas sobre delitos informáticos, vem se concluindo que não há mais como cogitar soluções nacionais para eles, devendo o assunto ser debatido em âmbito internacional, já que estes fenômenos são influenciados diretamente pela

[113] PINHEIRO, Patrícia Peck. **Direito Digital**. 2. ed. São Paulo: Saraiva, 2007, p. 39.
[114] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. Ed. São Paulo: Saraiva, 2002, p. 69.

globalização, sendo praticados de forma célere e com ultrapassagem de fronteiras geográficas dos países, com interdependência de ações praticadas em diversos locais[115].

A *internet* cria um ambiente no qual inexiste barreiras geográficas. Não é como no mundo real que há demarcação dos recursos físicos de um território e o raio de abrangência de terminada cultura. Naquela todos estão sujeitos aos mesmos efeitos, ações e reações. O direito eletrônico possui vários princípios norteadores para que possa se determinar qual a lei aplicável ao caso concreto. Há o princípio do endereço eletrônico, o do local em que a conduta se realizou ou exerceu seus efeitos, o do domicílio do consumidor, o da localidade do réu e o da eficácia na execução judicial[116].

Em termos de Brasil poderíamos suscitar, como uma provável solução para o referido problema, a teoria da ubiquidade, ou seja, a lei brasileira seria aplicada sempre que alguma parte de um ilícito penal seja cometida no território nacional. Desse modo, não é necessário que o delito ou a contravenção tenham sido integralmente praticados no Brasil[117].

Segundo artigo 6º, *caput*, do Código Penal Brasileiro, enuncia: "considera-se praticado o crime no lugar onde ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado". Assim, neste caso, determinando o lugar do crime, está naturalmente determinada a competência. Neste sentindo, se praticado o delito totalmente no território de um país, a competência, claro, será a competência interna. Se o delito, porém, for praticado entre dois países, há três teorias: teoria da atividade, teoria do

---

[115] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 170.

[116] PINHEIRO, Patrícia Peck. **Direito Digital**. 2. ed. São Paulo: Saraiva, 2007, p. 40.

[117] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 206.

resultado e a teoria da ubiquidade. A primeira teoria diz que o lugar do crime será aquele onde foi realizada a ação ou a omissão. Essa é a teoria adotada pelos juizados especiais. Já a segunda teoria enuncia que o lugar do crime será aquele onde ocorreu o resultado. Teoria esta, por sinal, adotada no Código Penal. E a terceira teoria, conforme dito anteriormente, preceitua que o local do crime será aquele no qual se realizou qualquer um dos fatos, ação ou resultado, tanto faz. Essa teoria, que resolve o problema dos crimes à distância, como no caso em tela, é a teoria adotada no Código de Processo Penal[118].

Nestes termos, pode-se observar julgado do Superior Tribunal Militar, a exemplo do abaixo colacionado:

> ESTELIONATO - COMPETÊNCIA - LUGAR DO CRIME - TEORIA DA UBIQUIDADE – CONCORRENDO DOIS OU MAIS JUÍZES IGUALMENTE COMPETENTES - REGRA DA PREVENÇÃO. Atividade delituosa iniciou-se em Brasília (11ª CJM), com a emissão e apresentação da declaração tida como falsa. Resultado ocorreu no Rio de Janeiro (1ª CJM), quando do recebimento do valor pecuniário. IPM instaurado em Manaus (12ª CJM), por ter o indiciado declarado ir residir em Tabatinga-AM. Art. 6° do CPM. Lugar do crime. Teoria da ubiqüidade, considerando tanto o crime praticado no lugar onde se desenvolveu a atividade criminosa, como também onde se produziu ou deveria produzir o resultado. Art. 88, do CPPM, competência determinada pelo lugar da infração. Diferença ante o art. 70 do CPP - Competência pelo lugar em que se consumar a infração - Teoria do resultado. Regra para dirimir aparente impasse: Prevenção. Auditoria da 11ª CJM praticou atos que previnem o referido Juízo.
> Provimento negado ao Recurso - Competente para conhecer o presente processo - Juízo da 11ª CJM, em Brasília. Decisão por maioria[119].

Essa teoria, entretanto, não se aplicaria tão eficazmente quanto um tratado ou uma convenção, pois sendo ela norma de eficácia interna, certamente surgiria um conflito de competências para processar e julgar determinada pessoa que possa ter vindo a cometer

---

[118] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 206.

[119] SUPERIOR TRIBUNAL MILITAR. 11ª CJM. Processo nº 1999.01.006538-0. Ementa: [...] Relator: Olympio Pereira da Silva Junior. Brasília, DF, 08 abr. 99. DJ 22.06.1999, p. 13.

uma parte da execução do crime no Brasil e outra parte na Alemanha. Neste caso, não somente ambos os países teriam competência para resolver tal lide, como também ambos iriam querer fazê-lo. Por isso, seria imprescindível a presença do Direito Internacional Público para resolver tal embate[120].

