Crimes informáticos uma abordagem dinâmica ao direito penal informático

Computer crimes: a dynamic approach on Computer Science Penal Law

João Araújo Monteiro Neto

Especialista em Direito Penal pela UNIFOR,
Advogado e Professor Universitário
e-mail: joaoneto@unifor.br

Resumo

O avanço da informatização da sociedade pós-industrial não revolucionou somente a vida cotidiana, mas também, teve seu uso desvirtuado. A criminalidade evoluiu e passou a utilizar os sistemas informatizados não apenas como meio para prática de crimes já conhecidos, mas acima de tudo, passou a lesionar os bens juridicos advindos do avanço tecnológico. Surgem os Crimes Informáticos. Diante dessa nova realidade criminosa discute-se o conceito de crime informático, seus objetivos, suas classificações e a aplicabilidade ou não das normas penais existentes a essas novas condutas.

Palavras-chave: *Direito Penal. Direito Informático. Crimes Informáticos. Internet.*

Abstract

The advance of informatization on the pos-industrial society dont revoluces only the habitual life. At the same time the criminality became more powerful and use computer facilitys to make illegal conducts. That´s the computer crime. This new criminality reality is the object of this article. What means Computer Crime. It´s objective. It´s Classifcattions and the big question: The brazilian law offers any protection in the case of the computer crimes.

Keywords: *Criminal Law. Eletronic Law. Computer Crimes. Internet.*

Introdução

O desenvolvimento da informática e o maior acesso da população às facilidades por ela gerada reformularam a vida cotidiana. Grande parte das atividades humanas foi englobada pela automatização em vários setores de produção. Reformaram-se conceitos e novas atividades econômicas surgiram. Um novo mundo carecedor de auto-afirmação e regulamentação nasceu: o mundo virtual.

A informatização da sociedade como fenômeno fático-social também se tornou suscetível a deformações. Isto ocorreu quando percebeu-se a carência de regulamentação jurídica aplicável às relações ocorridas em meio eletrônico. As facilidades proporcionadas pelos sistemas informáticos fizeram com que as redes computacionais se tornassem meio de efetivação de negócios envolvendo valores cada vez maiores.

A riqueza que circulava sem proteção nos meios informáticos atraiu a atenção da criminalidade, que diante dessas novas perspectivas também se informatizou, e passou a praticar ilícitos através de meios eletrônicos, lesando bens jurídicos já penalmente protegidos e bens não tutelados por normas penais, os bens computacionais. Antigos crimes ganharam novos meios de execução, em contrapartida surgiram situações lesivas aos bens computacionais, ou seja, os Crimes Informáticos.

Tema novo dentro do contexto da ciência penal, o assunto possui importância destacada pois a ausência de normas aplicáveis aos crimes eletrônicos deixa uma série de condutas ilícitas carentes de punição, o que se configura como um incentivo à criminalidade, aumentando a sensação de insegurança reinante no meio, contribuindo sobremaneira para o não aproveitamento de todas as vantagens oferecidas pela utilização dos sistemas informáticos.

A matéria provoca controvérsia. Ora, como definir o que seja o crime informático? Como amoldar as condutas delituosas que são eventualmente perpetradas entre computadores ou sistemas de processamento de dados ao direito vigente no Brasil? Que espécie de infração temos quando o uso pacífico do computador é desvirtuado para, com o apoio da tecnologia, causar dano a outras pessoas físicas ou jurídicas, seja pela apropriação de dados remotos ou por sua utilização para obter vantagens ilícitas? Pode-se falar em crime, sem prévia cominação legal? São essas as questões abordadas no decorrer deste trabalho.

1 Breve Histórico da Internet

Apesar de parecer ter surgido da simples conexão espontânea de computadores, a Internet não se desenvolveu do nada. Trata-se do fruto de um planejamento estratégico que remonta à década de 60.

Ameaçados pelo véu da Guerra Fria, e temerosos de ataques militares oriundos do bloco soviético, o governo norte-americano, por meio do Departamento de Defesa, fomentou o projeto ARPANET, que foi criado e desenvolvido pela *Advanced Research Projects Agency* – Rede de Agência de Projetos de Pesquisa Avançada – (ARPA).

Consistia o Projeto ARPANET em uma rede de comunicação entre computadores visando à troca de informações para que, no caso de destruição de uma máquina, estas não fossem perdidas. De forma singela caracterizava-se como uma série de pequenas redes de computadores locais que se interligavam com redes regionais que se comunicavam entre si, criando, desta feita, uma rede nacional que impedia, no caso de ataques soviéticos, que a rede de comando dos Estados Unidos fosse interrompida. Ademais, evitava a concentração de informações vitais em uma única máquina, o que tornava o sistema de defesa ianque bastante vulnerável.

Em meados de 1990, o projeto ARPANET foi desativado. Contudo, a semente da Internet já tinha sido plantada. Percebendo o enorme potencial oferecido por esse meio de comunicação, as Universidades norte - americanas aproveitaram a estrutura existente e interligaram-se, formando assim uma rede nacional de troca de informações científicas, uma vez que os custos de uso da Internet para o envio de informações escritas eram muito menos onerosos do que os dos meios então existentes. Em face das facilidades e dos baixos custos, a rede, que interligava as universidades americanas, se expandiu para fora dos limites dos Estados Unidos e acabou tomando um caráter mundial, passando a servir de elo de comunicação entre meios acadêmicos de todo o mundo.

O primeiro passo para a expansão da Grande Rede foi o surgimento do *Internetting Project* em 1973. Esse projeto visava à criação de um sistema que interligasse todas as redes locais até então existentes. Era necessária a criação de uma ferramenta que possibilitasse a interconexão das diversas redes. Tal fato não era tão simples, uma vez que os sistemas de computadores existentes eram formados por máquinas diferentes bem como utilizavam *softwares* distintos, dificultando assim a troca de informações. Esse obstáculo foi transposto em 1974 com o desenvolvimento do Protocolo de Comunicação TCP/IP. O *Transmission Control Protocol/Internet Protocol* criado por Robert Kanh, foi utilizado como sistema base de interligação entre computadores de diferentes modelos. O TCP/IP funciona como um elo de ligação entre as máquinas, ou seja, um dialeto comum, uma espécie de acordo que permite a comunicação e o processamento das informações trocadas.

O segundo elemento detonador da explosão da expansão da Internet foi o desenvolvimento da *"World Wide Web (WWW ou W3).* Criada em 1989 no Laboratório Europeu de Física e Altas Energias, caracteriza-se por ser composta de hipertextos, que são documentos (textos, imagens ou sons) que se manifestam de maneira particular, podendo inter-relacionarem-se com outros documentos. Isto tornou simples a utilização e o acesso a serviços e informações, uma vez que o usuário não precisa conhecer os vários protocolos de acesso, mas tão simplesmente clicar seu *mouse.*

Contudo, até então, a Internet resumia-se a uma grande rede de intercomunicação de meios acadêmicos, não despertando interesse por parte de investidores. A maioria dos autores especializados estabelece como o principal marco para que a Internet chegasse aos patamares atuais o desenvolvimento dos *Browsers* – Folheadores. Um *Browser*, batizado no Brasil de Navegador, é um programa que permite a reprodução de imagens, textos ou sons armazenados em outros computadores a muitas centenas de quilômetros de distância. A principal revolução inserida por este *software* foi que com a sua utilização pode-se passar de uma página para a outra sem a necessidade de conhecimentos técnicos acurados. Essas espécies de programas foram os principais facilitadores da utilização da Rede pelos usuários domésticos sendo que o primeiro foi criado em 1993 no Centro Nacional de Aplicações para Supercomputadores, da Universidade de Illianois, localizada nos Estados Unidos.

