A Tutela Penal do Patrimônio no âmbito da *Internet*

Por Fábio Portela Lopes de Almeida
Orientado por Ela Wiecko Volkmer de Castilho

1. Introdução

A *Internet* tem crescido exponencialmente nos últimos anos, proporcionando a gênese de uma série de novas relações inter-pessoais, tanto em nível nacional quanto em nível internacional.

A *Internet*, em sua forma original, era uma pequena rede de computadores com finalidade militar denominada *ARPAnet*, projetada no contexto da Guerra Fria (ARPA vem de *Advanced Research Projects Agency*, ou Agência Avançada de Desenvolvimento de Projetos)[1], cuja arquitetura foi desenvolvida entre os anos de 1959 e 1969. O objetivo inicial da *ARPAnet* era

[1] LYNCH, Daniel C. *Dinheiro Digital: o comércio na Internet*. Rio de Janeiro: Campus, 1996. p. 4

desenvolver um sistema de comunicação imune a um ataque nuclear, conforme nos atesta Manuel CASTELLS[2].

Em 1969 a *ARPAnet* era composta por apenas quatro computadores "*host"* [3]: SRI *International*, Universidade de Los Angeles, Universidade de Santa Bárbara e Universidade de Utah.

Na década de 1970, universidades e outras instituições, normalmente de origem militar, obtiveram permissão para se conectar à *ARPAnet*, propiciando seu crescimento. Em Dezembro de 1970, o *Network Working Group* (NWG) desenvolveu o primeiro Protocolo *Host-to-host* (denominado *Network Control Protocol – NCP*), que permitia aos usuários da rede o desenvolvimento de aplicações para a mesma. O Protocolo é, conforme nos assegura Gustavo CORRÊA: "uma designação formal dos formatos de mensagens e de regras de dois computadores que precisam ser seguidos para que possa haver troca de mensagens." [4] Ou seja, o protocolo permite a comunicação entre dois computadores distintos.

Em 1972, realizou-se a primeira demonstração pública da *ARPAnet*, na Conferência Internacional de Comunicação entre Computadores (ICCC). Também em 1972 o correio eletrônico, mais comumente conhecido por *e-mail*, foi desenvolvido.[5]

Apesar do desenvolvimento do *NPC* e dos recursos possibilitados por ele, com o crescimento da *ARPAnet* este protocolo tornou-se obsoleto e fez-se necessária a criação de um novo protocolo, o TCP/IP (*Transmission Control Protocol / Internet Protocol)*. A novidade do TCP/IP é que este proporciona confiabilidade, o grande defeito do protocolo anterior. A comunicação entre

---

[2] CASTELLS, Manuel. *A Sociedade em Rede – A Era da Informação: Economia, Sociedade e Cultura*. São Paulo: Paz e Terra, 1999. p. 375

[3] *Host,* do inglês, significa hospedeiro. Em informática, o termo é aplicado ao computador central de uma rede, aquele que "hospeda" os *sites* e dá acesso aos outros computadores da rede.

[4] CORRÊA, Gustavo Testa. *Aspectos jurídicos da Internet*. São Paulo: Saraiva, 2000

[5] *A Brief History of the Internet.*. Disponível em: www.isoc.org/internet-history/brief.html

computadores é realizada da seguinte forma: os dados a serem enviados por meio da rede são divididos em “pacotes” menores de informação, de modo que cada “pacote” tem a informação do computador de origem e do computador de destino, bem como a sua organização dentre todos os “pacotes”, para que a informação esteja ordenada no computador de destino, e se torne inteligível. A diferença entre os dois protocolos é a seguinte: enquanto no NPC, caso algum dos pacotes se perdesse no caminho, o protocolo paralisava todo o processo, tornando-se necessário seu reinício. Com o protocolo TCP/IP, ocorria diferentemente: os pacotes são enviados de um computador a outro até alcançarem o destino e, caso algum deles se perca, o emissor original o reenvia, corrigindo o erro do protocolo anterior. Além disso, o protocolo TCP/IP, que é utilizado até hoje, permitia o crescimento quase ilimitado da rede.

A *ARPAnet* estava aberta tanto aos meios acadêmicos quanto aos militares, e seus integrantes começaram a utilizá-la para todos os tipos de comunicação, fez-se necessária uma divisão entre a *ARPAnet* (dedicada ao uso acadêmico) e a MILNET (dedicada aos objetivos militares), o que ocorreu em 1983. Ainda nos anos 80, a Fundação Nacional da Ciência criou outra rede científica, a CSNET e, com a cooperação da IBM, foi criada ainda uma rede para estudos não-científicos, a BITNET. Todas estas redes tinham em comum o fato de dependerem da *ARPAnet* original como sistema de comunicação, ou seja, esta se tornou uma espécie de rede das redes, que foi chamada de ARPA-INTERNET e, mais tarde, apenas *Internet.*

No Brasil, os primeiros acessos à *Internet* ocorreram em 1988, no Laboratório Nacional de Computação Científica (LNCC, no Rio de Janeiro) e na Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp). Na verdade, não eram conexões diretas à *Internet,* mas à BITNET. Em 1989, a *Internet* começava a sair do âmbito acadêmico no Brasil, com a iniciativa pioneira do Instituto Brasileiro de Análises Sociais e Econômicas (Ibase), ao

criar o BBS Alternex, que possibilitava a troca de e-mails e grupos de discussão conectados à *Internet*.

A primeira conexão real à *Internet* no Brasil ocorreu em 1991, através da Fapesp, mas só em 1994 os primeiros servidores *World Wide Web* (WWW)[6] entraram em funcionamento. Apesar deste relativo atraso na abertura da *Internet* para o público não-acadêmico, já no final de 1995 eram 120.000 usuários brasileiros[7], número que cresceu até 7.675.000 de usuários em fins de 1999[8], denotando um crescimento de 6.395% em 4 anos.

Desta sorte, temos que a *Internet* atingiu uma importância efetiva em nossa sociedade, inclusive em termos econômicos.

A *Internet*, com sua estrutura e tecnologia, apesar de ser relativamente anárquica, pois não se submete a regime jurídico-político algum, envolve toda uma sociedade global. As estimativas indicam que no ano de 2010 serão 600.000.000 de usuários em todo o planeta, o que deverá representar algo em torno de 8% da população mundial.[9]

No presente estudo, devemos considerar a *Internet* não apenas como uma rede integrada de computadores, mas como um instrumento de coesão e integração social. José Henrique BARBOSA NETO[10] considera, inclusive, que a *Internet* levou à criação de uma nova sociedade: "A *Internet* propiciou o surgimento de uma nova sociedade, uma sociedade ao mesmo tempo virtual e global. Essa sociedade, formada de estratos culturais heterogêneos, tornou possível o aparecimento do denominado 'mundo virtual' ou 'ciberespaço'."

---

[6] A *World Wide Web* tornou mais fácil o uso da *Internet*, do ponto de vista da *interface* com o usuário. Consiste em arquivos e diretórios espalhados pela *Internet*, interligados por *links* de hipertexto (palavras-chave dispostas em um *site* e redirecionam o navegador para outros *sites*, que podem estar em qualquer outro computador da rede.)

[7] ERCÍLIA, Maria. *A Internet* – Coleção A Folha Explica. São Paulo: Publifolha, 2000

[8] Dados do Instituto Datafolha

[9] CORRÊA, *op. cit.*

[10] Palestra proferida no 1º fórum de Debates Jurídicos Via Internet realizado na Universidade Luterana do Brasil – ULBRA, Canoas – RS. Disponível em *www.juridica.com.br/Apres_Artigo.asp?CodArtigo=38*

Em 1996, a *Internet* já tinha cerca de 40.000.000 de usuários, sendo que destes, 160.000 eram brasileiros.[11] De acordo com pesquisa realizada pelo Instituto Datafolha[12], em fins de 1999 eram 220.045.000 de usuários na *Internet* somente nos 15 países que têm maior número de usuários, o que representa algo em torno de 3,6 % da população mundial. Somente no Brasil, no final de 1999, havia cerca de 7.675.000 usuários.

Economicamente, a importância da *Internet* também vem crescendo de maneira acelerada. Em 1997, somente nos Estados Unidos da América, o comércio feito por meio da *Internet* foi valorado em torno de US$ 2.108.000.000,00. Em apenas dois anos, este número cresceu para US$ 271.200.000.000,00. [13] Ou seja: se em 1997 os norte-americanos gastaram o equivalente ao PIB do Paraguai, em 1999 foi gasto o equivalente a um quinto do PIB brasileiro, o que demonstra a velocidade com que o comércio *online* vem crescendo e a importância econômica da I*nternet.*

No entanto, a *Internet* não tem sido utilizada apenas para os fins para os quais originalmente foi criada, quer dizer, principalmente ao final da década de 1980, com a abertura de seu uso ao público em geral, ampliaram-se também suas possibilidades, que não mais seriam restritas ao âmbito acadêmico, cultural ou militar. Desta sorte, ao mesmo tempo em que surgiram novas possibilidades de uso pacífico deste meio, também criaram-se meios de deturpação de seu uso. Neste sentido, por exemplo, temos a utilização da *Internet* para o extravio de cartões de crédito, o extravio de informações confidenciais de empresas e mesmo governamentais, a disseminação de mensagens racistas por meio de *home pages*, dentre outras condutas gravosas à sociedade. No entanto, em muitos destes casos, talvez por uma certa ausência de legislação específica para estas condutas, ainda não há uma persecução penal eficiente que permita a proteção aos diversos bens jurídicos tutelados pelo Direito Penal. Tendo em vista

[11] Fonte: MORON, Fernanda de Almeida. *A Internet e o Direito*. Disponível em: <www.juridica.com.br/Apres_Artigo.asp ?CodArtigo=23> Acesso em: 12/11/2000
[12] ERCÍLIA, *op. cit.*

a abrangência do tema, optou-se por analisar, nesta pesquisa, apenas as condutas (e seu tratamento jurídico-penal) que lesem o bem jurídico Patrimônio.

Outrossim, há também uma questão subsidiária que norteará toda a pesquisa: é realmente necessária uma nova legislação que crie novos tipos penais com a finalidade de proteger o patrimônio, ou os tipos existentes no Código Penal Brasileiro já são suficientes para efetivamente realizar tal proteção?

2. O Direito Penal Mínimo

Desde os primórdios da civilização, o Direito Penal representou um meio viável de evitar a vingança generalizada, i. é., a situação em que um homem, ao ser violentado em algum de seus direitos, buscava a justiça de punho próprio, sem recorrer a nenhuma instituição. Todavia, apesar de representar uma alternativa a esta situação de barbárie, o Direito Penal acabou por gerar um meio próprio de vingança institucionalizada.

De qualquer modo, há de se convir que o Direito Penal representou um avanço real, diante das inúmeras possibilidades de reação frente à violência. No entanto, a história do Direito Penal não é a história de sua abolição.[14] É, na verdade, a história dos abusos praticados pelo Estado e pelos indivíduos que abusam do poder a si delegados. Tal constatação permite recomendar que haja uma racionalização do sistema interventivo penal, possibilitando que se o minimize ao máximo: nenhum Estado que se Democrático de Direito pode ser conivente com o emprego desmedido da violência pública, mesmo que instituída.

Constitucionalmente, temos, numa simples alusão ao art. 5º, de maneira geral, que a proteção à inviolabilidade da vida, da igualdade, da integridade física, da propriedade, etc., representam uma manifestação de que o postulado fundamental

---

[13] Fonte: Nua internet surveys. Disponível em: <*www.nua.ie*> Acesso em: 09/10/2000

[14] QUEIROZ, Paulo de Souza. *Do Caráter Subsidiário do Direito Penal – Lineamentos para um direito penal mínimo*. Belo Horizonte: Del Rey, 1998. p. 23

do Estado Democrático é a regra da liberdade, surgindo a não-liberdade como exceção. A Carta Magna pressupõe a liberdade como um dos valores supremos constitucionais, somente admitindo a não-liberdade à absoluta necessidade social à adequação da intervenção penal.

