UNIVERSIDADE FEDERAL DO PARANÁ

GUSTAVO BECKERT TRINKEL

CRIMES CIBERNÉTICOS: CONFINANDO UMA CONDUTA DE REPERCUSSÕES GLOBAIS

CURITIBA
2010

GUSTAVO BECKERT TRINKEL

CRIMES CIBERNÉTICOS: CONFINANDO UMA CONDUTA DE REPERCUSSÕES GLOBAIS

Monografia apresentada ao Curso de Graduação em Direito, do Setor de Ciências Jurídicas da Universidade Federal do Paraná, como requisito parcial à obtenção do grau de Bacharel em Direito.

Orientador: Profª. Drª. Clara Maria Roman Borges

CURITIBA
2010

TERMO DE APROVAÇÃO

GUSTAVO BECKERT TRINKEL

CRIMES CIBERNÉTICOS: CONFINANDO UMA CONDUTA DE REPERCUSSÕES GLOBAIS

Monografia aprovada como requisito parcial para obtenção de Graduação no Curso de Direito, da Faculdade de Direito, Setor de Ciências jurídicas da Universidade Federal do Paraná, pela seguinte banca examinadora:

CLARA MARIA ROMAN BORGES
Orientador

PRISCILLA PLACHÁ SÁ
Primeiro Membro

FRANCISCO DE ASSIS DO REGO MONTEIRO ROCHA JUNIOR
Segundo Membro

RESUMO

Neste presente estudo pretende-se abordar alguns aspectos penais e processuais dos crimes cibernéticos, com um enfoque mais direcionado aos problemas relacionados à competência e eficácia da sentença, sempre tendo em vista que estes tipos de delitos são passíveis de afetarem um sem número de pessoas em todo o mundo em um mesmo instante, podendo clamar a pretensão punitiva diversos Estados soberanos, o que traria não apenas um conflito jurídico entre estes diversos entes, mas também conflitos sociais, ideológicos e políticos de maneira generalizada e globalizada.

Ademais, pretende-se mostrar que, em diversos pontos, não há consenso na doutrina brasileira acerca da tratativa deste tipo de conduta delituosa, complicando-se ainda mais quando comparado à doutrina internacional. Em uma análise do ordenamento jurídico brasileiro, demonstrar-se-ão as complicações que podem surgir ao analisar estes delitos à luz da legislação penal brasileira vigente, podendo vir a ter um efeito teratológico face à atual realidade social mundial, em que se procuram penas alternativas para condutas lesivas, pois é reconhecida a impotência do encarceramento na repressão, na prevenção ou sequer na reparação dos danos produzidos por qualquer lesão ou ofensa a direitos.

Palavras-chave: Crimes cibernéticos. Crimes na Internet. Crimes de Informática. Crimes Informáticos. Classificação. Vírus de Computador. Malware. Cavalo de Tróia. Trojan. Keylogger. Spyware. Tipificação. Autoria. Provedores de Acesso. Prevenção. Repressão. Descriminalização. Soberania. Jurisdição. Competência. Não Intervenção.

SUMÁRIO

1. INTRODUÇÃO

Todos usam, alguns abusam, mas poucos entendem seu funcionamento. Muitos se divertem, outros formam laços sociais e, cada vez mais, pessoas necessitam dela para sobreviver, seja com orientações culinárias, terapêuticas ou até mesmo como fonte de renda. A internet aos poucos se tornou algo essencial ao ser humano, envolvendo aspectos éticos, culturais, sociais, econômicos e morais. Seu vernáculo é tão influente que é uma das fontes mais férteis para a nossa língua nativa no que tange aos neologismos, tema este que causa espanto e pavor nos mais conservadores e contentamento nos mais liberais e progressistas. Para as engenharias, ela se tornou a maneira mais célere e eficiente nas pesquisas e discussões internacionais acerca de novos métodos. A medicina, ciência milenar e essencial à sobrevivência humana, não ficou para trás, e hoje utiliza cada vez mais a internet para a realização de pesquisas genéticas e demais pesquisas relacionadas, citando como exemplo o projeto "Folding @ Home"[1], de iniciativa da Stanford School of Medicine (Escola de Medicina de Stanford), projeto este que consiste, após a instalação, no computador, de um software específico para esta função, na utilização remota do potencial ocioso dos computadores conectados à Internet para criar um supercomputador ou a este se assemelhar, trazendo a capacidade de simular todas as possibilidades de enrolamento ou assimilação das proteínas no DNA e RNA humano e suas possíveis falhas – sendo possível, inclusive, prever possibilidades de doenças relacionadas a este processo muito mais complicadas que as já existentes na atualidade –, já que é necessário conhecer todas as possibilidades para entender, prevenir e, quiçá, curar mazelas como: doença de Alzheimer, Encefalopatia Espongiforme Bovina (BSE), doença de Creutzfeldt-Jakob, Esclerose Lateral Amiotrófica, doença de Huntington, doença de Parkinson, muitos cancros e síndromes relacionados com o cancro, que são doenças causadas pela má assimilação ou enrolamento das proteínas nos processos de replicação do DNA; além disso, hoje é possível, outrossim, comprar o mapeamento completo do DNA particular de cada um sem a necessidade de sair de casa com a utilização da Internet, serviço oferecido pelo projeto "23andme"[2], sendo necessário apenas uma amostra da saliva humana para ter acesso a uma ampla gama de informações

[1] Disponível em: http://folding.stanford.edu/
[2] Disponível em: https://www.23andme.com/

pessoais, como por exemplo a linhagem genealógica completa, as falhas no DNA e as doenças que a pessoa tenha propensão a pegar.

Não podemos esquecer também os avanços na transparência e na eficiência que a utilização do computador e da Internet estão causando na máquina estatal de todos os Países do mundo, com a difusão das informações governamentais em tempo real, como é o caso do IMPOSTÔMETRO no Brasil e os vários portais de Transparência dos Órgãos Públicos, trazendo eficiência e eficácia ao nosso Estado, sem contar a digitalização dos processos judiciários, com o 'Processo Eletrônico', tornado efetivo com a Lei 11.419/2006, o que possivelmente trará maior celeridade ao judiciário brasileiro.

Há, no entanto, aqueles que neste campo são versados e que dele se utilizarão, por quaisquer fins que se possa imaginar, para lesar ou lograr o seu semelhante, causando empecilhos para todos, desde a dona de casa que está tentando fazer, através de receitas na Internet, um bolo de aniversário para seu filho de um ano até o médico que pesquisa a cura de uma doença grave há 5 anos, anotando suas descobertas em um arquivo no computador, e qualquer informação errada enviada e salva levará mais alguns anos para ser identificada e corrigida, e isto sem contar a possibilidade de ser este arquivo apagado por terceiros mal intencionados. É por este e diversos motivos que o Direito não pode se deixar ser atropelado por este ímpeto de inovações, urgindo a necessidade de uma sólida e ao mesmo tempo eficiente regulamentação deste – já não tão – novo espaço virtual, permitindo, como sempre foi o seu papel, uma fluída navegação a todos, com igual aproveitamento aos "experts"[3] e aos "newbies"[4].

A máquina do computador, como a conhecemos hoje, é incapaz de interagir com o ser humano em um plano bilateral ou voluntário, sendo a sua *interface* limitada a um encadeamento reprodutivo de comandos emitidos pelo próprio homem, não podendo o computador, na presente atualidade, emitir atos voluntários[5]. Esta constatação para o presente trabalho é essencial, uma vez que aqui

---

[3] Segundo o Dicionário Online Priberam: 'expert' ou 'experto': "Que ou quem é muito experimentado ou tem grandes conhecimentos em determinada área do conhecimento. = especialista, perito". Disponível em: http://www.priberam.pt/dlpo/default.aspx?pal=expert.

[4] Segundo o Wikipédia: "'Newbie', ou 'noob', também grafado como 'n00b', é uma palavra inglesa para novato ou ainda, neófito. O termo é originado de 'new boy' ('garoto novo'), gíria comum entre os militares norte-americanos designando um novato que acaba de chegar." Disponível em: http://pt.wikipedia.org/wiki/Newbie.

[5] NICOLESCU, Basarab. **O Manifesto da Transdisciplinaridade**, 3. ed., São Paulo: TRIOM, 2005, pp. 86 e 89.

restringimos as possibilidades de agentes criminosos: ou seja, exclui-se da possibilidade de realizar ações ou omissões o próprio computador, podendo apenas estas recair sob a pessoa do seu usuário ou programador. Porém, aqui poderia surgir outro problema, que não convém destrinchar no presente trabalho, que seria a criação de um programa lesivo que fosse de impossível ou difícil anulação e que sequencialmente continuasse a causar danos repetitivos e sucessivos, evoluindo seu modo de atuação com o tempo, porém, contando com o singelo detalhe da ausência de um ser humano operando tal programa e estando o seu criador já falecido... A princípio, sabemos que o objeto de estudo do Direito Penal são as "condutas humanas descritas de forma positiva (ações) ou de forma negativa (omissões de ações) em tipos legais de condutas proibidas", segundo o professor Juarez Cirino dos Santos[6], e também que a inteligência artificial dos computadores respeita apenas os comandos a ela atribuídos. Assim sendo, como poderia o Direito Penal atuar, nestes casos[7], na efetiva reprovação ou prevenção do crime, como idealiza o artigo 59 do Código Penal? Restariam totalmente prejudicados os objetivos[8] do Direito Penal, quais sejam: a proteção dos bens jurídicos da sociedade (objetivo declarado) ou o controle social nesta (objetivo real)? Isto demonstra a imensa proporção que este tema pode adquirir bastando-se uma pequena abstração.

Tendo definido o objeto de estudo como sendo as condutas humanas realizadas por meio de um computador, cabe fazer uma delimitação ainda maior, tendo em vista tratar-se de uma área pantanosa, onde há muita pesquisa a ser feita. Será, portanto, estudado com maior profundidade o tema da competência jurisdicional em crimes cibernéticos.

Por ser um tema novo para o Direito, inúmeros são os problemas que estão emergindo, como já foi demonstrado, porém estes surgem em uma proporção maior do que são solucionados. Entre eles, estão desde os assuntos mais basilares da matéria, em relação à nomenclatura a ser adotada pelo ramo do direito responsável

---

[6] SANTOS, Juarez Cirino dos. **Direito Penal**: Parte Geral, 2. ed., Curitiba: Lumen Juris, 2007, p. 3.

[7] STANDLER, Ronald B. **Computer Crime**, 1999. Disponível na Internet via WWW. URL: http://www.rbs2.com/ccrime.htm. Arquivo consultado em 23 de outubro de 2010. Especialmente tendo em vista que um programador consegue, facilmente, criar um programa que só entrará em funcionamento em uma data que possivelmente já estará morto. Hoje são conhecidos como "logic bomb" ou "time bomb". Mais sobre o tema, cf. RAYSMAN, Richard; BROWN, Peter. **Computer Law**: drafting and negotiating forms and agreements, v. 2. New York: Law Journal Press, 1984, p. 13-24.34 a 13-24.35.

[8] SANTOS, Juarez Cirino dos. Obra citada, p. 4-9.

pelo seu estudo, até os mais complexos e prejudiciais à sociedade como um todo, como a falta de tipificação dos novos crimes, os quais antes eram inimagináveis pelos penalistas. Tendo em vista a carência de estudos sobre o tema, convém proceder a uma breve exposição do tema para melhor fixar o objeto de estudo.

Porém, embora seja novo, deve ser abordado levando-se em conta o Direito Penal e o Direito Processual Penal já existentes. Não há que se falar em autonomia deste ramo do Direito, pois é o Direito Penal que dará as premissas básicas para a punibilidade concreta e o Direito Processual Penal que servirá de instrumento nesta, estando já delimitados os caminhos básicos a serem seguidas. Alfredo Augusto Becker e Paulo de Barros defendem que o ordenamento jurídico é indecomponível. Aquele doutrinador já dizia:

> Pela simples razão de não poder existir regra jurídica independente da totalidade do sistema jurídico, a "autonomia" (no sentido de independência relativa) de qualquer ramo do direito positivo é sempre e unicamente didática para, investigando-se os efeitos jurídicos resultantes da incidência de determinado número de regras jurídicas, descobrir a concatenação lógica que as reúne num grupo orgânico e que une este grupo à totalidade do sistema jurídico.[9]

Complementando tal entendimento, Paulo de Barros Carvalho consolida:

> [...] Com isso se predica banir a pretensa autonomia científica que chega a lhe conferir autores da melhor suposição. Repetimos a inadmissibilidade de tais foros de autonomia científica, sem destruir aquele que é o mais transcendental entre os princípios fundamentais do direito – o da unidade do sistema jurídico. O direito tributário está visceralmente ligado a todo universo de regras jurídicas em vigor, não podendo dispensar, nas suas construções, qualquer delas, por mais distante que possa parecer.[10]

Há um ordenamento jurídico, não havendo um ramo do direito independente dos demais. O que poderíamos ter é uma divisão, autonomia didática, apenas, especialmente pelo fato deste novo ramo do direito ser totalmente diferente dos demais no que tange à matéria e à linguagem utilizada, sendo esta divisão uma maneira mais acessível de expô-lo.

---

[9] BECKER, Alfredo Augusto. **Teoria Geral do Direito Tributário**. São Paulo: Saraiva, 1963, p. 28-29.
[10] CARVALHO, Paulo de Barros. **Curso de Direito Tributário**, 13. ed. São Paulo: Saraiva, 2000, p. 15-16.

2. CRIMES CIBERNÉTICOS

Apenas para se ter uma ideia sobre o que se enfrenta nesse tema, cabe a citação de Ivette Senise Ferreira sobre o tema:

> Num país como o nosso, em que a legislação encontra-se extremamente defasada e desvinculada da realidade, urge disciplinar a utilização abusiva da informática, hoje transformada num dos mais importantes veículos de comunicação de todo o mundo, dando-se atenção à questão da definição dos limites da licitude, e da conveniência para o meio social, do material que é transmitido por essa via.
> A ausência de maior previsão de incriminações e as dificuldades na apuração da autoria das condutas, bem como a atuação cada vez mais criativa dos infratores, estão a sugerir a apreciação dos fatos também pelo prisma da Ética, complementarmente à aplicação do Direito, devendo-se para isso poder contar com a necessária colaboração dos provedores e usuários para a consecução dos objetivos visados.[11]

2.1. A problemática acerca da nomenclatura

Embora pareça simples e supérfluo, a falta de uma unificação da nomenclatura desta matéria pode trazer consequências graves para o seu estudo doutrinário e acadêmico e resultados ineficazes, inexpressivos ou divergentes em sua aplicação prática. Com a harmonia do *nomen juris* dado à matéria, toda pesquisa sobre o tema se embasaria em uma única e abrangente terminologia jurídica, com suas convenientes ramificações para as aplicações jurisdicionais. Basta se imaginar a dificuldade que seria caso o Direito Ambiental tivesse diversas denominações menores, como: Direito do Meio Ambiente, Direito da Flora, Direito da Fauna, Direito das Florestas, Direito das Espécies em Extinção, etc.

Dentre as nomenclaturas atualmente utilizadas, há as seguintes: Crimes na Internet[12], Delito Informático[13], Crimes Digitais[14], Crimes via Internet[15], Delitos

---

[11] FERREIRA, Ivette Senise. A criminalidade informática *in* **Direito & Internet**: Aspectos jurídicos relevantes, Bauru, SP: Edipro, 2000, p. 236-237.
[12] INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**, 2. ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009 e BRITO, Eduardo Valadares de. **Crimes na Internet**. [online] Disponível na Internet via WWW. URL: http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/view/4714/4284. Arquivo consultado em 22 de outubro de 2010.
[13] VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**: Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Editora Forense, 2003, p.13.
[14] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2000, p.43.

Praticados por meio da Internet[16], Crimes de Computador[17], Crime Praticado por meio da Informática[18], Crimes de Informática[19], Crimes Cibernéticos[20], Crimes Eletrônicos, Crimes Telemáticos, dentre outros. Embora alguns autores utilizem a mesma nomenclatura, é verificada, nitidamente, uma divergência grande entre eles, cito como exemplo inicial, dois doutrinadores do tema: o Professor João Marcello de Araújo Júnior e Marco Aurélio Rodrigues da Costa, dois pioneiros neste estudo. Para o primeiro, crimes de informática seria qualquer conduta lesiva praticada com a utilização de dispositivos informáticos[21], já para o último, estes crimes seriam apenas aqueles que atentassem contra os dados[22], estejam armazenados, compilados, transmissíveis ou em transmissão. Ainda, para Marco Aurélio Rodrigues da Costa, 'dado', no ramo da computação, define-se como:

> (...) qualquer parte de uma informação, ou como algo que tem o poder de trazer qualquer informação. Também pode significar, quando relacionado com computadores e informática, uma informação numérica de formato capaz de ser entendido, processado e armazenado por um computador ou parte integrante de um computador. Ou, ainda, uma informação preparada para ser processada, operada e transmitida por um sistema de computador

---

[15] MIRANDA, Marcelo Baeta Neves. **Abordagem dinâmica aos crimes via Internet**. Jus Navigandi, Teresina, a. 4, n. 37, dez. 1999. Disponível na Internet via WWW. URL: http://socorromultiply.multiply.com/notes/item/617. Arquivo consultado em: 23 de outubro de 2010.

[16] MARTINELLI, João Paulo Orsini. **Aspectos relevantes da Criminalidade na Internet**. [online] Disponível na Internet via WWW. URL: http://www1.jus.com.br/DOUTRINA/texto.asp?id=1829. Arquivo consultado em 23 de outubro de 2010.

[17] BRASIL, Angela Bittencourt. **Informática Jurídica** - O Ciber Direito. Rio de Janeiro: Juris Doctor; 2000, p. 42.

[18] GOUVÊA, Sandra. **O Direito na Era Digital**: Crimes praticados por meio da Informática. Rio de Janeiro:Mauad, 1997, p. 25.

[19] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**, 2. ed. rev. ampl. e atual. Rio de Janeiro: Lumen Juris, 2003, p. 8.

[20] MPF. **Crimes cibernéticos**: manual prático de investigação, São Paulo, Abril de 2006, p. 9; CAMARGO SANTOS, Coriolano Aurélio Almeida. **Atual cenário dos crimes cibernéticos no Brasil**. [online] Disponível na Internet via WWW. URL: http://www2.oabsp.org.br/asp/comissoes/sociedade_informacao/artigos/crimes_ciberneticos.pdf. Arquivo consultado em 23 de outubro de 2010; e FREITAS, Gustavo. **Crimes Cibernéticos**. [online] Disponível na Internet via WWW. URL: http://www.gfsolucoes.net/gustavo/blog-tecnico/seguranca/crimes-ciberneticos/. Arquivo consultado em 23 de outubro de 2010.

[21] ARAÚJO JÚNIOR, João Marcelo. **Computer Crime**. Anais da Conferência Internacional de Direito Penal, 1988. Rio de Janeiro: Procuradoria Geral da Defensoria Pública, 1988, p. 461.

[22] Mais sobre o tema cf. TORRES, Gabriel. **Hardware**: Curso Completo. 4. ed. Rio de Janeiro, Axcel Books, 2001. A palavra 'dado' deriva do latim datum, a qual significa a forma passada do verbo "dar", "coisa dada", sendo, portanto, uma representação de um fato, figura ou ideia. Dados são com frequência vistos como a menor partícula que derivam informações e conhecimentos. Na ciência da computação, dados são números, palavras, imagens, etc. Os dados, na computação, são representados por 1 byte, sendo cada um destes formado por um conjunto de 8 bits, estes, por sua vez, representados pelos números 0 (desligado) ou 1 (ligado), que é o que conhecemos por dígitos binários (binary digits).

> ou programa de computador. Os dados podem expressar fatos, coisas certas, ou comandos e instruções.[23] [24]

Certamente a nomenclatura mais restrita é o de Crimes na Internet, pelo simples fato de estes poderem ser realizados apenas em âmbito *on-line*, ou seja, com a utilização da própria Internet, não abrangendo os crimes cometidos contra ela própria, mas a sua adoção por alguns doutrinadores não lhes retira a credibilidade, vez que indubitavelmente a maioria dos crimes perpetrados com o uso do computador se materializam exclusivamente pela utilização da rede interconectada de computadores[25], a Internet, desconsiderando, destarte, a possibilidade de ser cometido o mesmo crime em outras espécies de rede de computadores, como as redes locais.

Os que defendem que a nomenclatura a ser adotada deveria ser mais ampla, como, por exemplo, Ivette Senise Ferreira[26], falando em Crimes de Computador, defendem-na pelo fato de que o objeto de estudo expandir-se-ia para todo delito que detivesse uma relação direta com o uso do computador, independente de estar ou não conectado a uma rede interligada de computadores, como a Internet. Porém, é reconhecida, atualmente, a insuficiência desta classificação, visto que até mesmo os telefones móveis possuem as mesmas – senão mais – funcionalidades que o próprio computador *strictu sensu*.

Outros defendem que a nomenclatura deveria ser Crimes de Informática, pois abrangeria os outros dois anteriores e também todo e qualquer meio eletrônico associado. Segundo Vladmir Aras seriam "delitos que ofendem interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos (hardwares[27]), redes de computadores e programas de

---

[23] COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. [online] Disponível na Internet via WWW. URL: http://jus2.uol.com.br/doutrina/texto.asp?id=1826. Arquivo consultado em 23 de outubro de 2010.

[24] *Idem*

[25] CANTU, Eduardo. **Redes de Computadores e Internet**, São José: CEFET/SC, 2003, p. 3. "Uma rede de comutadores é conexão de dois ou mais computadores para permitir o compartilhamento de recursos e a troca de informações entre as máquinas."; Embora pareça muito simplista, esta é a verdadeira definição de 'rede de computadores', sendo a própria Internet uma espécie desta, em que vários computadores estão conectados ao mesmo tempo. Mais sobre o tema cf. TORRES, Gabriel. Redes de Computador: Versão Revisada e Atualizada, São Paulo, Novaterra: 2009.

[26] FERREIRA, Ivette Senise. Obra citada, p. 209.

[27] ALLEN, Mark. **Basic Hardware Guide**. [online] Disponível na Internet via WWW. URL: http://www.comptechdoc.org/basic/basictut/index.html. Arquivo consultado em 23 de outubro de 2010. É o termo que designa o artefato de existência física de uma tecnologia. Significa também o componente físico de um sistema de computador, na forma de um 'hardware de computador', como,

computador[28] (estes denominados softwares[29])"[30]. Para Carla Rodrigues Araújo de Castro, estes seriam aqueles praticados "contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador".

Há ainda uma quarta doutrina, que defende uma nomenclatura ainda mais abrangente, tratando estes delitos como Crimes Cibernéticos [31]. Existe uma explicação física e filosófica para que muitos julguem ser este o termo mais adequado. Seguindo este entendimento, tem-se que o mundo cibernético é concebido como um 'espaço-tempo cibernético', ou ETC [32], segundo Basarab Nicolescu, onde a transmissão de sinais se dá na velocidade da luz, estando delimitado, inicialmente, pelas quatro dimensões conhecidas pelo ser humano[33]. Seria este epaço-tempo ao mesmo tempo *natural* como *artificial*[34]. É natural uma vez que se origina do mundo quântico, um mundo invisível aos olhos humanos, mas existente efetivamente[35], formado pela associação dos códigos binários 0 e 1, meta-números que se traduziriam em 'porta fechada' e 'porta aberta', respectivamente, no mundo quântico. Sendo também artificial, uma vez que a codificação destes meta-

---

por exemplo, o teclado, o monitor, o mouse, a placa-mãe, o disco rígido, a placa de vídeo, dentre outros.

[28] FELLEISEN, Matthias; FINDLER, Robert Bruce; FLATT, Matthew; KRISHNAMURTHI, Shriram. **How to Design Programs**: An Introduction to Computing and Programming. Cambridge: The MIT Press, 2001, section 2, 2.2. Disponível na Internet via WWW. URL: http://www.htdp.org/2003-09-26/Book/curriculum-Z-H-5.html#node_sec_2.2. Arquivo consultado em 23 de outubro de 2010. Programa é uma sequência de instruções escritas para realizar uma tarefa específica para um computador. Um computador requer programas para funcionar, tipicamente executando as instruções dos programas em um processador central. O programa tem uma forma executável que o computador pode usar diretamente para executar as instruções. O mesmo programa na sua forma de 'código fonte', uma maneira legível para o ser humano, da qual os programas são derivados ou compilados, permite um programador estudar e desenvolver os seus algoritmos, que é propriamente a sequência finita de comandos ou instruções bem definidas e não ambíguas.