As maiores economias nacionais vêem a Internet, o Ciberespaço, como um campo extremamente fértil para o desenvolvimento de suas empresas, uma vez que se trata de um sistema ágil

e em grande expansão. Exemplificando o poder da rede e sintetizando a sua capacidade de auto expansão, transcreve-se trecho da obra " Informática Jurídica – O Ciber Direito"(BRASIL, 2000, p. 21):

> Veio surgindo então um sistema ágil e interativo de acesso a informações como jamais visto anteriormente, que trouxe um novo modo de distribuição de riquezas e de produção completamente diferenciado dos métodos até então conhecidos. Exatamente quando essa revolução começou é de difícil precisão, porque sempre ficará a dúvida se foi com a expansão dos micro computadores ou se com o surgimento do primeiro programa que facilitava a navegação pelas páginas da WEB. O que podemos conferir é que 5 anos depois do lançamento do primeiro provedor de acesso à Internet nos Estados Unidos, 40% das casas americanas estavam conectadas à rede. Se olharmos para trás, vamos ver que fora m necessários 35 anos, à partir do surgimento da primeira usina geradora de energia para que 40% das residências norte americanas desfrutassem da luz elétrica.

2 Criminosos Virtuais

O mundo supostamente complexo da informática, suas expressões e linguagens peculiares, bem como a especificidade de conhecimentos virtualmente exigidos fazem crer que o criminoso de informática, ou seja, o agente ativo das condutas ilícitas, venha a ser um exímio perito na operação de computadores e sistemas computacionais.

Passou-se o tempo em que o perfil do criminoso virtual era esse. Atualmente com as facilidades ocasionadas pelo desenvolvimento de *Softwares e Hardwares*, bem como as inúmeras informações disponíveis na própria rede acerca do assunto, qualquer indivíduo que possua as mínimas noções de como operar um computador pode ser considerado um criminoso informático em potencial.

Ao contrário do que se apresentava nos anos 70 e 80, quando o criminoso de informática possuía conhecimentos específicos e detalhados, chegando a ser contratado, após o cumprimento de suas penas, por empresas especializadas em segurança de sistemas, os crimes informáticos ou os cometidos através da Internet passaram a ser conhecidos como os "*Special Oportunity Crime*", Crimes de Oportunidade. Normalmente os criminosos também são de oportunidade, não sendo afeitos à prática de condutas ilícitas, mas em face das facilidades e da oportunidade que surgem praticam o fato. Na maioria das vezes, são profissionais que laboram na área de informática e com freqüência praticam os delitos contra seus empregadores.

Os meios de comunicação divulgaram no correr dos anos um perfil extremamente romântico do criminoso informático, o que gerou dentro da sociedade uma sensação de aceitabilidade equivocada em relação a eles, pois acreditava-se que os delitos perpetrados possuíam menor potencial lesivo, não passando de brincadeiras de estudantes de classe média altamente especializados em informática, com boa escolaridade, inteligentes e normalmente acometidos da síndrome de *Robin Wood,* criando em favor de si uma certa simpatia social. O que em muito os distinguiam dos criminosos ditos comuns, pertencentes às classes D e E

O perfil criado e amplamente divulgado pela mídia tem o criminoso virtual como sendo em regra indivíduo do sexo masculino, que trabalha de alguma forma com a utilização de computadores e sistemas informáticos, com idade entre 16 e 33 anos de idade, avesso à violência e possuidor de inteligência acima da média. São extremamente audaciosos e aventureiros, movidos acima de tudo pelo desejo de conhecimento e de superação da máquina.

Hoje tais delinqüentes são, em geral, pessoas que trabalham no ramo informático, normalmente empregadas, não tão jovens nem inteligentes; são *insiders*, vinculados a empresas (em regra); sua característica central consiste na pouca motivabilidade em relação à norma (raramente se sensibilizam com a punição penal); motivos para delinqüir: ânimo de lucro, perspectiva de promoção, vingança, apenas para chamar a atenção etc.

Escondem-se normalmente atrás do sentimento de anonimato, que permeia a Rede, que serve para bloquear os parâmetros de entendimento da conduta que praticam como ilegal. Alegam ainda o desconhecimento do crime que praticaram e se escondem atrás do fato de praticarem o ato simplesmente por "brincadeira".

Notavelmente podem-se dividir as condutas ilícitas praticadas em três estágio de motivação (objetivos do criminoso). A primeira fase surge com seu instinto aventureiro; movidos pelo desafio de superação da máquina perpetram condutas criminosas. Uma vez superada a máquina e satisfeito o ego, percebem um meio fácil, e sob sua óptica seguro, de ganhar dinheiro extra, este é o segundo estágio. O terceiro caracteriza-se como um prolongamento dos segundo, uma vez que passam a praticar infrações com o intuito de sustentarem seus altos custos de vida que se resumem à compra de equipamentos de informática de última geração.

A questão é extremamente alarmante e perigosa. Para ilustrar tal situação, experimente pensar em um jovem brilhante estagiário de informática do centro de processamento de dados de uma Universidade, que altera as notas e as freqüências dos alunos, ou um promissor programador de computador de uma gigante multinacional ávido por reconhe-cimento que rompe os sistemas de segurança para depois apresentar-se como solução.

Verifica-se de maneira assustadora que o perfil do "criminoso virtual" difere em muito do criminoso comum, e isto embaça sobremaneira o trabalho de investigação e repressão a estes delitos.

Contudo, a figura mais associada à prática de ilícitos por intermédio de sistemas informáticos é a do *hacker.* Termo lendário e gerador de inúmeras polêmicas, o *hacker* está ligado diretamente ao surgimento dos primeiros sistemas informatizados e de forma genérica pode ser definido como aqueles que burlando os sistemas de segurança de redes de computadores obtêm acesso não autorizado ao sistema ou aos recursos por ele disponibilizados.

A origem da palavra *hacker* é bastante controvertida, indo desde o simples fato de dar um golpe cortante até o indivíduo que viola sistemas de informática. Procurando esclarecer o assunto David Casacuberta e José Luis Martín Más (2000, on-line) afirmam que:

> Según la leyenda, el primer uso no 'tradicional' del términp se debe a alguien que sabía donde dar el puntapié ("hack") exacto en una máquina de refrescos para conseguir una botella gratis. Ya sea en ese sentido o en el de cortar algo en pedazos, lo cierto es que el primer uso genuino de hacker en el mundo de la informática era el de alguien que conocá de forma tan detallada un sistema operativo (lo habáia 'cortado en pedazos' por así decirlo) que podía obtner de él lo que quisiera (como el señor de la leyenda urbana acerca de una máquina de refrescos). Así, en el sentido originario, un hacker es simplemente alguien que conoce los sistemas operativos (y por tanto los ordenadores) como la palma de su mano.

Apesar de possuir origem conturbada, o vocábulo *hacker* popularizou-se, principalmente por força dos meios de comunicação, como o criminoso informático. Contudo, no submundo virtual, a terminologia "hacker" dificilmente é associada a fins criminosos, sendo correlacionada tão somente a um indivíduo extremamente hábil no campo informático.

Dentro desse grupo, criou-se uma nova denominação, os *crackers.* No seio da comunidade informática, repousa quase que sagrada a divisão entre *hackers e crackers,* visto que os primeiros invadem sistemas computacionais com o objetivo tido, por eles, como nobre, por exemplo, verificar a segurança de determinada rede, ou somente para aprimorar suas técnicas. Já o *crackers*, tidos como os *hackers* não éticos, ou "maus", são os que enveredam pela criminalidade informática invadindo sistemas com interesses patrimoniais ou danosos.