Segundo esse ramo do Direito, os tratados e/ou convenções têm a função de universalizar algumas leis para que todos os países membros não tenham dificuldade em resolver algumas questões[121]. Assim, não haveria, por exemplo, o problema do conflito de leis para saber se determinada pessoa seria processada e julgada sob o crivo da lei do país A ou sob a do país B. Apenas seria aplicado o tratado e todos os países-membros teriam a mesma solução.

De acordo com a Convenção de Viena de 1969:

> Tratado significa um acordo internacional concluído entre Estados de forma escrita e regulado pelo Direito Internacional, consubstanciado em um único instrumento ou em dois ou mais instrumentos conexos, qualquer que seja a sua designação específica.

Poderia vir à mente alguma dúvida a respeito da eficiência desta solução no que diz respeito à soberania, cultura e costumes das nações, já que muito vem se discutindo se uma Convenção não se sobreporia às essas características essenciais do Estado, fazendo-o perder um pouco da sua identidade. Com certeza, não é fácil submeter-se a uma lei que não fora criada pelo próprio país. Porém, em alguns casos faz-se necessário tal submissão tendo em vista que o assunto, sendo de suma importância, precisa ser tratado em âmbito

---

[120] BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico:** A Internet e os Tribunais. São Paulo: Edipro, 2001, p. 206.

[121] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 166.

internacional, já que unilateralmente, nenhum país conseguiria combater os delitos informáticos.

Portanto, há urgente necessidade de se facilitar a cooperação internacional como meio eficaz de combate a esse tipo de criminalidade. Os programas de computadores utilizados por usuários do mundo todo são praticamente os mesmos. Nessa medida, frente à importância dada a esse assunto e as características globais dos crimes informáticos, a existência de várias leis nacionais com o intuito de legislar sobre eles poderia levar à criação de paraísos criminais[122]. Assim, tais soluções nacionais devem ser banidas para os arquivos do passado, já que têm sua aplicação limitada a um território específico[123].

A Convenção de Budapeste[124], elaborada em 21 de setembro de 2001, na cidade que leva o mesmo nome com mais de quarenta países-membros, dentre os quais os Estados Unidos da América, o Canadá, o Japão e a África do Sul, postula a produção de uma política criminal comum para fornecer proteção à sociedade contra a criminalidade no espaço virtual, enfatizando a necessidade de se ter uma legislação adequada com o desenvolvimento tecnológico atual. Este presente estudo visa analisar a possível inclusão do Brasil nesta Convenção e os impactos que isso produziria no ordenamento jurídico brasileiro.

Esse é o primeiro tratado internacional a abordar os crimes informáticos, tratando especificamente da segurança de redes de computadores, das violações de direitos autorais, da fraude por meio de computadores e da pornografia infantil. Ele foi criado com o intuito de uniformizar a legislação européia, utilizando-se de uma política criminal comum

---

[122] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 166 e 167.
[123] Ibidem.
[124] Ibidem.

para defender a sociedade dos crimes informáticos, indicando a legislação apropriada, trazendo facilidades e agilizando a cooperação internacional por meio da adoção de tipos legais e procedimentos penais uniformes[125].

O acordo entrou em vigor no dia 1 de julho de 2004, depois que cinco países o ratificaram, sendo três integrantes do Conselho Europeu composto por quarenta e seis membros. Até o dia 14 de março de 2007, dezenove países haviam ratificado o tratado. Os Estados Unidos são o único país de fora do Conselho Europeu que o ratificou, em 29 de setembro de 2006.

Para a autora Esther Dyson[126], na *Internet* existiriam três níveis de jurisdição: o espaço físico, que vincula a pessoa ao espaço corpóreo que habita, cada qual tendo suas próprias leis, devendo os cidadãos respeitá-las; o dos provedores de acesso, que vincula a pessoa à submeter-se às leis vigentes no país onde se situa tal provedor e o dos domínios e comunidades, que operam sem respeitar fronteiras internacionais ou de outros provedores.

Nessa convenção o espaço cibernético foi definido como um tipo de espaço comum que é usufruído por todos aqueles que trafegam na *internet* ao se conectarem aos serviços de comunicação e informação[127]. Diante disso, tal convenção foi elaborada não somente para criar novos tipos penais, mas também para estipular normas de processo penal,

---

[125] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 167.

[126] Apud CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 71.

[127] BOITEUX, op. cit., p. 170.

conciliando procedimentos de direito penal internacional e estabelecendo acordos referentes à tecnologia da informação[128].

A referida Convenção tem como objetivos[129]:

> Harmonizar as legislações penais substantivas, elementos do delito e outras provisões conexas sobre delitos de informática; promover alterações nas legislações processuais nacionais de forma a conceder poderes de investigação e persecução criminal necessários para combater delitos praticados com o uso de sistemas de computador, ou nos demais tipos de delitos nos quais as provas devam ser obtidas mediante meios eletrônicos e estabelecer um regime rápido e efetivo de cooperação internacional.

Os objetivos da referida Convenção são bem claros no sentido de harmonizar as legislações penais substantivas, promovendo alterações nas legislações processuais internas e estabelecendo um regime célere de cooperação internacional[130].