[29] ALLEN, Mark. Obra citada.É uma coleção de programas de computador e dados relacionados que providenciam instruções dizendo ao computador o que fazer. O termo foi criado para contrastar do termo antigo 'hardware'. Enquanto este significa algum aparelho de existência física, os softwares não são tangíveis, ou então, 'não podem ser tocados'. É às vezes utilizada de uma forma mais limitada, significando apenas aplicativos, que são conjuntos de programas criados para realizar uma única tarefa ou várias tarefas específicas interconectadas. Algumas vezes o termo inclui dados que não têm sido tradicionalmente associados com computadores, como filmes, fitas e gravações.

[30] ARAS, Vladmir. **Crimes de Informática**: Uma nova criminalidade. [online] Disponível via WWW. URL: http://www.informatica-juridica.com/trabajos/artigo_crimesinformticos.asp. Arquivo consultado em 23 de outubro de 2010.

[31] MPF. Obra citada; CAMARGO SANTOS, Coriolano Aurélio Almeida. Obra citada; e FREITAS, Gustavo. Obra citada.

[32] NICOLESCU, Basarab. Obra citada, p. 86.

[33] As quatro dimensões referidas seriam: os três planos cartesianos, *x*, *y* e *z*, acrescidos do fenômeno temporal como quarta dimensão.

[34] NICOLESCU, Basarab. Obra citada, p. 86.

[35] Comprovado através das experiências de acelerações de partículas.

números matematicamente, através de coordenações e aplicações de equações é capaz de gerar uma infinidade de imagens possíveis, sendo estes resultados obtidos pelo próprio ser humano. É exatamente de um conjunto destes elementos que se formam, concretamente, os dados e, consequentemente, as informações[36], como correta e resumidamente exposto por Túlio Vianna[37], sendo o número 'zero' representando a ausência de corrente elétrica – portanto, desligado – e o 'um' representando a presença de corrente elétrica – portanto, ligado. Segundo esse estudioso, essa linguagem é capaz de expressar qualquer informação humana podendo a informação ser transmitida, processada e armazenada em aparelhos eletrônicos específicos, como os 'discos rígidos', que é um hardware responsável pelo armazenamento dos dados.

Por isto Marco Aurélio Rodrigues da Costa[38] defende a importância de ser atribuída proteção jurídica a ambos, dados e informações, porém com a ressalva de que a legislação penal deve embasar-se nos dados e não nas informações, vez que esta última detém um caráter subjetivo[39].

Ademais, este ETC é de *natureza material*[40], e não imaterial, como se poderia imaginar. "A informação que circula no ETC é tão material[41] quanto uma cadeira, um carro ou uma partícula quântica."[42] Aqui se teria uma relação de transformação nova: a formação de imagens devido à aplicação das equações matemáticas. Pode-se citar, grosso modo, que a substituição do papel-moeda pela moeda virtual ou informática é uma das modificações que a criação da cibernética trouxe.

Assim sendo, a nomenclatura 'crimes cibernéticos' abrangeria todos os delitos cometidos contra este ETC e por meio deste, sendo estes delitos substancialmente diferentes dos cometidos no 'mundo real', pois apesar de eles estarem sujeitos a registros, normalmente afastando qualquer dúvida acerca da materialidade do fato – da sua prática ou não –, eles também exigem um maior conhecimento técnico para o

---

[36] Enquanto os 'dados' têm uma existência física evidente a informação é a interpretação que uma pessoa faz de algum objeto ou escrito, e isto dependerá de inúmeras variáveis, como por exemplo: o nível de escolaridade deste sujeito, a utilização de um programa adequado para a visualização de um arquivo específico , dentre outros fatores. Para exemplificar, ao tentarmos abrir um arquivo do Paint (*.png) com o programa do Word, aparecem apenas objetos ininteligíveis.
[37] VIANNA, Túlio Lima. Obra citada, p. 3-8.
[38] COSTA, Marco Aurélio Rodrigues da. Obra citada.
[39] Vide nota de rodapé nº 36.
[40] NICOLESCU, Basarab. Obra citada, p. 87.
[41] *Idem, ibidem.* "Na física moderna a matéria está associada ao complexo (substância/energia/informação/ espaço-tempo)".
[42] *Idem, ibidem.*

seu manuseio, exigindo uma investigação mais cientificamente abastada, com uma equipe de peritos extremamente versados no tema.

2.2. Classificação dos delitos cibernéticos

Antes de adentrar no tema seguinte, cabe fazer uma breve análise da classificação dos delitos cibernéticos sob a luz da tese de mestrado do professor Túlio Lima Vianna[43], sem alteração da nomenclatura por ele adotada, porém perfeitamente aproveitável nestes moldes.

Segundo ele, quatro são os delitos possíveis, não havendo confusão entre eles, os quais serão analisados:

Os Delitos de Informática Próprios ou Puros são aqueles em que ambos o meio e o fim pretendido pelo infrator encontram-se no próprio campo da informática. Trocando em miúdos, ele utiliza-se da informática para danificar ou atingir elementos integrantes da própria informática, como os *softwares*, *hardwares* e os dados contidos em quaisquer chips[44], seja contra um único indivíduo ou contra vários ou ainda contra outros entes, como a própria Internet. Exemplo clássico deste tipo de delito é o acesso não autorizado a um sistema informático utilizando-se de um computador, objeto de estudo do professor Túlio, demonstrando, inclusive, que este delito ainda não se encontra tipificado ordenamento jurídico brasileiro.

Em seguida há os Delitos Informáticos Impróprios, dando-se quando o computador é utilizado como meio na prática de algum delito já tipificado, não sendo um delito informático próprio pelo fato de não alterar o funcionamento do sistema informático alheio. Os casos mais comuns que se enquadram nestes tipos de delitos são os crimes contra a honra em *sites* de relacionamentos, como o "Orkut", em que o infrator utiliza-se destes como meio para difundir a sua ofensa mais rápida e eficientemente.

---

[43] VIANNA, Túlio Lima. Obra citada, p. 13-26.

[44] SHEPLEY, Phil. **What is a computer chip?** [online] Disponível na Internet via WWW. URL: http://www.wisegeek.com/what-is-a-computer-chip.htm. Arquivo consultado em 23 de outubro de 2010. Em eletrônica, é um circuito integrado (também conhecido como 'CI', 'microcomputador', 'microchip', 'chip de silício', 'chip' ou 'chipe') é um circuito eletrônico miniaturizado (composto principalmente por dispositivos semicondutores e também por componentes passivos), que tem sido produzido na superfície de um substrato fino de material semicondutor. Estes são usados em quase todos os aparelhos eletrônicos em uso nos dias de hoje e revolucionaram o mundo dos eletrônicos. Computadores, telefones celulares e outros aparelhos digitais são agora inextrincavelmente partes da estrutura da moderna sociedade, tornada possível pelos baixos custos de produção dos circuitos integrados , ou simplesmente chipes.

Há também os Delitos Informáticos Mistos, delitos estes de natureza mais complexa e mais graves, mesclando tanto a proteção da inviolabilidade dos dados como também outros bens jurídicos de naturezas diversas. São derivados do acesso não autorizado a sistemas informáticos, pois que na prática do delito o infrator viola os dados, manuseando-os a seu bel-prazer, porém exigindo uma tipificação mais apurada por tratar-se de delito mais grave que o mero acesso não autorizado a sistema computacional. O autor cita como exemplo o crime de acesso não autorizado a sistemas computacionais do sistema eleitoral, presente no inciso VII do artigo 67 da Lei 9.504/97, do qual se extrai:

> Art. 67. Obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos.

Por fim há os Delitos Informáticos Mediatos ou Indiretos, sendo a utilização do computador um mero meio para a obtenção de um fim específico e diverso do campo da informática, como, por exemplo, a invasão de um sistema informático bancário para transferir fundos monetários de uma conta a outra sem o consentimento do dono da conta bancária. Neste caso ter-se-ia apenas o crime de furto, porém não se confundiria com o delito informático impróprio pelo fato de ter havido, neste caso, a violação direta de dados informáticos, porém sendo de inferior gravidade frente ao delito patrimonial realizado.

2.3. Crimes cibernéticos: crimes materiais ou crimes formais?

Durante muito tempo, uma dúvida paira acerca da natureza dos crimes cibernéticos: seriam eles crimes materiais ou crimes formais? A resposta a esta pergunta trará sérias consequências quando analisados os aspectos processuais deste tema.

Um crime material é aquele que necessariamente trará um resultado externo à sua ação, o qual estará descrito em lei, sendo este resultado tipificado e punível, e destacando-se lógica e cronologicamente da própria conduta. Nos crimes materiais, a sua consumação se dá no instante em que ocorrer o resultado da conduta lesiva.

Como exemplo de crime material há o homicídio, em que o que é punível é o resultado da ação de "matar alguém", ou seja, a morte de alguém.[45]

Já no crime formal a existência de um resultado próprio independe para que o crime seja punível, sendo a mera prática da conduta reprimível por si só. Nos crimes formais, a consumação se dá no mesmo momento em que a conduta é realizada, pois não depende do acontecimento do resultado para que se possa o levar a juízo. Cita-se como exemplo de crime formal a ameaça, a injúria, a extorsão, dentre inúmeros outros em que a mera prática da conduta é punível independentemente do resultado.[46]

Para Maria Helena Junqueira Reis, os crimes cibernéticos seriam crimes materiais, afirmando que:

> Os crimes conectados aos computadores são crimes materiais, aqueles que só se tornam perfeitos com a realização do resultado fixado como característico do tipo legal (...) crimes de resultado, chamam-lhes os autores alemães.[47]

Já Gabriel Cesar Zaccaria de Inellas ressalta que os crimes cibernéticos devem ser considerados crimes formais, pelos seguintes motivos:

> Para mim, os crimes cometidos pela Internet, através de computadores, são crimes formais, consumando-se no local onde foi realizada a ação. É cediço que, para a ocorrência de uma infração penal, faz-se necessária uma conduta humana, positiva ou negativa (ação ou omissão), típica, antijurídica e culpável (Tribunal de Justiça de São Paulo, Apelação Criminal n. 8.544. Relator: Desembargador Weiss de Andrade. RT, 555/324-325; Superior Tribunal de Justiça, RHC n. 4.801 – Sexta Turma – Relator: Ministro Vicente Carnicchiaro, DJU de 18.12.1995, p. 44.624). Nos crimes materiais, o resultado só é imputável a quem lhe deu causa, exigindo-se a produção do resultado. Nos crimes formais, não se exige a produção do resultado. Suas características são, apenas, a ocorrência do fato típico e sua antijuridicidade (RJTJSP 124/19). Tanto que, em se tratando de extinção da punibilidade, nos crimes materiais, o termo inicial da Prescrição da Pretensão Punitiva, é a data da produção do resultado enquanto que, nos crimes formais, o momento consumativo coincide com a realização do ato antijurídico, anterior à produção do resultado. Nos crimes cometidos através da Internet, o agente ativos, ao realizar a ação, evidentemente, buscava atingir um resultado, um objetivo. Mas, se não conseguir efetivar tal objetivo, querido e desejado, já terá cometido o crime.48

---

[45] PEDROSO, Fernando de Almeida. **Competência Penal**, Belo Horizonte: Livraria Del Rey Editora, 1998, p. 48-49.
[46] *Idem*, p. 55.
[47] REIS, Maria Helena Junqueira. **Computer Crime**, Belo Horizonte: Livraria Del Rey Editora, 1997, p. 47.
[48] INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 129-130.

Como visto e previsível, não existe ainda, no ordenamento jurídico brasileiro, um consenso para um direcionamento na busca de uma classificação.

Não se há de crer que haja apenas uma resposta, com uma classificação que seja o suficiente para açambarcar todos os delitos informáticos existentes. Como já vimos, existem quatro tipos de delitos em âmbito informático, os delitos informáticos: i) Próprios ou Puros; ii) Impróprios; iii) Mistos; iv) Mediatos ou Indiretos.

i) Nos casos dos delitos informáticos Próprios ou Puros, é difícil dizer se seriam crimes materiais ou formais, vez que grande quantidade destes delitos sequer encontra-se tipificado, como se demonstrará mais adiante. Porém, seria mais sensato, tendo em vista suas características próprias, tratá-los como crimes formais, pois a sua mera prática já é reprovável, independendo, destarte, do resultado obtido.

ii) Nos casos de delitos informáticos Impróprios, por se tratarem de delitos ofensivos a bens jurídicos já protegidos no ordenamento jurídico atual, cada delito poder-se-ia reger pela própria previsão legal já regulamentada, assim se teria: no crime de estelionato, o crime seria material, já no caso de injúria, verificar-se-ia um crime formal, pois a lei assim prevê. Certamente isto se justificaria ainda mais nos casos dos crimes cometidos através da Internet, pois no caso de uma injúria publicada abertamente em um sítio de relacionamentos sociais, como o Orkut [49], esta seria visualizável por todas as pessoas online que acessassem aquela página no exato instante em que a mensagem injuriosa fosse enviada.

iii) Igualmente ao primeiro caso, os delitos informáticos Mistos também deveriam ser tratados como crimes formais, pois, por se tratarem de delitos ainda mais nocivos que os anteriores, a mera prática da conduta, independente do resultado, já justificaria a sua punição. Nos exemplos, dentre os delitos já tipificados, percebe-se que o próprio legislador acertou em tratá-los como crimes formais, tomando como exemplo o já referido artigo acerca do acesso não autorizado a sistemas computacionais do sistema eleitoral, presente no inciso VII do artigo 67 da Lei 9.504/97, em que a mera obtenção do acesso aos computadores do serviço eleitoral já

[49] Desconsiderando-se as opções de privacidade.

é punível, independente de o infrator ter conseguido alterar os dados nele contido ou não.

iv) Por último, nos delitos informáticos Mediatos ou Indiretos, também seria mais adequado tratá-los como crimes formais, pois, assim como os delitos informáticos próprios ou puros e os mistos, também têm uma etapa inicial que exige a invasão de um computador e a possível alteração de dados para que posteriormente se cometa um crime diverso. Nesta invasão, como já defendido, caso o infrator não consiga realizar qualquer delito posterior, ter-se-ia um delito autônomo de acesso não autorizado, sendo desnecessário algum resultado posterior para ser punível. Porém, em se concretizando um crime posterior, caracterizado por ser um crime material, como o furto, este se sobrepõe ao anterior, pois é considerado de maior gravidade que aquele.

O motivo da discordância para com os doutrinadores supramencionados se dá pelo fato de haver condutas que exigem a sua reprovação no momento em que o resultado se concretiza, e não no momento em que a ação é realizada. Imagine-se um caso hipotético de alguém que dispara arma de fogo ou aciona munição em lugar habitado ou em suas adjacências, em via pública ou em direção a ela, não tendo como finalidade a prática de outro crime, nos exatos moldes do artigo 15 da Lei n. 10.826/03. Esta pessoa será punida com reclusão, de 2 (dois) a 4 (quatro) anos, e multa, sendo punível a partir do momento em que ocorreu o disparo. Agora se esta mesma pessoa, nas mesmas circunstâncias, houvesse acertado e matado um transeunte, ela seria punida por homicídio culposo, com reclusão de 2 (dois) a 4 (quatro) anos, por se tratar de concurso formal de crimes, previsto no artigo 70 do Código Penal, porém com a diferença que aqui se tem um crime material, punível no momento em que a conduta causar o resultado. Agora, embora impossível ou extremamente improvável na atualidade, idealize-se um caso em que alguém pudesse disparar arma de fogo ou acionar munição em lugar habitado ou em suas adjacências, em via pública ou em direção a ela, com a habilidade de controlar mentalmente a direção da munição disparada. Suponha-se também que ninguém seja capaz de parar ou neutralizar esta munição. No momento em que houve o disparo, já se afirmou que o delito seria punível pelo artigo 15 da Lei n. 10.826/03. Então imagine agora que o poderoso infrator seja capturado,julgado e condenado a

3 anos de reclusão no exato momento em que ele disparou a munição, ocorre que, sem que se possa saber, ele havia mandado a sua munição telepaticamente controlada acertar o seu arqui-inimigo em exatos 15 anos daquele momento. E como era de se esperar, 15 anos depois, lá está ele novamente para ser julgado, porém agora há um detalhe: ele já foi punido pela ação que causou a morte do seu arqui-inimigo! Em sendo punido novamente com reclusão pela morte deste, violar-se-ia o Princípio do "*Non Bis In Idem*", pois ele estaria sendo condenado, no todo, a uma pena de 4 (quatro) a 8 (oito) anos. E se, da mesma maneira, este sujeito fizesse inúmeros alvos consecutivos, em intervalos menores, poderia ocorrer de, inclusive, ter-se uma punição atrás da outra, estando este sujeito condenado a uma pena perpétua, proibida no ordenamento jurídico brasileiro pela Constituição Federal, em seu artigo 5º, inciso XLVII, alínea *b*. Este seria, sem sombra de dúvida, um caso que geraria infinitas discussões.

Depois desta tamanha abstração, porém com motivos nobres para o presente estudo, imagine-se agora a disseminação de um vírus de computador[50] na internet. Certamente não há dúvida que esta ação por si só já é reprovável, independente de haver algum outro resultado mais grave ou não, portanto, crime formal. Porém, se um vírus disseminado na Internet causa danos a um computador, destruindo, inutilizando ou deteriorando vários programas e demais dados presentes neste aparelho, esta conduta seria punida, atualmente, apenas pelo delito de "Dano" (Código Penal, artigo 163), sendo um crime material, e, consequentemente, punível no momento em que o resultado se verificasse. Agora poderia haver um caso, atualmente possível, de um vírus disseminado que esteja programado para destruir todos os sistemas operacionais[51] em uma data posterior e pré-estipulada, seja a termo ou com alguma condição, como nos casos dos já vistos vírus do tipo 'logic

---

[50] GREGORY, Peter. **Computer Viruses for Dummies**. Hoboken: Wiley Publishing Inc., 2004, p. 209-210. Os vírus de computador propriamente ditos são programas que conseguem se copiar e infectar os arquivos de um computador, sendo, na maioria das vezes, de difícil remoção, e escondendo-se em arquivos de pastas ocultas ou do sistema, pastas de difícil localização para a maioria dos iniciantes em computação. O objetivo do vírus é o de corromper ou alterar o arquivo-alvo infectado.

[51] SILBERSCHATZ, Abraham; GALVIN, Peter Baer; GAGNE, Greg. **Operating system concepts**, 8 ed. Wiley & Sons, 2008, p. v. Também conhecido como 'SO', é um software, consistente em um conjunto de programas e dados, que funciona em computadores e administra os hardwares do computador e provê serviço comum para a eficiente execução de vários softwares aplicativos. Este tipo de software são encontrados em quase todos os aparelhos que contêm um computador: de telefones celulares e consoles de vídeo games até supercomputadores e servidores da Internet. Como exemplos de sistemas operacionais populares e modernos para computadores pessoais, temos o Windows da Microsoft, o Linux e o Mac OS X.

bomb' ou 'time bomb'. Neste caso, deparar-se-ia com os mesmos problemas do caso do atirador telepático: como punir alguém que já foi punido por uma determinada conduta? E o mais importante: como se utilizar dos recursos jurídicos existentes para coibir a prática desses atos? Não apenas os vírus prejudiciais ao funcionamento dos computadores, temporizados ou não, mas todos os Malwares[52], como: os Worms[53], os Cavalos de Tróia[54], os Spywares[55], os Keyloggers[56], os Adwares[57], os Ransonwares[58] e os Rootkits[59].

---

[52] Mais sobre o tema cf. MILLER, Frederic P; VANDOME, Agnes F; MCBREWSTER, John. **Malware**. VDM Publishing House, 2009. É um termo resumido para 'software malicioso', tendo a função de adentrar no sistema computacional de um usuário sem o seu consentimento informado. A expressão é um termo geral usado por profissionais da computação para designar várias formas de softwares hostis, intrusivos ou irritantes. O termo "vírus de computador" é algumas vezes usado para englobar todos os tipos de Malwares, como os vírus de computador propriamente ditos, worms, cavalos de tróia, spywares, adwares desonestos, crimewares, a maioria dos rootkits, além de outros softwares maliciosos não desejados.

[53] GREGORY, Peter. Obra citada, p. 208. Worm é um programa de computador capaz de se autorreplicar e enviar cópias de si mesmo para outros computadores conectados à rede, fazendo isto sem a necessidade da intervenção do usuário e, diferentemente dos vírus, sem a necessidade de se prender a um programa já existente no computador. O objetivo do worm é causar empecilhos ao uso do computador, normalmente reduzindo a velocidade de utilização da Internet.

[54] *Idem, ibidem*. Cavalos de Tróia, do inglês "trojan horse", é um programa lesivo que parece legítimo em que usuários tipicamente são enganados a descarregar e executá-los nos seus computadores, sendo desta maneira instalados nestes, e a partir deste ponto, a pessoa que tem controle deste programa consegue a qualquer momento realizar um acesso não autorizado no sistema computacional deste usuário.

[55] *Idem*, p. 32 e 165. Spywares são espécies de programas que são sorrateiramente instalados nos computadores para coletar pequenos pedaços de informação por vez sem que os usuários percebam, sendo a frequência da coleta de dados variável de acordo com o próprio programa. A presença destes programas é usualmente escondida do usuário e pode ser de difícil detecção. Os tipos mais comuns de spyware, no entanto, vão muito mais além do simples monitoramento. Estes programas estão cada vez evoluídos, sendo capazes de coletar informações pessoais dos usuários, como *web sites* mais visitados e hábitos correntes na Internet, além de espontaneamente redirecionar o usuário para outros e diversos sites e instalar programas não desejados, mudar as configurações do computador, deixando a velocidade de conexão mais lenta, perda de algumas funcionalidades da Internet em relação a alguns programas, dentre outras consequências. Por estes motivos, os Spywares também são conhecidos como 'softwares invasores de privacidade'.

[56] STEVENSON, Larry; ALTHOLZ, Nancy. **Rootkit for Dummies**. Hoboken: Wiley Publishing Inc., 2007, p. 289-290. Algumas vezes grandes corporações do ramo de informática, donas de computadores compartilhados ou de computadores públicos podem instalar programas como *keyloggers*, que registram todas as teclas digitadas no teclado e alguns mais avançados registram, inclusive, todos os movimentos detalhados do mouse, para secretamente monitorar o uso do computador.

[57] *Idem*, p. 13. Diferentemente dos Spywares, os Adwares são programas que por si só são inofensivos, sendo apenas um pacote de software que toca, mostra ou descarrega propagandas em um computador, sendo estas ações previamente autorizadas pelo usuário. O objetivo destes programas normalmente é fazer a divulgação de produtos e serviços, assim como qualquer propaganda de televisão, trazendo lucro para o autor deste programa. O problema começa quando ele vem associado com algum tipo de Spyware, como um *keylogger* ou outro programa invasor de privacidade, causando todos os transtornos já referidos.

[58] MILLER, James. **Making the Most of the Internet**: And the Other Less/More Important Things in Life. East Green Farm: Daisy Analysis Ltd., Janeiro de 2006, p. 36 e 72-73. Mais recentemente surgiu um outro tipo de programa malicioso, o Ransomware. O seu funcionamento consiste em criptografar os arquivos existentes no computador, fazendo com que estes se tornem inutilizáveis até que a senha para decodificá-los seja inserida. Desta maneira, o criador do programa consegue exigir que o

2.4. A falta de tipificação

Alguns doutrinadores entendem que não há a necessidade de criação de novos tipos penais, outros afirmam veementemente que a criação destes é urgente. Mas afinal, há ou não há a necessidade de novos tipos penais? Em uma breve análise, é facilmente perceptível esta urgência, e é, inclusive, por este motivo que já houve vários projetos de lei no Congresso Nacional tentando estipular os limites e as penas para o incorreto manuseio do computador e seus consequentes[60], como por exemplo os projetos de lei: 1.806/1999[61], de autoria do Deputado Freire Júnior; 84/1999, de autoria do Deputado Luiz Pauhylino e 1.713/1996[62], de autoria do Deputado Cássio Cunha Lima.