É neste sentido, que no desenrolar do presente texto, adotou-se como teoria de base a linha do **Direito Penal Mínimo**, que preza pela intervenção penal apenas nos casos extremos, necessários para que haja paz e harmonia social.

3. Aspectos Técnicos da Internet

O objetivo deste capítulo é estudar o funcionamento completo da *Internet*, desde a integração dos computadores na rede até a análise dos *softwares* utilizados tanto para a comunicação entre os computadores quanto para a prática das condutas a serem discutidas posteriormente. No entanto, a fim de proporcionar um entendimento completo deste tema, tendo em vista o fato desta ser uma monografia jurídica e os conceitos aqui referidos serem oriundos da Ciência da Computação e da Informática, a precisão semântica não será tão rígida, o que não seria necessário para atingir o objetivo de informar as possibilidades e estrutura básica da *Internet*.

Assim, a primeira pergunta que devemos formular para atingir a proposta deste capítulo é: o que é a *Internet* e como ela funciona? Segundo Lars DAVIES[15]:

[15] DAVIES, Lars. *Contract Formation on the Internet – Shattering a few myths*. In*: Law and the Internet – Regulating Cyberspace*. Oxford: Hart Publishing, 1997. p. 100

Trad: "A primeira e talvez mais importante coisa a saber sobre a *Internet* é que ela não existe realmente. Não existe nenhuma coisa como a *Internet*. Este afirmação pode parecer um pouco estranha tendo em vista a grande publicidade que a "*Internet"* tem recebidonos últimos anos, mas permanece sob exame constante. O que realmente existe é um grupo de desenvolvimento de redes de comptadores nacionais e internacionais, privados e públicos que conectam-se e comunicam-se entre si, e são estas redes, quando tomadas em conjunto, o que forma a "coisa" a qual as pessoas comumente referem-se excitadamente como a "*Internet"*. Qualquer domínio ou controle que puder existir prevalece em cada uma destas redes discretas que fazem o caminho para o que é a *Internet*."

> *"The first and perhaps most important thing to know about the Internet is that it does not actually exist. There is no such thing as the Internet. This statement may seem a little strange given the vast publicity that the "Internet" has received over the past couple of years but it stands examination nevertheless. What does exist is a developing group of national and international, private and public computer networks which can and do connect to and communicate with each other, and it is these networks, when taken together, which form the thing which people often refer to excitedly as the "Internet". There is, therefore, no single entity which controls the Internet. Instead any ownership and control which may exist vests in each of the discrete networks that make up the patchwork that is the Internet."*

Percebe-se, assim, que a *Internet* não existe como entidade autônoma: é apenas, conforme observado no capítulo anterior, uma rede de computadores que é integrada por diversas outras redes menores, unidas pela capacidade de comunicação, uma com as outras.

Característica importante da *Internet* passível de ser apreendida do trecho supra-selecionado é a independência e autonomia de cada uma destas redes de computadores, uma vez que estas não são (necessariamente[16]) dependentes de ordem jurídica alguma, sendo composta por computadores públicos e privados, nacionais e internacionais.

Os computadores que integram as redes, a fim de se comunicar, utilizam-se de protocolos. No entanto, os computadores não se comunicam por meio de alfabetos fonéticos, e sim por meio da linguagem binária, que é composta de apenas dois significantes: o zero e o um. Na verdade, o significado destes não é numérico, uma vez que apenas representam estados: ligado ou desligado, verdadeiro ou falso, preto ou branco. A denominação técnica de cada um destes significantes é *bit*. Sobre a importância dos *bits,* NEGROPONTE[17] afirma: "os bits sempre foram a partícula subjacente à computação digital, mas, ao longo dos últimos 25 anos, expandimos bastante nosso vocabulário binário, nele incluindo muito mais do que apenas números. Temos sido capazes de digitalizar diferentes tipos de informação, como áudio e vídeo, reduzindo-os

[16] Obviamente, há a possibilidade de um computador – ou uma rede – ser subordinado e regulado por determinada ordem jurídica, o que não faz deste fato a regra geral para os computadores integrantes da *Internet.*

[17] NEGROPONTE, Nicholas. *A Vida Digital.*. São Paulo: Companhia das Letras, 1995. p. 19

também a uns e zeros." Os *bits*, fisicamente, são uma representação de impulsos elétricos: se o impulso estiver presente, o computador registra "1"(ligado); se estiver ausente, registra "0"(desligado).

Assim, a linguagem utilizada pelos computadores é o *bit*. Ao conjunto de 8 *bits* forma-se uma estrutura denominada *byte*, de maior significância para nosso estudo. O número de 8 *bits* na composição de um *byte* não foi definido por acaso: uma seqüência de 8 bits representa a possibilidade de 256 estados diferentes e é nestes estados que toda a informação é registrada na memória do computador. O padrão *byte* é utilizado porque, com ele e suas 256 combinações, criou-se a tabela ASC II, que torna possível a inteligibilidade dos zeros e uns na linguagem humana (a tabela ASC II contém a representação de todas as letras do alfabeto, os números e alguns outros elementos gráficos na linguagem de máquina.) Assim, por exemplo, o "A" do alfabeto é representado por uma seqüência de 8 *bits* (um *byte*): 01000001.

Entendida a linguagem de máquina, resta ainda compreender o processo de comunicação entre computadores, uma vez que é em falhas neste processo que os *hackers*[18] atuam, praticando as condutas a serem estudadas posteriormente nesta monografia.

Os computadores comunicam-se por meio de protocolos, sendo que o mais utilizado é o TCP/IP, já referido no primeiro capítulo. O protocolo permite a comunicação entre computadores distintos utilizando duas técnicas. Na primeira, o protocolo divide a informação a ser compartilhada em pequenos pacotes (*packets)*, que chegam ao computador de destino ordenadamente. Nota-se que cada *packet* pode tomar um caminho diferente na *Internet*, seguindo por computadores distintos, mesmo que em países diferentes. Na segunda, o protocolo manipula o mecanismo de endereçamento dos computadores, permitindo que cada máquina procure, identifique e se

[18] Neste ponto, a precisão terminológica científica cede espaço à realidade, pois *hacker* é o termo comumente utilizado para designar os indivíduos que, com seu conhecimento, compromete a segurança da rede.

comunique com a outra. O endereçamento de cada computador é composto por números compostos por 32 *bits*, ou seja, são 4 algarismos, e denominam-se *Internet Protocol (IP) address*. É esse endereço (*address*) que indica a localização do computador na rede.

Além do TCP/IP, existem outros protocolos, cada qual com uma função distinta no estabelecimento da comunicação da rede: o *Address Resolution Protocol* (ARP), o *Internet Control Message Protocol* (ICMP e o *Simple Mail Transfer Protocol* (SMTP)[19]. O ARP é um protocolo cuja função consiste em permitir o mapeamento dos endereços na *Internet* transformando-os em endereços físicos e identificando a origem de cada pacote de dados que estão sendo transmitidos. A função do ICMP é controlar mensagens que são transmitidas entre os computadores durante o processo de transferência de dados. Já o SMTP é o protocolo que permite o envio de mensagens via *e-mail.*

Na *Internet* existem duas categorias básicas de computadores, segundo a sua função: clientes e servidores. O servidor é o computador que utiliza programas para providenciar acesso à rede, enquanto o cliente é o computador que pode acessar os serviços disponíveis pelo servidor. Nota-se que um único computador pode servir às duas funções (servidor e cliente), indistintamente. Um exemplo prático da comunicação entre computadores é citado por Lars DAVIES[20]: o *e-mail.* Segundo o autor, a percepção que o usuário tem ao enviar o e-mail é a seguinte: ele utiliza um programa de correio eletrônico para redigir o *e-mail*, endereça a mensagem para o destinatário e o envia. No entanto, o que ocorre é o seguinte: o programa de correio eletrônico (*Outlook Express*, por exemplo) envia a mensagem para o servidor do usuário que está enviando o *e-mail*, que o manda para o servidor do destinatário e este, por sua vez, posta a mensagem para o computador cliente do usuário. Na verdade, toda a comunicação feita por computadores cliente pela *Internet* ocorre

[19] GOMES, Olavo José Anchieschi. *Segurança Total – Protegendo-se Contra os Hackers*. São Paulo: Makron Books, 2000. p. 8-10
[20] *Op. cit.* p. 102

desta maneira, indiretamente, pois depende tanto do servidor do usuário quanto do servidor do destinatário, que oferece serviços, como o *e-mail* e o acesso a *sites*.

Identificada a estrutura técnica da *Internet*, resta dissertar sobre as principais técnicas utilizadas para pelos *hackers p*ara invadir um sistema e realizar cada uma das condutas a serem estudadas.

A primeira técnica consiste no *Scanner.* O *scanner* é um *software* que detecta as falhas de segurança de um computador, o que pode permitir a obtenção de informações-chave para que um sistema de computador seja invadido. Além disso, o *scanner* permite a localização de qualquer computador específico na *Internet*, facilitando o processo de invasão.

Uma segunda técnica, mais específica e que permite diretamente (uma vez que o *scanner* é apenas uma técnica indireta, uma vez que com as informações obtidas através dele um *hacker* pode acessar um sistema informático e utilizar-se de outras técnicas para tirar proveito desta invasão.) a prática delituosa é o *cracking* (*to crack,* em inglês, significa quebrar), que consiste em destruir um sistema de segurança, descobrindo a chave de acesso (que pode ser uma senha, por exemplo, ou um avançado sistema criptográfico). O *cracking* pode ser utilizado para descobrir números de cartões de crédito ou desativar a proteção de uma senha qualquer, conforme atestado por Olavo GOMES[21].

Outra maneira de invadir e danificar um sistema informático, causando prejuízos para aqueles que dele dependem, é a disseminação de vírus, que pode ser realizada de diversas maneiras, uma vez que a entrada de dados em um computador pode ser feita via CD-ROM, disquetes e, obviamente, pela *Internet.* O vírus nada mais é que um *software* que visa a destruição (ou

---

[21] *op. cit.* p. 69-91

alteração) de dados na máquina infectada, bem como sua proliferação, infectando novas máquinas. Antes do advento da *Internet*, este processo era relativamente mais lento e controlável, uma vez que a única forma de comunicação entre computadores era por meio de disquetes. No entanto, com a *Internet*, os computadores podem comunicar-se com mais facilidade, e a disseminação dos vírus ocorre cada vez mais rapidamente. Em março de 1999, por exemplo, o vírus Melissa[22] espalhou-se por quase todo o planeta, causando milhões em prejuízo. Ele atuava da seguinte forma: após ter infectado um computador, procurava a lista de *e-mails* disponível no computador infectado e enviava uma réplica do vírus para os 50 primeiros endereços encontrados, infectando assim 50 novas máquinas.

Outra técnica utilizada para a invadir e danificar um computador (ou mesmo uma rede de computadores) é o chamado *trojan horse* (ou cavalo de tróia). Assim como o *scanner*, o *trojan horse* também é um *software*. No entanto, enquanto aquele se presta apenas a fornecer informações de um sistema informático para o usuário do programa, este possibilita diversas funções. Um *trojan horse* denominado *Back Orifice*, por exemplo, permite que o *hacker* obtenha controle integral do sistema infectado, possibilitando que arquivos sejam deletados, lidos e alterados.[23]

A última técnica relatada por Olavo GOMES[24] é o *Sniffer* (ou ataque por monitoração), que é qualquer procedimento que permite a captura de informações ao longo da rede. Uma possível utilização desta técnica é a captura de uma senha digitada pelo usuário de um micro-computador, por exemplo. O *sniffer* captura o tráfego da rede, independentemente do protocolo utilizado, e carrega os pacotes de dados transmitidos pela rede, permitindo a futura análise

[22] A história completa do caso encontra-se em *www.cybercrime.gov/melissa.htm*. Acesso em 12/10/2000

[23] GOMES, *op. cit.* 123-137

[24] *Idem.*

dos mesmos. Assim, se o pacote tiver informações pessoais do usuário, estas informações poderão ser lidas e utilizadas por aquele que controlar o *sniffer.*

4. Espaço de Fluxos e Espaço de Lugares

Segundo Manuel CASTELLS[25], a *Internet* insere-se em um contexto maior, o da sociedade da informação, o que envolve tanto as comunicações quanto a estrutura produtiva e econômica sociais. De acordo com o autor, há que se distinguir entre dois paradigmas de espaço: o espaço de lugares e o espaço de fluxos.