A bem da verdade, independentemente dos objetivos ou das motivações pessoais, *hackers e crackers* invadem sistemas informáticos e invariavelmente violam a privacidade e o sigilo dos dados contidos nesses sistemas, o que por si só já configura crime na maioria dos países de primeiro mundo. Inúmeros estudos tentaram classificar os diversos tipos de *hackers*. Dentre eles podemos destacar Landreth[2], Hollinger e Rogers, mas é a classificação desenvolvida por Túlio Lima Vianna (2003). Para o professor mineiro, os criminosos informáticos se classificam da seguinte forma:

- Crackers de Servidores – hackers que invadem computadores ligados em rede;
- Crackers de Programas – hackers que quebram proteções de *softwares* cedidos a título de demonstração para usá-los por tempo indeterminado;
- Phreakers – hackers especialistas em telefonia móvel ou fixa;
- Desenvolvedores de Vírus, Worms e Trojans – programadores que criam pequenos *softwares* que causam algum dano ao usuário;
- Piratas – Indivíduos que clonam programas fraudando direitos autorais;
- Distribuidores de *Warez* – *webmaters* que disponibilizam em suas páginas *softwares* sem autorização dos detentores dos direitos autorais.

Dentro desses vários grupos de criminosos informáticos, devemos destacar que tudo se originou com os chamados Crackers de Servidores, os quais foram responsáveis tecnicamente pelas invasões de computadores, de redes. Essa categoria do gênero *hacker* se subdivide, segundo o entendimento de Túlio Lima Vianna (2003), nas seguintes sub-categorias:

- Curiosos – movidos por curiosidade, não causam danos aos dados armazenados ou em tráfego pelas redes informáticas, restringindo-se somente a violar a privacidade das vítimas e o sigilo dos dados em trânsito pelos sistemas computacionais;
- Pichadores Digitais – procuram auto-afirmação dentro da rede, agindo com o único objetivo de serem reconhecidos e famosos no universo virtual;
- Revanchistas – formados por ex-funcionários ou empregados descontentes que se utilizam dos conhecimentos auferidos na empresa para sabotá-la;
- Vândalos – agem simplesmente pelo prazer de causar danos às vítimas;

[2] *Landreth classificou os hackers em seis níveis: Os novatos (Novice) que possuíam menor capacidade técnica e lesiva; Os estudantes (Student) que ao revés de se dedicar a seus afazeres acadêmicos passa seu tempo invadindo sistemas; O turista (Tourist) que invade sítios pela sensação de aventura; O estilhaçador (Crasher) que invade sistemas com objetivos de danificá-los, e o Ladrões (Thief) que possuem objetivos econômicos).*

- Espiões – agem com a finalidade de adquirirem informações confidenciais armazenadas nos sistemas computacionais das vítimas. As informações podem ter caracter comercial ou não;
- Ciberterroristas – possuem motivações políticas ou religiosa e utilizam-se do meio digital para realizarem atividades criminosas que possibilitem a divulgação de suas crenças;
- Ladrões e Estelionatários – têm objetivos de lesar o patrimônio das vítimas.

A realidade social e cultural que permeia o ambiente digital torna extremamente complexa a confecção de um perfil do chamado criminoso virtual. Contudo, a complexidade de relações ilícitas potencializadas pela utilização das redes informáticas, bem como as inúmeras possibilidades de classificação desses criminosos, o que torna essa atividade muito mais *sui generis,* fazem com que a criminologia cada vez mais se interesse pelo tema e busque, dentro de seus pressupostos científicos, erigir um conceito científico a ser adotado pelo direito penal.

3 Direito Penal e Informática

O desenvolvimento tecnológico, principalmente no campo da informática, modificou de forma irreversível o cotidiano das atividades humanas.

A revolução da informação, que gerou uma nova classe de excluídos: os *unplugged,* que constituem um proletariado *off line* ao lado de uma elite *on line,* abalou de forma cabal as estruturas do Direito.

Além de propiciar facilidades e vantagens até então nunca cogitadas, as redes informáticas também se revelam um extremo facilitador para a perpetração de ilícitos, uma vez que os meios existentes para as práticas de delitos informáticos são inúmeros e dada as características dessas infrações, os vestígios deixados são mínimos, o que torna a repressão e a persecução a estes atos tarefa árdua.

A informática se tornou fator de suma importância nas relações econômicas, sociais, em suma, situações jurídicas de natureza diversa. Colocar em risco tais relações, que movimentam vultosas quantias, é uma afronta à regulamentação social.

É nesse contexto que aflora a importância da relação entre o Direito Penal e a Informática. "Partindo da premissa que o Direito é a única forma de controle capaz de conter o avanço da criminalidade no mundo virtual, isto porque, de todos os sistemas de controle social, o Direito, possuindo estrutura imperativo atributiva, e (...) a coercitividade, sancionando assim as condutas ilícitas" qualquer que seja a angulação enfocada, penal, civil ou trabalhista (DOUN; BLUM. In: LUCCA; SIMÃO FILHO, 2000,p 119).

Neste sentido o Professor de Direito Penal, Luiz Flávio Gomes (*apud* ELIAS, 2001, on-line), reivindica a criminalização específica dos crimes informáticos no Brasil. Em nosso ordenamento jurídico já existem normas que tipificam algumas condutas, como a Lei 9.983/00 e a Lei 9504/97, dentre algumas poucas outras. Contudo são tipos penais extremamente específicos, que visam a proteger bens jurídicos restritos amparando tão somente a administração pública, o processo eleitoral e a previdência social. Ressalte-se que a existência de legislação específica não serve de óbice à elaboração de legislação penal mais geral. Nesta linha de pensamento o uso da informática pode ser considerado um fator criminógeno por que:

a) Abre novos horizontes ao delinqüente (que dela pode valer-se para cometer infindáveis delitos – é a instrumentalização da informática);

b) Permite não só o cometimento de novos delitos (p.ex.: utilização abusiva da informação armazenada em detrimento da privacidade, intimidade e imagem das vítimas) como a potencialização dos delitos tradicionais (estelionato, racismo, pedofilia, crimes contra a honra etc.);

c) Dá ensejo, de outro lado, não só aos delitos cometidos com o computador, senão também os cometidos contra o computador (contra o *hardware, o software* ou mesmo contra a própria informação – Computer Crime) (GOMES *apud* ELIAS, 2001, on-line);

Pactuando desse entendimento, Henry Bosly (*apud* FERREIRA. In: BARRA; ANDREUCCI, 1992) estabelece a existência de três esferas distintas de relações entre o Direito Penal e a Informática: a informatização da documentação penal; a informatização dos procedimentos administrativos e judiciais; a informática a serviço da delinqüência.

A informatização da documentação penal relaciona-se com os processos informáticos que revolucionaram o tratamento de dados policiais e judiciários. Compreende além dos famosos fichários policiais, os arquivos judiciários e os dos serviços de segurança. É justamente contra essas espécies de documentos informáticos que muitas vezes se faz necessário reforçar medidas de proteção às garantias individuais, uma vez que com certa freqüência se verifica uma excessiva ou leviana intromissão dos órgãos estatais reguladores e administradores desta fontes de informação na vida privada dos cidadões. Nestes casos a informática funciona como uma ferramenta que agiliza a coleta, a organização, o armazenamento e a manipulação desses bancos de informações indispensáveis às atividades investigativas. Ressalte-se que, visando a coibir os abusos praticados na criação e utilização dessas informações, muitas vezes sigilosas, nossa

Constituição Federal instituiu em nosso ordenamento jurídico a garantia constitucional do Habeas Data, que assegura ao impetrante o direito de conhecer e até retificar as informações constantes nestes bancos de dados relacionadas à sua pessoa.