Aqueles que defendem a tese de que os tipos penais já existentes são suficientes, devendo apenas ser melhor adequados às situações reais, como Marco Aurélio Rodrigues da Costa[63] e Vicente Grego Filho[64], assim o dizem em relação aos

---

usuário do computador pague uma quantia estipulada para que ele forneça a senha correta, inclusive ameaçando a vítima dizendo que excluirá um arquivo aleatório a cada 15 minutos de demora no envio do dinheiro. Certamente estaríamos diante de um crime de extorsão, e, pasmem, um extremamente eficiente, pois que o usuário desprovido de cópias de segurança de seus arquivos importantes terá de pagar, de uma forma ou de outra, para reaver seus arquivos, caso não pretenda vê-los excluídos, pois que as únicas duas maneiras de decodificar os arquivos é mediante a inserção da senha ou então levando o computador infectado em uma empresa especializada em criptografia e decodificação, porém é sabido que esta empresa levará um tempo indeterminado para realizar este processo, que poderá, inclusive, demorar inúmeros anos nos casos mais extremos.

[59] STEVENSON, Larry; ALTHOLZ, Nancy. Obra citada, p. 20-23. Rootkit é um software que habilita o acesso contínuo e privilegiado a um computador enquanto ativamente escondendo a sua presença dos seus administradores por meio da subversão das funcionalidades padrões do sistema operacional e demais programas. Usualmente, um hacker instala um rootkit em um computador logo em seguida à obtenção do acesso privilegiado pela primeira vez, tanto pela exploração de uma conhecida vulnerabilidade na segurança do computador ou pela quebra de uma senha interna. Assim que o rootkit é instalado, ele permite que um invasor esconda a sua presença e ganhe acesso privilegiado ao computador, se esquivando das autenticações normais e demais mecanismos de autorização do computador. Embora os rootkits sirvam para uma ampla variedade de fins, eles ganharam notoriedade como sendo malwares, apropriando-se dos recursos do computador ou furtando senhas sem o conhecimento dos administradores e usuários dos sistemas infectados.

[60] Cite-se, como exemplo, os Projetos de Lei: 1.806/1999, de autoria do Deputado Freire Júnior; 84/1999, de autoria do Deputado Luiz Pauhylino e 1.713/1996, de autoria do Deputado Cássio Cunha Lima.

[61] Projeto arquivado nos termos do Artigo 105 do Regimento Interno da Câmara dos Deputados em 31/01/2003.

[62] Projeto arquivado nos termos do Artigo 105 do Regimento Interno da Câmara dos Deputados em 31/01/2007, sendo desarquivado em 12/03/2007, porém sem qualquer movimentação posterior.

[63] COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. Jus Navigandi, Teresina, ano 1, nº 12, Maio de 1997, p. 3. [online] Disponível na Internet via WWW. URL: http://jus2.uol.com.br/doutrina/texto.asp?id=1826. Arquivo consultado em 23 de outubro de 2010.

[64] GRECO FILHO, Vicente. **Algumas observações sobre o Direito Penal e a Internet**. Boletim IBCRIM, ano 8, nº 95, p. 3.

tipos já presentes na parte especial do Código Penal, os delitos informáticos impróprios, pois que certamente para estes não haveria a necessidade de mudança, como, por exemplo, colocando "na Internet" ou "por meio do computador" para serem válidos. Certamente ninguém discutiria se uma injúria no site de relacionamentos "Orkut" seria punível ou não pelo fato de ser escrita e não falada pessoalmente à vítima, não sendo a ausência de algum artigo ou inciso sobre a Internet um empecilho para o fiel cumprimento da lei. Mas já se encontra comprovado que existem, sim, atos atentatórios contra o próprio computador e a rede integrada destes que não encontra respaldo em qualquer tipo penal, estando esta lacuna, segundo estes doutrinadores, sujeita a abusos por parte de alguns especialistas, trazendo a atipicidade e, consequentemente, a impunidade[65].

Para Rita de Cássia Lopes, no mundo virtual, justamente por este ser uma criação humana, não existem limites físicos nem naturais, e em sendo artificial, tudo se realiza por vontades e impulsos humanos e em uma velocidade que não é acompanhada por nenhum dos Poderes, seja o Executivo, o Judiciário ou o Legislativo. Desta maneira, acerta que:

> O Direito deve buscar respostas adequadas para facilitar a transição entre o meio físico e o virtual. Um dos caminhos a ser seguido é exatamente incorporar aquelas normas que nasceram no ambiente virtual de forma que a resposta jurídica do mundo real seja um reflexo da resposta adequada e exigida no meio virtual, evitando efeitos legais divergentes[66].

Segundo o professor Juarez Cirino, um dos cernes do Princípio da Legalidade é a 'proibição de analogia da lei penal *in malam partem*', ou seja, seria a "aplicação da lei penal a fatos não previstos, mas semelhantes aos fatos previstos"[67], não sendo isto permitido em qualquer ordenamento jurídico que respeita o referido princípio. E nesse sentido, em não havendo um tipo penal específico em lei prévia e escrita para a conduta lesiva no âmbito da computação, não haverá, destarte, um delito penal, seguindo a máxima do '*nullum crimen, nulla poena sine lege*'. Então, para que haja uma efetiva repressão dos delitos cibernéticos, fazem-se necessárias, além de prévias e escritas, leis adequadas à realidade social atual, vez que é notório

---

[65] CASTRO, Carla Rodrigues Araújo de. Obra citada, p. 15.
[66] SILVA, Rita de Cássia Lopes. **Direito Penal e Sistema Informático**. In Ciência do Direito Penal Contemporâneo, v. 4. São Paulo: RT, 2003, p. 29.
[67] SANTOS, Juarez Cirino dos. Obra citada, p. 21-22.

o fato de que os encarceramentos apenas geram mais criminalidade, e com muito mais frequência, sem efetivamente solucionar a crescente perpetração de crimes.

Em contrapartida, há os que defendem a urgência da criação de novos tipos penais, justamente para não criar uma verdadeira sensação de impunidade, como Lucivaldo Vasconcelos Barros[68], que além de defender este ponto, defende também a urgência de uma ação político-social efetiva contra a ampliação dos crimes cibernéticos, pois que a mera tipificação, como já se vê na atualidade brasileira com todos os delitos hoje cometidos apesar das duras penas impostas pelo Código Penal brasileiro, não é suficiente. Para Gabriel Cesar Zaccaria de Inellas:

> Não possuímos legislação específica a respeito de crimes virtuais e o nosso Código Penal data de 1940. Evidentemente, no combate aos crimes virtuais, a Justiça utiliza o Código Penal, pois, a grande maioria das infrações penais cometidas através da Internet, pode ser capitulada nas condutas criminosas previstas no Código Penal. Todavia, o ideal seria a existência de lei especial, onde estivessem capituladas as condutas específicas, isto é, as condutas criminosas praticadas através da Internet.[69]

Apenas para exemplificar algumas condutas graves e de difícil enquadramento legal devido à ausência de tipos penais específicos[70], cita-se: o acesso não autorizado a sistemas computacionais, o furto de tempo e o dano causado pelos *malwares*, como o vírus de computador. Esta dificuldade decorre do fato de serem condutas delituosas que têm como objetivo a violação da própria informática como bem jurídico autônomo, não havendo uma proteção específica nestes casos[71]. Porém, embora não haja uma tipificação específica para alguns delitos, não há como não concordar com Túlio Lima Vianna:

> Reconhecida, pois, a existência de um bem jurídico a se proteger, tem-se que há crime sob o aspecto material, sendo que a simples omissão normativa não é suficiente para descaracterizá-lo como objeto de estudo do Direito Penal, já que este reconhece sua existência sob o aspecto material.[72]

---

[68] BARROS, Lucivaldo Vasconcelos. **O crime na era da informação**, 2002. [online] Disponível na Internet via WWW. URL: http://jus2.uol.com.br/doutrina/texto.asp?id=3675/. Arquivo consultado em 23 de outubro de 2010.
[69] INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 35.
[70] VIANNA, Túlio Lima. Obra citada, p. 3-4.
[71] AGUIAR, Rebeca Novaes. **Competência territorial para apurar crimes na internet**. [online] disponível na Internet via WWW. URL: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=1225. Arquivo consultado em 23 de outubro de 2010.
[72] VIANNA, Túlio Lima. Obra citada, p. 3.

Partindo desse pressuposto e da análise realizada, seria mais sensato que os crimes cibernéticos comuns fossem resolvidos por outras esferas do Direito, como a Civil, nas reparações e indenizações por danos ou prejuízos causados à vítima, ou ainda pelo ramo administrativo do Direito, em casos que envolvam a Administração Pública, deixando o Direito Penal apenas para os casos de maior gravidade e que de fato deveriam ser punidos com penas de reclusão ou detenção, quando outras soluções não forem mais viáveis. Para estes últimos casos, deve-se agilizar o processo doutrinário e na criação de leis penais e processuais específicas para conduzir o correto funcionamento da Justiça Penal, trazendo efetivamente o caráter preventivo e garantista do Direito Penal, e de maneira similar, impedindo que abusos sejam cometidos durante qualquer fase do processamento do caso, seja no inquérito policial ou no julgamento do acusado.

Segundo Gabriel Cesar Zaccaria de Inellas e Carla Rodrigues Araújo de Castro, há delitos cibernéticos que já possuiriam uma adequada tipificação[73] no Código Penal brasileiro, como: ameaça, dano, furto, estelionato, pornografia infantil, racismo, crimes contra a honra, crimes contra o sistema financeiro, interceptação do fluxo de dados em tráfego por serviço de telecomunicações, crimes contra a inviolabilidade dos segredos, crimes contra a ordem tributária, crimes eleitorais, violação de correspondência, incitação ao crime, inserção de dados falsos em sistema de informações, apologia de crime ou de criminoso, violação de direito autoral, induzimento, instigação ou auxílio ao suicídio, favorecimento da prostituição, jogos de azar, rufianismo, tráfico de substâncias entorpecentes e armas de fogo, crimes contra a Segurança Nacional, ultraje a culto e impedimento ou perturbação de ato a ele relativo, crimes contra o consumidor; pois se tratam de ofensas contra bens jurídicos já protegidos pelo ordenamento jurídico vigente.

Não será objeto de estudo a análise aprofundada de todos estes delitos, mas cabe algumas observações e problematizações em alguns tipos específicos mais polêmicos.

---

[73] Mais sobre o tema cf. INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 35-110; CASTRO, Carla Rodrigues Araújo de. Obra citada, p.15-63. Neste sentido, a autora referida por último entende ser o crime de 'apropriação indébita' um crime específico de informática, citando como exemplo o caso de alguém se apropriar de um *scanner*, porém entende-se não ser este o melhor entendimento para estes crimes de que trato, vez que se trata de um crime comum, da mesma maneira que apropriar-se de qualquer outro objeto alheio, não sendo a informática nem um meio nem um fim neste delito, sendo o *scanner* apenas um objeto de valor econômico e utilidade para o infrator.

2.4.1. Dano

Devido à falta de tipificação, recentemente vem-se utilizando o crime de 'dano' nos casos em que é disseminado um vírus ou outro *malware* relacionado que cause danos no funcionamento de um computador. Porém, o crime de dano no âmbito da informática é diferente do dano em objetos materiais. A começar pelo momento da sua consumação: "o crime de dano é material e consuma-se no momento do resultado, já o dano causado por vírus só se consuma muito tempo após o último ato"[74], podendo, seguindo esta lógica, trazer dificuldades na sua aplicação. Imagine-se, neste caso, um vírus do tipo '*time bomb*' ou '*logic bomb*' que esteja programado para destruir todos os sistemas computacionais infectados em uma data pré-estipulada, como 2012 – ano que se tornou polêmico recentemente –, causando danos irreparáveis, e adicione-se a isto o fato de o seu programador ter falecido um ano antes da ativação desta sua criação. Certamente instaurar-se-ia um impasse.

No artigo 163 do Código Penal está tipificado o crime de dano: "Destruir, inutilizar ou deteriorar coisa alheia". Aqui há um outro problema, problema este que ocasiona um longo embate doutrinário, que é a consideração de dados de computador como 'coisas'. Para Flávia Rahal e Roberto Soares Garcia[75] os dados não podem ser considerados como tais, não podendo ser aplicada a letra do artigo 163 no caso dos vírus de computador. Já Túlio Vianna[76] e Heleno Cláudio Fragoso[77] entendem que os dados podem, sim, ser considerados coisas, pois têm valor relevante para a sociedade, sendo, destarte, bens jurídicos que devem ser protegidos pelo Direito Penal vigente.

2.4.2. Furto

Quanto ao crime de furto, o Código Penal brasilerio expõe, no seu artigo 155: "Subtrair, para si ou para outrem, coisa alheia móvel", porém ao se alterar os valores

---

[74] FARACO, Sabrina. **O vírus como crime de informática**, p. 3-4. [online] disponível na Internet via WWW. URL: http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/6038/5607. Arquivo consultado em 23 de outubro de 2010.

[75] RAHAL, Flávia; GARCIA, Roberto Soares. **Vírus, direito à intimidade e a tutela penal da Internet**. In Revista do Advogado. v. 23, n. 69, São Paulo:maio de 2003, p. 26.

[76] VIANNA, Túlio Lima. Obra citada, p. 2.

[77] FRAGOSO, Heleno Cláudio. **Lições de direito penal**: a nova parte geral, 8ª ed. Rio de Janeiro: Forense, 1985, p. 147.

das contas bancárias de uma pessoa e os transferir para outra, embora ninguém questione que se trata de um delito de furto, não houve a subtração física que o legislador penal pensou ao elaborar o referido dispositivo legal, além de ser difícil imaginar os dados armazenados no *site* de algum banco como uma coisa móvel tangível. Há quem defenda que o furto de pequena quantia, como alguns centavos, pudesse cair no crime de bagatela, cair no conceito da insignificância, porém quando se utiliza o sistema informático para furtar pequenas quantias de várias contas, resultando assim um montante considerável, não há como se desprezar o enriquecimento ilícito do infrator, como bem analisou a professora Liliana Minardi Paesani[78] ao estudar este tipo de golpe, também conhecido como *salami slicing* (fatias de salame), punindo os responsáveis pelo delito com o tipo penal do furto, embora com uma considerável dificuldade de enquadramento neste, da mesma maneira como já foi exposta no delito de dano.

2.4.3. Estelionato

Código Penal, art. 171: "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento". Por meio deste último trecho, tem-se a possibilidade de o estelionato ser praticado com a utilização do computador, bastando a sua utilização como meio fraudulento, sendo esse o entendimento dos tribunais brasileiro na atualidade[79]. Porém, será que se poderia imaginar a possibilidade de induzir ou manter em erro um sistema informático propriamente dito? Tome-se como exemplo um caixa eletrônico. Com um pequeno aparelho, vulgarmente conhecido como "chupa-cabra"[80], é possível conseguir o número e a senha de um cartão introduzido em um caixa eletrônico com um aparelho destes instalado sem que o seu usuário sequer perceba que foi vítima de um crime, crime este que vem sendo cada vez mais comum na atualidade. Mas há também uma outra possibilidade de delito já registrada, que é a inserção de um cartão adulterado no caixa eletrônico, cartão este que a máquina interpreta ser legítimo, porém transmitindo informações fraudulentas, afirmando que o usuário tem disponível

---

[78] PAESANI, Liliana Minardi. **Direito e Internet**. São Paulo: Atlas, 2000, p. 38-40.
[79] Vide, por exemplo, Tribunal de Alçada Criminal de São Paulo, RT 762/633.
[80] Vide notícia em http://www.odiariodeteresopolis.com.br/leitura_noticias.asp?IdNoticia=6875. Arquivo consultado em 23 de outubro de 2010.

valores que não existem, e quando este usuário aplica o comando de sacar dinheiro, a máquina realiza a ação de acordo com a sua programação, vez que entende tratar-se de um cartão legítimo e com fundos suficientes. Neste caso estar-se-ia diante de um delito similar ao estelionato, realizado contra o próprio sistema computacional desta máquina?

2.4.4. Pornografia Infantil

Com a sua criação, a lei 8.069/90 ou Estatuto da Criança e do Adolescente, no artigo 241, trouxe o crime de pornografia infantil, porém este se encontrava repleto de imperfeições. Na redação original, o crime de pornografia infantil era assim descrito: "fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente". Nestes moldes, como bem observou Carla Rodrigues Araújo de Castro, o ato de enviar um *e-mail* com pornografia envolvendo criança ou adolescente não seria considerado crime, sendo, portanto, atípica, mas após duas grandes reformas, a letra deste mesmo artigo 241[81] hoje engloba esta possibilidade, além de cercar outras possibilidade semelhantes.

---

[81] [ECA]Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
§ 1o Nas mesmas penas incorre quem:
I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
§ 2o As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.
Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
§ 1o A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
§ 2o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
I – agente público no exercício de suas funções;
II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.

Tem-se, neste caso, um exemplo de adaptação da legislação brasileira para se apropriar aos crimes cibernéticos atualmente cometidos.

2.4.5. Interceptação do Fluxo de Dados em Tráfego por Serviço de Telecomunicações

Diz o artigo 10 da lei 9.296/96: "Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.", em seguida, o parágrafo único do artigo 1º desta mesma lei expõe: "O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática." Consoante tal redação, a transmissão de dados pela Internet poderia ser enquadrada como meio de comunicação, estando sujeitas as interceptações destas transmissões às penas previstas nessa lei. Assim sendo, os perigosos programas que registram teclas digitadas, como por exemplo os *Keyloggers*, famosos por captar contas e senhas bancárias dos computadores, poderiam, com alguma dificuldade, ser enquadrados neste delito.

2.4.6. Violação de correspondência

No artigo 151 do Código Penal e seus parágrafos encontra-se o crime de violação de correspondência:

---

§ 3o As pessoas referidas no § 2o deste artigo deverão manter sob sigilo o material ilícito referido.
Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo.
Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
Parágrafo único. Nas mesmas penas incorre quem:
I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.
Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.

> Art. 151 - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º - Na mesma pena incorre:
> I - quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói;
> II - quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas;

Porém, seria possível enquadrar a correspondência eletrônica, o *e-mail*, no conceito de correspondência, vez que o legislador evidentemente pensou na correspondência física, que poderia ser subtraída e devassada ou ocultada do seu destinatário, e não na mera transmissão e captação de dados eletrônicos? É de se espantar, mas o artigo 56 da lei 4.117 de 1962, o Código Brasileiro de Telecomunicações, é que resolve a questão, criada muito antes de a Internet ser disponibilizada ao público, o que se deu em 1993, trazendo o seguinte regramento:

> Art. 56. Pratica crime de violação de telecomunicação quem, transgredindo lei ou regulamento, exiba autógrafo ou qualquer documento do arquivo, divulgue ou comunique, informe ou capte, transmita a outrem ou utilize o conteúdo, resumo, significado, interpretação, indicação ou efeito de qualquer comunicação dirigida a terceiro.
> § 1º Pratica, também, crime de violação de telecomunicações quem ilegalmente receber, divulgar ou utilizar, telecomunicação interceptada.

Trazendo as seguintes penas, ainda mais severas que a do Código Penal:

> Art. 58. Nos crimes de violação da telecomunicação, a que se referem esta Lei e o artigo 151 do Código Penal, caberão, ainda as seguintes penas:
> I - Para as concessionárias ou permissionárias as previstas no artigos 62 e 63, se culpados por ação ou omissão e independentemente da ação criminal.
> II - Para as pessoas físicas:
> a) 1 (um) a 2 (dois) anos de detenção ou perda de cargo ou emprego, apurada a responsabilidade em processo regular, iniciado com o afastamento imediato do acusado até decisão final;

Observa-se uma enorme diferença na aplicação da pena nestes casos, sendo a pena da violação da telecomunicação muito maior do que a de violação de correspondência, e, desse modo, os tribunais superiores vêm aplicando o disposto no Código Penal, entendendo o *e-mail* como uma forma de correspondência[82]. Alguns doutrinadores, como Gabriel Cesar Zaccaria de Inellas, entendem que o

[82] Neste sentido, vide, por exemplo, STM – Recurso Criminal 6.337-0 RS.

correto no ordenamento jurídico brasileiro, por ter um texto que melhor se adapta à situação em questão, fosse a aplicação do Código Brasileiro de Telecomunicações[83], vez que é lei mais específica sobre o assunto, porém a infundada discrepância na previsão da pena entre esses dois dispositivos legais urge uma atualização dos mesmos à realidade social atual.

Ademais, interpretando tais previsões legais à luz da teoria agnóstica da pena e, destarte, vindo de encontro aos entendimentos anteriores, não seria sensato aplicar uma lei tão severa que data de 1962 a delitos que recém foram pensados. O Direito Penal, acima de tudo, deve ser visto na sua função garantista, impedindo que os poderes políticos e vontades de vingança, inerente ao ser humano de qualquer época, prevaleçam sobre os direitos à liberdade e à vida digna. É por este motivo que Augusto Jobim do Amaral afirma que se deve "fugir de algum tom lírico no discurso penal manifesto na impotência de encontrar um fundamento racional à punição"[84], atuando, o discurso penal, de maneira sensata e "nunca perdendo de vista a flexibilidade de *táticas* não universais em prol de uma *estratégia* clara de *limitação do poder punitivo*, na busca de salvar o maior número possível de vidas humanas"[85].

2.4.7. Violação de direito autoral

Este é um dos crimes mais praticados na Internet, estando previsto, no ordenamento jurídico brasileiro, no artigo 12 da lei 9.609/98 e parágrafos, na qual se lê:

> Art. 12. Violar direitos de autor de programa de computador:
> Pena - Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
> Pena - Reclusão de um a quatro anos e multa.
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

---

[83] INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 85-87.
[84] AMARAL, Augusto Jobim do. **Ensaio sobre uma teoria agnóstica da pena**: Fronteiras entre o político e o direito penal. *In*: Encontro Preparatório para Congresso Nacional do CONPEDI, 17., 2008, Salvador, BA. Anais do: XVII Encontro Preparatório para o Congresso Nacional do CONPEDI, Florianópolis: Fundação Boiteux, 2008, p. 1607.
[85] *Idem,* p. 1608.

Observe que o crime só se dá nos casos em que há, de alguma maneira, o comércio ilícito de cópias de programas de computador, os quais são equiparados a bens móveis, pensando o legislador nos casos de comércios de lojas e em camelôs de rua, mas deixa em aberto os casos em que há o compartilhamento altruísta deste mesmo, como ocorre nos *sites*[86] que disponibilizam a descarga de músicas, jogos e programas diversos sem o dispêndio de um centavo sequer que, embora não tenha fins propriamente ilícitos, causam enormes danos nas empresas produtoras desses bens ou programas. Por mais que não haja uma tipificação no ordenamento jurídico brasileiro, esta prática já está começando a ser punida pelas legislações dos países mais desenvolvidos.

2.5. Condutas não tipificadas:

Embora o Direito Penal seja a ultima ratio na efetiva repressão a qualquer delito, tendo em vista a sua insuficiência para efetivamente corrigir qualquer anomalia humana através da aplicação padronizada de penas pré-estipuladas, ficará demonstrada, pouco mais adiante, a real intenção deste tópico referente às condutas não abrangidas por qualquer tipo penal.

2.5.1. Acesso Não Autorizado a Sistemas Computacionais

Em sua tese e livro, *Fundamentos de Direito Penal Informático*, Túlio Lima Vianna disserta sobre esta conduta, mostrando que no ordenamento jurídico brasileiro não há, ainda, um tipo penal punindo tal conduta, embora socialmente reprovável. O seu tipo objetivo constitui-se na ação de acessar, que se traduz no:

> Ler, escrever ou executar dados armazenados em sistemas computacionais. A leitura é a recuperação dos dados armazenados no sistema com sua consequente interpretação como informações humanamente inteligíveis. A escrita consiste na inserção, remoção ou alteração de dados no sistema. A execução de dados, mais precisamente

[86] Cite-se como exemplo o antigo *site* do Mininova.org (http://www.mininova.org/), que era um dos *sites* mais eficientes na divulgação de cópias de programas não autorizadas e que em 2009 foi condenado pela Corte alemã de Utrecht a cancelar todas as divulgações de programas não autorizadas pelos autores dos mesmos, restando apenas a possibilidade de divulgar os conteúdos autorizados e pagos.