Primeiramente, é necessário conceituar o espaço social. O espaço, segundo CASTELLS, é "o suporte material de práticas sociais de tempo compartilhado. Espaço é tempo cristalizado." O espaço de lugares é o espaço comumente observado, historicamente enraizado na nossa experiência comum; já o espaço de fluxos é "a organização material das práticas sociais de tempo compartilhado que funcionam por meio de fluxos." Mas o que são fluxos? São, ainda segundo CASTELLS: "seqüências intencionais, repetitivas e programáveis de intercâmbio e interação entre posições fisicamente desarticuladas, mantidas por atores sociais nas estruturas econômica, política e simbólica da sociedade."

Mas qual seria o suporte material da chamada *era da informação*, do espaço de fluxos? CASTELLS indica três níveis de suportes materiais que, unidas formam o próprio espaço de fluxos. O primeiro nível é constituído por um circuito de impulsos eletrônicos, formando a base material última desta sociedade. É a configuração essencial do espaço de fluxos, uma vez que é neste nível que as práticas simultâneas ocorrem, pois é a infra-estrutura tecnológica formadora da rede. É neste nível que a comunicação via *Internet* atua.

[25] CASTELLS, *op. cit.* 405

O segundo nível do espaço de fluxos constitui-se pelos centros de importantes funções estratégicas e centros de comunicação. Estes centros localizam-se em uma rede eletrônica; são lugares específicos com características (sociais, econômicas, culturais e fucionais) bem definidas. Não necessariamente são "lugares eletrônicos": um exemplo deste segundo nível do espaço de fluxos é citado por CASTELLS[26]:

> "Por exemplo, era improvável que Rochester, Minnesota ou o subúrbio parisiense de Villejuif se tornassem os nós centrais de uma rede mundial de pesquisas e tratamentos médicos avançados, mantendo estreita interação entre si. Mas a localização da Clínia Mayo, em Rochester, e de um dos principais centros da Administração Francesa de Saúde para o tratamento de câncer em Villejuif – em ambos os casos por razões históricas fortuitas – articulou um complexo de geração de conhecimento e tratamento médico avançado ao redor destes dois locais inusitados. Uma vez estabelecidos, esses lugares atraíram pesquisadores, médicos e pacientes de todo o mundo: transformaram-se em um nó da rede médica mundial."

O mesmo ocorre com a *Internet*: os seus nós podem estar espalhados por todo o planeta, mas dentro da lógica interna da rede, podem estar muito próximos.

O terceiro e último nível importante do espaço de fluxos refere-se à organização espacial das elites gerenciais dominantes, responsáveis pelo direcionamento dos fluxos espaciais. Estas elites são os atores sociais que definem a lógica espacial dos interesses dominantes na sociedade. No âmbito da *Internet*, esta elite é menos percebida, uma vez que, pela própria estrutura anárquica da rede, não há um agente social específico que a comande ou a direcione.

5. A Internet e a Lesão ao Patrimônio

Este capítulo dividir-se-á em dois: em uma primeira etapa, verificaremos a possibilidade de criação de uma taxionomia própria para as

[26] *Op. cit.* p. 438

condutas praticadas no âmbito da *Internet,* de modo a facilitar o estudo das mesmas.

Na segunda parte do capítulo, apresentam-se, de modo exemplificativo, as condutas mais comumente encontradas no que tange à *Internet*.

5.1. Classificação dos *Cybercrimes*

Diversas são as classificações propostas para os *cybercrimes* ou *computer crimes*, de acordo com diferentes critérios.

Um primeiro critério consiste na enumeração dos delitos cometidos com o auxílio de um sistema informático, como a proposta por Martine BRIAT[27]. Segundo a autora, estes crimes poderiam ser classificados em:

1) manipulação de dados e/ou programas a fim de cometer uma infração já prevista pelas incriminações tradicionais;

2) falsificação de dados ou de programas;

3) deterioração de dados e de programas e entrave à sua utilização;

4) divulgação, utilização ou reprodução ilícitas de dados e de programas;

5) uso não autorizado a sistemas de informática.

Esta classificação foi baseada no trabalho de Ulrich SIEBER[28], que distingue os *cybercrimes* como:

1) manipulação de dados;

2) espionagem de dados e pirataria de programas;

[27] BRIAT, Martine.*La fraude informatique: une approche de Droit Comparé*. In Revue de Droit Pénal et de Criminologie, n 4.

3) sabotagem de dados;

4) acesso não autorizado aos sistemas.

O critério utilizado pelos supracitados autores é falho, uma vez que a enumeração de condutas, além de não ser um critério científico (posto que, ao enumerar os crimes, deixa-se de contemplar condutas novas que podem surgir com a evolução da tecnologia), é incompleto. É impossível caracterizar todas as condutas criminosas que possam ocorrer pela *Internet*, e sempre haveria lacunas nesta classificação.

Há ainda outros critérios para a classificação dos *cybercrimes*. Um destes é a formulação de um sistema baseado na finalidade visada pelo autor do delito, como quer Jean PRADEL[29]:

1) manipulações para a obtenção de dinheiro;

2) manipulações para a obtenção de informações;

Trata-se de outra classificação desprovida de rigor científico. As motivações que levam os *cyber* criminosos a utilizar-se de seus conhecimentos para fins lesivos a outrem são diversas, assim como a finalidade destas condutas. Assim, esta classificação também não parece satisfatória aos fins do estudo científico.

Classificação pouco mais científica e abrangente é a proposta por Hervé CROZE e Yves BISMUTH[30], cujo critério é baseado na natureza do bem lesionado:

1) os atos dirigidos contra um sistema de informática;

---

[28] SIEBER, Ulrich *Delitos informáticos e outros delitos contra a tecnologia de informação. Comentário e questoionário para o Colóquio da Association Internationale de Droit Penal*. Würzburg, 1992

[29] PRADEL, Jean e FEUILLARD, Cristian. *Les infractions commises au moyen de l'ordinateur*. In Revue de Droit Pénal et de Criminologie, n. 4. Bruxelas, 1985

[30] CROZE, Hervé e BISMUTH, Yves. *Droite de l'Element de Droit à l'Usage dês Informaticiens.* Paris: Econômica: 1986

2) os atos que atentam contra outros valores sociais ou outros bens jurídicos, cometidos através de um sistema de informática.

É uma classificação, apesar de pouco mais abrangente, incompleta. Assim, proponho a seguinte classificação para os crimes envolvendo sistemas informáticos, baseado na posição assumida pelo computador dentro da conduta ilícita:

1) o computador como instrumento do crime;

2) o computador como objeto do crime;

3) o computador como objeto e instrumento do crime.

Na primeira classificação, o computador é utilizado como um mero instrumento para a prática delituosa. Neste sentido, o objeto visado pelo sujeito ativo é diverso da informática, mas o uso do computador é imprescindível para sua consumação. É o que ocorre, por exemplo, quando um *hacker* invade um sistema bancário e consegue transferir valores para sua conta bancária. O computador, neste caso, é apenas um instrumento para a prática de outro crime.

Na segunda classificação, o computador é o próprio objeto material do crime e, na verdade, não se trata de *cybercrime*, uma vez que este é definido como “infração cometida por meio do computador”. Entrariam neste caso condutas comuns no “mundo real” (em oposição a virtual) cujo objeto material seja o computador. Assim, se uma pessoa qualquer furta o computador, pode ser facilmente enquadrada no art. 155 do CP, que trata do crime de furto, sem maiores problemas hermenêuticos.

O terceiro tópico da classificação, assim como o primeiro, encerra o cerne desta monografia. Entendo que este tópico inclui os crimes nos quais existem, basicamente, dois computadores envolvidos: um é instrumento da conduta lesiva e o outro, o objeto do crime. Assim, inclui-se nesta categoria, por

exemplo, a situação na qual um *hacker* invade um computador e altera informações constantes no seu disco-rígido.

5.2. Condutas mais comuns

a) Furto

1. "Estelionatário cibernético é identificado"[31]

O garçom Fábio Florêncio da Silva, apontado como estelionatário[32] na reportagem, foi identificado como responsável pela transferência, , via *Internet*, de dinheiro de contas correntes e aplicações, causando prejuízo a centenas de pessoas.

Na verdade, o autor é parte de uma quadrilha que conta com outros quatro integrantes, também indiciados por estelionato: Luís Cleber da Silva Perecin, José Pereira, Joana dos Santos Silva e Marcela Fontes de França. A quadrilha transferia o dinheiro de agências localizadas em Maceió, Recife, Goiânia, Belém, São José do Rio Preto, e São Paulo capital.

Dentre os prejuízos causados pela quadrilha, a reportagem cita o de José Roberto Barbosa, que perdeu R$ 15.000,00 com as operações.

2. Advogado perde R$ 72.000,00 pela *Internet*[33]

O advogado Bension Coslovisk, apesar de não realizar transações comerciais via *Internet*, teve um prejuízo de R$ 72.000,00 com a transferência de dinheiro de sua conta via *Internet* para a de Jorgina Luiza Nascimento de Carvalho, nome que a polícia desconfia ser falso.

---

[31] ver reportagem em: www.estadao.com.br/tecnologia/internet/2000/out/04/3/6.htm

[32] Não se trata de estelionato. A conduta típica deste crime exige que haja fraude, por meio de artifício, ardil ou qualquer outro meio fraudulento contra **o sujeito passivo** da relação jurídica. No caso dos casos em análise, a suposta fraude é contra o sistema informático. Ora, um sistema informático não tem capacidade de raciocínio sequer para ser enganado. Não faz sentido, portanto, classificar tais condutas dentro do estelionato. Configura-se, outrossim, o crime de furto.

[33] ver reportagem completa em: www.estado.com.br/editorias/2000/10/04/cid3/3.htm

3. Polícia apura golpe eletrônico em correntista[34]

Esta reportagem reflete a preocupação da polícia com os saques indevidos a contas bancárias, muitos deles cometidos pela *Internet.*

Segundo Mauro Marcelo de Lima e Silva, do Setor de Investigação Sobre Crimes de Alta Tecnologia, os golpes variam de R$ 500,00 a R$ 70.000,00.

4. *Hackers* invadem computadores da Nasa[35]

Um rapaz de 16 anos de idade foi condenado a seis meses de detenção, nos Estados Unidos da América, por invadir e obter informações essenciais dos computadores da NASA. O rapaz, além disso, fez *download* de *softwares* de propriedade da NASA, com valor estimado em US$ 1.700.000,00.

b) Dano

1. Ex-empregado de Companhia Norte-americana causa US$ 10.000.000,00 em prejuízo.

Allen Lloyd causou danos irreparáveis aos computadores da companhia de engenharia Omega, de New Jersey, ao ativar um *software* que deletou permanentemente todos os programas de produção da empresa. Ao todo, a Omega perdeu US$ 10.000.000,00 entre produtividade perdida e danos aos computadores.

2. O Caso Melissa

O vírus Melissa espalhou-se por milhares de computadores em todo o planeta, em Março de 1999, infectando-os por meio de e-mails. Ao infectar um computador, o vírus automaticamente copiava seu código e espalhava-se para

[45] ver reportagem em www.estado.com.br/editorias/2000/10/04/cid3/0.htm
[35] www.cybercrime.gov/comrade.htm

50 novos e-mails, crescendo exponencialmente e danificando os computadores. Os prejuízos estimados com o vírus chegaram a US$ 80.000.000,00.

c) Estelionato e outras fraudes

1. Microsoft vítima de estelionatários[36]

Três empresas norte-americanas estão sendo acionadas pela Microsoft por terem elaborado esquema fraudulento contra os consumidores da empresa. O esquema das três empresas (OSCOA, NATM-NET e IWI LLC consistia em enviar a milhões de pessoas e-mails contendo propaganda de *software* da Microsoft. No entanto, o *software* vendido a preços mais baixos era uma falsificação do verdadeiro, e obviamente não continha nenhuma garantia de bom funcionamento. Ao todo, foram 25 milhões de e-mails enviados a usuários de vários países.