Todos os crimes definidos na referida Convenção são dolosos[131], ou seja, não se admite a possibilidade de conduta delituosa perpetrada por meio de computador sem que tenha havido a verdadeira intenção de fazê-la. Além do mais, no que tangeria à modificação da legislação nacional, tal Convenção dispõe de alguns roteiros que têm como objetivo maior fazer com que os países signatários se comprometam a adotá-los em seus sistemas jurídicos, não sendo exigido, entretanto, que estes venham a copiá-los podendo somente utilizar definições equivalentes.

---

[128] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 170.
[129] Ibidem.
[130] Ibidem.
[131] Ibidem, p. 171.

A Convenção de Budapeste[132] está organizada de maneira clara e estratégica, possuindo apenas quatro capítulos. O primeiro define os crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computadores, tais como "acesso ilegal à integralidade ou parte de sistema de computadores sem autorização" (*illegal Access*- art. 2)[133], "interceptação ilegal"(*illegal interception*- art. 3)[134], "interferência ou dano em dados de computador" (*data interference*- art. 4)[135] e "interferência em sistemas" (*system interference*- art. 5)[136]. O segundo capítulo, por sua vez, dispõe sobre aqueles crimes que já foram tipificados nas legislações penais comuns, mas que também podem ser cometidos com a utilização do computador, por exemplo, os crimes de falsificação eletrônica ou praticada por meio de computadores (*computer-related forgery*- art. 7)[137] e fraude informática (*computer-related fraud*- art. 8)[138]. Já o terceiro capítulo trata das ofensas relacionadas à pornografia infantil[139]. Por fim, o capítulo quatro preconiza os crimes relacionados à violação de direitos de autor em geral, ou condutas delituosas contra a propriedade intelectual.

---

[132] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 172.

[133] Estes crimes podem ser cometidos pela violação das medias de segurança, com a intenção de obter dados de computadores ou outra intenção desonesta, estando tal sistema de computador conectado ou não a uma rede de computadores.

[134] Trata-se de interceptação sem autorização, por meios técnicos, de transmissões privadas de dados, envolvendo um sistema de computadores, incluindo emissões eletromagnéticas de um sistema de computadores capacitado para processar tais dados. Pode a ofensa ser cometida com intenção desonesta em sistemas conectados a outros sistemas de computação (rede).

[135] Estão previstas no referido artigo as ações de danificar, apagar, deteriorar, alterar ou suprimir dados de computadores sem autorização, podendo ser exigido para a configuração do delito que a conduta tenha resultado em grave lesão.

[136] A tipificação se refere à restrição ao bom funcionamento de um sistema de computadores, sem autorização por, meio de inserção, transmissão, dano, exclusão, deterioração ou supressão de dados.

[137] A descrição típica sugerida é a inclusão, alteração, exclusão ou supressão de dados de computador, que resultem na inautenticidade dos dados com a intenção de se fazer passar, ou sendo utilizado para fins legais como se autêntico fosse, mesmo se a informação não é diretamente legível e/ou inteligível. Pode-se exigir intenção de defraudação ou outra intenção semelhante, para atribuição da responsabilidade criminal.

[138] Neste artigo 8, está prevista a ação de causar lesão a bens de uma pessoa por meio das seguintes práticas: i) inclusão, alteração, exclusão ou supressão de dados de computadores; ii) interferência no funcionamento de sistema de computador; em ambos os casos com intenção fraudulenta ou desonesta, e sem autorização, tendo como objetivo a obtenção de vantagem econômica para si ou para outrem.

[139] BOITEUX, op. cit., p. 173.

Diante de diversas discussões[140] a respeito do tema relacionado à imposição de sanções mais duras naquilo que concerne à posse de material pornográfico, a Convenção deixou a critério dos países-membros a opção de criminalizá-la ou não, de acordo com o que consta da redação do artigo 9, que trata dos crimes relacionados à pornografia infantil (*offenses related to child pornography*)[141]. Outras condutas delituosas controvertidas, tais como o jogo ilegal pela *internet* e o terrorismo cibernético, foram deixadas de fora da Convenção para que cada Estado pudesse decidir criminalizá-las ou não. Já em relação à responsabilidade de pessoa jurídica, a Convenção se restringe apenas a dizer que ela poderá ser responsabilizada criminal, civil ou administrativamente.

Em 28 de janeiro de 2003, foi assinado um Protocolo Adicional[142] à Convenção de Budapeste, recomendando a criminalização dos atos de racismo e xenofobia cometidos por meio de computador.

A referida Convenção prevê ainda que as legislações nacionais adotem procedimentos específicos que têm como objetivo atualizar a legislação processual para a geração atual da informática, fornecendo aos doutrinadores e operadores do direito meios rápidos e eficazes para reprimir as condutas ilícitas e desvendar seus autores, salvaguardando

---

[140] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 173.