> de programas, é o processamento de informações automatizadas de acordo com instruções preestabelecidas.[87]

Sendo o seu objeto material os próprios dados ou programas, *softwares*, informáticos. Não se verifica, nestes moldes, qualquer tipo penal protegendo este bem jurídico, sendo esta conduta uma evidente ofensa ao "direito à privacidade, devendo, portanto, ser reconhecida como bem jurídico essencial para a convivência numa sociedade"[88].

Há que considerar, no entanto, as condutas que realmente e consideravelmente ofendam o bem jurídico – no caso considerado como os dados informáticos –, para não ecoar na insignificância [89], já que diariamente os computadores estão sujeitos a pequenas invasões e acessos não autorizados, como no caso dos *spams*[90] e *cookies*[91], que, embora incontroláveis na atualidade, são em sua grande maioria inofensivas.

Ainda dentro desta conduta, pode-se piorar um pouco a situação: apagar permanentemente um arquivo do computador, causando um dano irreparável no sistema operacional deste, haveria uma possibilidade de enquadrar essa conduta no delito de dano. No art. 23 do Projeto de Lei n. 1.713/96, de autoria do deputado Cássio Cunha, haveria uma tipificação a esta conduta nos seguintes moldes: "Art. 23. Obstruir o funcionamento de rede integrada de computadores ou provocar-lhe distúrbios. Pena – detenção, de 1 (um) a 2 (dois) anos, e multa", hipótese em que se teria uma obstrução total ou parcial do funcionamento do computador em questão[92]. Similarmente, poderia ser apagado um arquivo meramente sentimental ou ainda um arquivo que continha uma pesquisa ou um trabalho importante, sem que resultasse em complicações ao funcionamento do computador, podendo, inclusive, ocorrer um furto derivado deste acesso não autorizado, como no simples caso de uma invasão de uma conta de um jogo de vídeo-game onde é subtraído do usuário algum item

---

[87] VIANNA, Túlio Lima. Obra citada, p. 93.
[88] *Idem,* p. 3.
[89] *Idem,* p. 55-57.
[90] SULLIVAN, Dan. **The Definition Guide to Controlling Malware, Spyware, Phishing and Spam.** RealtimePublishers.com, 2007, p. 19. Spam consiste na utilização de um sistema eletrônico de envio de mensagens para mandar enormes quantidades de mensagens de e-mail, indesejadas e não solicitadas, indiscriminadamente.
[91] VIANNA, Túlio Lima. Obra citada, p. 56. "São pequenos arquivos-textos gravados no computador da vítima, contendo suas informações pessoais e, em geral, seus hábitos de consumo.
[92] RODRIGUES, Francisco de Assis. **A tutela penal dos sistemas de computadores**, p. 2. [online] Disponível na Internet via WWW. URL: http://jus2.uol.com.br/doutrina/texto.asp?id=2813&p=2. Arquivo consultado em 23 de outubro de 2010.

obtido com seu esforço próprio, ou ainda tem seu personagem destruído nessa invasão não autorizada. Nestes casos, haveria uma dificuldade para encontrar um tipo penal que condenasse esta conduta, porém poder-se-ia, sem prejuízo de uma repressão adequada – e sendo ainda mais ideal na realidade brasileira atual –, aplicar o Direito Civil para solucionar estas questões com uma adequada indenização e possivelmente com cumulação de danos morais decorrentes desta ofensa à intimidade ou à vida privada ou profissional da pessoa.

2.5.2. Furto de tempo

Segundo Sérgio Ricardo Gonçalves, esta conduta "consiste em uso do computador fora do propósito pelo qual se tem acesso ao equipamento, seja esta conduta motivada por fins de lucro ou apenas por passatempo" [93], podendo, outrossim, recair em outros aparelhos eletrônicos integrantes da rede de computadores envolvida, possivelmente trazendo prejuízos para empresas ou outras instituições como a própria Administração Pública, atrasando processos ou programas automáticos e manuais. Não há, também, nestes moldes, um tipo penal que enquadre esta conduta como delituosa, podendo, quiçá, tratá-lo como furto, embora o mais correto fosse o furto de uso[94], conduta que inclusive não é tipificada pelos dispositivos penais em vigor no Brasil, pois é uma conduta de baixo potencial lesivo, podendo ser resolvido pelo Direito Civil ou Administrativo.

Desconsiderando esse fato, no Projeto de Lei n. 1.806/99, de autoria do deputado Freire Júnior, há a previsão desta conduta, prevendo a alteração, para isto, do parágrafo 3º do artigo 155 do Código Penal da seguinte maneira:

> Art. 155.
> (...)
> § 3º Equipara-se à coisa móvel:
> I – a energia elétrica ou qualquer outra que tenha valor econômico;
> II – o acesso aos serviços de comunicação;
> III – o acesso aos sistemas de armazenamento, manipulação ou transferência de dados eletrônicos.

---

[93] GONÇALVES, Sérgio Ricardo M. **Hackers, Crakers e Spammers**: quem são e o que fazem? [online] Disponível na Internet via WWW. URL: http://www.mundojuridico.adv.br/sis_artigos/artigos.asp?codigo=659. Arquivo consultado em 23 de outubro de 2010.

[94] ROVER, Aires José. **Crimes de Informática**, p. 5. [online] Disponível na Internet via WWW. URL: http://www.infojur.ufsc.br/aires/arquivos/CRIMES%20DE%20INFORMATICA%20public.pdf. Arquivo consultado em 23 de outubro de 2010.

2.5.3. *Criação ou Disseminação de Malwares*

Esta é uma conduta potencialmente lesiva para todos os usuários de algum equipamento eletrônico, estando ou não conectados a uma rede de computadores, como a Internet, pois que os *Malwares*, já explicados e exemplificados neste trabalho, são capazes de causar vários prejuízos, desde a mera lentidão de funcionamento do aparelho eletrônico até a destruição de arquivos importantes e essenciais com danos irreparáveis.

Não há um tipo penal para esta conduta, mas no art. 13 do Projeto de Lei n. 88/99, de autoria do Deputado Luiz Piauhylino, há a previsão da conduta de criação de vírus de computador, não havendo, no entanto, previsão para o ato de disseminar o vírus, sendo esta a conduta que realmente deveria ser reprimida, vez que a criação do vírus poderia ser considerada como fase de preparação do ato de disseminar o vírus, conduta esta que tem um potencial lesivo muito maior que a anterior, podendo chegar a níveis inimagináveis de destruição.

No entendimento de alguns doutrinadores, a criação de um vírus de computador que não seja disseminado não poderia ser considerado como crime[95], pois no ordenamento jurídico brasileiro isso seria considerado como mero planejamento ou cogitação de crime, o que, segundo este sistema, não é punível.

Note-se, também, que não há qualquer menção quanto aos outros *Malwares*, que podem ser tão ou ainda mais lesivos que os comuns vírus de computadores.

2.6. Descriminalização

Interessante ponto levantou Ederlei Norberto Majolo em sua monografia ao abordar sobre a incongruência da tipificação frente a uma época de descriminalização[96], indagando se realmente seria interessante a tipificação dos delitos informáticos ou se seria mais eficiente deixar a sua apreciação para outros ramos do Direito, não submetendo estas condutas lesivas aos sistemas

---

[95] INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 64.

[96] MAJOLO, Ederlei Norberto, **Informática e Crime**. Monografia apresentada como requisito parcial à obtenção do título de bacharel em Direito, na Faculdade de Direito do Setor de Ciências Jurídicas, da Universidade Federal do Paraná, em 29/10/2006, p. 33-34.

computacionais à apreciação do direito penal, já que "o direito penal é a forma mais drástica de intervenção na vida social, gerando grande desconforto"[97].

Juntamente com os computadores e, principalmente, com a Internet, surgiram-se, imediatamente, novos riscos, e segundo o entendimento doutrinário de Jorge de Figueiredo Dias, estes novos riscos deveriam, inicialmente, ser tratados por uma periferia ao Direito Penal, a periferia jurídico-penal, nas suas palavras, que embora não faça parte do cerne clássico deste Direito, que é caracterizado pela defesa dos direitos, liberdade e garantias tradicionais, tem uma importância muito grande no papel da constante renovação deste ramo.[98]

O problema da falta de lei nesse ramo do Direito é a possibilidade de serem causados danos imensos e irreparáveis sem que haja qualquer tipo de punição imediata – como finalidade retributiva, mas sem descartar a finalidade preventiva sempre presente no Direito Penal – para o agente causador dos danos, como foi o caso do vírus informático "I love you", criado por um cidadão filipino, que mesmo com os imensos danos registrados, não pode ser punido pela ausência de qualquer tipo legal previsto no ordenamento jurídico das Filipinas.[99]

Desta maneira, segundo Majolo, percebe-se a necessidade urgente da criação de tipos penais tantos quantos forem suficientes para proteger os bens jurídicos[100] envolvidos na utilização do computador, para que todos possam usufruir deste objeto sem estarem sujeitos a – ou ao menos reduzindo esta possibilidade – serem vítimas de condutas lesivas.

Porém, não se pode pensar desenfreadamente que o Direito resolverá todos os problemas da atualidade. Deve-se sempre ter consciência do que é feito, pondera Vladmir Aras:

> É conveniente ressaltar que não se defende uma intervenção desnecessária ou máxima do Direito no ciberespaço, ou em parte alguma. O que se preconiza é a atuação razoável do Direito para assegurar proteção a bens jurídicos valiosos, quando não seja possível conferir essa proteção por outros meios igualmente eficazes.[101]

---

[97] *Idem*, p. 33.
[98] FIGUEIREDO DIAS, Jorge. **Direito Penal**: Parte Geral, Tomo I. Coimbra Editora: Coimbra, 2004, p. 133-134.
[99] *Idem*, p. 169.
[100] Sobre a evolução do Direito Penal e a necessidade de criação de novos bens jurídicos e a descriminalização de outros, cf. FIGUEIREDO DIAS, Jorge. Obra citada, p. 127-128.
[101] ARAS, Vladmir. Obra citada

2.6.1. Combate aos crimes cibernéticos

Diante da realidade de impunidade dos crimes cibernéticos, a sociedade se vê defronte de uma necessidade que não pode ser diferida: "temos de agir antes de sermos forçados a reagir"[102] – é o que afirmou Jonas Böttler.

Mas como se poderia agir tendo em vista as características dos crimes cibernéticos? Esta ação prévia poderia se dar de duas maneiras: a prevenção e a repressão.

Para prevenir a ocorrência de mais delitos cibernéticos, deve-se restringir ou, ainda, impedir o anonimato[103] durante a navegação na Internet, a maior educação[104] das pessoas acerca dos riscos de ataques virtuais e dos modos de preveni-los, além de serem utilizadas, com mais frequência, técnicas de segurança neste âmbito, como: a criptografia de arquivos[105], a assinatura digital[106], dentre outras que vierem a surgir. Acerta Cesare Bonesana Beccaria ao afirmar que "o meio mais seguro, mas ao mesmo tempo mais difícil de tornar os homens menos inclinados a praticar o mal, é aperfeiçoar a educação"[107], implicando que o único jeito de realmente se ver erradicada a prática de crimes, não só os cibernéticos, mas todos, é evitando-se o aparecimento de novos criminosos através de uma boa educação desde o começo de qualquer vida humana.

Quanto à repressão dos crimes cibernéticos através de leis tipificadas e suas aplicações, já foi dito que certamente esta não é a melhor maneira de impedir e controlar a atividade criminosa, como diariamente é demonstrado pela enorme quantidade de crimes cometidos constantemente em qualquer parte do mundo, independentemente da quantidade ou gravidade das penas, porém esta tipificação

---

[102] BÖTTLER, Jonas. **Threats posed by Cyber Terror and Possible Responses of the United Nations**. Canada: UNISCA, 12 de dezembro de 2002, p. 13.
[103] BARROS, Lucivaldo Vasconcelos. Obra citada.
[104] MENDES, Nelson Pizotti. **Problemas atuais da criminologia**. São Paulo: Resenha Universitária, 1976, p. 108.
[105] FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**, 3. ed. São Paulo: Bookman Editora, 2004, p. 692-693. "A palavra criptografia é de origem grega e significa "escrita secreta". Entretanto, hoje em dia, o termo criptografia refere-se à ciência e à arte da transformação de mensagens tornando-as seguras e imunes a ataques", se dá através de um processo de cifração ou codificação de um arquivo, sendo posteriormente decifrado por um receptor específico por meio de uma chave de acesso.
[106] ROHRMANN, Carlos Alberto. **Curso de Direito Virtual**. Belo Horizonte: Del Rey Editora, 2005, p. 66-67. "Trata-se de um recurso da técnica da computação que visa a atribuir a cada pessoa um único código identificador bastante protegido para estabelecer a sua identidade na Internet."
[107] BECCARIA, Cesare Bonesana. **Dos delitos e das penas**. Bauru: EDIPRO, 1993, p. 103.

não é de todo desnecessária e inútil, vez que o seu conhecimento pode causar medo e desmotivar um sujeito à prática de um delito, além de também poder barrar a continuidade de uma determinada conduta delituosa, especialmente se tendo em vista que os crimes cibernéticos tendem a ser cometidos pela classe social mais privilegiada tanto cultural quanto economicamente. Deve-se sempre ter em mente, no entanto, como afirma Lucivaldo Vasconcelos Barros, que "como repressão a pena deve situar-se, outrossim, na perspectiva pedagógica de reinserção social, tendo em vista que a pena de prisão cria muitos problemas, não somente no indivíduo, mas em relação à sua família e à sociedade"[108].

2.7. Autoria

Neste momento, convém fazer uma análise doutrinária acerca do já polêmico tema da autoria, utilizando-se como obra de referência o estudo realizado pelo professor Juarez Cirino dos Santos[109]. Para ele, existem duas formas de relações do sujeito ativo com o fato típico: relação de autoria e relação de participação. De forma simplificada seria a autoria *do* e a participação *no* tipo de injusto, segundo o próprio autor[110], podendo a autoria ser de três maneiras:

i) Individual, quando o próprio sujeito pratica o delito;
ii) Mediata, quando o sujeito utiliza-se de um terceiro como instrumento para a realização do delito; ou
iii) Coletiva ou coautoria, quando vários sujeitos praticam o delito conjuntamente.
iv) Discute-se, ainda, a possibilidade de uma autoria colateral, em que vários autores realizam o mesmo fato doloso sem qualquer relação de dependência entre eles.

Já a participação pode se dar das seguintes maneiras:

i) Instigação, quando o sujeito induz um terceiro à prática de crime, sendo este fato punível pelo artigo 286 do Código Penal, sendo punível apenas

[108] BARROS, Lucivaldo Vasconcelos. Obra citada.
[109] Mais sobre o tema, cf. SANTOS, Juarez Cirino dos. Obra citada. p. 349-378.
[110] SANTOS, Juarez Cirino dos. Obra citada, p. 349.

quando o crime é, pelo menos, tentado, segundo regra do artigo 31 desta mesma lei; ou

ii) Cumplicidade, quando há a ajuda dolosa de alguém para que um terceiro consiga praticar o delito.

Existem quatro construções teóricas acerca do tema da autoria: a teoria unitária de autor; o conceito restritivo de autor; a teoria subjetiva de autor; e a teoria do domínio do fato.

Para a teoria unitária de autor, "autor é quem produz qualquer contribuição causal para a realização do tipo legal" [111]. Sendo este um dos mais arcaicos conceitos de autoria, não se verifica uma nítida diferenciação entre autor e partícipe, dificultando a aplicação individualizada, como medida da culpabilidade de cada um dos concorrentes no delito, da pena, podendo ocorrer a punição de sujeitos que não deveriam ser punidos ou a punição exacerbada de sujeitos que tiveram uma contribuição ínfima no delito. Embora assim seja, ainda encontra-se presente no dispositivo penal brasileiro, em seu artigo 29, tendo como única vantagem a inexistência de lacunas de punibilidade, como bem explica o prof. Cirino dos Santos[112], simplificando consideravelmente a aplicação do Direito Penal.

Para a teoria do conceito restritivo de autor, este seria apenas aquele que realiza o fato descrito no tipo penal, como a ação de matar no crime de homicídio, sendo o partícipe considerado aquele que instiga ou contribui de maneira não tipificada por si só. Esta teoria possui seus méritos pela quebra do paradigma anterior, mas ainda não resolveu todos os problemas da temática, ficando os pontos referentes à autoria mediata e à coautoria ainda em aberto.

A teoria subjetiva de autor traz o elemento volitivo à tona. Para ela, o autor teria a vontade de ter o fato como seu próprio, tendo, portanto, o *animus auctoris*, mesmo não realizando efetivamente o fato típico, como por exemplo, um sujeito que contrata um atirador de elite e leva-o ao local da execução seria, neste caso, considerado coautor do delito. Já o partícipe teria uma vontade própria de partícipe, contribuindo causalmente, não pretendendo ter o fato como seu próprio, agindo, destarte, com o chamado *animus socii*. Esta teoria sofre inúmeras críticas, principalmente o fato de que não há uma maneira de determinar diretamente a

---

[111] *Idem*, p. 350.
[112] *Idem*, p. 351.

vontade das pessoas no ato da realização do crime, ficando, portanto, imprecisa. Outra crítica seria o fato de alguns delitos excluírem a autoria mediata, como os delitos de mão-própria, em que estariam excluídos da autoria os sujeitos não qualificados, e, de igual maneira, teriam de ser incluídos os sujeitos qualificados, por mais que estes desejassem ser apenas partícipes do fato, ou seja, pouco importando as suas vontades.

Já a teoria do domínio do fato parte do conceito restritivo de autor na sintetização dos aspectos subjetivos e objetivos da conduta, sendo, desta maneira, uma teoria eclética, por isto também conhecida como 'teoria objetiva material' ou 'teoria objetivo-subjetiva', sendo elaborada por Claus Roxin[113], sendo a autoria dividida em três elementos: (i) domínio da ação, (ii) domínio de vontade e (iii) domínio funcional.

i) Do ponto de vista subjetivo, seria autor aquele que possui efetivamente e voluntariamente o controle, o domínio, do fato e de suas circunstâncias, sendo partícipe aquele que não domina a realização ou execução do delito. Mas, para esta teoria, também seria considerado autor aquele que se utiliza de um terceiro como instrumento ou que controla o curso dos fatos através de planejamentos e premeditações na perpetração do crime, hoje considerados, respectivamente, como autoria mediata e autoria intelectual.

ii) No caso do domínio de vontade, estar-se-ia determinando outras hipóteses em que um autor mediato também seria punido como se autor fosse, pois este detém o domínio das circunstâncias, como nos casos de indução ao erro, coação, no emprego de menores e inimputáveis, e nos mecanismos de organização do crime (crime organizado – em que os executores são meras peças descartáveis da máquina criminosa).

iii) Em se falando de crime organizado e demais execuções planejadas, é sabido que cada sujeito tem uma determinada fração do domínio do fato criminoso, mas se se seccionasse o delito para averiguar qual tipo penal cabe a qual sujeito, deparar-se-ia com pessoas isentas de punição pelo fato de não haver tipo penal específico para cada ação específica. Nestes

---

[113] Mais sobre o tema, cf. ROXIN, Claus, **Täterschaft und Tatherrschaft**, Beck, 1994, p. 60.

casos, fala-se em domínio funcional do fato, sendo todos os executores considerados como autores, especialmente em casos em que na retirada de um dos agentes, possivelmente o crime não teria sido concluído, tanto nas partes da execução como do planejamento ou preparação. Participação seria, neste caso, "uma contribuição acessória dolosa em fato principal doloso de outrem"[114], podendo se dar nas formas de instigação, quando o sujeito induz um terceiro à prática de crime; e cumplicidade, quando há a ajuda dolosa de alguém para que um terceiro consiga praticar o delito.

2.7.1. Problemática da autoria nos crimes cibernéticos

Elemento essencial para que o Ministério Público ou o querelante possam realizar a imputação do delito, a autoria do crime deve sempre estar expressa na narrativa dos fatos para que o juiz possa citar o acusado, possibilitando, com a ciência e a defesa deste último, a operação do devido processo legal, e com este, a punição, ou não, do acusado.

O problema em relação à autoria nos crimes cibernéticos não se exaure na minuciosa análise doutrinária das teorias de autoria e participação, indo muito mais além, citando como ponto inicial deste tópico, o trecho da obra de Marco Aurélio Greco:

> Como identificar o agente? Para termos uma ideia das dificuldades e da complexidade que o tema dos controles assume, por exemplo, na Internet, basta mencionar que podem existir serviços que poderiam ser denominados de 'serviço de máscara'. A hipótese é mais ou menos a seguinte: se alguém quiser enviar e-mails na Internet, sem ser identificado, faz um cadastro no Site e, a partir daí, passa a ter um e-mail fornecido pelo Site, não sendo acessível o e-mail verdadeiro da pessoa que está por trás dele. Neste caso, o verdadeiro autor da mensagem fica oculto e o Site envia o que a pessoa oculta quiser, com um nome fictício, e a correspondência encaminhada para o nome fictício será entregue no endereço verdadeiro da pessoa que está oculta.[115]

Em 31 de maio de 1995 foi criado o Comitê Gestor da Internet do Brasil (CGI.br)[116] através da Portaria Interministerial número 147, tornando efetiva a

---

[114] SANTOS, Juarez Cirino dos. Obra citada, p. 354.
[115] GRECO, Marco Aurélio. **Internet e Direito**, 2ª. ed. São Paulo: Dialética, 2000, p. 66.
[116] CGI.BR. http://www.cgi.br/sobre-cg/index.htm.

participação da sociedade nas decisões envolvendo a implantação, administração e uso da Internet, sendo este Comitê composto por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica, operando, assim, com democracia, transparência e multilateralidade. Segundo o próprio órgão, suas principais atribuições são "coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados". Em determinado momento, este Comitê resolveu mostrar a ausência de controle da navegação na Internet, comprovando, através de uma simulação de invasão a um computador da Rede Nacional de Provedores, utilizando-se de um provedor[117] de internet gratuita, que no caso de uma eventual ocorrência, seria impossível identificar o usuário responsável.[118]

Com base nesse exemplo, percebe-se a atual dificuldade de se identificar o real perpetrador, mas esta não é a única dificuldade que ocorre na identificação do autor do delito. De fato, quando alguém realiza um delito pela Internet, como o envio de uma mensagem preconceituosa nos sítios de relacionamentos, como o Orkut, grandes possibilidades há de que o indivíduo está se utilizando de uma identidade falsa com os demais dados informados também falsos, o que dificulta uma identificação imediata do autor do fato, não sendo este, porém, o pior dos casos, podendo ocorrer, inclusive, a personificação de um sujeito por outro, ou seja, casos em que alguém se faz passar por uma pessoa apenas para cometer delitos e possivelmente incriminar esta pessoa. Casos ainda mais difíceis seriam os em que um indivíduo descobre, por qualquer meio, a senha de um usuário legítimo, adentrando em sua conta e utilizando-se dela e do seu nome, que nela se encontra subscrito, para cometer diversos delitos[119]. Levando-se em consideração estas informações, o mínimo que poderia ocorrer no âmbito da Internet seria a impunidade, e no pior dos casos, poder-se-ia acabar punindo alguém inocente, algo inaceitável e repugnante em qualquer sociedade.

Por causa destes motivos, é consensual a ideia de que não se pode identificar os usuários da Internet pelas identidades ou documentos ostentados. Em

---

[117] CASTRO, Carla Rodrigues Araújo de. Obra citada, p. 68-69. "Provedores de acesso são instituições que se conectam na Internet via um ou mais acessos dedicados e disponibilizam acesso a terceiros a partir de suas instalações". Entende-se que não há a necessidade de haver um pagamento efetivo do usuário para o Provedor para que haja aqui uma relação jurídica protegida tanto pelo Direito Civil como pelo Direito do Consumidor. São exemplos de provedores de Internet aqui no Brasil: IG, UOL, AOL, Net Virtua, GVT, etc.