A informatização dos procedimentos administrativos e judiciais tem como escopo o melhoramento e o aperfeiçoamento da distribuição da justiça. É através da informatização de emissão de documentos da *pareis* forense, como certidões, alvarás, termos de audiência, bem como outros de cunho administrativo, que se tem de certa forma aliviado os trabalhos judiciários e ajudado a fiscalização e controle do cumprimento das sentenças e da execução das penas. É notório nos grandes centros urbanos brasileiros, o nível de modernização dos órgãos da justiça penal, as antigas máquinas de datilografar e os obsoletos fichários manuais vêm sendo substituídos por aparelhos mais modernos e sistemas de processamento automático de dados. O que se tornou não uma conveniência mas sim uma necessidade em face do grande número de processos que se acumulam nos tribunais. Exemplo cabal das facilidades e segurança geradas pela informatização desses procedimentos na esfera penal é a emissão da certidão de antecedentes criminais exarada por meio de consulta a banco de informações informatizado que interliga todas as varas criminais.

A informática a serviço da delinqüência comporta as infrações informáticas e as infrações comuns cometidas através de sistemas informáticos."De fato, esses crimes de informática ora representam novas maneiras de executarem-se as figuras delituosas tradicionais já tipificadas na lei penal, ora apresentam aspectos específicos pouco conhecidos, que não se adaptam a incriminações convencionais nem seus autores aos modelos criminológicos comuns." (FERREIRA. In: BARRA; ANDREUCCI,1992, p.144).

A utilização de meios informáticos para a prática de atos ilícitos gera duas situações distintas. A primeira é aquela na qual o uso da informática consubstancia-se como ferramenta para a perpetração de conduta já tipificada como crime por lei penal. A segunda se caracteriza pela prática de ato não abarcado no ordenamento jurídico penal, ou seja, condutas ilícitas realizadas através de meios informáticos ou contra estes, que não se amoldam a nenhum fato típico descrito em lei, consistindo assim em uma nova figura delitiva.

As formas delituosas são inúmeras e de natureza distintas, tem-se as mais diferentes formas de fraudes, furto, apropriação indébita, vandalismo, crimes do colarinho branco, violações autorais, sabotagem, espionagem industrial e diversos outros delitos.

Existem ainda as condutas que atentam contra a integridade da própria máquina, como por exemplo, a disseminação intencional dos chamados "vírus de computador"[3] que podem inutilizar todos os dados existentes em uma máquina, causando prejuízos incalculáveis ao proprietário.

As facilidades para a prática desses delitos, adicionada à possibilidade de serem praticados em locais distantes de onde se operaram os resultados, e a sensação de impunidade reinante no meio informático fazem com que a situação se torne extremamente perigosa beirando se tornar incontrolável.

Extremamente necessário é o desenvolvimento do Direito Penal Informático para que se discipline a matéria, evitando assim a ampliação do caos reinante, que gera a sensação de que os meios informáticos, principalmente a Internet, são carentes de regulamentação, sendo territórios anárquicos, férteis para a prática de ilícitos, e isto deve ser coibido.

Entretanto, necessário é o estudo aprofundado do mundo virtual para que se possa disciplinar juridicamente a matéria por meio da elaboração de mecanismos jurídicos que acompanhem a evolução tecnológica da informática, evitando-se dessa forma os perigos de uma inflação legislativa relacionada à matéria. Desta feita, a legislação aplicável ao tema estaria revestida de um embasamento doutrinário jurídico que evitaria o seu "engessamento" em face do avassalador desenvolvimento tecnológico, podendo ser aplicável e eficaz mesmo com o surgimento de inovações alteradoras da realidade fática atinente ao assunto. Assim não cairiam em desuso uma vez que se adequariam às novas realidades vindouras, não se tornando "letra morta". (DOUN; BLUM. In: LUCCA; SIMÃO FILHO, 2000, p. 121)

4 Conceito de Crime Informático

O surgimento e a evolução da informática vêm resultando na crescente informatização das atividades rotineiras, reformulando de forma inquestionável o cotidiano mundial.

Entretanto, esse avanço tecnológico tornou-se uma ferramenta extremamente facilitadora para a perpetração de delitos. Novas formas de praticar crimes já existentes surgiram, bem como condutas criminosas inéditas foram criadas. Nasceram assim os crimes informáticos ou *Computer Crimes,* cujo

[3] *Ricardo Cidale define o vírus de computador como "um programa como outro qualquer. Entretanto, enquanto a maioria dos programas visa ao aumento da produtividade no ambiente de trabalho, o programa -vírus quer destruí-la", danificando o sistema informático. (CIDALE apud REIS, 1997, p.33.*

conceito, por se tratar de figura nova no mundo jurídico, vem sendo formulado através de verdadeiras batalhas doutrinárias, o que lhe confere uma mutabilidade *sui generis*.

Valdir Sznich (*apud* COSTA, 2001, on-line) define Crime de Informática "como qualquer ato ilegal onde o conhecimento especial de tecnologia de informática é essencial para a sua execução, investigação e acusação."O conceito suso mencionado se caracteriza por ser muito amplo e atrela necessariamente a prática do delito ao conhecimento de técnicas de informática, não mencionando a necessidade de o objeto do delito ser um sistema de informática ou um conjunto de dados, tornando-se, assim, um conceito muito amplo e abrangente, não delimitando de forma objetiva o objeto de estudo.

João Marcello de Araújo Júnior (*apud* MELO, 2000) conclui que o Crime Informático consiste em "uma conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder à obtenção de uma vantagem ilícita, porém praticada, sempre com a utilização de dispositivos habitualmente empregados nas atividades de informática".

Apesar de incorrer nos mesmos deslizes da definição supra mencionada, o Professor João Marcello Araújo estabelece um novo elemento em sua conceituação: A ausência de obtenção de vantagem ilícita. Em verdade, verifica-se muitas vezes que nos crimes informáticos a sua perpetração não corresponde à obtenção de uma vantagem ilegal, mas simplesmente a satisfação do ego ou um teste ao delinqüente que superou os sistemas de segurança da rede de informática, por exemplo.

Na mesma linha de pensamento Dom Parker (1997, p. 25) afirma que "Abuso de computador é amplamente definido como qualquer incidente ligado à tecnologia do computador, no qual uma vítima sofreu, ou poderia ter sofrido, um prejuízo, e um agente teve, ou poderia ter tido, vantagens."

Os conceitos suso mencionados se caracterizam ora por sua grande abrangência, ora por limitarem-se a alguns aspectos dos Crimes Informáticos. Nessa esteira a OECD – Organização para Cooperação Econômica e Desenvolvimento define o Crime Informático como " qualquer conduta ilegal, não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados". (REIS, 1997, p. 25) Verifica-se que as definições acerca do que seja um Crime Informático não satisfazem a necessidade de identificar de maneira objetiva o que seja um *Computer Crime* e qual o seu objeto. Michael Gemignani (*apud* REIS, 1997, p. 25) com muita ironia levanta questionamentos acerca do tema: "Se uma secretária cansada de ser desfalcada pelo computador, deliberadamente jogasse café na máquina, isto seria um crime informático ou um ato de vandalismo contra a propriedade da empresa?" (GEMIGNANI *apud* REIS, 1997, p.25).

Apesar dos inúmeros entendimentos colacionados se pode concluir que a definição de Crime de Informática deve estar intrinsecamente relacionada ao bem jurídico que se almeja proteger. Ao contrário dos delitos tradicionais, que podem ser perpetrados contra os sistemas de computação ou contra os *softwares* (por exemplo o furto), o crime informático é aquele perpetrado contra bens jurídicos computacionais e o conjunto de dados/informações contidos nos sistemas informáticos, estando estes armazenados, sob manipulação ou em transmissão.

Desta feita a célula básica para uma definição do crime informático parte da análise do bem jurídico a ser tutelado pela lei penal incriminadora, o que culmina com a conclusão de que a proteção estatal deve recair sob a proibição de condutas que atentem contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela inserção, manipulação, compilação, armazenamento, processamento e transmissão de dados/informações.

Depreende-se a existência de dois pressupostos necessários para a caracterização do crime informático:

- O crime deve ser perpetrado contra dados aptos ao processamento informático (O agente deve possuir a vontade subjetiva de lesar os dados);
- Sejam perpetrados através do computador (Deve ser perpetrado por meio da utilização de Hardware ou Software).