[141] Estão previstos os seguintes tipos relacionados à pornografia infantil, praticados mediante o uso de sistemas de computadores: a) produzir pornografia infantil com o propósito de distribuição; b) oferecer ou tornar disponível pornografia infantil; c) distribuir ou transmitir pornografia infantil; d) adquirir pornografia infantil para si ou para outrem; e) ter em seu poder pornografia infantil no sistema de computadores ou em qualquer meio de arquivo externo de computação (exemplos: disquete ou CD). O parágrafo 2º deste mesmo artigo define como pornografia infantil material que demonstre visualmente: a) um menor engajado em conduta sexualmente explícita; b) pessoas aparentando serem menor de idade em conduta sexualmente explícita; c) imagens realistas representando menor engajado em conduta sexualmente explícita, sendo certo que o termo menor, para fins deste parágrafo, significa pessoas com menos de dezoito anos de idade, podendo os Estados-parte exigir um limite de idade de até dezesseis anos.

[142] BOITEUX, op. cit Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 174.

a proteção aos direitos humanos e as liberdades individuais, além da previsão de condições específicas de deferimento destas medidas, incluindo a necessidade de autorização judicial, exigência de certas limitações, bem como respeitando-se parâmetros comuns já previstos em convenções internacionais de direitos humanos, conforme dispõe seu artigo 15.

São medidas processuais recomendadas pela Convenção[143]:

> i) determinação ou ordem de preservação de dados armazenados em sistemas de computadores (*expedited preservation of stored computer data)*[144], com duração de até 90 dias, que permite às autoridades pleitear posteriormente uma ordem de abertura ou revelação (*disclosure*) de tais dados, o que seria equivalente à nossa quebra de sigilo (art. 16); ii) ordem de preservação e parcial abertura de fluxo de dados (*expedites preservation and partial disclosure of traffic data*)[145]; iii) ordem de fornecimento de dados às autoridades (*production order*-art. 18)[146]; iv) busca e apreensão para acessar sistemas e dados de computadores, incluindo meios de armazenamento de dados eletrônicos (CD-*rom*, disquetes e similares- art. 19)[147]; v) obtenção, coleta ou gravação em tempo real de fluxo de dados (*real-time collection of traffic data*- art. 20)[148]; vi) interceptação de dados (*interception of content*

[143] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 173.

[144] Trata-se de um tipo de apreensão no qual o detentor de dados específicos, inclusive fluxo de dados, que estejam armazenados em seu sistema, está obrigado a preservá-la por um prazo maior de tempo, evitando-se, dessa forma, a possibilidade de modificação ou perda. Tal medida permitirá ao detentor dos dados continuar a utilizar normalmente seu sistema, desde que preservando determinadas informações de interesse de investigação, tendo como contrapartida a obrigação de manter confidencial tal fato, evitando-se que o investigador tome conhecimento.

[145] Esta medida tem por objetivo preservar e revelar as informações referentes ao fluxo de dados no sistema, permitindo o acesso das autoridades às informações sob a forma eletrônica, do caminho percorrido pelo usuário , mesmo havendo um ou mais provedores envolvidos em tal transmissão, de forma a se chegar até seu destino final. As medidas previstas nos artigos 16 e 17 se aplicam aos dados armazenados que já tenham sido coletados pelos seus detentores, tais como provedores de acesso à rede.

[146] Na medida prevista no art. 18, a autoridade competente ordena que lhe sejam fornecidos dados específicos armazenados em computadores, incluindo os dados pessoais dos assinantes contidos nos arquivos dos provedores fornecidos por ocasião do contrato, além de outras informações sobre tipos de equipamentos utilizados e outras provisões técnicas que auxiliem as autoridades nas investigações. Neste caso, a autoridade não busca ou apreende, mas ordena que informações sejam fornecidas por terceiros que estejam na posse destas sob a forma de dados.

[147] Neste tipo de medida investigativa, as autoridades poderão ter acesso, congelar ou bloquear um sistema de computadores ou qualquer meio de armazenamento de dados, assim como fazer cópias dos dados contidos nos computadores, ou mesmo tornar inacessível ou remover tais dados do sistema.

[148] No caso do artigo 20, enquanto os dados são transmitidos pelo computador, a autoridade poderá ter acesso simultâneo à nota percorrida por tais informações, ou ainda compelir o provedor a fazê-lo, podendo ser gravadas tais informações obtidas. Esse procedimento visa apenas identificar a circulação das informações, mas não seu conteúdo, o que poderá ser objeto da medida prevista no art. 21.

> *data*) transmitidos por meios de comunicação eletrônica. Em tempo real (art. 21)[149].

Mostra-se importante que tenha também uma polícia técnica desenvolvida, com profissionais capacitados e especializados na área da informática e que detenham o domínio das novas tecnologias, para que possam avaliar os dados coletados. Assim, para que os crimes cibernéticos possam ser combatidos, inevitável será que as autoridades policias os investiguem através do mesmo meio empregado para criá-los, qual seja, o computador.