[118] INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 13-14.

[119] *Idem,* p. 111.

substituição a isto, utilizam-se os endereços IP, que é um código numérico que identifica todo e qualquer dispositivo conectado a uma rede de computadores, seja esta interna como externa, como é o caso da Internet, identificando o tipo de conexão estabelecida. A sua numeração e identificação é caracterizada pela seguinte função: "Um nome indica o que procuramos. Um endereço indica onde está. Uma rota indica como chegar lá"[120]. Destarte, com um endereço IP consegue-se localizar com precisão qual foi o computador do qual emanou os fatos típicos e qual o caminho que esta ação tomou, identificando-se, deste modo, qual o provedor de Internet utilizado pelo usuário infrator.

Mas os problemas não acabam no momento em que se descobre exatamente de qual computador emanaram os fatos típicos. Há a possibilidade de este computador ser compartilhado por uma família inteira, não havendo como determinar, inicialmente, quem foi o autor do fato. Há também a possibilidade de ser o computador um mero dispositivo integrante de um comércio de disponibilização de acesso à Internet, mais conhecidas como 'LAN-Houses' ou 'Internet-cafés', dentre outras possibilidades, todas exigindo uma minuciosa investigação por parte da autoridade policial para se determinar com precisão a pessoa que utilizou o computador para a prática do delito. Ainda quanto a esta última possibilidade, a das LAN-Houses, as mais corretas registram todas as pessoas que utilizam cada um dos seus computadores e o horário e tempo de utilização, exatamente para o caso de algum dos seus usuários cometerem delitos através de seus computadores. Por outro lado, em alguns estados já há leis que estipulam a regularização deste registro, como São Paulo, com a Lei Estadual 12.228, de 11 de Janeiro de 2006, e Rio de Janeiro, com a Lei Estadual 5.132, de 14 de Novembro de 2007, dentre outros, esta última dispondo:

> Art. 1º – Ficam obrigados todos os estabelecimentos comerciais que locam terminais de computadores para acesso à Internet, a terceiros (público em geral), no âmbito do Estado do Rio de Janeiro, a exigir identidade dos usuários de quando das locações e a manter livro, com data, hora e identificação do usuário, bem como do terminal utilizado.
> Parágrafo único – Estão inseridas no presente artigo todas as empresas que, de forma promocional ou não, cederem acesso à Internet ao público, excetuando-se os sistemas do tipo Intranet.

---

[120] Trad. Livre. INTERNET ENGINEERING TASK FORCE (IETF). RFC 791: Internet Protocol, DARPA Internet Program Protocol Specification, September 1981, p. 7. [online] Disponível na Internet via WWW. URL: http://www.ietf.org/rfc/rfc791.txt. Arquivo consultado em 22 de outubro de 2010. "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

> Art. 2º – Na hipótese de inobservância das disposições acima, será aplicada ao infrator multa de 100 a 1.000 UFIR-RJ, independente de qualquer outra sanção aplicável.

Mais acertado seria a criação de uma lei federal fixando este regramento, vez que é de interesse de todos os entes da federação, e não específico de cada estado ou município, motivo pelo qual se justificaria a atribuição de competência comum à União, Estados, Distrito Federal e Municípios, para legislar sobre o assunto, e não apenas restando aos Estados a competência residual para tratar desta matéria.

2.7.2. Responsabilização dos provedores

Pelo fato de o Código Penal brasileiro seguir a teoria restritiva de autoria, não há que se falar em coautoria dos provedores de Internet, exceto nos casos em que estes efetivamente incentivam e disponibilizam os seus serviços a alguém com o conhecimento de que serão realizados atos ilícitos.

Há casos, no entanto, em que o provedor poderá ser responsabilizado, não como autor ou coautor do delito, mas com o crime próprio que praticar, como no caso de este fornecer, ao Juízo, nome e endereço falso de algum de seus usuários requisitado pelo Poder Judiciário, respondendo, neste caso, pelo crime de falso testemunho[121].

Com um estudo aprofundado sobre o tema, analisado à luz do artigo 29 do Código Penal, Deborah Fisch Nigri faz a seguinte conclusão:

> Se o provedor oferece os serviços de hospedagem de páginas e, porventura, alguma página por ele hospedada veicular conteúdo indevido, ele deverá ser oficialmente notificado para retirar a página do ar, sob pena de não o fazendo, ser coautor do eventual crime. Caso o provedor esteja colaborando na elaboração de uma página de conteúdo ilegal (pedofilia, racismo, etc.); desde que se comprove sua participação, ele poderá ser responsabilizado.[122]

Para Gabriel Cesar Zaccaria de Inellas, os provedores de acesso à Internet poderiam cometer os seguintes delitos: (i) desobediência, tipificado no artigo 330 do Código Penal, quando se recusa a fornecer informações exigidas pela Justiça; (ii) falsidade ideológica, artigo 299 do Código Penal, quando fornece informações

---

[121] CASTRO, Carla Rodrigues Araújo de. Obra citada, p. 12. [sic]

[122] NIGRI, Deborah Fisch. **Crimes e Segurança na Internet**. *In* Doutrina jurídica brasileira, Caxias do Sul: Editora Plenum, 2001.

falsas; (iii) favorecimento pessoal, em concurso material, presente no artigo 348 do Código Penal, em casos que há o auxílio efetivo da provedora a um criminoso, preservando a privacidade do usuário para que este escape da investigação, processo e possível punição de um delito; (iv) favorecimento real, capitulado no artigo 349 do Código Penal, quando a provedora auxilia criminoso, tornando, desta maneira, proveitoso e seguro a prática do crime.[123]

Este doutrinador entende ser extremamente complicada a efetiva responsabilização penal das provedoras de acesso, que são empresas dotadas de personalidade jurídica própria, no ordenamento jurídico brasileiro, porém demonstra que elas já estão sendo responsabilizadas em ordenamentos jurídicos de países mais desenvolvidos como Portugal, que prevê a punição das pessoas jurídicas no artigo 3º da Lei n. 109, de 17 de agosto de 1991[124]. Já no Brasil, é imprescindível, atualmente, localizar a pessoa física responsável pelo serviço de acesso, a qual responderá pelas eventuais atividades criminosas cometidas com a utilização do serviço da empresa que representa, vez que não se reconhece a possibilidade de ser punida penalmente uma pessoa jurídica, exceto nos crimes ambientais. Neste sentido, e afirmando que as provedoras de acesso poderiam, sim, ser responsabilizadas criminalmente em alguns casos, conclui o referido doutrinador e Promotor de Justiça:

> Se é verdade que no Direito Penal aprende-se que *societas delinquere non potest*, é – de igual modo – verdade, que a Constituição da República Federativa do Brasil determinou a responsabilidade penal da pessoa jurídica nos atos praticados contra a ordem econômica e financeira e contra a economia popular, *sem prejuízo da responsabilidade individual dos dirigentes da pessoa jurídica* e responsabilizou penalmente a pessoa jurídica, nas atividades lesivas ao meio ambiente.[125]

2.8. Investigação e provas

Segundo Gabriel Cesar Zaccaria de Inellas:

---

[123] INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 30-34.
[124] Art. 3º. "As pessoas colectivas, sociedades e meras associações de facto são penalmente responsáveis pelos crimes previstos na lei, quando cometidos em seu nome e no interesse colectivo pelos seus órgãos ou representantes."
[125] INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 29.

> Os crimes cometidos através da Internet são delitos como quaisquer outros; somente seu modo de execução é diferente. De igual sorte, a parte investigatória é diferente e difícil. Por exemplo, nos crimes praticados através da Internet, a prisão em flagrante delito é praticamente impossível de ser realizada.[126]

Para que o crime cibernético seja apurado com precisão, a passagem por uma perícia especializada e minuciosa é um procedimento essencial e indispensável, visto tratar-se de um crime complexo, sendo a parte investigatória ainda mais complexa.

Segundo o Manual Prático de Investigação[127], escrito pelo Grupo de Combate aos Crimes Cibernéticos, Ministério Público Federal e Procuradoria da República no Estado de SP, o primeiro passo é sempre a discriminação do meio utilizado na prática do delito, seja ele o e-mail, uma sala de bate-papo, um programa utilizado na troca de arquivos, dentre outros. E há de se ter muito cuidado, pois as evidências têm características muito singelas, dentre elas:

> a) possuem formato complexo (arquivos, fotos, dados digitalizados, etc.);
> b) são voláteis, i.e., podem ser apagadas, alteradas ou perdidas facilmente;
> c) costumam estar misturadas a uma grande quantidade de dados legítimos, demandando, por isso, uma análise apurada pelos técnicos e peritos que participam da persecução penal.[128]

Em seguida busca-se o endereço IP do agressor, possibilitando a descoberta, com base neste, do endereço exato do equipamento físico que enviou ou realizou a conduta lesiva e a identificação do servidor que hospeda a página[129]. Juntamente com o endereço IP, devem constar, igualmente, a data e a hora exata da comunicação estabelecida entre os computadores e o fuso horário do sistema. Isto se dá por dois motivos, primeiro pelo fato de possibilitar a descoberta de qual usuário se encontrava no computador do qual emanou a ofensa, utilizando-se, para isto, qual meio for mais adequado para o caso, e também como requisito para se exigir a quebra de sigilo dos dados telemáticos junto aos provedores de acesso e às companhias telefônicas:

---

[126] *Idem*, p. 35.
[127] MPF. Obra citada, p. 15-40.
[128] *Idem,* p. 15.
[129] *Idem,* p. 23-25. Há sites especializados nesta identificação, como por exemplo o http://www.registro.br, quando se tratar de sites brasileiros.

> Nos pedidos feitos aos provedores de acesso e às companhias telefônicas, é imprescindível que haja, no mínimo, a menção a esses três indicadores: a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC. Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos.[130]

Pelo fato de alguns *sites* ofensivos não terem qualquer vínculo com o Brasil, o recomendado é informar a INTERPOL ou ainda a INHOPE[131], associação que se encarrega de rapidamente informar a polícia responsável no local do delito, a qual realizará as devidas diligências.

Sem que haja um mínimo suporte probatório, não haverá justa causa para se intentar uma ação penal [132], portanto, para que haja indícios de autoria e materialidade do delito, uma perícia nos crimes cibernéticos deve ser extremamente ágil e precisa, pois, como já foi dito, o corpo de delito do crime é extremamente volátil, sendo recomendado, inclusive, a impressão do material ofensivo ou o descarregamento do seu inteiro teor através de um aplicativo especializado, como o *HTTrack*[133], garantindo-se em um suporte físico a integridade dos dados. Outro problema passível de ser encarado é a possibilidade de não se ter certeza sobre qual foi a pessoa que utilizou o computador na prática do delito, como nos casos em que uma família inteira utiliza o computador e não houverem meios de descobrir qual pessoa utilizara este objeto na hora registrada do delito.

Para cercar o conjunto probatório, é exigido a busca e apreensão do computador[134] do qual emanou o ato ofensivo, estando esta diligência prevista no artigo 240 do Código de Processo Penal, sendo de ofício ou a requerimento das partes, segundo o artigo 242 do CPP, indicando, segundo o artigo 243 deste mesmo dispositivo, com a maior precisão possível: o local em que será realizada a diligência, o nome do respectivo proprietário ou morador, o motivo e os fins da diligência e devendo ser assinado pela autoridade que o fizer expedir, sendo subscrito pelo escrivão[135]. Após a apreensão, este computador deve ser enviado aos peritos para que confirmem se este foi de fato o computador do qual emanou o relatado ato lesivo.

---

[130] *Idem,* p. 15.
[131] http://www.inhope.org.
[132] CASTRO, Carla Rodrigues Araújo de. Obra citada, p. 80.
[133] http://www.httrack.com.
[134] CASTRO, Carla Rodrigues Araújo de. Obra citada, p. 114-115.
[135] A não observação destes procedimentos trará a inadmissibilidade da prova, como demonstra o julgado do STF, AP-307/DF, de 1994, devendo a busca e apreensão ser requerida em juízo e a perícia realizada por perito oficial.

É atribuição da Polícia Federal e da Polícia Civil de cada estado a investigação dos delitos cometidos com a utilização da Internet. Por exemplo, em São Paulo existe um setor da Secretaria de Segurança Pública, controlada pelo GRADI – Grupo de Repressão e Análise dos Delitos de Intolerância e pelo Delegado de Polícia, Dr. Mauro Marcelo de Lima e Silva, que cuida desses delitos, chamado Setor de Crimes pela Internet[136]. No Rio de Janeiro há a Delegacia de Repressão aos Crimes de Informática, também chamada de Delegacia Virtual e uma Coordenadoria de Investigações Eletrônicas – CIE –, "responsável por coletar dados e informações e prestar auxílio às Promotorias de Justiça de todo o Estado"[137]. Em Brasília, 1995, foi criado, agregado ao Instituto Nacional de Criminalística, a Seção de Crimes por Computador, ligada diretamente à Polícia Federal, tendo como superior hierárquico o Delegado de Polícia Marcelo Correia Gomes e sendo operada por sete peritos especializados em crimes cibernéticos, tendo competência para elaborar Laudos oficiais, os quais serão anexados aos Inquéritos Policiais Federais, servindo como prova nas denúncias realizadas pelo Ministério Público Federal.[138]

[136] INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 36-37.
[137] CASTRO, Carla Rodrigues Araújo de. Obra citada, p. 106.
[138] INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 37.

3. DA COMPETÊNCIA PARA JULGAMENTO.

Roger Darlington, sobre o tema, problematiza: "leis são nacionais, mas o espaço cibernético é global. Como aplicar mais de 170 diferentes e separados sistemas legais à Internet?"[139]

Segundo o Manual das Nações Unidas sobre prevenção e controle de crimes relacionados ao computador:

> Hoje é tecnologicamente possível um operador apertar um teclado em um país A, modificando dados alocados em um país B, sem que este operador sequer saiba que os dados estavam alocados neste país, e ter estes dados modificados transferidos para vários outros países por meio de uma rede de telecomunicações, causando um resultado em um país C. Considerando o ato físico, a modificação técnica, a transmissão dos dados falsificados e as suas consequências, no mínimo três países terão sido envolvidos e poderão alegar ter competência jurisdicional.[140]

Inicia-se esta parte do trabalho com a apresentação de alguns conceitos básicos que serão essenciais mais adiante:

3.1. Soberania nacional

> A soberania é una e indivisível, não se delega a soberania, a soberania é irrevogável, a soberania é perpetua, a soberania é um poder supremo, ei os principais pontos de caracterização com que Bodin fez da soberania no século XVII um elemento essencial do Estado[141].

A soberania nacional se resume na delegação de poder a um único ente, o Estado, ela é una, integral e universal, não sendo limitada por nenhum outro poder. Poderia ser resumida, no conceito de Bodin, como "o poder absoluto e perpétuo de uma República".

---

[139] Trad. livre. DARLINGTON, Roger. **Internet Ethics**: Oxymoron or Orthodoxy?, 2002. [online] Disponível na Internet via WWW. URL: http://www.rogerdarlington.co.uk/Internetethics.html. Arquivo consultado em 23 de outubro de 2010. "Laws are nation-based but cyberspace is global. How does one apply up to 170 separate and different legal systems to the Internet?"

[140] Trad. livre. UNITED NATIONS. **International review of criminal policy** - United Nations Manual on the prevention and control of computer-related crime, 1999, p. 50. [online] Disponível na Internet via WWW. URL: http://www.uncjin.org/Documents/irpc4344.pdf. Arquivo consultado em 25 de outubro de 2010. "Today, it is technologically possible for an operator to punch a keyboard in country A so as to modify data stored in country B, even the operator does not know that the data are stored there, to have the modified data transferred over a telecommunications network through several other countries, and to cause an outcome in country C. On the basis of the physical act, the technical modification, the transmission of the falsified data and the consequences, three or perhaps more countries will have been involved and may have a claim to jurisdictional competency."

[141] BONAVIDES, Paulo. **Ciência Política**, 10. ed. São Paulo: Editora Malheiros. 1996, p. 126

Todo país tem um território em que ele exerce com plenitude a sua soberania nacional, é o chamado território nacional.

3.2. Jurisdição

Segundo Fernando Capez, "jurisdição é a função estatal exercida com exclusividade pelo Poder Judiciário, consistente na aplicação de normas de ordem jurídica a um caso concreto, com a consequente solução do litígio. É o poder de julgar um caso concreto, de acordo com o ordenamento jurídico, por meio do processo."[142] É, destarte, um poder-dever que vincula o Poder Judiciário a julgar uma determinada lide ou caso concreto, sobrepondo-se à vontade das partes envolvidas em um determinado processo de maneira definitiva, imutável, e se concretizando com estas práticas judiciárias[143].

A jurisdição é um poder soberano do Estado que não pode ser limitado ou dividido, ou seja, é um poder indivisível. Segundo a professora Clara Roman Borges, "a única coisa que pode ser limitada é o exercício desse poder".[144]

Neste sentido, alguns princípios norteiam a definição da jurisdição. Serão, portanto, analisados alguns dos mais relevantes deles para o presente estudo:

i) Princípio do Juiz Natural: este princípio deriva de normas constitucionais positivadas nos incisos XXXVII e LIII do artigo 5º da Constituição Federal. Devido à importância deste princípio para a presente análise, há de ser tratado em um tópico a parte.

> XXXVII - não haverá juízo ou tribunal de exceção;
> LIII - ninguém será processado nem sentenciado senão pela autoridade competente;

ii) Princípio do Devido Processo Legal: princípio este trazido pelo inciso LIV do artigo 5º da Constituição Federal, é de suma importância para qualquer

---

[142] CAPEZ, Fernando, **Curso de Processo Penal**, 13ª ed., São Paulo: Saraiva, 2006, p. 199.
[143] BORGES, Clara Maria Roman. **O princípio do juiz natural como garantia de um processo penal democrático: uma breve análise da competência penal por prerrogativa de função**. In: Alexandre Coutinho Pagliarini; Clèmerson Merlin Clève; Ingo Wolfgang Sarlet. (Org.). Direitos Humanos e Democracia. 1 ed. Rio de Janeiro: Forense, 2007, v. 1, p. 198-199.
[144] BORGES, Clara Maria Roman. **A competência nos crimes plurilocais e o princípio do juiz natural**. Dissertação apresentada ao Programa de Pós-graduação em Direito da Universidade Federal do Paraná como requisito parcial para outorga do título de Mestre em Direito, 2001, f. 93.

ordenamento jurídico. Nas lições de Jacinto Nelson de Miranda Coutinho: "o princípio do devido processo legal exige que o órgão julgador seja submetido ao princípio da inércia, buscando garantir, ao máximo, a sua imparcialidade e eqüidistância das partes" [145]. Ainda, segundo Luiz Rodrigues Wambier:

> o princípio do devido processo legal está inserido no contexto, mais amplo, das garantias constitucionais do processo, e que somente mediante a existência de normas processuais, justas, que proporcionem a justeza do próprio processo, é que se conseguirá a manutenção de uma sociedade sob o império do Direito.[146]

> LIV - ninguém será privado da liberdade ou de seus bens sem o devido processo legal;

iii) Princípio da Indeclinabilidade da Prestação Jurisdicional ou Princípio do Acesso à Justiça: presente no inciso XXXV do artigo 5º da Constituição, este princípio diz que além de a todos ser assegurado a apreciação de suas lides pelo órgão jurisdicional competente, este órgão não poderá declinar o exercício da função jurisdicional sem justo motivo.

> XXXV - a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito;

3.3. Competência

A competência não deve ser confundida com o próprio conceito de jurisdição supra mencionado. A doutrina comumente tende a tratar a competência a partir de teorias contratualistas, como sendo a divisão do poder jurisdicional e a sua consequente limitação, sendo "a medida e o limite da jurisdição, dentro dos quais o órgão judicial poderá dizer o direito", segundo Fernando Capez[147]. Há que perceber, no entanto, que, segundo uma visão mais acertada, não há como limitar, dividir ou

---

[145] COUTINHO, Jacinto Nelson de Miranda. **Introdução aos princípios gerais do Processo Penal brasileiro**. In: Revista da Faculdade de Direito da UFPR, Curitiba, ano 30, nº 30, 1998, p. 178.
[146] WAMBIER, Luiz Rodrigues. **Anotações sobre o princípio do devido processo legal**. São Paulo: RT, 1989, p. 34.
[147] CAPEZ, Fernando. Obra citada, p. 201.

mensurar o poder, vez que este se encontra espalhado por toda a sociedade[148], estando isto em conformidade com o entendimento de Michel Foucault, que complementa: "el poder está en todas partes; no es que lo englobe todo, sino que viene de todas partes"[149]. Segundo a doutrina mais acurada, jurisprudência não poderia ser dividida – o que poderia ser dividido é o exercício deste poder jurisdicional, e mesmo nestes casos, não poderia se dar de maneira condicionada e limitada. Segue tal entendimento, Clara Maria Roman Borges:

> Competência pode ser vista como um conjunto de parâmetros que condicionam o exercício do poder jurisdicional e podem fazê-lo funcionar de modo normalizador, se forem subjugados pela nova mecânica de poder, ou antinormalizador, se fixado a partir de focos de resistência presentes na sociedade em que se constituem.

Esta divisão do exercício do poder jurisdicional, além de objetivar o impedimento do uso arbitrário e totalitário deste por parte de algum órgão jurisdicional, se efetua também pelo simples fato de ser fisicamente impossível atribuí-lo a um único juiz, sendo conveniente, portanto, a adequada e delimitada divisão deste poder entre os diversos órgãos jurisdicionais existentes no território nacional. Cada órgão jurisdicional, no entanto, fica adstrito a um limite material e territorial no manuseio deste poder, limite este estipulado de acordo com as regras de distribuição da competência.

Quanto à distribuição ou divisão da competência, Chiovenda e Wach elaboraram um esquema desta, sendo amplamente aceito nos diversos ordenamentos jurídicos existentes, dentre os quais o italiano, o alemão e o brasileiro, o da *repartição tríplice*[150]. Segundo uma leitura de Chiovenda[151], adaptada ao Direito Processual Penal, neste esquema a divisão dar-se-ia em três aspectos diferentes:

---

[148] BORGES, Guilherme Roman. **Michel Foucault: uma interlocução com o discurso filosófico-jurídico**. Monografia apresentada como requisito parcial à obtenção do título de bacharel em Direito, na Faculdade de Direito, do Setor de Ciências Jurídicas, da Universidade Federal do Paraná, em 25/10/2002, p. 635.

[149] FOUCAULT, Michel. **Historia de la sexualidad**: La voluntad de saber, tomo 1. Madrid, Siglo XXI, 1992, p. 113.

[150] DINAMARCO, Cândido Rangel; GRINOVER, Ada Pellegrini; CINTRA, Antonio Carlos de Araújo. **Teoria Geral do Processo**, 23. ed. São Paulo: Malheiros Editores, 2007,p. 251-252.