Assim a secretária que, desejando se vingar do computador, jogou café contra a máquina, não cometeu um crime informático, mas sim um delito comum, uma vez que, apesar de atingir o dados armazenados no aparelho, a vontade subjetiva da mesma não era a de lesar bens jurídicos informáticos, além do mais deve a conduta ser perpetrada através de meio informático, o que não engloba a utilização de café.

Considerando a moderna doutrina penal para a conceituação de crime exposta no capítulo anterior, verifica-se a necessidade de adequar o conceito de crime informático ao conceito clássico de crime ao qual nosso ordenamento jurídico se filia.

Assim o fazem Ivette Senise Ferreira (In: LUCCA; SIMÃO FILHO, 2000, p. 210) e Alexandre Jean Doun (In: BLUM, 2001 p.206) : "Constitui crime de informática toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou pela sua transmissão."

Abrangendo uma ampla gama de relações sociais e individuais abarcada pela utilização da

informática e suscetíveis à prática delituosa, essa definição consagra ainda os elementos necessários à criminalização de condutas nos termos da teoria adotada pelos legisladores pátrios.

Qualquer comportamento humano, quer comissivo, quer omissivo, encontra-se abrangido pelo conceito de ação. Ressalte-se que a conduta deva ser típica, correspondendo a um modelo previsto em lei como crime, sempre respeitando-se o princípio basilar do direito penal "*nullun crimem nulla poena sine lege.*"[4]

É com base nos comentários acima tecidos que o Secretário Executivo da Associação de Direito e Informática do Chile, Cláudio Libano Manzur (*apud* PINHEIRO, 2001) conseguiu captar quase todos os elementos necessários a definir com clareza o crime informático como:

> Todas aquellas aciones u omissiones típicas, antijurídicas y dolosas, trátase de hechos aislados o de una série de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la infromación y destinadas a producir un perjuicio en la victema a tráves de atentados a la sana técnica infrormática, lo cual generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, repontándose, muchas veces, un beneficio ilícito en el agente, sea no se caracter patrimonial, actúe com o sin ánimo de lucro.

Apesar da clareza do doutrinador chileno, uma nova discussão deve ser levantada visando a uma conceituação mais técnica. A maioria dos conceitos formulados revela a existência de uma bipolarização acerca do objetivo dos crimes informáticos. De um lado existe a corrente que pugna pela proteção dos dados e das informações contidas no sistema computacional; do outro requer-se tão somente a proteção aos sistema informáticos.

A escolha de um só desses objetivos como sendo o único a ser alvo dos delitos informáticos criará lacunas que tornarão insustentável a regulamentação jurídica do tema, pois surgiram vácuos carentes de proteção legal propiciando a prática de inúmeros delitos.

Neste sentido defende-se que o objetivo do crime informático deve recair sobre os sistemas informáticos e sobre os dados e informações nestes contidos. Desta feita os bens jurídicos a serem protegidos por meio de norma informática penal incriminadora possuiriam aspecto mais amplo abarcando uma série de condutas a serem prevenidas.

Após tecer-se as considerações suso colacionadas, pode-se compor um conceito de crime informático que se coadune com as proposições doutrinárias seguidas bem como preencha os requisitos formais estabelecidos por nosso ordenamento jurídico.

Assim, o crime informático pode ser conceituado como toda ação típica, antijurídica e culpável perpetrada contra um sistema de informática ou contra os dados e informações existentes no sistema computacional, não importando se o ato ocorre na introdução, no tratamento, no armazenamento ou na transmissão dos dados.

Nos delitos informáticos a conduta típica atentará contra um sistema de informática, contra o processamento automático de dados ou em sua transmissão. Consiste na utilização de uma sistema de informática para atentar contra sistemas computacionais ou contra os dados contidos nestes.

Com base no bem juridicamente ofendido, tece-se a classificação da ação ilícita em categorias distintas, surgindo assim novos problemas específicos que desafiam os aplicadores do direito. Em face disto sustenta-se a necessidade de elaboração de uma nova construção doutrinária aplicada ao Direito Penal da Informação, dos dados e dos bens intangíveis, que são as bases dos sistemas informáticos e dos ilícitos praticados sob a égide de Crimes Eletrônicos.

5 Sistemas de Classificação do Crime Informático

Por se tratar de matéria nova no cenário jurídico, não possuindo ainda bases doutrinárias sólidas, afluem diversos sistemas de classificações acerca do Crime Informático. Estes sistemas se utilizam de vários critérios para efetuarem suas classificações, dentre os existentes destacam-se os abaixo mencionados. Partindo da forma de atuação do autor, o Professor Sieber (1997, p. 29) estabelece a seguinte classificação: Fraude por manipulação de um computador contra um sistema de processamento de dado; Espionagem informática e furto de software; Sabotagem Informática; Furto de tempo; Acesso não autorizado; Ofensas tradicionais.

A fraude por manipulação de um computador contra um sistema de processamento de dados consiste na modificação de dados dentro de um sistema informático com intuito de se obter vantagem ilícita. Pode ocorrer por meio da introdução de dados falsos ou também por meio da alteração dos resultados.

Os delitos capitulados sob a classificação de Espionagem Informática consistem nos ilícitos que possuem como objetivo a obtenção de dados ou

[4] *Brocado latino de significado: Não há crime nem pena sem lei que os defina.*

informações sigilosas por meio de sistemas de informática. Um exemplo de espionagem informática oferecido pelo autor é a coleta de dados através da radiação eletrônica emitida por um terminal informático que pode ser captada e armazenada até aproximadamente um quilômetro de onde está situado o terminal. Já o furto de *software*, que pode ser realizado pelo modo descrito anteriormente, restringe-se não a apropriação do meio físico de suporte do programa, mas sim à apropriação de elementos formadores da estrutura do *software*, elementos imateriais basilares da composição do programa, que servem para a elaboração de programas similares concorrentes ao *software* espionado.

A Sabotagem Informática é um dos mais danosos delitos praticados por meio de um sistema informático e tem como objeto o próprio sistema. Efetua-se principalmente por dois meios. O primeiro é a destruição do programa ou dos dados por meio de elementos criados pelos sabotadores como vírus ou mini - programas que, quando ativados, inutilizam os programas principais destruindo-os ou distorcendo o seu funcionamento, tornando o sistema inapto a processar. O segundo ocorre quando estes mecanismos desfiguram os dados já armazenados, o que acarreta inúmeros prejuízos aos programas principais.

O Furto de Tempo é a modalidade ilícita mais comum e mais difundida dos crimes informáticos. Ocorre o furto de tempo quando pessoas sem autorização utilizam-se de sistemas informáticos para fins particulares. Normalmente ocorre em empresas quando o funcionário sem possuir autorização para acessar a rede informática burla os sistemas de segurança e utiliza o computador e seus recursos para fins alheios aos interesses do empregador. O acesso não autorizado pode render ao infrator vantagens ilícitas como dinheiro e informações. Algumas legislações estrangeiras já consideram como propriedade da empresa o tempo de uso do computador, incriminando o seu uso não autorizado.

O acesso não autorizado a sistema informático configura-se de longe como o crime informático que mais se desenvolveu com o surgimento da Internet. É através da rede mundial de computadores que os *hackers e crackers* encontram meios para as invasões em massa a sistemas informáticos particulares. Consiste de maneira simples em um acesso por pessoa não autorizada a um sistema de informática restrito, no qual o invasor, de maneira ilegal, pode ter acesso a informações sigilosas, manipulando-as, de forma a destruí-las, alterá-las ou praticar outras ações delituosas.