Há alguns anos[150], no Centro de Treinamento das Polícias Federais nos Estados Unidos- FLETC- na Geórgia, um dos agentes federais ali presentes instigou a risada de seus colegas quando disse que os policias em breve seriam chamados de *cybercops* e necessitariam, além de armas e distintivos, de um *notebook* para combater os crimes de computadores[151].

Hoje, aquela afirmação não soa mais num tom de piada. Ao contrário, o grande avanço tecnológico desse meio de comunicação tem preocupado tanto os sociólogos como os profissionais de polícia, já que a celeridade com que essas inovações tecnológicas ocorrem é maior do que a capacidade de assimilá-las e não conseguem ter medidas de segurança capazes de proteger as informações.

Por isso que, do mesmo modo que se utilizam armas para perseguir ladrões, o uso da informática dentro da polícia e do Poder Judiciário trará vários ajustes na sociedade

---

[149] Pode-se chamar de "grampo" ou interceptação de dados transmitidos entre computadores. A ordem da autoridade neste caso permite coletar e gravar os dados transmitidos, ou compelir o provedor a fazê-lo com seus meios de técnicos, prestando assistência às autoridades.

[150] SILVA, Mauro Marcelo de Lima (Coord.). **Internet Legal:** O Direito na Tecnologia da Informação: Doutrina e Jurisprudência: Crimes da Era Digital. São Paulo: Juruá, 2005, p. 27.

[151] Ibidem.

atual, dentre as quais se tem a detecção, a prevenção e o devido processo daqueles crimes informáticos puros[152].

A Convenção recomenda, ainda, critérios de atribuição de jurisdição, para que todos os países possam ter competência sobre as práticas criminais digitais, além de solução para conflitos que possam vir a surgir sobre tal questão. Ademais, de maneira a tornar mais ampla a cooperação entre os países membros no combate aos crimes envolvendo computadores, a Convenção traz previsões referentes à assistência, extradição e cooperação mútua, mesmo naqueles casos que não haja base legal (tratado ou reciprocidade) entre os Estados[153].

Há alguns pressupostos para a identificação de abuso contra as redes de computadores. Um deles tem a função de englobar a imposição de medidas de segurança em sistemas, tendo como base a observância do advento de novas condutas ilícitas[154].

O melhor meio para que os agentes infratores não cometam delitos com tanta freqüência seria a criptografia, impedindo que arquivos sejam modificados ou destruídos[155].

Para os governos, a técnica da criptografia poderia ser utilizada tanto para impedir os crimes digitais como, também, para dificultar o rastreamento e a identificação de

---

[152] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 69.
[153] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 174.
[154] CORRÊA, op. cit., p. 72.
[155] Ibidem, p. 77.

determinados criminosos, tendo em vista que alguns documentos criptografados pelos mesmos não teriam solução imediata[156].

Nos Estados Unidos, por exemplo, a criptografia é considerada arma, constando na lista de munições e no Regulamento Internacional de Vendas de Armas. Para eles, ela está relacionada como "artigo de defesa", de acordo com a Lei de Controle à Exportação de Armas, sob o crivo de ser necessária para a paz mundial, a seguridade e para ações internacionais do governo norte-americano[157].

A Convenção demonstra como relevante o fenômeno de que todas as disposições legais estabelecidas pelos países-membros estão obrigadas a respeitar os direitos humanos fundamentais e as liberdades civis, tais como o direito a privacidade, a intimidade, a liberdade de expressão e o acesso público ao conhecimento e a Internet[158].

A importância desta análise para o direito brasileiro refere-se ao fato de que os crimes praticados pela Internet, sejam eles tradicionais ou não, estão em conflito direto com a competência e atuação territorial das autoridades nacionais, uma vez que as leis nacionais têm sua aplicação limitada a um território específico e são totalmente ineficientes no que tange à violação aos direitos humanos e às liberdades individuais. Desse modo, somente um instrumento internacional poderia ter eficácia na luta contra estes crimes.

---

[156] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002, p. 77.
[157] Ibidem, p. 79.
[158] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004, p. 175.

CONCLUSÃO

A maneira como as transformações se desenvolvem no tempo e no espaço é uma barreira à eficaz aplicação do Direito e suas legislações, devido ao fato de que elas ocorrem com uma velocidade muito além do que o ordenamento jurídico possa vir a acompanhar.

Neste contexto, surge um cenário composto por dois personagens principais: O computador e a *internet*, mais conhecida como a rede telemática internacional que une interesses de particulares, organizações de pesquisa, institutos de cultura, institutos militares, bibliotecas e corporações de todos os tamanhos. Essa conectividade advinda da informatização trouxe a possibilidade de comunicação em tempo real, inexistindo barreiras geográficas que impeçam as pessoas de fazer o que quiserem neste novo meio.

Assim, ao mesmo tempo em que estes novos institutos trouxeram grandes oportunidades ao desenvolvimento tecnológico, eles também trouxeram grandes riscos e desafios para o universo jurídico, tendo em vista que algumas práticas delituosas advieram concomitantes a esta profunda transformação.