[151] CHIOVENDA, Giuseppe. **Istituzioni di diritto processuale civile**, Náploes: Jenove, 1933 (trad. port. de J. Guimarães Menegale: Instituições de direito processual civil, 3ª ed., vol. II, São Paulo, Saraiva, 1969, p. 154-187).

i) Competência objetiva ou material, em razão da índole do crime, analisada levando-se em conta determinadas situações ou qualidades do sujeito ativo ou do bem jurídico ofendido (critério qualitativo), ou ainda em razão da gravidade da pena, a qual será tabelada pela intensidade e quantidade da pena (critério quantitativo); [152]

ii) Competência territorial ou de foro[153] será dada na decisão sobre qual juízo, dentre os materialmente competentes, virá a julgar um determinado caso concreto. Para tanto, inicialmente, deve-se ter em mente a localização da prática do delito no território – em sendo impossível determinar este local, outros critérios se aplicam para a correta aplicação da competência territorial.[154]

iii) Competência funcional é extraída "da natureza e das exigências especiais das funções que se chama o magistrado a exercer num processo"[155], segundo Chiovenda, ou seja, teria ele preponderância quando: "a) as diversas funções desenvolvidas no mesmo processo ou destinadas à atuação da mesma vontade da lei são atribuídas a juízes ou órgãos jurisdicionais diversos", segundo o professor Antonio Carlos Marcato, ou ainda "b) uma causa é destinada ao órgão jurisdicional de determinado território, considerando-se, para tanto, o fato de assim tornar-se mais fácil ou mais eficaz a sua função (v.g., no processo falimentar)." [156]

No artigo 69 do Código de Processo Penal há as orientações iniciais para a busca do órgão jurisdicional competente para processar e julgar determinado caso penal:

> Art. 69. Determinará a competência jurisdicional:
> I - o lugar da infração:
> II - o domicílio ou residência do réu;
> III - a natureza da infração;
> IV - a distribuição;

---

[152] LEONE, Giovanni. **Lineamenti di diritto processuale penale**. 2. ed. Napoli: Jovene, 1951, p. 85.
[153] DINAMARCO, Cândido Rangel; GRINOVER, Ada Pellegrini; CINTRA, Antonio Carlos de Araújo. Obra citada, p. 254-255.
[154] GOMEZ COLOMER, Juan-Luis. **El proceso aleman: introduccion y normas básicas**. Barcelona: Bosch, 1985, p. 70 e ss.
[155] CHIOVENDA, Giuseppe. Obra citada, p. 154-155.
[156] MARCATO, Antonio Carlos. **Breves considerações sobre jurisdição e competência**, p. 1. [online] Disponível na Internet via WWW. URL: http://jus2.uol.com.br/doutrina/texto.asp?id=2923. Arquivo consultado em 23 de outubro de 2010.

> V - a conexão ou continência;
> VI - a prevenção;
> VII - a prerrogativa de função.

Quando é operada a divisão da competência, algumas especificidades podem surgir, as quais serão analisadas nos tópicos subsequentes. Porém, não há como continuar o presente estudo sem antes ser feita uma breve análise, um pouco mais aprofundada, do Princípio do Juiz Natural.

3.3.1. Princípio do Juiz Natural

Instituído com o histórico objetivo de estabelecer um limite aos poderes autoritários dos governantes de quaisquer regimes políticos e concretizar um regime democrático, o Princípio do Juiz Natural é uma garantia processual, trazida pelo texto constitucional, que é de uma nobreza imensa, tal que o próprio constituinte não se satisfez em apenas trazer seu conceito, estendendo sua previsão legal para abranger assuntos que tecnicamente não seriam de natureza constitucional e trazendo a sua aplicação prática[157]. Este princípio encontra-se consolidado em dois incisos do artigo 5º da Constituição Federal brasileira: o XXXVII e o LIII:

> XXXVII – Não haverá juízo ou tribunal de exceção
> (...)
> LIII – Ninguém será processado nem sentenciado senão pela autoridade competente.

Estes incisos garantem, ainda que implicitamente, o princípio do juiz natural, o qual leva em consideração três aspectos, que a professora Clara Maria Roman Borges brilhantemente expôs:

> (...) [aspecto] da fonte, pois só a lei pode instituir o juiz natural e fixar-lhe a competência; do tempo, na medida em que a fixação do juiz e da sua competência devem ser feitas em lei vigente ao tempo da prática do delito, e da taxatividade, que impõe a necessidade de se fixar o juiz natural de acordo com uma ordem taxativa de competências capaz de impedir a escolha de um juiz mais conveniente.[158]

---

[157] BORGES, Clara Maria Roman. **O incidente de deslocamento de competência e o princípio do juiz natural**. Raízes Jurídicas (UNICENP), v. 4, 2008, p. 117-122.
[158] *Idem,* p. 119-120.

Com isso pode-se perceber que este princípio em muito supera a mera preconstituição, em lei, de um determinado juiz para julgar determinada causa, como defendia Vincenzo Manzini [159], sendo um "direito fundamental do cidadão ser processado e julgado pelo seu juiz, com a competência definida em lei anterior à ocorrência do fato"[160].

3.3.2. Competência material ou objetiva

Tratando-se de processo penal, inicialmente, há de perquirir se se trata de caso da justiça comum ou da justiça especializada. Segundo o regramento da Constituição Federal, há as seguintes especializações na jurisdição em relação à matéria ou à natureza da infração penal:

i) No artigo 118 a 121 é delimitada a jurisdição especializada da Justiça Eleitoral, competente para julgar as matérias referentes aos crimes Eleitorais;

ii) No artigo 124 verifica-se a jurisdição especializada da Justiça Militar, a qual é competente para julgar os crimes militares assim definidos por lei;

iii) Há ainda que se falar em jurisdição especializada nas matérias de competência política do Senado Federal, que por mais que seja atividade jurisdicional atípica, não pode ser desconsiderada[161]. Ocorre, segundo o artigo 52 e incisos da Constituição Federal, nos casos em que o Senado é competente para julgar os crimes de responsabilidade cometidos pelos Ministros do Supremo Tribunal Federal, membros do Conselho Nacional de Justiça e do Conselho Nacional do Ministério Público, também sendo competente para julgar estes mesmos crimes quando cometidos pelo Procurador-Geral da República, Advogado-Geral da União, presidente e vice-presidente da República, assim como, nestes dois últimos casos, os Ministros de Estado e os Comandantes da Marinha, do Exército e da

---

[159] MANZINI, Vincenzo. **Tratado de derecho procesal penal**. Trad. Santiago Sentís Meledo y Marino Ayerre Redín. Buenos Aires: EJEA, 1951, p. 228 e ss.
[160] BORGES, Clara Maria Roman. **O incidente de deslocamento de competência e o princípio do juiz natural**, p. 120-121.
[161] CAPEZ, Fernando. Obra citada, p. 202.

Aeronáutica nos crimes conexos àqueles e da mesma natureza, segundo regra do inciso I do artigo 52 da CF.

Nas demais matérias, será a justiça comum a competente para julgamento, havendo apenas a necessidade de verificação se se trata de competência da jurisdição comum federal ou estadual, a qual será feita com base na Constituição Federal:

i) À justiça federal caberão os casos previstos nos artigos 108 e 109 da CF. Nos casos previstos no inciso IV do artigo 109, mais comum no processo penal, há as atribuições da justiça federal, sendo de sua competência os casos em que a União, ou a administração direta e indireta a ela relacionada, for parte em processo penal em que haja ocorrido algum crime, excluído, portanto, as contravenções penais, pois estas serão de competência da justiça estadual, segundo a Súmula 38 do STJ[162].

ii) À justiça estadual caberão todos os demais casos não abrangidos pela justiça federal, seguindo a regra da competência residual.

Em havendo crime doloso contra a vida, poder-se-ia falar em competência do Tribunal do Júri, podendo ser da jurisdição comum estadual ou federal, segundo regramento da alínea *d* do inciso XXXVIII do artigo 5º da Constituição Federal.[163]

Há ainda a necessidade de se verificar qual será o órgão jurisdicional competente para conhecer e julgar a matéria em primeira instância: se será o juiz, o tribunal ou o tribunal superior. Trata-se da competência em relação à pessoa, nos casos de prerrogativa de função ou foro privilegiado em relação à função da pessoa. Essas regras também podem ser encontradas na Constituição Federal. Competirá:

i) Ao Supremo Tribunal Federal, nos casos previstos nas alíneas *b* e *c* do inciso I do artigo 102, processando e julgando originariamente: (*b*) – "nas infrações penais comuns, o Presidente da República, o Vice-Presidente, *os membros do Congresso Nacional, seus próprios Ministros e o*

[162] STJ, Súmula 38 – "Compete à Justiça Estadual Comum, na vigência da Constituição de 1988, o processo por contravenção penal, ainda que praticada em detrimento de bens, serviços ou interesse da União ou de suas entidades."
[163] CAPEZ, Fernando. Obra citada, p. 203.

Procurador-Geral da República;" e (*c*) – "nas infrações penais comuns e nos crimes de responsabilidade, os Ministros de Estado e os Comandantes da Marinha, do Exército e da Aeronáutica, ressalvado o disposto no art. 52, I, os membros dos Tribunais Superiores, os do Tribunal de Contas da União e os chefes de missão diplomática de caráter permanente;"

ii) Ao Superior Tribunal de Justiça, nos casos previstos na alínea *a* do inciso I do artigo 105, processando e julgando originariamente: (*a*) – "nos crimes comuns, os Governadores dos Estados e do Distrito Federal, e, nestes e nos de responsabilidade, os desembargadores dos Tribunais de Justiça dos Estados e do Distrito Federal, os membros dos Tribunais de Contas dos Estados e do Distrito Federal, os dos Tribunais Regionais Federais, dos Tribunais Regionais Eleitorais e do Trabalho, os membros dos Conselhos ou Tribunais de Contas dos Municípios e os do Ministério Público da União que oficiem perante tribunais;"

iii) Aos Tribunais Regionais Federais, nos casos previstos no inciso I do artigo 108, processando e julgando originariamente: "os juízes federais da área de sua jurisdição, incluídos os da Justiça Militar e da Justiça do Trabalho, nos crimes comuns e de responsabilidade, e os membros do Ministério Público da União, ressalvada a competência da Justiça Eleitoral;"

iv) Aos Tribunais de Justiça dos Estados, segundo o inciso X do artigo 29, caberá o julgamento o julgamento dos crimes cometidos pelos Prefeitos, porém não se restringe a apenas estes casos, podendo haver mais previsões nas Constituições dos Estados acerca da competência destes tribunais, segundo regramento do §1º do artigo 125 da Constituição Federal, dizendo que a lei de organização judiciária será de iniciativa do próprio Tribunal de Justiça.

3.3.3. Competência funcional

Esta competência é dada em relação a três aspectos[164]: i) a fase do processo, podendo ser de conhecimento, de execução, dentre outras; ii) o objeto do juízo, podendo ser competência dos jurados na resposta aos quesitos ou do juiz na dosimetria da pena; ou iii) o grau de jurisdição, podendo ser em grau originário ou em sede de recurso.

3.3.4. Competência territorial

Também conhecida por "competência de foro" ou "*ratione loci*", é a competência que mais interessa nesse presente estudo. Via de regra, será dada pelo local onde ocorreu o delito, segundo regramento do artigo 70 do Código de Processo Penal, do qual se extrai:

> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.

Subsidiariamente, quando desconhecido o lugar da infração, a competência territorial será estabelecida em razão do domicílio ou residência do réu, segundo estabelece o artigo 72 e 73 do CPP:

> Art. 72. Não sendo conhecido o lugar da infração, a competência regular-se-á pelo domicílio ou residência do réu.
> (...)
> Art. 73. Nos casos de exclusiva ação privada, o querelante poderá preferir o foro de domicílio ou da residência do réu, ainda quando conhecido o lugar da infração.

Depois de estabelecida a competência territorial, em havendo mais de um juiz competente na mesma circunscrição judiciária, saber-se-á qual será o juízo competente para conhecimento e julgamento do processo após feita a distribuição do processo, estando tal procedimento previsto no artigo 75 do CPP.

> Art. 75. A precedência da distribuição fixará a competência quando, na mesma circunscrição judiciária, houver mais de um juiz igualmente competente.

---

[164] *Idem*, p.220.

A distribuição não se procederá se houver competência pela natureza da infração já pré-estipulada nas leis de organização judiciária local. Também não será realizada nos casos em que se tratar de crimes dolosos contra a vida, nos quais a competência será privativa do Tribunal do Júri (art. 74, §1º, do CPP), quando houver conexão ou continência com outro processo (art. 76 a 78 do CPP) ou ainda quando houver juízo prevento em relação à ação penal sendo proposta (art. 83 do CPP).

3.4. Lei aplicável

Segundo o artigo 5º do Código Penal, será aplicada a lei brasileira nos processos em que o crime tenha sido cometido no território nacional, sendo adotado, portanto, o Princípio da Territorialidade. E segundo o artigo 6º deste mesmo dispositivo de lei, que traz a Teoria da Ubiquidade, "considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado", ou seja, será o local do crime aquele em que foi realizado qualquer dos momentos do *iter criminis*.

Há ainda outros casos em que a lei brasileira será aplicada, segundo o artigo 7º do CP, nos quais se verificam os casos de extraterritorialidade da lei brasileira. Segundo este artigo, ficariam sujeitos à lei brasileira, independente do local do acontecimento, os crimes:

> Inciso I:
> Contra a vida ou a liberdade do Presidente da República;
> Contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público;
> Contra a administração pública, por quem está a seu serviço;
> De genocídio, quando o agente for brasileiro ou domiciliado no Brasil;
> Inciso II:
> Que, por tratado ou convenção, o Brasil se obrigou a reprimir; (Incluído pela Lei nº 7.209, de 1984)
> Praticados por brasileiro; (Incluído pela Lei nº 7.209, de 1984)
> Praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados.

Segundo o §1º do artigo 7º do CP, que trata dos crimes previstos no inciso I, o agente será punido nos moldes da lei brasileira, ainda que tenha sido absolvido ou condenado no estrangeiro. E segundo o §2º deste mesmo artigo, que trata dos

crimes previstos no inciso II, é necessário verificar as seguintes condições para que a lei brasileira venha a ser aplicada:

> Entrar o agente no território nacional;
> Ser o fato punível também no país em que foi praticado;
> Estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição;
> Não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena;
> Não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.

A Lei Penal em vigor no Brasil, destarte, adotou uma série de princípios para determinar a aplicação da lei brasileira em determinados casos, os quais podem ser assimilados, segundo Gabriel Cesar Zaccaria de Inellas, da seguinte maneira:

> Pelo *Princípio da Territorialidade*, a Lei Penal só é aplicável ao crime cometido no Brasil. Pelo *Princípio da Proteção*, a lei brasileira aplica-se aos crimes cometidos por estrangeiro, contra brasileiro, fora do Brasil. Pelo *Princípio da Justiça Universal*, aplica-se a lei brasileira, aos crimes que, por tratado ou Convenção, o Brasil se obrigou a reprimir. Pelo *Princípio da Nacionalidade Ativa*, a Lei Penal brasileira aplica-se aos brasileiros, onde quer que se encontrem. Pelo *Princípio da Representação*, aplica-se a Lei Penal brasileira, aos crimes cometidos em aeronaves ou embarcações brasileiras, mercantes ou privadas, quando em território estrangeiro e aí não serem julgados. [165]

3.5. Os problemas da competência em crimes cibernéticos

Ultrapassada as etapas iniciais do estabelecimento da competência e da lei aplicável, cabe fazer uma análise dos problemas jurídicos que podem surgir ao serem analisados, especificamente, os crimes cibernéticos, problemas estes enfrentados por vários doutrinadores que se deparam com este tema, como bem demonstrou Marco Aurélio Greco: "Além das repercussões na idéia de soberania e na eficácia das legislações, não se pode deixar de mencionar os reflexos que serão gerados em relação ao exercício da função jurisdicional"[166].

Segundo o já exposto e o regramento do artigo 109 da Constituição Federal, por não haver qualquer previsão acerca dos crimes cibernéticos nesta Carta Magna, conclui-se que a competência material para julgamento destes delitos seria da

---

[165] INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 120-121.
[166] GRECO, Marco Aurélio. Obra citada, p. 15.

justiça estadual[167]. Porém, segundo Fernando da Costa Tourinho Filho, esta justiça é competente para "julgar as causas da competência dentro das Circunscrições Territoriais em que está dividido o Brasil: Estados-Membros e Distrito Federal"[168], podendo vir a gerar problemas em casos de crimes que ultrapassam a jurisdição da justiça estadual, a qual é representada pela circunscrição territorial que esta ocupa, não sendo muito raro, inclusive, casos de crimes cibernéticos em que as próprias fronteiras do país são ultrapassadas. A principal preocupação nestes casos é a eficácia da sentença e o seu cumprimento, exigindo-se para tal, a expedição de cartas precatórias ou, ainda, rogatórias, dependendo se se trata de um delito plurilocal ocorrido entre estados-membros da federação ou um crime à distância quando se desenvolvem em países distintos, respectivamente.

Assim sendo, tendo ocorrido um delito, a primeira coisa que se deve analisar é se ele encontra-se consumado ou apenas tentado, para saber qual será a lei aplicável e o foro competente para conhecimento e julgamento da matéria. Quanto à lei aplicável, aplicar-se-á a lei brasileira nos casos previstos nos artigos 5º a 7º do Código Penal, ou seja, tendo ocorrido, mesmo que em parte, no Brasil ou aqui surtido efeitos ou ainda sendo o acusado brasileiro, serão estes casos julgados pela lei brasileira. Com base no artigo 70 do CPP, no primeiro caso, a competência territorial recairá sobre o local onde o ato se consumou, já no caso da tentativa, a competência recairá sobre o local onde foi praticado o último ato de execução.

Num primeiro momento não aparenta haver grandes dificuldades, porém isto está longe de ser simples. Observa-se que, segundo o artigo 70 e seus parágrafos do Código de Processo Penal, se um delito produziu algum efeito no território brasileiro, mesmo que parcialmente, este será competente para julgar o caso, sendo aplicada, de similar maneira, pela regra dos artigos 5º a 7º do Código Penal, a lei brasileira para julgar o caso. Ora, pode-se afirmar, portanto, que a lei brasileira será *sempre* aplicada e o Brasil será *sempre* competente para julgar os casos de delitos

---

[167] Há quem entenda, no entanto, que a competência da Justiça Federal está, sim, prevista no artigo 109 da Constituição Federal. Cf. VIANNA, Túlio Lima. **Dos crimes pela internet**. Belo Horizonte: UFMG, 2000, p. 19. "Quando o crime for cometido pela Internet, julgamos que a competência deverá ser da Justiça Federal, de acordo com o art. 109 IV, da Constituição Federal, já que o interesse da União em ter a Internet resguardada dentre dos limites brasileiros é evidente. Além do mais, este é um crime em que o resultado nem sempre se produz no lugar da ação, podendo até ocorrer em países diversos (crime à distância), com repercussões internacionais que nos fazem crer ser prudente deixar a competência para a Justiça Federal."

[168] TOURINHO FILHO, Fernando da Costa. **Processo Penal**, v. II., 24. ed. ver. e atual. São Paulo: Saraiva, 2002, p. 82.

que ofendam bens jurídicos genéricos (e não os que ofendam apenas uma pessoa exclusiva de maneira particular, como no caso do e-mail privado) ocorridos na Internet, pois esta está presente de igual modo em todos os países do mundo. Se encarado em termos de altruísmo, nenhum problema em isto ocorrer, acontece que estas sentenças dificilmente terão os seus cumprimentos verificados.

Alguns delitos cibernéticos de resolução mais simples têm sua solução encontrada mais facilmente, porém não escapam a críticas quando observadas por um olhar atento:

Imagine-se um e-mail contendo uma mensagem extorsiva. Alguém que receba uma mensagem desta será vítima de um crime tipificado no artigo 158 do Código Penal, podendo certamente gerar dúvida acerca do foro competente para se propor uma ação penal contra o remetente da mensagem, como foi demonstrada no caso concreto de "CONFLITO DE COMPETÊNCIA Nº 40.569 - SP (2003/0187145-1)"[169], quando num primeiro momento não se sabia ao certo se o crime havia sido consumado ou apenas tentado. Decidiu o STJ, por unanimidade, que o mero recebimento da mensagem extorsionária já caracteriza o crime consumado de extorsão, sendo o foro competente o do local onde o ofendido primeiro tomou conhecimento do teor da mensagem.

Destarte, e considerando a mobilidade que o computador adquiriu nos dias de hoje com os notebooks, laptops, netbooks e afins, poder-se-ia ter uma insegurança jurídica, visto que seria extremamente difícil, senão impossível, determinar com precisão qual foi o local onde um computador móvel visualizou um e-mail de caráter ofensivo pela primeira vez, ficando a vítima com ampla liberdade para escolher o local onde irá propor a ação penal.

---

[169] STJ - Informativo N° 0201 Período: 8 a 12 de março de 2004.
COMPETÊNCIA. EXTORSÃO. MENSAGENS ELETRÔNICAS.
As vítimas foram constrangidas mediante mensagens eletrônicas ameaçadoras enviadas pela internet, segundo as quais se pretendia infligir-lhes mal injusto se não providenciassem valores, o que levou as vítimas a ofertar a notícia-crime ao Ministério Público. Assim, não há como entender existir mera tentativa punível, pois o crime se consumou no local em que os ofendidos receberam os e-mails e deles tomaram conhecimento, local em que se fixa a competência, mostrando-se sem influência o de onde foram enviadas as mensagens.
No presente caso, concluiu o Min. Rel. José Arnaldo da Fonseca - "Tal o contexto, pouco importa o local de onde enviadas as últimas mensagens eletrônicas, pois o crime de extorsão se consumou no lugar no qual os ofendidos receberam os e-mails e deles tomaram conhecimento, no caso, no Município de Guarapuava, sede da empresa administrada pelas pessoas extorquidas."
https://ww2.stj.jus.br/revistaeletronica/Abre_Documento.asp?sLink=ATC&sSeq=1143055&sReg=200301871451&sData=20040405&sTipo=51&formato=PDF

De maneira similar ocorreu no caso concreto de CONFLITO DE COMPETÊNCIA Nº 99.133 - SP (2008/0218009-3)[170], em que o acusado havia sido denunciado pela prática do crime de atentado violento ao pudor contra a própria filha, além de ter gravado a prática de tal ato e enviado o vídeo desta gravação a uma outra pessoa que residia no Brasil. Neste caso concluiu-se que a competência para julgar este caso seria da justiça estadual, pois o crime comprovadamente não ultrapassou as fronteiras nacionais do Brasil, restringindo-se a uma conversa e ao envio direto do vídeo entre as duas pessoas. Igual entendimento foi dado no caso de "CONFLITO DE COMPETÊNCIA Nº 57.411 - RJ (2005/0207571-1)"[171].

Diferente tratativa teria o caso se restasse configurada a divulgação, pela Internet, desta gravação contendo pornografia infantil, como ocorreu no caso de "HABEAS CORPUS Nº 24.858 - GO (2002/0130648-1)"[172], em que os acusados fotografaram, filmaram e publicaram, na Internet, imagens contendo pornografia infantil. Nesse caso não há como negar a competência da justiça federal para julgar o caso, pois segundo o inciso V do artigo 109 da Constituição Federal, "os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no

---

[170] CONFLITO NEGATIVO DE COMPETÊNCIA. ATENTADO VIOLENTO AO PUDOR COM VIOLÊNCIA PRESUMIDA (ART. 214 C/C ART. 224, A E 226, II DO CPB). TROCA DE MENSAGENS ENTRE PESSOAS RESIDENTES NO PAÍS, PELA INTERNET, COM CONTEÚDO PORNOGRÁFICO ENVOLVENDO CRIANÇA. ART. 241, CAPUT DA LEI 8.069/90. AFASTAMENTO DA COMPETÊNCIA DA JUSTIÇA FEDERAL. INTELIGÊNCIA DO ART. 109, V DA CF. PRECEDENTES DO STJ. PARECER DO MPF PELA COMPETÊNCIA DA JUSTIÇA ESTADUAL. CONFLITO DE COMPETÊNCIA CONHECIDO PARA DECLARAR A COMPETÊNCIA DO JUÍZO ESTADUAL SUSCITANTE.

1. Comprovado que o crime de divulgação de cenas pornográficas envolvendo criança não ultrapassou as fronteiras nacionais, restringindo-se a uma comunicação eletrônica entre duas pessoas residentes no Brasil, a competência para julgar o processo é da Justiça Estadual. Inteligência do art. 109, V da CF. Precedentes do STJ.

2. Conflito de competência conhecido, para declarar a competência do Juízo de Direito da 3a. Vara Criminal de Osasco/SP, o suscitante, em consonância com o parecer do douto MPF.

[171] CONFLITO DE COMPETÊNCIA. DIREITO PROCESSUAL PENAL. ARTIGO 241, CAPUT, DA LEI Nº 8.069/90. DIVULGAÇÃO. CRIME PRATICADO NO TERRITÓRIO NACIONAL POR MEIO DE PROGRAMA DE COMUNICAÇÃO ELETRÔNICA ENTRE DUAS PESSOAS. COMPETÊNCIA DA JUSTIÇA ESTADUAL.