2. Fraude à Receita Federal pela *Internet*[37]

Em 1999, no Ceará e no Rio Grande do Norte, foram fraudadas 8.500 declarações via *Internet*, gerando um direito de restituição, em alguns casos, de até R$ 1.000,00 aos fraudadores.

6. Análise Jurídico-penal

6.1. Reinterpretando o conceito de coisa móvel

Neste capítulo far-se-á necessária uma reflexão filosófica sobre o significado e a extensão de alguns conceitos, com a finalidade de adequá-los à nova realidade provocada pela mudança paradigmática ocasionada pelo advento de novas tecnologias, dentre as quais a Internet, aqui estudada.

[36] ver reportagem em: www.i2000.intremoi.com.br/internet-informatica/ll-20101999-1.htm
[37] reportagem em: www.globo.com./noticias/arquivo/economia/20000411/4j8sn.htm

O Direito não poderia ficar alheio a tais mudanças e, conforme ilustra Roberto AGUIAR[38], deve sofrer rupturas para que não pereça frente às novas realidades sociais. Também Roberto LYRA FILHO[39] aponta que o Direito evolui paralelamente à sociedade, posto que evolui com ela:

> "Direito é processo, dentro do processo histórico: não é uma coisa feita, perfeita e acabada; é aquele vir-a-ser que se enriquece nos movimentos de libertação das classes e grupos ascendentes e que definha nas explorações e opressões que o contradizem, mas de cujas próprias contradições brotarão as novas conquistas. "

A evolução do Direito não se dá apenas com a evolução do texto legal; é mister que juízes, advogados, enfim, todos os operadores do Direito interpretem o texto legal e dêem suporte intelectual para que os institutos jurídicos evoluam, adequando-se à sociedade que regem. Com isso concorda Damásio Evangelista de JESUS[40]:

"Interpretar é *inter pretare*m, que deriva de *inter press,* corretor, intermediário, mediador. Intérprete é o mediador entre o texto da lei e a realidade.

A interpretação consiste em extrair o significado e a extensão da norma em relação à realidade."

Prossegue o autor, na pág. 45 da obra supracitada:

> "Interpretação progressiva, adaptativa ou evolutiva é a que se faz adaptando a lei às necessidades e concepções do presente. Como dizia Asúa, o juiz não pode viver alheio às transformações sociais, científicas e jurídicas. A lei vive e se desenvolve em ambiente que muda e evolui e, uma vez que não queiramos reforma-la freqüentemente, é mister adaptar a norma, como sua própria vontade o permite, às novas necessidades da época."

Nota-se, assim, que a Ciência Jurídica dispõe de elementos suficientes para a adequação da instância jurídica à realidade social, o que inclui os comportamentos que ocorrem no âmbito da *Internet*. Todavia, a interpretação,

---

[38] AGUIAR, Roberto A R de. *Os filhos da flecha do tempo: pertinência e rupturas*. Brasília: Letraviva, 2000.

[39] LYRA FILHO, Roberto. *O que é Direito*. São Paulo: brasiliense, 1982. 17ª ed. p. 86

como em todas as ciências, insere-se em determinados paradigmas, muitas vezes difíceis de serem superados. É neste contexto que incluem-se os crimes cometidos por meio de computador e proponho uma interpretação interdisciplinar, com vistas a responder questões jurídicas novas provocadas pelos *cybercrimes.*

Antes de estudarmos os *cybercrimes*, urge fazer alguns esclarecimentos sobre uma questão conceitual que tem surgido por causa das novas perspectivas geradas pela natureza da *Internet*: o conceito de matéria no ambiente dos *bits.*

NEGROPONTE[41] aponta uma perspectiva muito interessante sobre a natureza dos *bits,* comparando-os aos átomos.

Conforme já apontamos, os bits são apenas um registro eletrônico de um estado: ligado ou desligado, verdadeiro ou falso. No entanto, de acordo com NEGROPONTE, fundador do Media Laab, laboratório de multimeios do MIT (*Massachussets Institute of Technology*), os *bits* são mais que isso: são o DNA da informação, a sua estrutura básica. Ainda segundo o autor, os *bits,* em alguns casos, podem valer financeiramente mais do que os átomos. Justifica o autor sua posição exemplificando:

> "Recentemente, visitei o quartel-general de uma das cinco maiores empresas americanas fabricantes de circuitos integrados. Pediram-me que assinasse um registro de entrada e me perguntaram se eu trazia comigo um laptop. É claro que sim. A recepcionista perguntou-me o modelo, o número de série e o valor do aparelho. 'Alguma coisa entre 1 e 2 milhões de dólares', respondi. 'Mas isso não pode ser, senhor', replicou ela. 'Como assim? Deixe-me vê-lo.' Mostrei a ela meu velho PowerBook, cujo valor ela estimou em 2 mil dólares. Registrou a soma, e eu pude entrar na empresa. A questão é que, embora os átomos não valessem tudo aquilo, os bits tinham um valor quase inestimável."

Assim, percebe-se a importância econômica dos *bits*. Em um apanhado histórico sobre a distinção em debate, Marco Aurélio GRECO[42] denota

---

[40] JESUS, Damásio Evangelista de. *Direito Penal. Vol 1.* São Paulo: Saraiva, 1999. 23ª ed. P. 33
[41] NEGROPONTE, *Op. cit.*, *loc. cit.*
[42] GRECO, Marco Aurélio. *Internet e direito*. 2ª Ed. São Paulo: Dialética, 2000. p. 16-18

que o paradigma utilizado pela civilização ocidental para basear as suas relações sociais sempre foi baseado em átomos. Assim, os bens têm seu valor aferido a partir das características físicas dos seus átomos: durabilidade, densidade ou mesmo a raridade. Neste sentido, por exemplo, é que o ouro adquiriu o valor econômico que lhe é dispensado até hoje.

Ainda segundo Marco Aurélio GRECO, as normas jurídicas, sempre produzidas a partir deste paradigma, foram criadas com vistas a reger situações relacionadas a átomos. Assim, exemplificando, cita o professor da PUC-SP alguns institutos jurídicos: "o furto como apropriação de uma 'coisa' (conjunto de átomos), a propriedade e a posse como reportando-se a objetos móveis ou imóveis (átomos); a tributação adotando como critério de sua incidência conceitos que retratam coisas (tributação de 'mercadoria')".

Percebe-se, assim, a impotência da instância jurídica, por força dos paradigmas por ela adotados, em lidar com problemas que envolvem *bits.* Resta, assim, procurar formular uma teoria que consiga inter-relacionar *bits* e átomos.

Mesmo a noção do que seja átomo precisa ser revista no âmbito jurídico. O Direito necessita estar lado a lado com as descobertas recentes das outras disciplinas, porque este, sendo um ciência social e, portanto, do dever ser, depende dos conceitos oriundos das ciências que estudam o ser. O ser sobrepõe-se ao dever-ser; logo, a ciência ontológica deve providenciar os conceitos com os quais as ciências do dever-ser trabalham, ou a estas não será possível conceder a posição de ciência: serão mera especulação metafísica.

Pode-se observar que o paradigma dentro do qual estes institutos jurídicos foram concebidos ainda era o do mundo mecânico reducionista concebido por Isaac NEWTON. Nele, a matéria difere-se da luz e, por conseguinte, da energia. No entanto, mesmo sob este paradigma, energia e matéria não são excludentes, uma vez que a luz tem tanto características de onda eletromagnética quanto de matéria.

6.1.1. A Revolução Científica e a problemática da matéria

NEWTON utilizou-se de um conceito postulado, basicamente, entre 470 e 361 aC, pelo filósofo grego DEMÓCRITO[43] de Abdera. Segundo ele, o ser é identificado por sua quantidade geométrica, comportando, portanto, a extensão. O ser é dividido em porções de extensão indivisíveis (daí o significado original da palavra átomo) que são separadas pelo vácuo.

A idéia de que a matéria é constituída por um conjunto de átomos **indivisíveis** só começou a perder sentido com a mudança de perspectiva que começou com as descobertas de DALTON (que, na verdade, nada mais fez que recuperar a noção de átomo pré-socrática de Demócrito), THOMPSON (a descoberta do elétron) e culminou com o Projeto Manhattan e a conseqüente invenção da bomba atômica. No conjunto destas transformações uma teoria proposta por Albert EINSTEIN em 1905 merece especial destaque dentro da discussão presente: a Teoria da Relatividade Especial.

Esta teoria chegou a conclusões que modificaram o pensamento humano no século XX, uma vez que são soluções pouco ortodoxas dentro de um paradigma newtoniano. No entanto, uma conclusão desta Teoria merece especial interesse, pois envolve uma nova concepção da natureza da matéria. Stephen HAWKING[44], físico que ocupa atualmente a cadeira que já foi de Isaac Newton em Cambridge, a aponta:

> "O postulado fundamental da teoria da relatividade, como foi chamada, é que as leis científicas são as mesmas para todos os observadores em movimento livre, não importa qual seja a sua velocidade. Isto era verdadeiro para as leis do movimento de Newton, mas agora a idéia abrangia também a teoria de Maxwell e a velocidade da luz: todos os observadores encontram a mesma medida de velocidade da luz, não importa o quão rápido estejam se movendo. Esta simples idéia tem algumas conseqüências notáveis: talvez as mais conhecidas sejam a equivalência de massa e energia, contida na famosa equação de Einstein $E=mc^2$ (onde E significa energia, m, massa, e c, velocidade da luz); e a lei que prevê que nada pode se deslocar com

[43] MARITAIN, Jacques. *Elementos de Filosofia I: introdução geral à filosofia*. Trad: Ilza das Neves e Heloísa de Oliveira Penteado. 18ª ed. Rio de Janeiro: Agir, 1998. p. 38-39

[44] HAWKING, Stephen W. *Uma Breve História do Tempo – Do Big Bang aos Buracos Negros*. Trad: Maria Helena Torres. Rocco: Rio de Janeiro, 1997. p. 42

> mais velocidade do que a própria luz. Por causa da equivalência entre energia e massa, a energia que um objeto tenha, devido a seu movimento, será acrescentada a sua massa."

Conclui-se, assim, que matéria e energia equivalem entre si. Objetar esta afirmação é o mesmo que dizer que um carro deixaria de ser um carro só porque está em movimento. Pela teoria da relatividade, a diferença entre Energia e Matéria é, basicamente, uma questão de velocidade; a Matéria, ao adquirir velocidades tais que se aproximem da velocidade da luz, vai adquirindo cada vez mais massa, uma vez que a Energia gasta para atingir tais velocidades iria se materializando. É por isso que a matéria não pode atingir a velocidade da luz: neste ponto, sua massa seria infinita e gastaria também uma quantidade infinita de energia neste processo.

Afinal, se $E = mc^2$, $c^2 = E/m$, de onde se extrai que, caso a relação de proporcionalidade entre m e E seja válida, E e m deverão ter valores altíssimos (Stephen HAWKING aponta, inclusive, como infinitos), o que é fisicamente impossível. Doutro modo pode-se concluir matematicamente a identidade entre Energia e massa. Dentro da obra Teoria da Relatividade Geral e Especial, EINSTEIN adota, numericamente, que a velocidade da luz equivale aproximadamente a 300.000 km/s (ou 300.000.000 m/s, no Sistema Internacional de medidas). Substituindo tal valor, temos que:

$$E = mc^2 \rightarrow E = (300.000.000)^2 \cdot m$$

Que isso significa? Apenas que Energia e massa (matéria) são idênticos, desde que à velocidade da luz. Por esta equação conclui-se também que, conforme a citação de Stephen HAWKING, à medida que a matéria atinge velocidades próximas à da luz, a energia passa a converter-se em matéria. Resumindo: energia é massa à velocidade da luz elevada ao quadrado. Por que então nosso senso comum, desarmado de postulados científicos, percebe diferentemente a massa e a matéria, por vezes classificando ambas como sendo opostos (tangível e intangível, concreto e abstrato, por exemplo)? Isso acontece porque a conversão de energia em massa não é um fenômeno observável no

dia-a-dia. Neste sentido, a luz, conforme atesta Stephen HAWKING, tem natureza de onda eletromagnética e também de partícula (matéria).