Diante disso, partindo-se da premissa de que não há nenhuma situação sem solução, o referido trabalho se propõe a demonstrar que para solucionar referido problema, faz-se necessário a criação de leis que venham criminalizar determinadas condutas para poder atender às diversas formas de manifestação da sociedade. Neste sentido, surgiria o Direito Digital.

A importância desta análise para o direito brasileiro refere-se ao fato de que os crimes praticados através da *internet*, sejam eles puros ou impuros, estão em conflito direto com a competência e atuação territorial das autoridades nacionais, uma vez que a aplicação de leis internas sobre o referido tema ficaria limitada a somente um território específico e seriam totalmente ineficientes no que diz respeito à violação aos direitos humanos e às liberdades individuais, de acordo com o que foi demonstrado pelo projeto de lei substitutivo aos PLS 76/2000, PLS 137/2000 e PLC 89/2003.

Portanto, conclui-se que não há como cogitar soluções nacionais para tais crimes, devendo o assunto ser debatido em âmbito internacional, com a assinatura do Brasil na Convenção de Budapeste, tornando-se um País membro. Os objetivos desta Convenção restaram claramente demonstrados, considerando a necessidade da previsão legal de tipos penais específicos, além do incremento da cooperação internacional, fundada na universalização de delitos perante os reflexos internacionais destes tipos de condutas.

As barreiras encontradas pelos operadores do direito brasileiro no combate e na prevenção aos crimes digitais serão superadas com a agilidade da colaboração dos países signatários, além da otimização de seus procedimentos, conciliados sempre com os direitos humanos fundamentais, como o direito a privacidade e liberdade de expressão.

REFERÊNCIAS

BLUM, Renato M. S. Opice. et. al. **Direito Eletrônico: A Internet e os Tribunais.** São Paulo: Edipro, 2001.

BOCCHINI, Bruno. **Práticas cotidianas na Internet podem virar crime, avalia professor.** Disponível em: <http://www.ecosdanoticia.com.br/index.php?option=com_content&task=view&id=6299&Itemid=84>. Acesso em 1 out. 09.

BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002.

DRUMMOND, Victor Gameiro. Internet, Privacidade e Dados Pessoais.1 ed. Rio de Janeiro: Lumen Juris, 2003.

FELITTI, Guilherme. **Crime digital:** compare as principais leis mundiais com o projeto de lei. Disponível em: <http://www.safernet.org.br/site/noticias/crime-digital-compare-principais-leis-mundiais-com-projeto-brasileiro>. Acesso em: 03 out. 09.

Folha Online. Críticos comparam lei sobre internet ao AI-5. São Paulo, 11 mai. 09. Disponível em: <http://www.tudoagora.com.br/noticia/18768/Criticos-comparam-lei-sobre-internet-ao-AI-5.html>. Acesso em: 4 out. 09.

GRECCO, Rogério. **Curso de Direito Penal**: parte geral. 11. ed. São Paulo: Impetus, 2009, vol. 1, p. 40.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet.** 1. ed. São Paulo: J. de Oliveira, 2004.

It Web. Projeto de lei para crimes na internet passa no Senado. São Paulo, 10 jul. 09. Disponível em: <http://www.itweb.com.br/noticias/index.asp?cod=49540>. Acesso em: 4 out. 09.

KAMINSKI, Omar. **Internet Legal:** O direito na tecnologia da informação. 1 ed. Curitiba: Juruá, 2003.

MAIA, Felipe. Críticos comparam lei sobre internet ao AI-5 e anunciam protesto em SP. **Folha Online,** São Paulo, 11 mai. 09. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u562920.shtml>. Acesso em: 1 out. 09.

MARTINS, Paulo Mário. **Críticas ao Projeto de lei de Crimes Digitais dão tom â audiência esvaziada.** Disponível em: <http://www.safernet.org.br/site/noticias/cr%C3%ADticas-ao-projeto-lei-crimes-digitais-d%C3%A3-tom-audi%C3%AAncia-esvaziada>. Acesso em: 03 out. 09.

PAESANI, Liliana Minardi. **Direito e Internet**. 2 ed. São Paulo: Atlas, 2003.

PINHEIRO, Patrícia Peck. **Direito Digital**. 2. ed. São Paulo: Saraiva, 2007.

SILVA, Mauro Marcelo de Lima (Coord.). **Internet Legal:** O Direito na Tecnologia da Informação: Doutrina e Jurisprudência: Crimes da Era Digital. São Paulo: Juruá, 2005.

SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. São Paulo: Revista dos Tribunais, 2003.

SUPERIOR TRIBUNAL DE JUSTIÇA. 1ª Turma. HC nº 76.689. Ementa:[...]Relator: Sepúlveda Pertence. Brasília, DF, 28 set. 98. DJU 6.11.1998.

SUPERIOR TRIBUNAL DE JUSTIÇA. 6ª Turma. HC nº 15.026, Ementa: [...] Relator: Vicente Leal. Brasília, DF, 24 set. 02. DJ 04.11.2002.

SUPERIOR TRIBUNAL MILITAR. 11ª CJM. Processo nº 1999.01.006538-0. Ementa: [...] Relator: Olympio Pereira da Silva Junior. Brasília, DF, 08 abr. 99. DJ 22.06.1999.