1. "Aos juízes federais compete processar e julgar: os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente. " (Constituição Federal, artigo 109, inciso V).

2. Em se evidenciando que os crimes de divulgação de fotografias e filmes pornográficos ou de cenas de sexo explícito envolvendo crianças e adolescentes não se deram além das fronteiras nacionais, restringindo-se a uma comunicação eletrônica entre duas pessoas residentes no Brasil, não há como afirmar a competência da Justiça Federal para o processo e julgamento do feito.

3. Conflito conhecido, para declarar competente o Juízo Estadual suscitante.

[172] - Competência da Justiça Federal estabelecida no art. 109, V, da Constituição de 1988, para o processo e julgamento de crime previsto "em tratado ou convenção internacional, quando iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro..."

- Ordem denegada.

País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente", sendo que o tratado que versa sobre o combate aos crimes de pornografia infantil e pedofilia está previsto em Convenção Internacional sobre os Direitos da Criança, aprovada pelo Decreto Legislativo 28/90 e promulgada pelo Decreto Presidencial nº 99.710, de 21 de novembro de 1990.

Percebe-se, portanto, que não basta o mero fato de o crime ser previsto em Convenção ou Tratado Internacional para que a justiça federal seja competente para julgar o caso, é necessário que, impreterivelmente, a execução ou o resultado tenham se produzido em país estrangeiro.

3.6. A soberania e o princípio da não intervenção

Há, no entanto, inúmeros outros problemas a serem solucionados neste novo tema, casos estes que não são do interesse única e exclusivamente de um só país, mas de todo o mundo. É o que defende Gabriel Cesar Zaccaria de Inellas:

> Um dos maiores problemas que se enfrenta, no combate aos crimes cometidos através da Internet, é a questão da competência. Como a Rede da Internet é mundial e sem fronteiras e sem donos, torna-se quase impossível para qualquer País, aplicar e executar leis para regular o denominado ciberespaço. Tal situação é evidente. O Brasil pode proibir, por exemplo, a pornografia na Internet; todavia, poderá fiscalizar o cumprimento da lei, apenas entre as Provedoras e os usuários do território brasileiro. Se o material pornográfico, no exemplo citado, for lançado na Rede, por usuários residentes em outros Países, tal material será acessível a qualquer pessoa, em qualquer parte. Devido ao seu caráter internacional, na Internet não existem fronteiras; por conseguinte, o que for veiculado através dela, estará ,instantaneamente, em todo o mundo. [173]

Certamente o combate aos crimes cibernéticos é um tema que está muito longe de ser solucionado, e isto se dá pelo já referido fato de o espaço cibernético não se ater a qualquer tipo de fronteira estabelecida pelo ser humano. Utilizando-se do trecho citado, monta-se a seguinte situação: um determinado sujeito 'F' encontra-se em um País 'A', sendo que neste país, pornografia infantil não é crime, utiliza-se de uma câmera fotográfica para fotografar, sem deslocar-se do país A, um sujeito 'V', menor, sem roupa e simulando uma relação sexual com uma boneca, em seu país de origem 'B'. Utilizando-se da Internet, 'S' divulga as fotos de 'V' pela Internet, sendo visualizado por todos os habitantes de 'B', país em que estas fotos seriam

---

[173] INELLAS, Gabriel Cesar Zaccaria de. Obra citada, p. 119.

consideradas *puníveis como pornografia infantil. Embora hipotético*, muitos casos similares podem e possivelmente ocorrem nos dias de hoje sem que qualquer solução possa ser alcançada.

No começo deste capítulo, mostrou-se um exemplo de um caso fictício em que poderia facilmente surgir um problema acerca de qual país teria competência para julgar determinado caso, imaginando-se para tanto legislações similares à brasileira, que se rege basicamente pelo Princípio do Territorialidade para decidir tanto a lei aplicável quanto o foro competente para julgamento. Sem sombra de dúvida todos os países envolvidos em casos como o apresentado terão interesse em julgar determinada causa, por entender ser a sua legislação mais adequada e atualizada que as demais, por entender ter mais recursos para julgar o caso, por entender se tratar de um nacional do seu país, dentre diversos outros argumentos que poderiam surgir, inclusive o válido argumento de que o delito teria ocorrido dentro do seu território, invocando, segundo o Princípio anteriormente citado, a competência para julgar a questão. Não é apenas o arbitramento do foro competente para julgamento que preocupa os doutrinadores, mas a correta aplicação das regras do "*Non bis in idem*" e da "*Lex mitior*", impedindo que um sujeito venha a ser punido mais de uma vez por um mesmo ato e também que ele faça jus a uma aplicação retroativa da lei mais benéfica, especialmente nos casos em que é de extrema dificuldade a investigação de quando se deu a primeira atuação do acusado, como nos afamados vírus de computador do tipo "Time-Bomb"[174].

Segundo o manual das Nações Unidas sobre o tema da prevenção e controle dos crimes relacionados ao computador, que corrobora com o entendimento da doutrina majoritária:

> A primazia do princípio da territorialidade é geralmente aceita na esfera da jurisdição criminal. Este princípio é baseado no respeito mútuo da igualdade de Soberania entre Estados e está conectado com o princípio da não-intervenção nos assuntos e domínios exclusivos de outros Estados. Até mesmo no excepcional evento de um país poder aplicar jurisdição extraterritorial no interesse de proteger seus próprios interesses vitais, a primazia do princípio extraterritorial não é alterado.[175]

---

[174] UNIDED NATIONS. Obra citada, p. 50.

[175] Trad. Livre. *Idem, ibidem*. "The primacy of the principle of territoriality is generally accepted in sphere of criminal jurisdiction. The principle is based on mutual respect of sovereign equality between States and is linked with the principle of non-intervention in the affairs and exclusive domain of other States. Even in the exceptional event that a country might apply extraterritorial jurisdiction for a sake of protecting its own vital interests, the primacy of the extraterritorial principle is not altered."

Consolidando a preocupação da doutrina, Vladmir Aras afirma que: "Problemas de soberania, jurisdição e competência estarão cada dia mais presente no cotidiano dos juristas e dos operadores do Direito que se defrontarem com questões relativas à Internet."[176]

Seguindo esta linha evolutiva, percebe-se que não tardará muito para que verdadeiras guerras sejam travadas no ambiente cibernético, seja por motivos de represálias a decisões judiciais protetoras de infratores de mesma nacionalidade dos órgãos julgadores, seja uma intenção megalomaníaca de domínio do território cibernético, ou qualquer outro motivo neste meio de campo. Já é comum, hodiernamente, alguns tipos de ataques virtuais, citando como exemplo o famigerado "Ataque DoS", que se traduz em um "Ataque de Negação de Serviço" – ou do inglês, "Denial of Service" –, em que há uma espécie de sobrecarga de acessos a determinados sítios ou serviços da Internet, fazendo com que o computador em que se encontra hospedado o servidor daquele determinado veículo não consiga suportar a quantidade massiva de pedidos de comunicação externa e consequentemente venha a ser debilitada a capacidade de funcionamento desta máquina, não respondendo ou respondendo tão lentamente que praticamente impossibilite a transmissão de informação[177]. Este tipo de ataque vem sendo utilizado como maneira de protesto em determinados casos, porém pode ser utilizado sem qualquer motivo específico, podendo ser, inclusive, realizado pela vontade de uma única pessoa, através da manipulação, por meio de um Malware específico, de vários computadores infectados. Esta prática não encontra respaldo jurídico em diversos países ao redor do mundo, sendo considerado crime grave em alguns países, como Inglaterra[178] e Estados Unidos[179], podendo a pena chegar a até 10 anos de reclusão, e não tendo qualquer proteção jurídica em outros países, como é o caso do Brasil[180], onde sequer há projetos de lei prevendo tal prática, sendo o Projeto de Lei da Câmara n° 89, de 2003 (n° 84, de 1999, na Câmara dos

---

[176] ARAS, Vladmir. Obra citada.
[177] SIEGEL, Larry J. **Criminology**, 10. ed. Belmont, CA: Cengage Learnin Inc., 2008, p. 422.
[178] ESPINER, Tom. **U.K. outlaws denial-of-service attacks**. [online] Disponível na Internet via WWW. URL: http://news.cnet.com/U.K.-outlaws-denial-of-service-attacks/2100-7348_3-6134472.html. Arquivo consultado em 23 de outubro de 2010.
[179] CERT. **Denial of Services Attacks**. [online] Disponível na Internet via WWW. URL: http://www.cert.org/tech_tips/denial_of_service.html. Arquivo consultado em 23 de outubro de 2010.
[180] OSTROCK, Guilherme. **DoS é crime?** [online] Disponível na Internet via WWW. URL: http://www.infolei.com.br/dos-e-crime/. Arquivo consultado em 23 de outubro de 2010.

Deputados), e os Projetos de Lei do Senado nº 76 e nº 137, ambos de 2000[181], substitutivos do projeto de lei do Senador Eduardo Azevedo, o qual mais chegou perto de prever legalmente tais atos, trazendo uma proposta de alteração no Código Penal, porém não sendo acurado o suficiente para que uma efetiva regulamentação se verifique, considerando-se a maneira que se encontra redigido os referidos textos hoje. Abaixo é destacado o artigo que interessa, no presente estudo, desses projetos de lei que foram referidos:

> Dano por difusão de código malicioso eletrônico, ou digital ou similar
> Art. 163-A: Criar, inserir, ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.
> Pena: Reclusão, de um (1) a três (3) anos, e multa.
> Dano qualificado por difusão de código malicioso eletrônico ou digital ou similar
> § 1º Se o crime é cometido com a finalidade de destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo titular, de dispositivo de comunicação, de rede de computadores ou de sistema informatizado:
> Pena: reclusão, de dois (2) a quatro (4) anos, e multa.
> Difusão de código malicioso eletrônico ou digital ou similar seguido de danos
> § 2º Se do crime resulta a inutilização, deterioração, alteração dificultação do funcionamento, ou funcionamento desautorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado e as circunstâncias demonstrem que o autor não quis o resultado, nem assumiu o risco de produzi-lo:
> Pena: reclusão, de 3 (dois) a cinco (5) anos, e multa (sic)
> § 3º A pena é aumentada da sexta parte se o agente se vale de nome falso ou da utilização da identidade de terceiros para a prática do crime.
> § 4º Não há crime quando a ação do agente é a título de defesa digital, excetuando o desvio de finalidade e o excesso.

Apenas para exemplificar, ativistas favoráveis à pirataria digital fizeram uma série de retaliações às ações realizadas contra um dos mais famosos sítios de compartilhamento de material não oficial. Nestas represálias, estes ativistas realizam ataques de Negação de Serviço a sítios de propriedade das indústrias de músicas e filmes americanas: o site CopyProtected.com da Motion Picture Association of America (MPAA) e os sites RIAA.com e RIAA.org da Recording Industry Association of America (RIAA) foram as últimas vítimas, ficando rendidos inativos por um longo período de tempo. De maneira similar, um grupo anônimo bloqueou acesso a sítios

[181] Todos estes tramitam conjuntamente.

importantes do governo australiano em protesto contra os planos do governo de introduzir filtros na Internet do país, o qual traria efeitos similares a uma censura.[182]

Eventos corriqueiros que tem efeito similar a este ataque, porém de ocorrência eventual, são as situações em que uma imensa quantidade de pessoas tem interesse em visualizar uma página específica da Internet ao mesmo tempo, o que causa a lentidão e muitas vezes causando o cancelamento da visualização por demora excessiva no carregamento, o "timeout" do Internet Explorer. Certamente a maioria das pessoas já passou alguma vez por situações similares, citando como exemplo os resultados de exames Vestibular e os resultados de Concursos Públicos, onde milhares de candidatos tentam desesperadamente acessar a página do resultado da sua prova com o intuito de ver se encontram-se aprovados ou não no teste realizado, porém muitos só conseguem visualizar horas depois de lançado o resultado na Internet.

Nesta breve análise já foi possível identificar a prática do mesmo ato com diferentes motivações e características, e é nesse sentido que a previsão legal, tanto nacional quanto internacional, para tais atos deve ser extremamente bem definida, caso contrário arriscaria criar uma legislação demasiadamente punitiva que acabaria prejudicando pessoas inocentes ou poderia criar uma legislação insuficiente a ponto de não ser aplicável em qualquer caso prático. É neste sentido que se deve ter uma legislação inteligente para que, suscitada uma competência para julgamento de um caso similar por um país qualquer, este tenha bem definido o que é uma conduta criminosa no território cibernético e o que não é, impossibilitando, assim, a existência de qualquer controvérsia internacional. O ideal seria, inclusive, criar uma legislação unificada mundialmente para que um efetivo combate aos crimes cibernéticos seja verificado. A União Européia já vem de longa data desprendendo esforços nesse sentido, unificando a legislação através de tratados e convenções internacionais acerca do tema, citando como exemplo a Convenção do Conselho Europeu sobre o Cibercrime, firmada em 23 de novembro de 2001, em Budapeste[183].

---

[182] BBC NEWS. **Activists target recording industry websites**. [online] Disponível na Internet via WWW. URL: http://www.bbc.co.uk/news/technology-11371315. Arquivo consultado em 23 de outubro de 2010.

[183] SAFERNET. **Brasil não pode aderir a Convenção de Budapeste sobre o Cibercrime**. [online] Disponível na Internet via WWW. URL: http://www.safernet.org.br/site/noticias/brasil-n%C3%A3-pode-aderir-conven%C3%A7-budapeste-sobre-cibercrime. Arquivo consultado em 25 de outubro de 2010.

Apenas para ilustrar o tamanho da paranóia que vem afetando os diversos países desenvolvidos do mundo, no dia 25/08/2010 foi publicado, na revista ISTOÉ, uma notícia intitulada "Obama vai desligar a Internet?", informando que foi criado, em 2009, pelo senador democrata John D. Rockefeller, um projeto de lei norte-americano [184] "que pretende garantir, assim como no caso do uso de armas nucleares, que o presidente tenho o 'poder absoluto' de bloquear o acesso a zonas da internet sob risco de ataques virtuais"[185], ou seja, seria uma espécie de botão que desliga instantaneamente a Internet de acordo com a vontade do Presidente Estadunidense, também chamado de "internet kill switch" pelos americanos. Este projeto sofreu várias críticas, e por isto, outro projeto de lei[186], agora de autoria do senador Joseph I. Lieberman, foi redigido, porém com efeitos muito similares.

Foi informado nesta referida notícia da ISTOÉ que o Senado americano votaria este projeto de lei em setembro de 2010, mas até a presente data, não houve a referida votação.[187]

Esta opção criada pelo senado americano foi demasiadamente precipitada, pois causaria diversos problemas políticos e sociais caso fosse definitivamente aprovada e muito maiores se o Presidente dos Estados Unidos viesse a utilizá-la em qualquer momento do seu governo, pois prejudicaria inúmeras pessoas que utilizam regularmente a Internet.

Quanto a isso, Greg Melick já havia se manifestado, e embora tenha defendido que algumas soluções impopulares devessem ser tomadas para assegurar um equilíbrio adequado para o retesado contexto atual, defendeu que "também há de haver uma solução sensata para a sempre presente tensão entre as urgências comerciais e da aplicação da lei" [188].

---

[184] Projeto de Lei: "S.773 - Cybersecurity Act of 2009", disponível em: http://thomas.loc.gov/cgi-bin/bdquery/D?d111:3:./temp/~bdKTVM::|/home/LegislativeData.php?n=BSS;c=111|

[185] GOMES, Hélio. **Obama vai desligar a Internet?** In: ISTOÉ, ano 34, n. 2128, 25 de agosto de 2010, São Paulo: Três Editorial, 2010, p. 88.

[186] Projeto de Lei: "S.3480 - Protecting Cyberspace as a National Asset Act of 2010", disponível em: http://thomas.loc.gov/cgi-bin/bdquery/z?d111:s.03480:

[187] O andamento dos projetos pode ser verificado nos links acima fornecidos.

[188] [Trad. Livre] MELICK, Greg. **Law Enforcement in Cyberspace**. Australia: National Crime Authority, 2010, p. 10. [online] Disponível na Internet via WWW. ULR: http://www.isrcl.org/Papers/Melick.pdf. Arquivo consultado em 25 de outubro de 2010. "There also has to be a sensible resolution to the ever present tensions between commercial and law enforcement imperatives"

4. CONCLUSÃO

O objetivo deste estudo não foi trazer uma solução imediata nem certeira acerca dos problemas levantados, tendo em vista serem estas dificuldades encaradas por qualquer estudioso ou pesquisador que se depara com este tema, mas sim fornecer ainda mais combustível à locomotiva que conduz este novo ramo do Direito, demonstrando que as soluções para os problemas levantados não serão adquiridas de maneira tão simples quanto afirmam alguns, exigindo-se enormes esforços e avanços nesse sentido.

Inicialmente, ficou demonstrada a desarmonia da doutrina acerca da nomenclatura a ser adotada neste tema. Embora todas as doutrinas tenham o seu mérito, sou mais favorável à adoção da denominação de crimes ou delitos cibernéticos, pois é perceptivelmente a mais abrangente de todas, facilitando a pesquisa doutrinária e a prática forense nesta área do Direito, conglobando todas as condutas que têm relacionamento com o espaço-tempo cibernético (ETC). Quando falamos de crimes comuns, concordo ser possível, também, adotar a nomenclatura 'Crimes na Internet', porém apenas para tratar dos delitos cometidos com a utilização da Internet para a sua perpetração, os quais seriam uma espécie de, nos termos de Túlio Lima Vianna, Delito Informático Impróprio. Já nos casos de Crimes Cibernéticos, todos os tipos de Delitos Informáticos tratados por este autor também estariam englobados neste singelo termo.

Ao serem analisadas as espécies de Delitos Informáticos trazidos por Túlio Lima Vianna, percebe-se que não há como tratar a totalidade dos Delitos Informáticos, ou ainda dos delitos cibernéticos, como crimes formais ou crimes materiais, devendo analisar cada um em específico

Foi também demonstrado a dificuldade que teria o ordenamento jurídico brasileiro em lidar com os casos como o dos vírus 'time bomb' ou 'logic bomb' e a sua impotência diante deles na contemporaneidade.

Em um segundo momento, demonstrou-se que não há consenso quanto à necessidade ou não de novos tipos penais para as emergentes e nocivas condutas no campo cibernético, porém igualmente foi demonstrado que há condutas ofensivas e definitivamente prejudiciais que não são de fácil solução penal com a vetusta legislação que temos.

Foi neste momento oportuno que se abriu um tópico para esclarecer a idéia de que não será com a proteção de mais um bem jurídico ou a mera tipificação de um ou algumas condutas lesivas que teremos a efetiva prevenção ou, sequer, repressão dos delitos cibernéticos, as quais se darão apenas quando o grau de educação e civilidade do ser humano se encontrarem em patamares platônicos, portanto, utópicos. Destarte, acredito que, pelo fato de, usualmente, os usuários de computadores serem dotados de um grau de escolaridade e cultura pouco mais elevados que o padrão das pessoas que não os utilizam, a proteção penal, tomada na sua vertente de repressão moral, possa ter uma justificativa plausível, porém não se deve acreditar que o Direito Penal por si só será capaz de prevenir a prática destes delitos, dando-se a efetiva prevenção – o que realmente se busca atualmente – com o aumento da segurança no âmbito cibernético, verificado na criptografia de documentos e com a redução do anonimato, principalmente verificado nas técnicas de assinatura digital e outros meios de identificação de usuário. Outra maneira igualmente eficaz, não só para os delitos cibernéticos, mas para todos os delitos atualmente cometidos, é com a melhoria da educação da população, pois assim haveria uma maior conscientização do imoral e do ilegal e uma tendência ao altruísmo, pretendendo-se, destarte, 'apagar a chama pela base', 'cortar o mal pela raiz', ou seja, ensinar aos novos seres humanos simplesmente que a prática de condutas lesivas não traz qualquer utilidade para o universo como um todo.

Passada a análise material dos delitos cibernéticos, adentrou-se nas partes processuais do tema, começando-se pela investigação e produção de provas para que houvesse uma adequada verificação dos indícios de autoria e materialidade do fato.

Em um primeiro momento, a perquirição da autoria da conduta poderia parecer simples, pois se consegue facilmente localizar o computador em que foi emitida a conduta delituosa, porém, como já foi dito, o computador é apenas um instrumento que recebe ordens de um ser humano, e, desse modo, como saber quem, dentre diversas pessoas possíveis em um caso concreto, especificamente, ordenou o computador a realizar tal conduta? Evidentemente que se houver uma dúvida relevante, não se deveria haver um traumático processo penal para que haja o risco de o juiz escolher, ao seu livre arbítrio – nestes casos em que uma certeza provavelmente nunca existirá –, qual ou quais pessoas deverão responder pela prática do ato. Nestes casos, não se deve haver a instauração de um processo

penal, pois não ficaram bem delineados os indícios de autoria, deixando esta solução para outros ramos do Direito, os quais, embora também não consigam solucionar o caso com precisão, não serão tão traumáticos e prejudiciais aos acusados como o Direito Penal e Processual Penal. Ainda neste ponto, tentou-se demonstrar que poderia haver a responsabilização penal das Provedoras de Acesso à Internet, que são pessoas jurídicas, o que já acontece em alguns países como Portugal, mas que no nosso ordenamento jurídico ainda encontra fortes barreiras.

Há ainda a necessidade de averiguar se está presente a materialidade do fato, e para que esta verificação seja inafastável, uma perícia extremamente bem realizada e documentada se faz necessário, especialmente tendo em vista a facilidade que determinadas pessoas têm de alterar dados no campo cibernético, alterações estas que, embora possam ficar registrada em certos componentes do computador, podem ser facilmente ocultadas por um *expert* neste ramo da ciência.

Tendo os crimes cibernéticos um caráter de crimes plurilocais e, às vezes, crime à distância, um problema acerca de qual será o juízo competente para conhecer e julgar o caso aparece. Foi demonstrado através da análise doutrinária e jurisprudencial que, em consonância com o artigo 109 da Constituição Federal, o juízo competente para julgar os crimes cibernéticos é o da justiça estadual, embora seja evidente a dificuldade que esta justiça venha a sofrer em delitos que ultrapassam a sua competência territorial ou ainda quando ultrapassa a própria circunscrição territorial em que está divido o Brasil. Neste sentido, uma maior agilidade na justiça é essencial, além de um melhoramento dos seus arcabouços financeiros e infraestrutural para que tenha capacidade para julgar tais delitos sem que barreiras cognitivas sejam impostas. Ficou claro, também, que é possível que a justiça federal seja competente para julgar determinado caso, mas apenas se tiver ocorrido o delito no exterior e este delito tenha previsão em tratado ou convenção internacional, ou ainda se tiver ocorrido em detrimento da União.

Ademais, ficou demonstrado que o problema dos crimes cibernéticos afeta todos os países de uma forma universal, sendo do interesse de todos que seja dado um fim definitivo a estas condutas potencialmente lesivas. Para tal, vários são os autores que clamam frenética e repetidamente para que uma ação conjunta e cooperativa seja realizada, tanto nacional como internacionalmente falando, unindo-se as forças de todos nesta empreitada, para que este tipo de conduta não seja o motivo e a munição das próximas guerras, e, por outro lado, para que uma solução

justa seja tomada, não necessitando de ações súbitas e ofensivas, como se tem visto ultimamente, ao livre manuseio do instrumento que mais une os povos do mundo, a Internet, as quais viriam a impedir, dessa maneira, a diversão, a formação de laços sociais, ou até mesmo a sobrevivência de diversas pessoas neste mundo, que se torna cada vez mais informatizado e interconectado, o qual não consegue mais se desfazer do imenso elo vital que criou em torno de si mesmo.

5. BIBLIOGRAFIA

AGUIAR, Rebeca Novaes. **Competência territorial para apurar crimes na internet**. [online] disponível na Internet via WWW. URL: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=1225. Arquivo consultado em 23 de outubro de 2010.

ALLEN, Mark. **Basic Hardware Guide**. [online] Disponível na Internet via WWW. URL: http://www.comptechdoc.org/basic/basictut/index.html. Arquivo consultado em 23 de outubro de 2010.