No entanto, mesmo sob o paradigma newtoniano poder-se-ia apontar a natureza material da energia (ou natureza energética da matéria?). Segundo Isaac NEWTON, em seus estudos sobre a Força Gravitacional, $F = (M \cdot m \cdot G) / d^2$, (F = força; M = massa de um corpo; m = massa de outro corpo; d = distância entre os dois corpos), i. é., um corpo (matéria) atrai outro corpo com determinada força, força esta cuja intensidade varia em razão inversa ao quadrado da distância entre os dois corpos.

É relativamente fácil perceber o efeito desta força, uma vez que é por causa dela que permanecemos fixos ao chão e os planetas orbitam o Sol, por exemplo.

No entanto, se considerarmos que a luz, sendo onda eletromagnética e, portanto, energia, não tem massa, a conclusão óbvia seria a de que nenhuma massa exerceria força gravitacional sobre a luz, pois:

1) Dados: M = massa do primeiro corpo; m = massa da luz = 0 g G = constante gravitacional universal; d = distância entre os corpos;

2) Dedução matemática

$$F = (M \cdot m. \cdot G)/d^2 \quad -> \quad F = (M \cdot 0 \cdot G)/d^2 \quad .\cdot. \quad F = 0$$

O que se conclui desta dedução é que a força gravitacional inexistiria. Apesar disto, não é o que ocorre. A luz sofre sim interferência da gravidade, e é desviada por ela. A luz, ao passar perto de um corpo com massa gigantesca, desvia, demonstrando que a força gravitacional é atuante; como já observado, premissa básica para esta força atue é a existência de dois corpos com **massa.** Conclui-se novamente que a luz pode ter natureza corpuscular. Sobre esta afirmação postula Stephen HAWKING:

> "(...) Pela dualidade onda/partícula da mecânica quântica, a luz tanto pode ser considerada onda como partícula. Segundo a teoria de que a luz é formada por ondas, não fica esclarecido o fato de ela responder à gravidade. Mas se a luz é composta por partículas, pode-se esperar que elas sejam afetadas pela gravidade , da mesma forma que balas de canhão, pedras ou planetas o são. Inicialmente, acreditava-se que as partículas de luz se deslocavam em velocidade infinita, de tal modo que a gravidade jamais seria capaz de atraí-las. Mas a descoberta de Roemer, de que a luz se propaga em velocidade finita, implica que a gravidade podia ter um efeito importante.
>
> Com base nesta suposição, um professor de Cambridge, John Michel, escreveu em 1783 uma obra nos *Trabalhos filosóficos da Royal Society de Londres*, no qual apontava para o fato de que uma estrela, com massa suficiente e devidamente compacta, poderia ter um campo gravitacional tão forte que a luz não lhe pudesse escapar: qualquer luz emitida pela superfície da estrela seria puxada de volta por sua atração gravitacional, antes que conseguisse se afastar muito. Michell sugeriu que deveria haver um grande número de estrelas nesta situação. Ainda que não fôssemos capazes de vê-las, porque sua luz não nos atingiria, poderíamos sofrer sua atração gravitacional. Estes objetos são o que chamamos atualmente de buracos negros, porque é exatamente isto o que eles são: vácuos escuros no espaço. "[45]

Note-se, no entanto, que a Teoria da Relatividade Geral explica o desvio da luz quando em área de atração gravitacional não tendo em vista a noção de força e de campo gravitacional como vislumbrado na física de Isaac NEWTON, mas sim pela noção geométrica não-euclidiana[46] do espaço-tempo. EINSTEIN, utilizando-se do programa de RIEMANN (embora inconscientemente), deduziu que não existem forças no sentido newtoniano; a gravidade é conseqüência de uma curvatura que matéria e energia produzem no espaço-tempo. Para compreender este raciocínio, pode-se pensar da seguinte forma:

> "Imagine, por exemplo, uma pedra posta sobre um lençol esticado. Obviamente a pedra vai afundar no lençol, criando uma suave depressão. Uma bolinha de gude jogada sobre o lençol irá então seguir uma trajetória circular ou elíptica em torno da pedra. Uma pessoa que contemple à distância a bola de gude orbitando em torno da pedra pode dizer que uma ´força´ instantânea está emanando da pedra e alterando a trajetória da bola de gude. No entanto, a uma observação mais atenta, é

[45] *Op. cit.* p. 119-120

[46] A Geometria Euclidiana não satisfazia à Relatividade: tornou-se necessário suplantar o paradigma matemático de então, e Einstein observou que a Geometria não-euclidiana satisfaria matematicamente os pressupostos de sua teoria.

> fácil ver o que realmente está acontecendo: a pedra empenou o lençol e, por conseguinte, a trajetória da bola de gude.
>
> Por analogia, se os planetas orbitam em torno do Sol, isso ocorre porque estão se movendo num espaço que foi encurvado pela presença do Sol. Assim, o motivo porque estamos plantados na Terra, e não sendo arremessados no vácuo do espaço cósmico, é que a Terra está empenando constantemente o espaço à nossa volta."[47]

Tendo em mente esta concepção da Matéria (derivada da famosa equação de EINSTEIN, segundo a qual matéria e energia têm a mesma natureza) , resta analisar a distinção supracitada entre *bits* e átomos proposta por Negroponte. O *bit*, como já vimos, é um estado de energia registrado em meio eletrônico. Economicamente, o *bit* enquanto *bit,* não é importante, uma vez que não tem valor por si só; só é importante na medida em que as informações registradas têm valor. Ou seja, os *bits* são importantes na medida em que são úteis. Na verdade, isto também ocorre no chamado "mundo dos átomos", uma vez que algo é valorizado economicamente de acordo com sua utilidade. Exemplificando, poderíamos citar o caso dos livros. Um livro, fisicamente, é uma folha de papel, uma capa de algum material mais durável, e tinta. No entanto, seu valor econômico não reflete apenas o que materialmente compõe o livro; importa, outrossim, a informação que está nele contida. O mesmo acontece com a informação veiculada por meio dos *bits*, ou seja, este é valorizado em função da utilidade daquela.

O que diferencia um livro dos *bits* não é a informação, mas sim o meio como ela é propagada. Marco Aurélio GRECO disserta sobre o tema:

> "(...) O valor não está mais atrelado necessariamente às características físicas das coisas. As informações, mensagens, dados, instruções, *softwares*, etc, adquiriram valor próprio, independente dos átomos de que é formado seu meio físico, valor este muitas vezes superior aos respectivos átomos. Isso se estende não apenas a valores de *softwares*, mas alcança o valor que possuem bancos de dados, registros financeiros de operações bancárias, registros contáveis etc. Até mesmo objetos que originalmente tinham natureza física, passaram a ter feição virtual; é o caso das ações de sociedades anônimas que até certo tempo atrás eram apresentadas em papel, geralmente, coloridas, numeradas, assinadas etc. e que hoje em dia foram substituídas pelas "ações escriturais"que nada mais são do que um "registro"

[47] KAKU, Michio. *Hiperespaço: uma odisséia científica através de universos paralelos, empenamentos do tempo e a décima dimensão*. Rio de Janeiro: Rocco, 2000. p. 111

> (conjunto de bits) na memória de um computador. E outros exemplos poderiam ser mencionados.
>
> Ou seja, há uma dupla mudança: por um lado, a informática deu vida a novos "bens" (*softwares*, bancos de dados, etc.); por outro lado, bens clássicos assumiram nova feição (virtual) em razão dos avanços da tecnologia e da informática (basta lembrar os chamados 'livros eletrônicos)." [48]

Os *bits,* sendo um estado da energia elétrica, deve comportar-se de acordo com as leis da física, subordinando-se, portanto, às premissas e conclusões da teoria da relatividade. E se uma destas conclusões é de que matéria e energia são equivalentes, os *bits* equivalem aos átomos: são matéria. Afirmar o contrário é o mesmo que afirmar que o gelo deixa de ser composto por duas moléculas de Hidrogênio e uma de Oxigênio só por causa da temperatura. Aliás, ironicamente, a razão é a mesma, embora em nível molecular: o processo de solidificação (transformação da água em gelo) ocorre por causa da diminuição da temperatura, que é a medida da velocidade de choque entre as moléculas.

Portanto, o Direito, para atualizar-se frente às novas tecnologias e responder adequadamente às questões jurídicas, deve aceitar as conquistas da física contemporânea, uma vez que a Internet, sendo uma sociedade gerada sob os paradigmas da relatividade geral e especial, não pode ser regida por um sistema normativo baseado na mecânica newtoniana.

6.2. Análise dos tipos presentes no Código Penal

a) Furto

Assim o CP define o crime de furto, em seu artigo 155:

"Art. 155. Subtrair, para si ou para outrem, coisa alheia móvel:

Pena – reclusão, de um a quatro anos, e multa.

[48] GRECO, *op. cit*. p. 19

§1º. A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.

§2º. Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.

§3º. Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico."

Desta forma, é necessário, primeiramente, proceder a uma discussão sobre o *caput* do artigo, que retrata a necessidade de subtração de ***coisa móvel*** para a consumação do crime. Afinal, de acordo com a teoria do crime, este é fato típico, antijurídico e culpável, donde se extrai a necessidade de interpretar o conceito de coisa móvel a fim de decidir sobre a tipicidade ou atipicidade da conduta frente ao tipo legal.

De acordo com Celso DELMANTO[49], o objeto material do crime "deve ser coisa móvel, não abrangendo, face à sua significação penal realista, as presunções da lei civil. A energia elétrica ou outras de valor econômico são equiparadas a coisa móvel." Já MIRABETE[50] define a coisa móvel como substância corpórea, material, ainda que não tangível, suscetível de apreensão e transporte, incluindo os corpos gasosos (...)". E Heleno FRAGOSO[51] sustenta que "É irrelevante o *meio* de que se serve o agente para operar a subtração, podendo servir, porém, para qualificar o crime. São coisas quaisquer objetos corpóreos."

Conforme já discutido, a interpretação destes autores é baseada em um paradigma newtoniano, ou mesmo, no senso comum. Não se trata, portanto,

[49] DELMANTO, Celso. *Código Penal Comentado*. 5ª ed. Rio de Janeiro: Renovar, 2000. p. 310
[50] MIRABETE, Julio Fabbrini. *Manual de Direito Penal*. Vol 2. 16ª ed. São Paulo: Atlas, 2000. p. 221
[51] FRAGOSO, Heleno Cláudio. *Lições de Direito Penal, parte especial: Volume I*. 9ª ed. Rio de Janeiro: Forense, 1987. p. 285

de uma definição científica, posto que, como já observado, matéria e energia são apenas duas expressões do ser que diferem apenas na velocidade com que este se move.

No sentido da interpretação destes autores, seriam furto, dentre os exemplos citados, as três primeiras condutas, posto que o objeto material daqueles crimes é o dinheiro, que é coisa corpórea, material, e tem importância econômica.

Entretanto, a última conduta, exemplifica o problema da adequação típica. Um *hacker* invadiu o sistema informático da NASA e, pelo processo de *download* copiou um *software* avaliado em US$ 1.700.000,00. Este caso merece uma especial análise, tendo em vista o problema já mencionado da dificuldade de adaptá-lo ao tipo legal.

Há duas dificuldades no caso em análise. O art. 155 refere-se a uma conduta (subtrair) e a um objeto material (coisa móvel). O primeiro problema consiste em que subtrair, conforme nos assevera Damásio, significa tirar, retirar. Ora, em informática, quando alguém copia um programa, este permanece na mídia de origem e apenas é transcrito para a mídia de destino (no caso, o computador do *hacker*). Segundo Ivette Senise FERREIRA[52], a lei 9.609, que dá proteção ao *software*, abrange esta conduta. Dispõe:

Art. 12. Violar direitos de autor de programa de computador:

Pena – Detenção de 6 (seis) meses a 2 (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 e 1 (um) a 4 (quatro) anos e multa.