A última categoria elencada por Sieber em sua classificação refere-se às ofensas tradicionais que podem ser praticadas por meio de um sistema de informática ou que tenha a sua parte tangível como objeto. Consubstancia-se na utilização de um sistema informático para a prática de ilícitos comuns, em que o computador ou o sistema computacional não passa de novo meio de execução, como por exemplo a falsificação de documentos.

Utilizando como base o trabalho do Dr. Sieber, Martine Briat (apud FERREIRA. In: BARRA; ANDREUCCI, 2000, p.213) estabelece uma classificação um pouco mais específica, mas que pouco difere da anterior disposta:

- Manipulação de dados e/ou programas a fim de cometer uma infração já prevista pelas incriminações tradicionais;
- Falsificação de dados, de programas e entrave a sua utilização; Divulgação, utilização ou reprodução ilícitas de dados e de programas; Uso não autorizado de sistema de informática; Acesso não autorizado a sistema de informática.

O sistema de classificação proposto por Briat não possui diferenças palpáveis em relação ao elaborado por Sieber, uma vez que a essência da classificação é a mesma, alterando-se tão somente o nome das classes de delitos.

Rompendo com a linha de pensamento inicialmente disposta, Marc Jaeger (*apud* FERREIRA. In: BARRA; ANDREUCCI, 2000, p.214) ao revés de utilizar a expressão crime informático, utiliza em sentido amplo o termo Fraude Informática para designar as ações ilícitas ou anti - sociais ligadas ao uso da informática, classificando tais ações em: Fraudes propriamente ditas.

- Atentados à vida privada.

Os atentados à vida privada compõem-se por condutas que, apesar de serem perpetradas através de meio informático, lesam interesses jurídicos distintos dos que formam o conjunto de bens informáticos, caracterizando a prática de crime comum. O conjunto de condutas danosas a esta reunião de bens computacionais configura as fraudes propriamente ditas, que comportam uma ampla gama de condutas lesivas aos sistemas informáticos e que se subdividem ainda em: nível da matéria corporal; nível do *input;* nível do tratamento; nível do *output*.

As fraudes no nível do Hardware são aquelas que atingem a integridade física do sistema informático, danificando-o ou inutilizando-o. As fraudes no nível de *input* são as perpetradas por meio da inserção de dados alterados em um sistema informático. Quando as fraudes são perpetradas ao nível de processamento, ocorre uma modificação no programa responsável pelo tratamento dos dados o que altera significativamente os resultados do processamento destes. Já as fraudes ao nível de *output* consubstanciam-se quando o autor altera dados corretos que passaram por um processamento

adequado estando aptos a serem externados. Logo é uma fraude ocorrida no intervalo de envios dos dados processados aos dispositivos de saída do sistema computacional.

Neste mesmo sentido o catedrático espanhol Romeo Casabona (*apud* REIS, 1997, p.31) estabelece que os crimes informáticos podem ser classificados em quatro categorias: Manipulação de entrada de dados (*input*); Manipulações no programa; Manipulações na saída de dados (*output*); Manipulações a distância**.**

A manipulação de entrada de dados perpetra-se por meio da manipulação de dados quando de sua introdução ao sistema computacional, quer seja pela introdução de dados falsos, quer pela alteração destes, ressaltando-se a possibilidade de a manipulação ocorrer em face da omissão do registro de dados que deveriam compor toda a informação. As manipulações no programa acontecem através de modificações ou eliminações de etapas do programa que fazem com que o processamento conduza a resultados errôneos, mesmo quando os dados inseridos no sistema são corretos. As manipulações na saída de dados ocorrem quando dados verdadeiros são tratados por programas inalterados mas os dados obtidos pelo processamento são alterados na saída do equipamento, como por exemplo quando estes estão sendo enviados à impressora. As manipulações a distância ocorrem quando o computador manipulado encontra-se conectado com outros formando assim uma rede. As alterações acontecem a distância sendo efetuadas por máquina distinta da que está sendo manipulada.

Mudando o parâmetro de classificação para a finalidade do delito, e excluindo os crimes já enquadrados nos ordenamentos jurídicos, Pradel (*apud* FERREIRA. In: BARRA; ANDREUCCI, 2000, p.214) assim os delimita:

- Manipulações para obtenção de dinheiro;
- Manipulações para obtenção de informações.

A manipulação para obtenção de dinheiro deve ser entendida em sentido amplo, qual seja de qualquer proveito econômico, comportando todas as atividades ilícitas que importem de alguma maneira em uma vantagem econômica para o autor. A manipulação em busca de informações paira sob um só aspecto: a utilização do sistema computacional para a obtenção de informações às quais o autor não possui direito, violando assim o sigilo das mesmas.

A classificação confeccionada por Pradel é uma das mais bem elaboradas, uma vez que exclui os delitos já abarcados pelo ordenamento jurídico, classificando tão somente os verdadeiros delitos informáticos. Contudo a mesma não abraça todos os possíveis ilícitos cometidos contra sistemas de informática, uma vez que estes novos crimes muitas vezes são praticados sem o intuito de obtenção de vantagem, mas simplesmente com o objetivo de causar prejuízo, danificando o equipamento, como na sabotagem informática.

Em outro contexto vem se consagrando na doutrina internacional o sistema binário de conceituação proposta por Hervé Croze e Yves Bismuth (*apud* FERREIRA. In: BARRA; ANDREUCCI, 2000, p. 215): Atos dirigidos contra um sistema de informática, independentemente da motivação do autor; Atos que atentam contra outros valores sociais através de um sistema informático.

Da classificação acima estabelecida obtêm-se o entendimento da existência de duas situações fáticas – jurídicas distintas. Existem condutas praticadas por meio de computador contra outros bens jurídicos, funcionando o sistema informático como instrumento da ação, e existem atos que são praticados contra dados ou informações armazenados, em processamento ou em transmissão, ou contra a integridade do próprio sistema, sendo estes objetos materiais da ação.

São os atos praticados contra um sistema informático os delitos computacionais autênticos, pois o sistema computacional funciona como instrumento e objetivo da ação, sendo meio e meta do ato, podendo está recair sob os dados e informações armazenados, bem como sob a própria máquina, seu suporte lógico e até os periféricos. Nos atos que atentam contra outros valores sociais o computador é apenas a ferramenta executória do crime fim.

Absorvendo os avanços doutrinários internacionais os autores nacionais passaram a acatar com quase unanimidade os elementos básicos da classificação suso exposta, Luis Flávio Gomes divide os crimes informáticos em duas categorias semelhantes as proposta por Croze & Bismuth, qual sejam os crimes praticados contra o computador em sentido amplo e crimes por meio de computador (ELIAS, 2001, on-line).

Nesta mesma corrente de pensamento Damásio Evangelista de Jesus (ARAS, 2001, on-line) classifica os crimes informáticos em duas categorias, os crimes informáticos puros ou próprios e os crimes informáticos impuros ou impróprios. Os delitos próprios são aqueles praticados por meio de um computador onde o resultado da conduta se opera em meio eletrônico, sendo a informática o bem jurídico protegidos (segurança do sistema e titularidade das informações, integridade da máquina e dos periféricos e etc.), já os crimes informáticos impróprios são aqueles em que o sistema computacional funciona como ferramenta para a prática de condutas lesivas a bem jurídicos já protegidos, não relacionados com a informática, produzindo resultado naturalísticos que ofendem o mundo real.

Verifica-se que a maioria dos sistemas de classificação podem ser resumidos as duas categorias elencadas por Damásio ou por Croze & Bismuth, resumindo-se em condutas que atentem contra o sistema informático ou a atos que lesem outros bem jurídicos já penalmente protegidos. Compreende-se a importância da discussão doutrinária à cerca da correta classificação dos crimes informáticos, bem como a necessidade de produção científica embasadora da matéria, contudo ao se proceder análise à cerca das classificações propostas se percebe que o objetivo alcançado por esta foi tão somente distinguir o crime informático do crime tradicional cometido por meio de um sistema informático. O uso do sistema computacional para a perpetração de condutas ilícitas já tipificadas como o furto ou o estelionato não se faz capaz de conferir a natureza de crime informático a conduta praticada, pois verifica-se que o computador funcionou como um novo meio de execução de conduta já descrita em norma penal incriminadora que protege outro valor social alheio aos bens computacionais. E isso em uma sociedade cada vez mais informatizada passará a ser mais comum, uma vez que a delinqüência, vislumbrando o surgimento de inúmeras oportunidades também se informatizará passando a utilizar em maior escala o computador para a prática de delitos comuns.