Uol. Senado aprova projeto de lei que tipifica crimes cometidos na Internet. Disponível em: <http://tecnologia.uol.com.br/ultnot/2008/07/10/ult4213u492.jhtm>. Acesso em 03 out. 09.

WALL, David S. Crimes and the Internet. 1 ed. Londres:Routledge, 2001.

WIKIPEDIA. Disponível em: HTTP://pt.wikipedia.org/wiki/Pretor. Acesso em: 05 de mai 2009.

GLOSSÁRIO

Ambiente: Nome utilizado para especificar o software de base do gerenciador do sistema no qual se está trabalhando. É o ambiente de trabalho que define a comunicação entre o usuário e o computador.

Antivírus: Programa ou software especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de códigos maliciosos.

ARPA: A ARPA (*Advanced Research Projects Agency Network)*, agência de pesquisas em projetos avançados, foi criada em 1957 por militares e pesquisadores estadunidenses sob a supervisão do presidente Eisenhower em reação dos Estados Unidos da América à vitória tecnológica da então União Soviética por ter lançado o primeiro satélite artificial da história, *Sputnik*.

ARPANET: A ARPANET (*Advanced Research Projects Agency Network*) foi desenvolvida pelo Departamento de Defesa dos Estados Unidos da América, sendo a primeira rede operacional de computadores à base de comutação de pacotes e a precursora da internet.

Arquitetura cliente/servidor: É toda arquitetura de rede onde estações (microcomputadores) executam aplicações clientes que se utilizam de programas servidores para transferência de dados do próprio servidor ou comunicação com outras estações e suas aplicações clientes.

Arquivo: É um agrupamento de bits que formam uma unidade lógica que possa ser interpretada pelo processador do PC. Na verdade, os arquivos são tudo o que compõe o software do computador. O sistema operacional, os aplicativos e os docuemntos que são

manipulados pela máquina compõem-se de milhares de arquivos. Cada arquivo é definido por um nome e uma extensão. A extensão é um código universal que determina o tipo de arquivo em questão. Combinado com o nome, identifica exclusivamente o arquivo dentro de um mesmo diretório.

Browser: Significa pesquisar e pode-se traduzir como navegador. Na internet, o termo deve ser interpretado como uma ferramenta que permite a paginação ou folheamento. O termo acabou virando sinônimo para os programas que permitem acessar e mostrar as Home Pages encontradas na Web. O primeiro browser a permitir o acesso gráfico, o MOSAIC, criado numa universidade Americana, serviu de padrão para a criação do conceito de Web. Atualmente, várias empresas estão disputando o mercado para impor seus produtos e modificar os padrões atuais. Os programas, que anteriormente serviam apenas para permitir a visualização de páginas escritas em HTML, estão evoluindo e incorporando outras atividades, tais como leitura de e-mail. Um browser é ferramenta indispensável para poder acessar a Internet gratificante, e com o surgimento de novas linguagens de criação das Homes Pages ou browsers têm se sofisticado cada vez mais, para poder suportar tais avanços.

Conexão segura: Conexão que utiliza um protocolo de criptografia para a transmissão de dados, como, HTTPS ou SSH.

Conteúdo: Qualquer informação multimídia (em formato texto, imagem, com, programa de computador, gráficos) publicadas por meio da rede aberta ou fechada (acesso restrito).

Criptografia: Método de codificação de dados que permite o acesso apenas de pessoas autorizadas, possuidoras de chave de acesso. Ciência e arte de escrever mensagens em forma cifrada ou em códigos. É uma parte de um campo de estudos que trata das comunicações

secretas. É usada, entre outras finalidades, para autenticar a identidade de usuários, autenticar transações bancárias; proteger o sigilo de comunicações pessoais e comerciais.

Cyberspace: Ciberespaço. Assim se designa habitualmente o conjunto das redes de computadores e serviços existentes na internet. É uma espécie de planta virtual, onde as pessoas se relacionam virtualmente, por meios eletrônicos. Termo inventado por William Gibson no seu romance *Neuromancer* e idealizado em analogia com o espaço sideral explorado pelos astronautas.

Disponibilidade: Garantia de que os usuários autorizados abtenham acesso à informção e aos ativos correspondentes sempre que necessário.

Domínio: Nome que descreve a organização com a qual um endereço na internet está vinculado. Faz parte da hierarquia de nomes de grupos ou hosts da internet, identificando as instituições na rede.

Endereço IP: É o endereço real de uma máquina na internet. Consiste em uma série de números separados por pontos. Cada máquina conectada à rede tem um endereço IP. Os *Domain Name Servers*servem então para relacionar os endereços com letras como endereço IP.

FTP: Protocolo de transferência de arquivos: protocolo da internet usado para transferir arquivos de um computador para outro.

Gerenciador de banco de dados: Interface de software entre o banco de dados e o usuário. Um sistema de gerenciamento de bancos de dados que trata de solicitações do usuário para

ações de bancos de dados e permite o controle centralizado da segurança e da integridade dos dados.