[52] FERREIRA, Ivette Senise Ferreira. *A Criminalidade Informática*. In:LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). *Direito & Intyernet – aspectos jurídicos relevantes*. Bauru, SP: EDIPRO, 2000

Esta hipótese certamente aplicar-se-ia ao caso da invasão da NASA. No entanto, caso o *hacker*, ao invés de copiar o *software* para seu computador, houvesse transferido-o, seria conduta atípica frente a este dispositivo legal, que apenas protege a reprodução, e não a transferência de dados. Assim, o núcleo do tipo "subtrair" adequar-se-ia à conduta descrita, uma vez que, admitindo-se que dados informáticos são 'coisa móvel', e a posse, bem jurídico do crime, é lesionada. Conclui-se que, quanto ao núcleo "subtrair", é possível aplicá-lo quanto à transferência ilícita de um *software;* no entanto, quanto à cópia do mesmo, parece aplicar-se a lei 9.609.

Ainda resta a análise do objeto material do tipo: a coisa móvel. O conceito de coisa móvel adotado pela doutrina, como já vimos, é tido dentro de uma perspectiva não-científica, postulada para atender aos problemas de uma sociedade analógica[53], e não digital.

Assim, para que se assuma a possibilidade jurídica de que os *bits* possam ter equivalência frente aos átomos, é necessário que se assumam as conclusões já relatadas da Teoria da Relatividade, permitindo um paralelo entre Energia e Matéria. Entendo que a interpretação jurídica não pode ser extensiva, com o intuito de condenar o sujeito passivo. No entanto, deve, como instrumento de atualização do Direito frente à realidade social, admitir a influência das conquistas científicas das outras ciências.

Também importa trazer à tona o pensamento de Karl LARENZ, segundo o qual a "natureza das coisas" também desenvolve importância fundamental para a análise do fenômeno jurídico. Segundo LARENZ, esta forma de interpretação (que, para o referido autor, não deixa de ser um critério teleológico-objetivo de interpretação) quer

> "dizer que, em primeiro lugar, certos dados fundamentais pertencentes à natureza corpórea ou à natureza anímica e espiritual do homem, que não são mutáveis, ou o são dificilmente e em períodos mais longos, têm que ser tidos em

[53] NEGROPONTE, em sua obra *A Vida Digital,* utiliza a distinção entre analógico e digital para referir-se às diferenças existentes entre o mundo "real", dos átomos, e o mundo "virtual", dos bits.

> conta pelo Direito se servem ao homem, não lhes deve exigir demais. (...) A "natureza das coisas" deixa constantemente margem para as mais variadas possibilidades de configuração, mas também exclui algumas por plenamente "alheias às coisas", inadequada às coisas. "[54]

LARENZ, com esta modalidade de interpretação, quer que o Direito não se abstraia da natureza mesma das coisas, ou seja, que a instância jurídica não pode contrariar o ser, pois perderia normatividade; trata-se da própria relação entre ser e dever ser. Desta forma, reiteramos, em consonância com o pensamento de LARENZ, a necessidade da apreensão das conquistas científicas, tendo em vista que em muitas situações é esta forma de cognoscibilidade que informará os parâmetros para evitar que se interprete o Direito de modo dissonante com a realidade.

Além disso, o legislador brasileiro já reconheceu a importância da energia elétrica dentro do contexto patrimonial, uma vez que, no §3º do art. 155, CP, equipara-se à coisa móvel a energia elétrica ***ou qualquer outra que tenha valor econômico***. Por uma interpretação gramatical simples, pode-se perceber que a expressão "qualquer outra" refere-se à energia; portanto, qualquer forma de energia que tenha valor econômico pode ser objeto material do furto. Os *bits,* como já vimos, têm natureza material por serem energia (conclusão extraída da análise da teoria da relatividade) e, portanto, são suscetíveis de posse.

Assim, podem, aparentemente incidir tanto o art. 155, *caput*, quanto o art. 155, §3º. No entanto, pelo princípio *lex specialis derogat legi generali*, deve-se aplicar o disposto no art. 155, §3º, de acordo com Assis Toledo[55]: "Se entre duas ou mais normas legais existe uma relação de especialidade, isto é, de gênero para espécie, a regra é a de que a norma especial afasta a incidência da norma geral. Considera-se especial (*lex specialis*) a norma que contém todos os elementos da geral (*lex generalis*) e mais o elemento especializador."

---

[54] LARENZ, Karl. *Metodologia da Ciência do Direito*. Trad: José Lamego. Lisboa: Fundação Calouste Gulbenkian, 1997. 3ª Ed. p. 589

[55] TOLEDO, Francisco de Assis. *Princípios Básicos de Direito Penal*. 5ª ed. São Paulo: Saraiva, 1994

b) Dano

De acordo com o Código Penal brasileiro, o crime de dano é definido como:

"art. 163. Destruir, inutilizar ou deteriorar coisa alheia:

Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa."

Assim, novamente torna-se necessária a análise do conceito de coisa. Primeiramente, para o crime de dano não há a equivalência entre energia elétrica e coisa, de onde se extrai que, se o *bit* tiver a mesma natureza desta, não poderá ser suscetível do crime de dano.

De acordo com parte da doutrina, o crime de dano contra dados informáticos seria atípico. Segundo José Henrique Moreira LIMA[56], os dados de computador são incorpóreos e, portanto, seriam insuscetíveis de sofrer dano. Esta conclusão o referido autor extrai de comentário de Nelson Hungria, ao afirmar que "objeto material do crime de dano é a coisa imóvel ou imóvel , devendo tratar-se obviamente, de coisa corpórea ou no sentido realístico, pois somente pode ser danificada por ação física." Deve-se ter em vista que o bem jurídico protegido pela interpretação de HUNGRIA é a coisa corpórea, a qual o Código não faz menção nenhuma; assim, o conceito de "coisa" depende de interpretação para que seu significado seja apreendido pelo Direito.

De acordo com a interpretação do objeto jurídico do dano concebida por MIRABETE, DAMÁSIO e FRAGOSO, no entanto, a o dano contra dados de computador é possível. Segundo tais autores, o objeto jurídico tutelado é o patrimônio e, sendo assim, este conceito abrange todas as formas possíveis de posse e propriedade. De acordo com MIRABETE: "o patrimônio, em especial a propriedade de coisas móveis ou imóveis, é o objeto jurídico do delito,

[56] MOREIRA LIMA, José Henrique. *Alguns Aspectos Jurídicos da Internet no Brasil*. Disponível em: <www.juridica.com.br/Apres_Artigo.asp?CodArtigo=37> Acesso em 10/10/2000

protegendo-se, eventualmente, a posse.". Também a interpretação de Fragoso permite a defesa da tese de que os dados informáticos estariam protegidos pelo art. 163, como parte da esfera de bens que compõem o patrimônio econômico de uma pessoa. Segundo Fragoso: "(...) Como dizem Schönke-Schröder, § 303, I, o objeto da tutela jurídica é a preservação do valor da coisa para o proprietário, **protegendo-se não só o seu valor substancial ou intrínseco como também o mero valor de utilidade**." (grifo nosso)

Como já observamos, o *bit* não é apenas energia: é um registro (físico, pois a informação a ser digitalizada é gravada no *hard disk* ou disquete, ou qualquer outra mídia, de modo concreto, uma vez que cada mídia dispõe de elementos físicos (o *hard disk*, por exemplo, utiliza-se de uma agulha de metal para a digitalização dos dados) de um estado de energia. Assim, a nosso ver, o *bit* , além de não ser apenas energia (pois energia também é matéria e, portanto, é corpórea), pela interpretação das conclusões Teoria da Relatividade, também é material dentro de um paradigma newtoniano, uma vez que é um registro físico. A nosso ver, portanto, cabe afirmar que é possível o crime de dano contra dados de computadores.

Além disso, como exemplificado no item anterior, é possível que as duas primeiras condutas do tipo objetivo (destruir, inutilizar e deteriorar) sejam praticadas contra dados informáticos. No primeiro caso, por exemplo, que retratava a situação em que o ex-empregado da companhia Omega distribuiu um *software* que **destruiu** (no sentido próprio que Fragoso dá ao termo: fazer desaparecer em sua individualidade) todos os programas de produção da companhia. Já no segundo caso, que retratava o vírus Melissa, nota-se que o mesmo **inutilizou** (tornou imprestável ou inútil) os computadores infectados.

Cabe também a aplicação, no crime de dano, o mesmo princípio disposto no art. 155, § 3º, pelo qual se estabelece ser a energia elétrica equiparável à coisa móvel, sendo possível sua subtração e, tal como pensamos, também sua danificação. De outro modo não seria razoável apontar, tendo em

vista que o próprio legislador dá essa interpretação ao dispositivo, na exposição de motivos do Código Penal, em seu p. 56: "toda energia economicamente utilizável e suscetível de incidir no poder de disposição material e exclusiva de um indivíduo (como, por exemplo, a eletricidade, a radioatividade, a energia genética dos reprodutores, etc) pode ser incluída, mesmo do ponto de vista técnico, entre as *coisas móveis*, a cuja regulamentação jurídica, portanto, deve ficar sujeita". Assim, por um critério teleológico de interpretação, temos a tutela jurídico-penal à coisa móvel "energia" extensível também ao crime de dano. Outrossim, também uma interpretação sistemática, com a finalidade de tornar o CP coerente, impediria uma situação na qual considera-se a energia como sendo coisa móvel em um caso, mas não noutro; no furto, e não no dano. Seria uma contradição em seus termos: ou a energia É ou NÃO É coisa móvel: o próprio princípio da identidade abominaria tal interpretação; se a energia é coisa móvel e, portanto, suscetível de furto, também o é para o dano.

Assim, a nosso ver, cabe a aplicação do tipo penal descrito no art. 163, CP, sem prejuízo do princípio da legalidade.

c) Estelionato

Dentro do capítulo VI dos crimes contra o patrimônio, destacam-se duas condutas, prescritas nos arts. 171 e 175.

Quanto ao art. 171, conforme nos atesta Ivette FERREIRA[57], a figura do estelionato é o crime mais praticado na *Internet*. Segundo a autora, outro exemplo da prática deste crime na *Internet* seriam as transferências de fundos nas contas bancárias. No entanto, não concordo plenamente com a afirmação da autora. Se o delito se dá com o engano do sujeito passivo, realmente caracteriza-se o crime de estelionato (exemplo é o caso em que um *hacker* engana um consumidor desatento e, fraudulentamente, consegue registrar o número do cartão de crédito e, com ele, faz a transferência de fundos) ; no

[57] FERREIRA, *Op. cit.*

entanto, há casos em que um *hacker* invade um sistema bancário e, com a invasão, consegue acesso ao registro de números de cartões e, com essas informações, transfere os fundos. Na primeira hipótese, realmente configura-se o crime de estelionato, uma vez que a *fraude* exigida no tipo legal é contra a pessoa (induzir ou manter *alguém* em erro); no entanto, a segunda hipótese consiste em fraude contra o sistema informático, e é meramente técnica, não se tratando portanto, de estelionato, e sim de furto, como já estudado.

Já quanto a o art. 175 (fraude no comércio), que consiste em enganar o adquirente ou consumidor, vendendo mercadoria falsificada ou deteriorada como perfeita, ou entregando uma mercadoria por outra, também já foi vista a possibilidade de acontecer, no primeiro exemplo citado.

Assim, conclui-se que a legislação brasileira, no referente ao estelionato e outras fraudes, está apta a resolver os problemas que surgirem, tendo em vista que a *Internet* é apenas um meio para a prática destes crimes.

6.3. Análise da Legislação Estrangeira e Projetos de Leis Brasileiros

a) Furto

A Lei nº 109/91, de Portugal, traz a legislação daquele país sobre os crimes informáticos. Referente à conduta em análise, do crime de furto, é o art. 7º desta lei lusa. Neste artigo, pune-se o acesso não-autorizado a sistemas informáticos com a intenção de alcançar benefício ou vantagem indevidos. É interessante observar que este benefício ou a vantagem englobam o objeto material do furto, que pode ser dinheiro ou mesmo a cópia de *softwares* . Aliás, é agravante se, através do acesso ilegal, o agente tomar conhecimento de segredos ou dados confidenciais.