O simples surgimento de um novo meio de execução de uma conduta já tipificada não altera o seu núcleo nem o objeto protegido, não alterando sua classificação nem sua natureza, exemplo cabal disso foi o surgimento da arma de fogo que apesar de ter sido um novo meio de execução do homicídio não alterou a sua figura típica, pois o cerne do fato típico ficou inalterado uma vez que a descrição: matar alguém[5], adapta-se a prática do delito por inúmeros meios, inclusive com uso de arma de fogo.

Desta feita percebe-se que os esforços em busca da classificação dos crimes informáticos não alcançaram os seu desiderato de forma completa pois tão somente ajudaram a sedimentar a distinção entre crime informático e crime comum, ressaltando-se a importância do caracter didático destas classificações.

Neste sentido faz-se necessário a reformulação dos sistemas de classificação extirpando-se dos seus conteúdos os crimes já abarcados por normas penais tuteladoras de outros interesses jurídicos que não os computacionais, como por exemplo: Quantos aos efeitos dos crimes informáticos:

- Crimes informáticos de efeitos tangíveis;
- Crimes informáticos de efeitos intangíveis.

Classificam-se como crimes de informática de efeitos tangíveis aquelas condutas que além de perpetrarem-se em meio eletrônico produzem também efeitos diretos no mundo real, exemplo cabal destes ilícitos é a ação de sabotagem informática que além de danificar ou inutilizar os dados efetua danos muitas vezes irreparáveis na máquina. Já a ações que debelam crimes informáticos intangíveis lesam tão somente os elementos imateriais formadores do sistema informático com os dados armazenados, em processamento ou em transmissão. Quanto aos objetivos: Crimes informáticos de mero acesso; Crimes informáticos de dano ou lesão.

Os crimes informáticos de mero acesso consubstanciam-se com o simples acesso ao sistema informático, não necessitando que do acesso resulte algum dano a dados ou ao próprio sistema. Por outro lado os crimes informáticos de dano ou lesão são aqueles que de maneira direta danificam o sistema computacional sem necessidade da obtenção de alguma vantagem econômica ilícita para o autor, é o que ocorre na sabotagem informática ou na disseminação de vírus.

São classificações neste sentido que devem ser elaboradas pois facilitam o estudo e divisão da matéria, não se desmerecendo o valor doutrinário e didático dos sistemas classificatórios enunciados neste trabalho, mas deve-se ressaltar que estes sistemas serviram para evidenciar a distinção entre crimes comuns (tradicionais) e crimes informáticos, uma vez que o uso do computador para praticar condutas já incriminadas por tipos penais não pode ser considerado um crime informático pois o sistema informático não passou de um meio de execução, e isto no máximo pode render a tal prática a qualificação da conduta alterando-lhe a pena pois o núcleo do tipo penal permaneceu inalterado.

Nesses casos cabe ao legislador a criação de qualificadoras e elementos majorantes genéricos para as condutas perpetradas por computador que atentem contra bens juridicamente já protegidos, evitando-se a criação de tipos penais extremamente específicos unicamente pelo surgimento de um novo meio de execução.

6 O Princípio da Reserva Legal

Após se delimitar com mais clareza os horizontes do Crime Informático, bem como distingui-lo do crime comum, necessária é agora a análise dos delitos informáticos existentes no ordenamento jurídico brasileiro e dos principais projetos de lei que visam regular a matéria.

[5] *Artigo 121 do Código Penal Brasileiro.*

É com essa evolução legislativa influenciada pelo direito comparado que surge um novo ramo do Direito Penal, o Direito Penal Informático, que apresenta elementos peculiares adequando-se a nova realidade e a nova onda criminológica que surge.

Diante do conceito clássico de crime, que estabelece como elementos indispensáveis deste, a ocorrência de fato típico, antijurídico e culpável, se deve tecer algumas considerações à cerca do princípio da reserva legal, pois tratar crime sem lei que o defina , é tratar do assunto em ordem inversa.

A cerca do surgimento do princípio da reserva legal existem entendimentos variados. Boa parte do entendimento doutrinário sustenta que esta garantia surgiu por intermédio da Carta Magna do Rei João Sem Terra em 1215. Em contrapartida outra corrente de pesquisadores afirma que o núcleo do princípio da reserva legal surgiu em 1816 no Direito Ibérico durante o Reinado de Afonso IX.

O mais importante neste período medieval é que apesar do surgimento ainda embrionário do princípio da reserva legal e de sua natureza rudimentar, neste período ainda se permitia a analogia por parte do arbitro judicial e do Rei para a criação de crimes, gerando uma insegurança criadora de enormes tensões sociais.

Seguindo com a evolução deste princípio Beccaria(1998, p.41) defende que só por meio da lei se pode fixar as penas de cada delito, e esta função, ou seja legislar sobre matéria penal compete exclusivamente ao Poder Legislativo.

O amadurecimento da teoria que culminou com o estabelecimento do Princípio da Reserva Legal nos moldes atuais ocorreu com a sua inclusão na ordem jurídica Austríaca em 1787. Contudo foi com a Revolução Francesa, influenciada pela teoria da Tripartição dos Poderes de Montesquieau, que o Princípio da Reserva Legal foi consagrado, uma vez que fez parte da declaração dos Direitos do Homem e do Cidadão em 1749. Desta forma o princípio em análise evoluiu até ser consagrado em diversos ordenamentos jurídicos mundiais.

Na ordem jurídica nacional o Princípio da Reserva Legal possui também o status de garantia constitucional, pois possui sentido político garantidor da liberdade individual. Quando a Constituição Federal de 1988 expressamente preceitua que " Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal."[6], depreende-se a necessidade da prescrição da conduta por lei anterior ao fato para que determinado ato seja considerado como crime, sendo assim lícita qualquer ação positiva ou negativa não prescrita como crime em norma penal incriminadora.

Como conseqüência direta do princípio da reserva legal temos o princípio da tipicidade de um fato. Um fato, uma conduta humana, seja uma ação ou omissão, só poderá ser considerada como afrontosa a ordem jurídica penal, ou seja, será típico, se existir norma penal incriminadora prévia que descreva de forma taxativa e pormenorizada todos os elementos da conduta humana tida como ilícita.

A questão reputa-se importante diante da notória ausência de regulamentação dos crimes informáticos, ou seja, raras são as normas de natureza penal que estabelecem as condutas criminosas informáticas, quando o fazem são extremamente específicas a determinados sujeitos ativos ou passivos, não possuindo assim caráter abrangente, não punindo condutas similares mas com legitimados ativos e passivos distintos dos expressos em lei. É a não regulamentação da matéria que facilita o incremento da criminalização informática. Urge pois a elaboração de normas penais que venham a reger o assunto coibindo e punindo a prática de ilícitos desta natureza.

7 Crimes Informáticos no Ordenamento Jurídico Brasileiro

Inseridas no conjunto de normas legais formadoras do ordenamento jurídico nacional, encontram-se de maneira esparsa alguns tipos penais de natureza informática contidos em normas específicas de determinado ramo o direito, como por exemplo o Direito Eleitoral.

Neste sentido a Lei Federal 8.137 de 27 de dezembro de 1990, que define os crimes contra a ordem tributária, econômica e contra as relações de consumo, entre ouras providências estabelece:

- Artigo 2º - Constitui crime da mesma natureza[7]:

> V - utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública.