AMARAL, Augusto Jobim do. **Ensaio sobre uma teoria agnóstica da pena**: Fronteiras entre o político e o direito penal. *In*: Encontro Preparatório para Congresso Nacional do CONPEDI, 17., 2008, Salvador, BA. Anais do: XVII Encontro Preparatório para o Congresso Nacional do CONPEDI, Florianópolis: Fundação Boiteux, 2008, p. 1591-1611.

ARAS, Vladmir. **Crimes de Informática**: Uma nova criminalidade. [online] Disponível via WWW. URL: http://www.informatica-juridica.com/trabajos/artigo_crimesinformticos.asp. Arquivo consultado em 23 de outubro de 2010.

ARAÚJO JÚNIOR, João Marcelo. **Computer Crime**. Anais da Conferência Internacional de Direito Penal, 1988. Rio de Janeiro: Procuradoria Geral da Defensoria Pública, 1988

BARROS, Lucivaldo Vasconcelos. **O crime na era da informação**, 2002. [online] Disponível na Internet via WWW. URL: http://jus2.uol.com.br/doutrina/texto.asp?id=3675/. Arquivo consultado em 23 de outubro de 2010.

BBC NEWS. **Activists target recording industry websites**. [online] Disponível na Internet via WWW. URL: http://www.bbc.co.uk/news/technology-11371315. Arquivo consultado em 23 de outubro de 2010.

BECCARIA, Cesare Bonesana. **Dos delitos e das penas**. Bauru: EDIPRO, 1993.

BECKER, Alfredo Augusto. **Teoria Geral do Direito Tributário**. São Paulo: Saraiva, 1963.

BONAVIDES, Paulo. **Ciência Política**, 10. ed. São Paulo: Editora Malheiros. 1996.

BORGES, Clara Maria Roman. **A competência nos crimes plurilocais e o princípio do juiz natural**. Dissertação apresentada ao Programa de Pós-graduação em Direito da Universidade Federal do Paraná como requisito parcial para outorga do título de Mestre em Direito, 2001.

_____. **O incidente de deslocamento de competência e o princípio do juiz natural**. Raízes Jurídicas (UNICENP), v. 4, p. 101-128, 2008.

_____. **O princípio do juiz natural como garantia de um processo penal democrático: uma breve análise da competência penal por prerrogativa de função**. In: Alexandre Coutinho Pagliarini; Clèmerson Merlin Clève; Ingo Wolfgang Sarlet. (Org.). Direitos Humanos e Democracia. 1 ed. Rio de Janeiro: Forense, 2007, v. 1, p. 195-220.

BORGES, Guilherme Roman. **Michel Foucault: uma interlocução com o discurso filosófico-jurídico**. Monografia apresentada como requisito parcial à obtenção do título de bacharel em Direito, na Faculdade de Direito, do Setor de Ciências Jurídicas, da Universidade Federal do Paraná, em 25/10/2002.

BÖTTLER, Jonas. **Threats posed by Cyber Terror and Possible Responses of the United Nations**. Canadá: UNISCA, 12 de dezembro de 2002.

BRASIL, Angela Bittencourt. **Informática Jurídica** - O Ciber Direito. Rio de Janeiro: Juris Doctor; 2000.

BRITO, Eduardo Valadares de. **Crimes na Internet**. [online] Disponível na Internet via WWW. URL: http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/view/4714/4284. Arquivo consultado em 22 de outubro de 2010.

CAMARGO SANTOS, Coriolano Aurélio Almeida. **Atual cenário dos crimes cibernéticos no Brasil**. [online] Disponível na Internet via WWW. URL: http://www2.oabsp.org.br/asp/comissoes/sociedade_informacao/artigos/crimes_cibernéticos.pdf. Arquivo consultado em 23 de outubro de 2010

CANTU, Eduardo. **Redes de Computadores e Internet**. São José: CEFET/SC, 2003.

CARVALHO, Paulo de Barros. **Curso de Direito Tributário**, 13. ed. São Paulo: Saraiva, 2000.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**, 2. ed. rev. ampl. e atual. Rio de Janeiro: Lumen Juris, 2003.

CERT. **Denial of Services Attacks**. [online] Disponível na Internet via WWW. URL: http://www.cert.org/tech_tips/denial_of_service.html. Arquivo consultado em 23 de outubro de 2010.

CHIOVENDA, Giuseppe. **Istituzioni di diritto processuale civile**. Náploes: Jenove, 1933 (trad. port. de J. Guimarães Menegale: Instituições de direito processual civil, 3ª ed., vol. II, São Paulo, Saraiva, 1969).

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2000.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. Jus Navigandi, Teresina, ano 1, nº 12, Maio de 1997. [online] Disponível na Internet via WWW. URL: http://jus2.uol.com.br/doutrina/texto.asp?id=1826. Arquivo consultado em 23 de outubro de 2010.

COUTINHO, Jacinto Nelson de Miranda. **Introdução aos princípios gerais do Processo Penal brasileiro**. In: Revista da Faculdade de Direito da UFPR, Curitiba, ano 30, nº 30, 1998.

DARLINGTON, Roger. **Internet Ethics**: Oxymoron or Orthodoxy?, 2002. [online] Disponível na Internet via WWW. URL: http://www.rogerdarlington.co.uk/Internetethics.html. Arquivo consultado em 23 de outubro de 2010.

DINAMARCO, Cândido Rangel; GRINOVER, Ada Pellegrini; CINTRA, Antonio Carlos de Araújo. **Teoria Geral do Processo**, 23. ed. São Paulo: Malheiros Editores, 2007.

ESPINER, Tom. **U.K. outlaws denial-of-service attacks**. [online] Disponível na Internet via WWW. URL: http://news.cnet.com/U.K.-outlaws-denial-of-service-attacks/2100-7348_3-6134472.html. Arquivo consultado em 23 de outubro de 2010.

FARACO, Sabrina. **O vírus como crime de informática**, p. 3-4. [online] disponível na Internet via WWW. URL:

http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/6038/5607. Arquivo consultado em 23 de outubro de 2010.

FELLEISEN, Matthias; FINDLER, Robert Bruce; FLATT, Matthew; KRISHNAMURTHI, Shriram. **How to Design Programs**: An Introduction to Computing and Programming. Cambridge: The MIT Press, 2001. [online] Disponível na Internet via WWW. URL: http://www.htdp.org/2003-09-26/Book/curriculum-Z-H-5.html#node_sec_2.2. Arquivo consultado em 23 de outubro de 2010.

FERREIRA, Ivette Senise. A criminalidade informática. **Direito & Internet**: Aspectos Jurídicos Relevantes. Bauru, SP: Edipro, 2000.

FIGUEIREDO DIAS, Jorge. **Direito Penal**: Parte Geral, Tomo I. Coimbra Editora: Coimbra, 2004.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**, 3. ed. São Paulo: Bookman Editora, 2004.

FOUCAULT, Michel. **Historia de la sexualidad**: La voluntad de saber, tomo 1. Madrid, Siglo XXI, 1992.

FRAGOSO, Heleno Cláudio. **Lições de direito penal**: a nova parte geral, 8ª ed. Rio de Janeiro: Forense, 1985.

FREITAS, Gustavo. **Crimes Cibernéticos**. [online] Disponível na Internet via WWW. URL: http://www.gfsolucoes.net/gustavo/blog-tecnico/seguranca/crimes-ciberneticos/. Arquivo consultado em 23 de outubro de 2010.

GOMES, Hélio. **Obama vai desligar a Internet?** In: ISTOÉ, ano 34, n. 2128, 25 de agosto de 2010, São Paulo: Três Editorial, 2010.

GOMEZ COLOMER, Juan-Luis. **El proceso aleman: introduccion y normas básicas**. Barcelona: Bosch, 1985.

GONÇALVES, Sérgio Ricardo M. **Hackers, Crakers e Spammers**: quem são e o que fazem? [online] Disponível na Internet via WWW. URL:http://www.mundojuridico.adv.br/sis_artigos/artigos.asp?codigo=659. Arquivo consultado em 23 de outubro de 2010.

GOUVÊA, Sandra. **O Direito na Era Digital**: Crimes praticados por meio da Informática. Rio de Janeiro:Mauad, 1997.

GRECO, Marco Aurélio. **Internet e Direito**, 2. ed. São Paulo: Dialética, 2000.

GRECO FILHO, Vicente. **Algumas observações sobre o Direito Penal e a Internet**. Boletim IBCRIM, ano 8, nº 95.

GREGORY, Peter. **Computer Viruses for Dummies**. Hoboken: Wiley Publishing Inc., 2004.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**, 2. ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009.

INTERNET ENGINEERING TASK FORCE (IETF). **RFC 791: Internet Protocol, DARPA Internet Program Protocol Specification**, September 1981. [online] Disponível na Internet via WWW. URL: http://www.ietf.org/rfc/rfc791.txt. Arquivo consultado em 22 de outubro de 2010.

LEISTER, Margareth. **Princípio da não-intervenção e soberania nacional**. *In*: Âmbito Jurídico, Rio Grande, 31 de agosto de 2005. [online]. Disponível na Internet via WWW. URL: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=330. Arquivo consultado em 22 de outubro de 2010.

LEONE, Giovanni. **Lineamenti di diritto processuale penale**. 2. ed. Napoli: Jovene, 1951, p. 85.

LOPES JR., Aury. **Direito Processual Penal** e sua conformidade constitucional, v.1, 4. ed., Rio de Janeiro: Editora Lumen Juris, 2009.

MAJOLO, Ederlei Norberto. **Informática e Crime**. Monografia apresentada como requisito parcial à obtenção do título de bacharel em Direito, na Faculdade de Direito do Setor de Ciências Jurídicas, da Universidade Federal do Paraná, em 29/10/2006.

MANZINI, Vincenzo. **Tratado de derecho procesal penal**. Trad. Santiago Sentís Meledo y Marino Ayerre Redín. Buenos Aires: EJEA, 1951.

MARCATO, Antonio Carlos. **Breves considerações sobre jurisdição e competência**. [online] Disponível na Internet via WWW. URL: http://jus2.uol.com.br/doutrina/texto.asp?id=2923. Arquivo consultado em 23 de outubro de 2010.

MARTINELLI, João Paulo Orsini. **Aspectos relevantes da Criminalidade na Internet**. [online] Disponível na Internet via WWW. URL: http://www1.jus.com.br/DOUTRINA/texto.asp?id=1829. Arquivo consultado em 23 de outubro de 2010.

MELICK, Greg. **Law Enforcement in Cyberspace**. Australia: National Crime Authority, 2010. [online] Disponível na Internet via WWW. ULR: http://www.isrcl.org/Papers/Melick.pdf. Arquivo consultado em 25 de outubro de 2010.

MENDES, Nelson Pizotti. **Problemas atuais da criminologia**. São Paulo: Resenha Universitária, 1976.

MILLER, Frederic P; VANDOME, Agnes F; MCBREWSTER, John. **Malware**. Mauritius: VDM Publishing House, 2009.

MILLER, James. **Making the Most of the Internet**: And the Other Less/More Important Things in Life. East Green Farm: Daisy Analysis Ltd., Janeiro de 2006.

MIRANDA, Marcelo Baeta Neves. **Abordagem dinâmica aos crimes via Internet**. Jus Navigandi, Teresina, a. 4, n. 37, dez. 1999. [online] Disponível na Internet via WWW. URL: http://socorromultiply.multiply.com/notes/item/617. Arquivo consultado em: 23 de outubro de 2010.

MPF. **Crimes cibernéticos**: manual prático de investigação, São Paulo, Abril de 2006.

NICOLESCU, Basarab. **O Manifesto da Transdisciplinaridade**, 3.ed. São Paulo: TRIOM, 2005.

NIGRI, Deborah Fisch. **Crimes e Segurança na Internet**. In: Doutrina jurídica brasileira, Caxias do Sul: Editora Plenum, 2001.

OSTROCK, Guilherme. **DoS é crime?** [online] Disponível na Internet via WWW. URL: http://www.infolei.com.br/dos-e-crime/. Arquivo consultado em 23 de outubro de 2010.

PAESANI, Liliana Minardi. **Direito e Internet**. São Paulo: Atlas, 2000.

PEDROSO, Fernando de Almeida. **Competência Penal**. Belo Horizonte: Livraria Del Rey Editora, 1998.

RAHAL, Flávia; GARCIA, Roberto Soares. **Vírus, direito à intimidade e a tutela penal da Internet**. In: Revista do Advogado. v. 23, n. 69, São Paulo: maio de 2003.

RAYSMAN, Richard; BROWN, Peter. **Computer Law**: drafting and negotiating forms and agreements, v. 2. New York: Law Journal Press, 1984.

REIS, Maria Helena Junqueira. **Computer Crime**. Belo Horizonte: Livraria Del Rey Editora, 1997.

RODRIGUES, Francisco de Assis. **A tutela penal dos sistemas de computadores**. [online] Disponível na Internet via WWW. URL: http://jus2.uol.com.br/doutrina/texto.asp?id=2813&p=2. Arquivo consultado em 23 de outubro de 2010.

ROHRMANN, Carlos Alberto. **Curso de Direito Virtual**. Belo Horizonte: Del Rey Editora, 2005.

ROVER, Aires José. **Crimes de Informática**. [online] Disponível na Internet via WWW. URL: http://www.infojur.ufsc.br/aires/arquivos/CRIMES%20DE%20INFORMATICA%20public.pdf. Arquivo consultado em 23 de outubro de 2010.

ROXIN, Claus. **Täterschaft und Tatherrschaft**. Beck, 1994

SAFERNET. **Brasil não pode aderir a Convenção de Budapeste sobre o Cibercrime**. [online] Disponível na Internet via WWW. URL: http://www.safernet.org.br/site/noticias/brasil-n%C3%A3-pode-aderir-conven%C3%A7-budapeste-sobre-cibercrime. Arquivo consultado em 25 de outubro de 2010.

SANTOS, Juarez Cirino dos. **Direito Penal**: Parte Geral, 2. ed. Curitiba: ICPC; Lumen Juris, 2007.

SHEPLEY, Phil. **What is a computer chip?** [online] Disponível na Internet via WWW. URL: http://www.wisegeek.com/what-is-a-computer-chip.htm. Arquivo consultado em 23 de outubro de 2010.

SILBERSCHATZ, Abraham; GALVIN, Peter Baer; GAGNE, Greg. **Operating system concepts**, 8 ed. Wiley & Sons, 2008.

SIEGEL, Larry J. **Criminology**, 10. ed. Belmont, CA: Cengage Learnin Inc., 2008.

SILVA, Rita de Cássia Lopes. **Direito Penal e Sistema Informático**. *In* Ciência do Direito Penal Contemporâneo, v. 4. São Paulo: RT, 2003.

STANDLER, Ronald B. **Computer Crime**, 1999. [online] Disponível na Internet via WWW. URL: http://www.rbs2.com/ccrime.htm. Arquivo consultado em 22 de outubro de 2010.

STEVENSON, Larry; ALTHOLZ, Nancy. **Rootkit for Dummies**. Hoboken: Wiley Publishing Inc., 2007.

SULLIVAN, Dan. **The Definition Guide to Controlling Malware, Spyware, Phishing and Spam**. RealtimePublishers.com, 2007.

TORRES, Gabriel. **Hardware**: Curso Completo. 4. ed. Rio de Janeiro: Axcel Books, 2001.

_____. **Redes de Computador**: Versão Revisada e Atualizada, 1. ed. São Paulo: Novaterra, 2009.

TOURINHO FILHO, Fernando da Costa. **Processo Penal,** v. II. 24. ed. ver. e atual. São Paulo: Saraiva, 2002.

UNITED NATIONS. **International review of criminal policy**: United Nations Manual on the prevention and control of computer-related crime, 1999. [online] Disponível na Internet via WWW. URL: http://www.uncjin.org/Documents/irpc4344.pdf. Arquivo consultado em 25 de outubro de 2010

VIANNA, Túlio Lima. **Dos crimes pela internet**. Belo Horizonte: UFMG, 2000.

_____. **Fundamentos de Direito Penal Informático**: Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Editora Forense, 2003.

WAMBIER, Luiz Rodrigues. **Anotações sobre o princípio do devido processo legal**. São Paulo: RT, 1989.

5.1. SITES CONSULTADOS

CGI.BR. http://www.cgi.br.

HTTRACK. http://www.httrack.com.

INHOPE. http://www.inhope.org.

SAFERNET. http://www.safernet.org.br.

STJ. http://www.stj.jus.br.

STF. http://www.stf.jus.br.

The LIBRARY of CONGRESS. http://www.loc.gov.

6. ANEXOS

6.1. S.773 - Cybersecurity Act of 2009

4/1/2009--Introduced.Cybersecurity Act of 2009 - Directs the President to establish or designate a Cybersecurity Advisory Panel to advise the President. Defines "cyber" as:
(1) any process, program, or protocol relating to the use of the Internet or an intranet, automatic data processing or transmission, or telecommunication via the Internet or an intranet; and
(2) any matter relating to, or involving the use of, computers or computer networks.Directs the Secretary of Commerce to:
(1) develop and implement a system to provide cybersecurity status and vulnerability information regarding all federal information systems and networks managed by the Department of Commerce; and
(2) provide financial assistance for the creation and support of Regional Cybersecurity Centers for small and medium sized U.S. businesses. Requires the National Institute of Standards and Technology (NIST) to establish cybersecurity standards for all federal government, government contractor, or grantee critical infrastructure information systems and networks. Makes NIST responsible for U.S. representation in all international cybersecurity standards development. Directs the Secretary to develop or coordinate a national licensing, certification, and recertification program for cybersecurity professionals and makes it unlawful to provide certain cybersecurity services without being licensed and certified. Requires Advisory Panel approval for renewal or modification of a contract related to the operation of the Internet Assigned Numbers Authority. Requires development of a strategy to implement a secure domain name addressing system. Requires the National Science Foundation (NSF) to support specified types of research and to establish a program of grants to higher education institutions to establish cybersecurity testbeds. Amends the Cybersecurity Research and Development Act to expand the purposes of an existing program of computer and network security research grants. Requires the NSF to establish a Federal Cyber Scholarship-for-Service program. Requires NIST to establish cybersecurity competitions and challenges to recruit talented individuals for the federal information technology workforce and stimulate innovation. Requires the Department of Commerce to serve as the clearinghouse of cybersecurity threat and vulnerability information. Grants the Secretary access to all relevant data concerning such networks notwithstanding any law or policy restricting access. Directs the President to:
(1) develop and implement a comprehensive national cybersecurity strategy;
(2) on a quadrennial basis, complete a review of the cyber posture of the United States; and
(3) work with representatives of foreign governments to develop norms, organizations, and other cooperative activities for international engagement to improve cybersecurity. Requires the Director of National Intelligence and the Secretary of Commerce to submit to Congress an annual report on cybersecurity threats to and vulnerabilities of critical national information, communication, and data network infrastructure. Establishes a Secure Products and Services Acquisitions

Board to review and approve high value products and services acquisition and establish validation standards for software to be acquired by the federal government.

6.2. S.3480 - Protecting Cyberspace as a National Asset Act of 2010

6/10/2010--Introduced.Protecting Cyberspace as a National Asset Act of 2010 - Establishes in the Executive Office of the President an Office of Cyberspace Policy, which shall:
(1) develop a national strategy to increase the security and resiliency of cyberspace;
(2) oversee, coordinate, and integrate federal policies and activities relating to cyberspace security and resiliency;
(3) ensure that all federal agencies comply with appropriate guidelines, policies, and directives from the Department of Homeland Security (DHS), other federal agencies with responsibilities relating to cyberspace security or resiliency, and the National Center for Cybersecurity and Communications (established by this Act); and
(4) ensure that federal agencies have access to, receive, and appropriately disseminate law enforcement, intelligence, terrorism, and any other information relevant to the security of specified federal, military, and intelligence information infrastructure. Requires the President to appoint a Director of Cyberspace Policy. Provides for access by the Director to specified cybersecurity-related information. Amends the Homeland Security Act of 2002 (HSA) to establish within DHS a National Center for Cybersecurity and Communications (NCCC), which shall be headed by a Director, who shall:
(1) work cooperatively with the private sector and lead the federal effort to secure, protect, and ensure the resiliency of the federal and national information infrastructure; and
(2) work with the Assistant Secretary for Infrastructure Protection to coordinate the information, communications, and physical infrastructure protection responsibilities and activities of NCCC and the Office of Infrastructure Protection. Transfers to NCCC the National Cyber Security Division, the Office of Emergency Communications, and the National Communications System. Establishes within NCCC the United States Computer Emergency Readiness Team (US-CERT), which shall:
(1) collect, coordinate, and disseminate information on risks to specified federal information infrastructure and security controls; and
(2) establish a mechanism for engagement with the private sector. Requires the NCCC Director to:
(1) establish a program for sharing information with and between NCCC and other federal agencies;
(2) develop guidelines to protect the privacy and civil liberties of U.S. persons and intelligence sources and methods;
(3) establish a program to promote and provide technical assistance relating to the implementation of best practices and related standards and guidelines for securing the national information infrastructure; and
(4) identify and evaluate the cyber vulnerabilities to covered critical infrastructure on a continuous and sector-by-sector basis and issue regulations establishing risk-based security performance requirements to secure covered critical infrastructure against cyber vulnerabilities. Authorizes the President to issue a declaration of a national cyber emergency to covered critical infrastructure. Requires the President to then notify the owners and operators of the infrastructure of the nature of the emergency, consistent with the protection of intelligence sources and methods. Requires the NCCC Director to take specified steps, including immediately directing the owners and operators to implement required response plans and to ensure that

emergency actions represent the least disruptive means feasible to operations. Terminates such an emergency measure or action 30 days after the President's declaration, with 30-day extensions authorized if the NCCC Director or the President affirms that such measure or action remains necessary to address the continuing emergency. Requires each owner or operator of covered critical infrastructure to certify to the NCCC Director whether the owner or operator has developed and implemented approved security measures and any applicable emergency measures or actions required for any cyber vulnerabilities and national cyber emergencies. Sets forth civil penalties for violations. Requires the DHS Secretary and the private sector to develop, periodically update, and implement a supply chain risk management strategy designed to ensure the security of the federal information infrastructure. Sets forth provisions regarding the information security authority and functions of the NCCC Director and executive agency responsibilities. Requires NCCC to annually oversee, coordinate, and develop guidance for the effective implementation of operational evaluations of the federal information infrastructure and agency information security programs and practices to determine their effectiveness. Authorizes the NCCC Director to order the isolation of any component of the federal information infrastructure if:
(1) an agency does not implement measures in an approved risk-based plan; and
(2) the failure to comply presents a significant danger to the federal information infrastructure. Establishes in the executive branch a Federal Information Security Taskforce, which shall be the principal interagency forum for collaboration regarding best practices and recommendations for agency information security and the security of the federal information infrastructure. Requires each agency with an Inspector General appointed under the Inspector General Act of 1978 to assess the adequacy and effectiveness of the information security program and evaluations. Requires the Director of the Office of Personnel Management (OPM) and the NCCC Director to assess the readiness and capacity of the federal workforce to meet the needs of the cybersecurity mission of the federal government. Requires the OPM Director to develop and implement a comprehensive workforce strategy that enhances the readiness, capacity, training, and recruitment and retention of federal cybersecurity personnel. Requires the head of each federal agency to:
(1) develop a strategic cybersecurity workforce plan as part of its performance plan; and
(2) measure and collect information on indicators of the effectiveness of the recruitment and hiring of a workforce needed to fulfill the agency's cybersecurity mission. Requires the OPM Director, in coordination with:
(1) the NCCC Director, to develop and issue comprehensive occupation classifications for federal employees engaged in cybersecurity missions; and
(2) the NCCC Director, the Director of National Intelligence, the Secretary of Defense (DOD), and the Chief Information Officers Council, to establish a cybersecurity awareness and education curriculum that shall be required for all federal employees and contractors engaged in the design, development, or operation of agency information infrastructure. Amends HSA to direct the Under Secretary for Science and Technology, in coordination with the NCCC Director, to carry out a research and development program for the purpose of improving the security of information infrastructure. Directs the DHS Secretary to establish a National Cybersecurity Advisory Council to advise the NCCC Director.