Quanto à lei norte-americana, há em especial uma (conhecida como *Fraud and Related Activity in Connection with*, que é a lei 18 U.S.C. 1030.), mas

como o sistema normativo norte-americano penal é autônomo em relação aos estados, muitos têm legislação independente.

Quanto ao 18 U.S.C. 1030, no que se refere ao crime de furto, destacam-se os incisos 1, 2 e 4 do artigo (a), . O primeiro inciso protege os computadores dos órgãos públicos governamentais norte-americanos, tendo em vista os riscos que uma invasão *hacker* e coleta de informações destes computadores poderiam significar um risco alto para a segurança nacional daquele país. A pena para estas condutas é de até 20 anos e multa, tendo em vista a gravidade desta para a segurança do país. Já o segundo inciso protege a cópia de informações de computadores de instituições financeiras e de departamentos ou agências não-governamentais, e sua pena é de até 10 anos, mais multa. Já o inciso 4 protege os computadores privados, e condena a até 5 anos de prisão mais multa, se o *hacker* conseguir, com a invasão, obter qualquer vantagem econômica.

Quanto às leis estaduais, destacam-se o Título 9 A do Código Penal de Washington, em seu artigo 9A.52.110, o Idaho Code @ 18-2202, o Kansas Criminal Code @ 21-3755, o Califórnia Penal Code Section 502.

O artigo 9A.52.110 do Código Penal de Washington é um tipo muito aberto, uma vez que condena, diretamente, apenas o acesso não-autorizado a computador, e o propósito de cometer outro crime é punido separadamente. Assim, são duas condutas: a de acesso indevido e o cometimento de outro crime, o que inclui o furto. Cada crime é julgado separadamente. Dentro de uma perspectiva do Direito brasileiro, seria errônea tal atitude, uma vez que a conduta de acesso não-autorizado é apenas um meio para o cometimento do outro crime, ou seja, aquela deveria ser absorvida por esta.

Já o Idaho Code @ 18-2202 é mais específico, e em seu artigo 1º, define a conduta de acesso não-autorizado a computador, sistema de

computadores ou uma rede de computadores com o intuito de obter dinheiro, propriedade ou serviços, entre outros.

O Kansas Criminal Code @ 21-3755, após definir uma série de conceitos, dentre os quais o de propriedade, que inclui a informação e os dados eletrônicos, especifica que crime de computador é qualquer conduta com o intuito de obter acesso e danificar, modificar, alterar, copiar ou obter posse de um computador, sistema de computador, rede de computador ou qualquer outra propriedade. Neste, que é o primeiro inciso do segundo artigo, tendo em vista a conceituação de propriedade fornecida no primeiro artigo desta lei, inclui-se como objeto material do furto a informação e os dados de computador, além do *software*.

A legislação californiana também é restritiva quanto ao furto, e admite como objeto material deste crime os dados de computador, a propriedade e dinheiro.

Resta, portanto, analisar como os projetos de lei em tramitação no Congresso Nacional analisam o furto cometido por meio de sistemas informáticos. Destacam-se três projetos: o PL 1.806/99, o PL 84/99 e o PL 1.713/96.

O PL 1.806/99, de autoria do sr. Deputado Freire Júnior, trata exclusivamente do crime de furto no âmbito dos sistemas informáticos. De acordo com o projeto de lei, dois incisos seriam acrescentados no parágrafo 3º do artigo 155. De acordo com o projeto, o acesso aos serviços de comunicação e aos sistemas de armazenamento, manipulação ou transferência de dados eletrônicos equiparar-se-iam à coisa móvel, ao lado da energia elétrica. É uma boa solução; no entanto, a redação é falha, uma vez que a coisa móvel deve ser um objeto corpóreo, e não algo etéreo e indefinido como o “acesso”. Gramaticalmente, o acesso é derivado do verbo acessar, e não é algo corpóreo:

quando alguém “furta” dados de computador, “furta” os dados em si, e não o acesso.

Quanto ao PL 84/99, de Luiz Piauhylino, no que se refere ao crime de furto, destaca-se a Seção IV, que trata da Obtenção indevida ou não autorizada de dado ou instrução de computador. A conduta do art. 11 refere-se a “obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador”. No entanto, interessa-nos a agravante do parágrafo único, inciso III, que torna agravada a conduta do *caput* caso a obtenção do dado ou da instrução seja feita com o intuito de lucro ou vantagem de qualquer espécie. Esta agravante resolveria sem maiores problemas o problema do furto cometido na *Internet*.

Quanto ao PL 1.713, de Cássio Cunha Lima, no que tange ao crime de furto, traz tipos autônomos, em seus artigos 20 e 28. O artigo 20 refere-se à obtenção de segredos empresariais ou informações de caráter confidencial, ou o já referido “furto de informação”. No entanto, o PL é omisso quanto à cópia de dados ou *softwares*, a não ser quando estes sejam oriundos de instituições financeiras, e mesmo assim quando a cópia tiver como finalidade a transferência de fundos. Ou seja, a transferência simples de *softwares* e dados seria conduta atípica, se desconsiderarmos a interpretação proposta neste trabalho para incluir os *bits* como coisa móvel.

b) Dano

A doutrina estrangeira encontra o mesmo problema que a brasileira, ao definir se há a possibilidade de dano contra dados de computadores. Sobre este assunto, analisando a interpretação da Corte de Apelações norte-americana sobre o *Criminal Damage Act*, NATHANSON[58] conclui sobre a possibilidade de dano a dados de computadores:

[58] NATHANSON, Nabarro. *The Laws of the Internet*. Inglaterra, 1997. p. 67

> *"This discussion on the technology suggests that a vírus causes no property damage. It is more accurate to state that virus damage causes no physical damage: property is a wide term and encompasses more than 'that which can be touched'.*
>
> *In two cases the criminal courts decided, for the purposes of the Criminal Damage Act 1971, that altering magnetic media can be classed as damage to property. The Court of Appeal, based on previous authorities, read widely the concept of damage.*
>
> *'Where... the interference with the disc amounts to an impairment of the value or usefulness of the disc to the owner, then the necessary damage is established.'*
>
> *Applying the reasoning that an impairment of the value or usefulness of a disk will constitute damage, it is clear that part of a damages claim would justifiably be for the price of the program which the disk held."*[59]

Assim, a interpretação da Corte de Apelações norte-americana admite a possibilidade de dano contra dados informáticos. No entanto, apesar desta interpretação solucionar a questão, o legislador daquele país preferiu produzir leis específicas, tanto em nível federal quanto em nível estadual. Em nível federal, destaca-se o 18 U.S.C. 1030 (*Fraud and Related Activity in Connection with Computers)*; em nível estadual, importa analisar o *Annotated Code of Maryland*, s.146, o *Idaho Code @* 18-2202, o *Kansas Criminal Code @21-3755, o Computer Law – State of Wisconsin,* 943.70, e o *Califórnia Penal Code,s. 502.*

Quanto ao 18 U.S. C. 1030, no que se refere ao dano cometido contra um sistema informático, destaca-se a seção a) 5). São três as situações previstas: na primeira, pune-se aquele que, sabidamente, causa a transmissão de programa, informação, código ou comando e, como resultado desta conduta, causa dano sem autorização a computador protegido (entende-se por computador protegido, em explicação nesta lei, aquele que é usado por instituição financeira, pelo governo dos Estados Unidos, ou aquele que é utilizado para fins comerciais.). Exemplo desta conduta é o vírus. Na segunda hipótese, pune-se aquele que, intencionalmente, acessar computador protegido e, como resultado desta conduta, causar, negligentemente, dano. A terceira e

[59] Trad: "A discussão sobre tecnologia sugere que um virus não causa dano propriamente. É mais acurado constatar que vírus não causa dano físico: propriedade é um termo amplo que engloba mais que "aquilo que pode ser tocado". Em dois casos as cortes criminais decidiram, para os propósitos do *Criminal Damage Act* 1971, que a mídia magnética modificável possa ser classificada como dano à propriedade. A Corte de Apelações leu amplamente o conceito de dano: ´aonde... a interferência no conteúdo dos discos levar a uma diminuição do valor ou do uso do disco a seu proprietário, então o necessário dano está concretizado. Aplicando a razão de que a diminuição no valor ou uso do disco configura dano, é claro que parte da conseqüência do dano é a restituição do valor do programa contido no disco."

última hipótese refere-se àquele que intencionalmente acessa computador protegido, sem autorização, e causa dano. A pena para estes crimes é de um a cinco anos de prisão, mais multa. Observa-se que esta lei protege apenas os computadores que são protegidos; o usuário comum permanece sem a proteção legal.

Quanto ao Annotated Code of Maryland, em seu artigo 28, seção 146, são definidos os *computer crimes.* Na subseção "c", no inciso 2, são definidas duas condutas que produzem dano contra sistemas informáticos. Na primeira, pune-se a pessoa que, intencionalmente e sem autorização, causar mal funcionamento ou interromper a operação de um sistema informático. Ou seja, o fato de alguém espalhar um vírus em vários computadores, como o *Melissa*, enquadrar-se-ia nesta conduta. Já a segunda conduta refere-se àquele que altera, danifica ou destrói dados ou computadores arquivados em um computador. As penas para estes crimes variam de 1 a 5 anos de prisão, mais multa, que varia de US$ 1.000,00 a US$ 5.000,00.

O Idaho Code @ 18-2201, em seu título 18, Capítulo 22, define, no artigo 2º, a conduta de dano a sistemas informáticas, baseado em três condutas típicas: alterar, danificar ou destruir dados de computadores.

Já o *Kansas Statutes Annotated*, no capítulo 21, em seu artigo 37, define também o crime de dano, cometido com o ganho não autorizado de acesso a um sistema informático, e com o dano, modificação ou destruição de dados.

A *Computer Law,* do Estado de Wisconsin, define de maneira parecida o crime de dano, dentro desta perspectiva, uma vez que este pode ser produzido também com a alteração ou destruição de dados. A pena, entretanto, chega a 20 anos de prisão, e a multa, a US$ 10.000,00.

Também é essa a definição da Código Penal Californiano, em sua seção 502. A pena, entretanto, pode chegar a US$ 5.000,00, e o tempo de

prisão é de 16 meses. Além disso, caso um menor cometa a infração, deve um de seus pais ou representante legal responder por sua atitude.

Outro país que tem legislação específica sobre o assunto é Portugal. No artigo 6º, denomina-se não como dano, mas como sabotagem informática, o fato de alguém introduzir, alterar, apagar ou suprimir dados ou programas informáticos. A penalidade para estas condutas é pena de prisão até 5 anos ou com pena de multa até 600 dias.

Quanto aos projetos de lei brasileiro, é nítida a influência da legislação estrangeira, conforme nos atesta Gustavo CORRÊA.[60] Destacam-se os projetos de lei nº 84/99 e 1.713/96.

Quanto ao projeto de lei 84/99, destaca-se a Seção I do Capítulo III, que trata do Dano a dado ou programa de computador. No artigo 8º, nota-se a influência da legislação estrangeira na feitura deste projeto, uma vez que os núcleos do tipo são os mesmos já referidos quando da análise das leis norte-americanas: apagar, destruir ou modificar. A pena para este crime é de detenção, de um a três anos, mais multa. Além disso, conforme observa-se no parágrafo único, a proteção aos computadores dos órgãos públicos é especial, uma vez que a pena pelo dano a dados nestes computadores é de dois a quatro anos de detenção, mais multa. Também é agravado o dano a dado ou programa de computador caso haja prejuízo considerável da vítima, com intuito de lucro ou vantagem de qualquer espécie, com abuso de confiança, por motivo fútil, com uso indevido de senha ou utilização de meio fraudulento qualquer.