Hackers: Indivíduos que faz todo o possível e o impossível para entrar num sistema de informática alheio, quebrando sistemas de segurança, para assim poder causar danos.

Hipertexto: São palavras marcadas no texto que permitem acesso a outros documentos relacionados com o assunto em questão, criando uma linha de pesquisa. Normalmente estão sublinhadas.

Host: Computador principal de um sistema de computadores ou terminais conectados por enlaces de comunicação.

HTM (**HTML**): Extensão para os arquivos gerados e salvos no formato Hiper Text Marked Language (Linguagem de Hipertexto Marcado), para construção de Home-Pages. As versões oficiais da HTML são definidas pelo W3 Consortium, em http://w3.org.

HTTP: HyperText Transfer Protocol. Este é o protocolo usado para transportar tráfego entre o computador do browser da Web e o site da Web.

HTTPS: Quando utilizado como parte de uma URL, especifica a utilização de HTTP com algum mecanismo de segurança.

Interface: O conceito de Interface se expressa pela presença de uma ou mais ferramentas para o uso e movimentação de qualquer sistema de informações, seja ele material, seja ele virtual. Pode significar um circuito eletrônico que controla a interligação entre dois dispositivos hardwares e os ajuda a trocar dados de maneira confiável.

Internet: Rede mundial de computadores e outros dispositivos interligados que possibilitam acesso à informação nela disponibilizada.

IP- Internet Protocol: Protocolo responsável pelo percurso de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP desenvolvida e usada na Internet.

MILNET: A MILNET (*Military Network*), criada em 1983 foi uma rede que cuidava das informações militares dos Estados Unidos da América. Foi uma expansão da ARPANET. Na década de 90, o nome mudou-se para NIPRNET.

NCP: A NCP (*Network Control Protocol*) foi o primeiro protocolo servidor a servidor da ARPANET. Ele foi criado em dezembro de 1971, pelo (*Network Working Group*).

NSF: A NSF (*National Science Foundation*) é um protocolo PDF (formato de arquivo), ou seja, apenas serve para mostrar o endereço IP/MOS de um computador para outro.

NSFNET: A NSFNET (*National Science Foundation Network*) é a junção de cinco centros de supercomputação, tendo sido um marco histórico na década de noventa.

P2P: Acrônimo para *peer-to-peer*. Arquitetura de rede em que cada computador tem funcionalidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, em que alguns dispositivos são dedicados a servir outros. Este tipo de rede é normalmente implementada via softwares P2P, que permitem conectar o computador de um usuário ao de outro para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens etc.

Protocolo: Código que permite a leitura universal da informação.

Provedor de acesso: Instituição que se liga à internet, via um ponto de presença ou outro provedor, para obter conectividade IP e repassá-la a outros indivíduos e instituições, em caráter comercial ou não. O provedor de acesso torna possível ao usuário final a conexão à Internet através de uma ligação telefônica local.

Rand Corporation: A *Rand Corporation,* com sede na Califórnia, é uma instituição sem fins lucrativos que realiza pesquisas para contribuir com a tomada de decisões e a implementação de políticas no setor público e privado.

Segurança da Informação: Protege a informação de uma gama extensiva de ameaças para assegurar a continuidade dos negócios, minimizar os danos empresariais e maximizar o retorno em investimentos e oportunidades. É caracterizada pela preservação da confidencialidade, integridade e disponibilidade.

SGML: A SGML (*Standard Generalized Markup Language*) é uma metalinguagem através da qual se pode definir linguagens de marcação para documentos. A SGML providencia uma variedade de sintaxes de marcação que podem ser usadas por várias aplicações.

Site: Local na internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações.

Software: Programas de computador, instruções que o computador é capaz de entender e executar.

TCP/IP: Protocolo para a comunicação entre computadores. O TCP/IP que controla a subdivisão das mensagens de dados em pacotes a serem enviados por meio do protocolo IP, e a remontagem e verificação das mensagens completas dos pacotes recebidos pelo IP.

URL: *Universal Resource Location*. É um identificado na internet que mostra qual tipo de servidor deve ser acessado, o equipamento em que a informação reside e sua localização nesse equipamento.

Usuário: Todo aquele que acessa a rede internet.

Usenet: Rede para distribuição de novos itens e mensagens.

Vírus: Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas ou arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa tornar-se ativo e dar continuidade ao processo de infecção.

Webcam: Webcam é uma câmera de vídeo de baixo custo que capta imagens, transferindo-as de modo quase instantâneo para o computador, podendo ser utilizada em uma grande gama de aplicações tais como videoconferência, editores de vídeo, editores de imagem, monitoramento de ambientes, entre outros.

Wi-Fi: Do inglês *Wirelles Fidelity*. Termo usado para se referir genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

WWW: Sistema de acesso e utilização de informações da internet por meio de hipertextos com capacidade de ler e transmitir várias tecnologias e tipos de documentos, identificados todos os conteúdos por um só URL.