O projeto de lei 1.713/96, de autoria de Cássio Cunha, por sua vez, define em um artigo a conduta tipificada no art. 8º do PL 84/99. No artigo 18, o dano é agravante do tipo definido: “art. 18. Obter acesso, indevidamente, a um sistema de computador ou a uma rede integrada de computadores: §3º Se o acesso tem por escopo causar dano a outrem: detenção, de 2 a 4 anos, e

[60] CORRÊA, *Op. cit.*

multa.” Parece equivocada a atitude do legislador ao dispor como agravante do acesso indevido o dano, uma vez que o dolo principal é o do dano, e não o do acesso não autorizado. Assim, um tipo autônomo faria mais sentido. O Art. 24 também abrange a conduta de dano definida na legislação estrangeira: “Art. 24 Falsificar, alterar ou apagar documentos através de sistema ou rede integrada de computadores e seus periféricos: Pena – reclusão, de 1 a 5 anos, e multa.” Nota-se que, para efeitos desta lei: “§2º. Considera-se documento o dado constante no sistema de computador e suporte físico como disquete, disco compacto, CD-ROM ou qualquer outro aparelho usado para o armazenamento de informação, por meio mecânico, ótico ou eletrônico.”

c) Estelionato e outras Fraudes

Os legisladores norte-americanos e portugueses optaram por deixar a conduta do estelionato na *Internet* solucionada por uma legislação não-específica, o que condiz com a interpretação por nós formulada, segundo a qual a *Internet* é apenas um meio para a prática da conduta típica.

O legislador brasileiro, em especial nos projetos de lei 84/99 e 1.713/96, também não dispõe sobre o assunto, tendo em vista que o CP, art. 171 e seguintes é suficiente para que haja a persecução ao criminoso.

7. Conclusão

O objetivo delineado para a presente pesquisa era, primordialmente, demonstrar que os tipos penais existentes no Código Penal brasileiro já seriam suficientes para promover a tutela penal do patrimônio. Em segundo plano, eram objetivos secundários verificar se a interpretação atual dos tipos existentes refletiria um paradigma ultrapassado, levantar os casos mais comuns de condutas lesivas ao patrimônio e, por fim, demonstrar a possibilidade de aplicar,

mediante reinterpretação, os tipos penais já existentes no Código Penal brasileiro. Tendo em vista tais objetivos, a pesquisa realizou-os plenamente.

Dentre as conclusões do trabalho, temos que uma das mais importantes é que a própria *Internet* não existe, tendo em vista que esta é apenas uma rede de computadores interligados que não se subordinam a controle algum. Deste modo, cada uma das redes internas da *Internet* é autônoma e independente, o que torna impossível que qualquer legislação pátria possa exercer jurisdição sobre toda a rede.

Outra conclusão importante realizada nesta pesquisa foi a classificação dos crimes virtuais. Nesta etapa discordou-se de classificações realizadas por outros autores, e propôs-se uma própria, que a nosso ver, é mais completa, sendo baseada na posição que o computador pode ocupar em um crime informático: como instrumento do crime, como objeto do mesmo e como instrumento e objeto do crime.

Já trabalhando com os objetivos delineados para a pesquisa, demonstramos que a ciência jurídica dispõe de instrumentos suficientes e adequados para que se proteja o bem jurídico patrimônio, sendo que a interpretação dos tipos penais inserem-se em determinados paradigmas, que muitas vezes são difíceis de ser superados. Demonstramos que no estágio atual, a interpretação do conceito de *coisa móvel*, importantíssimo principalmente nos crimes de furto e dano, é baseada no paradigma *newtoniano*, que considera serem de naturezas distintas matéria e energia, e propusemos uma interpretação (com base no modelo de interpretação segundo a natureza das coisas, exposto por Karl Larenz) que leve em conta os ensinamentos de Albert Einstein, em sua Teoria da Relatividade Geral, na qual expõe a natureza una de matéria e energia, que são, a rigor, o mesmo.

Ademais, realizou-se pesquisa de legislação brasileira e estrangeira, de modo extensivo e pertinente à temática da tutela penal do patrimônio

Deste modo, conseguimos demonstrar que a lei penal brasileira já é suficiente para promover a tutela penal do patrimônio, sendo aplicáveis os tipos dispostos no CP.

Bibliografia

AGUIAR, Roberto A. R. de . *Os filhos da flecha do tempo: pertinências e rupturas*. Brasília: Letraviva, 2000

ANDRADE FILHO, Edmar Oliveira. *Direito Penal Tributário: Crimes contra a Ordem Tributária*. São Paulo: Atlas, 1995

ARAÚJO JUNIOR, João Marcello de. *Dos Crimes Contra a Ordem Econômica*. São Paulo: Editora RT, 1995

BARROS, Suzana de Toledo. *Princípio da Proporcionalidade e o Controle de Constitucionalidade das Leis Restritivas de Direitos Fundamentais.* Brasília, 1995.

BOBBIO, Norberto. *A Era dos Direitos*. Rio de Janeiro: Campus, 1992. 10ª ed. Trad. Carlos Nelson Coutinho.

CASTELLS, Manuel. *A Sociedade em Rede – A Era da Informação*: Economia, Sociedade e Cultura. São Paulo: Paz e Terra, 1999

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

CYBERCRIME. Disponível em: <www.cybercrime.gov/comrade.htm>. Acesso em: 27 set. 2000

EDWARDS, Lilian; WAELDE, Charlotte. *Law and the Internet: regulating Cyberspace.* Oxford: Hart, 1998

ERCÍLIA, Maria*. A Internet* – Coleção A Folha Explica. São Paulo: Publifolha, 2000

FRAGOSO, Heleno Cláudio. *Lições de Direito Penal, parte especial: volume I – arts. 121 a 212 do CP*. 9ª ed. Rio de Janeiro: Forense, 1987

GATES, Bill. *A Estrada do Futuro.* São Paulo: Companhia das Letras, 1995

GOMES, Olavo Anchieschi. *Segurança Total: Protegendo-se Contra os Hackers*. São Paulo: Makkron Books, 2000

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

HAWKING, Stephen William. *Uma Breve História do Tempo: do Big Bang aos buracos negros*. Rio de Janeiro: Rocco, 1988

HOESCHL, Hugo César. *O Ciberespaço e o Direito*. Disponível em: <http://www.iaccess.com.br/~ciberjur/ciber3.html>. Acesso em: 25/11/2000.

INTERNET SOCIETY. *A Brief History of the Internet*. Disponível em: www.isoc.org/ internet-history/brief.html>. Acesso em: 20 set. 2000

JESUS, Damásio Evangelista de. *Direito Penal (vols. I e II)*. São Paulo: Saraiva, 1999

KAKU, Michio. *Hiperespaço: uma odisséia científica através de universos paralelos, empenamentos do tempo e a décima dimensão*. Rio de Janeiro: Rocco, 2000

KELSEN, Hans. *Teoria Pura do Direito*. 6ª ed. São Paulo: Martins Fontes, 1998

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Fundamentos de Metodologia Científica*. São Paulo: Atlas, 1996.

LARENZ, Karl. *Metodologia da Ciência do Direito*. Trad de José Lamego. 3ª ed. Lisboa: Fundação Caloust Gulbenkian, 1991

LIMA NETO, José Henrique Barbosa Moreira. *Sociedade Internet: uma volta ao passado.* Palestra proferida no 1º fórum de Debates Jurídicos Via Internet realizado na Universidade Luterana do Brasil – ULBRA, Canoas-RS). Disponível

em: <www.juridica.com.br/Apres_Artigo.asp/CodArtigo=38>. Acesso em: 10/12/2000

LIMA, André Felipe. *Hackers: uma molecagem que custa bilhões de dólares*. In: CanalWeb Digital. Disponível em: < www.canalweb.com.br/revistas/busines s.asp?bus_id=280>. Acesso em: 12/01/2001

LOMBARDI, Renato. *Estelionatário cibernético é identificado*. In: O Estado de São Paulo.Disponível em:<www.estadao.com.br/tecnologia/internet/2000/out/04/3/6.htm>. Acesso em: 02/11/2000

LUCCA, Newton De e SIMÃO FILHO, Adalberto (coord.) e outros. *Direito & Internet – aspectos jurídicos relevantes*. Bauru, SP: EDIPRO, 2000

LYNCH, Daniel C. *Dinheiro Digital: o comércio na Internet*. Rio de Janeiro: Campus, 1996

LYRA FILHO, Roberto. *O que é Direito*. 17ª ed. São Paulo: Brasiliense, 1995

MARITAIN, Jacques. *Elementos de Filosofia I: introdução geral à filosofia*. 18ª ed. Rio de Janeiro: Agir, 1998

MELLO, Marcos Bernardes de. *Teoria do Fato Jurídico – Plano da Existência*. São Paulo: Saraiva, 1999. 9ª ed.

MIRABETE, Julio Fabbrini. *Manual de Direito Penal*. 16ª ed. São Paulo: Atlas, 2000

MOREIRA LIMA, José Henrique. *Alguns Aspectos Jurídicos da Internet no Brasil*. Disponível em: <www.juridica.com.br/Apres_Artigo.asp?CodArtigo=37>. Acesso em: 10/10/2000

MORON, Fernanda de Almeida. *A Internet e o Direito*. Disponível em: <*www.juridica. com.br/ Apres_Artigo.asp?CodArtigo=23*> . Acesso em 13 out. 2000

NATHANSON, Nabarro. *The Laws of the Internet*. United Kingdon: Reed Elsevier, 1997

NEGROPONTE, Nicholas. *A Vida Digital*. São Paulo: Companhia das Letras, 1995

NUA INTERNET SURVEYS. Disponível em: <*www.nua.ie*> . Acesso em: 28 set. 2000

O ESTADO DE SÃO PAULO. Disponível em: <www.estado.com.br/editorias/ 2000/10/04/cid3/3.htm>. Acesso em: 26 set. 2000

_____. *Polícia apura golpe eletrônico em correntista*. In: O Estado de São Paulo. Disponível em: <www.estado.com.br/editorias/2000/10/04/cid370.html>. Acesso em: 08/10/2000

OPICE BLUM, Renato S. *A Internet e os Tribunais*. Disponível em: <www.jurídica.com.Br/Apres_Artigo.asp?CodArtigo=102>. Acesso em: 10/11/2000

PRADEL, Jean e FEUILLARD, Cristian. *Les infractions commises au moyen de l'ordinateur*. In Revue de Droit Pénal et de Criminologie, n. 4. Bruxelas, 1985

QUEIROZ, Paulo de Souza. *Do Caráter Subsidiário do Direito Penal*. Belo Horizonte: Del Rey, 1998

ROSENOER, Jonathan. *Cyberlaw: The Law of the Internet*. New York: Springer, 1997

SAGAN, Carl. *O Mundo Assombrado Pelos Demôios – A Ciência vista como uma vela no escuro*. São Paulo: Companhia das Letras, 1996

SIEBER, Ulrich *Delitos informáticos e outros delitos contra a tecnologia de informação. Comentário e questoionário para o Colóquio da Association Internationale de Droit Penal*. Würzburg, 1992

SZNICK, Valdir. *Novos crimes e novas penas no Direito Penal*. São Paulo: Livraria e Editora Universitária de Direito LTDA, 1992.

TEIXEIRA JÚNIOR. *Faroeste Digital*. In:Exame Negócios. Ed: 3. Ano: 1. Dez/2000.

TOLEDO, Francisco de Assis. *Princípios Básicos de Direito Penal*. 5ª ed. São Paulo: Saraiva, 1994

TURBIANI, Renata. Brasil lidera 'ranking' de ataques de hackers a sites. Diário Online. Disponível em: <www.dgabc.com.br/informatica/informatica. ldc?conta1= 184038>. Acesso em 14/11/2000

WILL, Clifford M. *Einstein Estava Certo?*. Trad. de Mary Grace Fighiera Perpétuo – Brasília: Editora UnB, 1996

ZAFFARONI, Eugênio Raul; PIERANGELI, José Henrique. *Manual de Direito Penal Brasileiro: Parte Geral*. 2ª ed. rev. e atual. São Paulo: Revista dos Tribunais, 1999

Disponível em : <http://www.internetlegal.com.br/artigos/fabioportela2.zip>
Acesso: 18/07/06