Além de constituir violação contra a ordem tributária, se trata de crime informático, pois o programa utilizado para o processamento dos dados inseridos no sistema altera o correto tratamento dos dados e faz com que o resultado do processo seja

[6] *Constituição Federal artigo 5º inciso XXXIX.*

[7] *Art. 1° Constitui crime contra a ordem tributária...*

maculado, uma vez que dados corretos são processados por programa alterado que modifica o resultado. Verifica-se ademais, que se trata de tipo penal extremamente específico, uma vez que só ocorre quando se viola interesse da fazenda pública. Contudo tal conduta qual seja a utilização de programa modificado para alteração dos resultados do processamento, pode ser perpetrada contra inúmero sujeitos passivos distintos do fisco, e nestes casos por falta de regulação legal, são condutas carentes de punição, apesar do juízo reinante de reprovabilidade social. Regulando inciso XII, parte final, do art. 5° da Constituição Federal[8], a Lei Federal 9.296 de 24 de julho de 1996 estabelece em seu bojo um crime de natureza informática:

> • Artigo 10 - Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

O dispositivo legal acima colacionado estabelece como crime o ato de interceptar uma comunicação, mas não é qualquer tipo de comunicação, até porque o ser humano possui inúmeras formas de se comunicar. Assim suso mencionada lei enumera quais os tipos de interceptação são passíveis de punição em face de serem consideradas ilícitas. Dentre os tipos dispostos na lei está a interceptação de comunicação informática. Logo qualquer interceptação não autorizada de comunicação realizada entre sistemas computacionais constitui ato ilícito tipificado pelo artigo 10 da Lei Federal 9.296/96. Exemplo singular da interceptação da comunicação informática, ou seja da troca de informações ou de dados feitas por meios informáticos, é a violação de *e-mails*[9].

Visando proteger os sistemas informáticos utilizados pela Justiça Eleitoral a Lei Federal 9504 de 30 de setembro de 1997 prevê a criação de três delitos informáticos:

> Artigo 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos: I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

Apesar da especificidade dos delitos, ou seja, só podem ser perpetrados contra sistemas informáticos utilizados pela Justiça Eleitoral, tratam-se de condutas que de forma genérica podem ser praticadas contra qualquer sistema informático, contudo, em face do "engessamento" cometido pelo legislador, estas situações ficaram desprotegidas uma vez que somente o caso específico foi regulamentado.

No delito tipificado no inciso I, temos a ocorrência de duas situações ilícitas. A primeira é o acesso não autorizado a sistema informático, que por si só já se configura como fato punível como crime informático. Entretanto o tipo penal atrela ao acesso o intuito de alterar-se os dados relativos a contagem dos votos. Só quando verificadas essas duas condições a conduta se torna punível. O ato lesa interesses jurídicos distintos dos bens computacionais, mas opera-se por meio de lesão a estes, uma vez que a segurança do sistema foi violada e a integridade dos dados foi deturpada em face de sua manipulação.

No crime capitulado no inciso II, tem-se um conjunto de condutas lesivas a bens informáticos tais como apagar ou transmitir dados e informações. O tipo penal visa proteger a corrupção do tratamento correto de dados utilizados pelo serviço eleitoral, quer seja pelo desenvolvimento ou pela introdução de comando, instrução ou programa que por qualquer meio, manipulação, transmissão de dados, entre outros, altere o correto processamento e o resultado dos dados inseridos no sistema computacional a serviço do pleito eleitoral.

No inciso III se verifica, mesmo que possua aplicação restrita, a tipificação da conduta entitulada pela doutrina como dano informático, ou seja, efetuar dolosamente dano ao equipamento utilizado na votação com objetivo de evitar o acesso aos dados nele contidos ou a própria destruição do suporte físico de armazenamento dos dados.

Os delitos tipificados pela Lei 9504/97 possuem aspecto extremamente restrito pois somente se aplicam a atos que atentem contra sistemas informáticos ou equipamentos envolvidos no processo eleitoral, o que deixa uma enorme lacuna o ordenamento jurídico penal, pois deixa sem punição condutas perfeitamente adequadas aos elementos incriminadores dispostos na norma penal, mas por não atingirem sistemas computacionais a serviço da Justiça Eleitoral não são puníveis. O que demonstra a necessidade de repensar-se o modo de elaboração das normas legais aplicáveis a matéria.

---

[8] *Constituição Federal de 1988. Artigo 5º inciso XII – É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no ultímo caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.*

[9] *O Supremo Tribunal Federal já pronunciou-se pela aplicabilidade da Lei 9296/96 a interceptação da comunicação informática.*

Com a escalada da criminalidade informática a Lei Federal 9.983 de 14 de junho de 2000 visando proteger e coibir a pratica de ilícitos contra os sistemas informáticos utilizados pela Administração Pública, inclusive os praticados por funcionários públicos, estabeleceu nova redação e introduziu artigos no Código Penal Brasileiro. As modificações operaram-se da seguinte forma:

> § 1º-A do artigo 153 do Código Penal - Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública.
>
> Artigo 313-A do Código Penal - Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano;
>
> Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa;
>
> Artigo 313-B do Código Penal - Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
>
> Parágrafo único - As penas são aumentadas de um terço até a metade se a modificação ou alteração resulta dano para a Administração Pública ou para o administrado.
>
> § 1º do artigo 325 do Código Penal Brasileiro - Nas mesmas penas deste artigo incorre quem:
>
> I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistema de informações ou banco de dados da Administração Pública;
>
> II - se utiliza, indevidamente, do acesso restrito:
>
> § 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem:

O delito capitulado no § 1º - A do artigo 153 do Código Penal, a violação de segredo, só adquire a natureza de delito informático quando as informações sigilosas estiverem contidas em meios informáticos como os bancos de dados computacionais, pois somente assim um bem computacional seria lesado pela pratica do ilícito, ou seja, se violaria o sigilo dos dados computacionais existentes no sistema.

O artigo 313 – A introduzido no Código Penal tipificou a conduta de manipulação de dados em sistema da Administração Pública. Dentre as peculiaridades do fato típico encontra-se mais uma vez a restrição da prática da conduta a determinados sistema informáticos, ou seja, aqueles a serviço da Administração Pública, bem como a necessidade de que o mesmo seja praticado por funcionário público, amputando-se assim o campo de incidência do tipo penal o que por força de sua extrema especificidade deixa uma série de condutas ilícitas carente de sanção legal. O crime em análise visa coibir de forma direta que um funcionário público manipule ou facilite a manipulação de dados contidos em sistema de informática ou banco de dados da Administração Pública. A manipulação pode consistir na inserção de dados falsos no sistema, na alteração ou exclusão de dados corretos, não importando se o interesse do autor da conduta era a obtenção de alguma vantagem econômica ilícita ou se causar dano.

Estabelece o artigo 313 – B do Código Penal o crime que comete o funcionário público que altera ou modifica sistema de informações ou programa de computador sem a devida autorização.

Ressalte-se que os delitos capitulados nos artigos 313-A e 313-B do Código penal nacional são considerados pela maioria da doutrina como crimes de mão própria, ou seja só podem ser cometidos por funcionários públicos, restringindo-se, desta forma, ainda mais o campo de aplicação da lei incriminadora.

O inciso I do artigo do § 1º do artigo 325 do Código Penal pune o funcionário que de alguma forma possibilita a terceiro não autorizado o acesso a banco de dados ou sistemas de informação da Administração pública, não importando qual o meio utilizado pelo agente para facilitar o acesso indevido. Trata-se de dispositivo legal extremamente importante que busca coibir a facilitação dos acessos indevidos. Entretanto este crime adquire aspecto peculiar em nosso ordenamento pois em virtude da ausência de dispositivos legais reguladores da matéria aplicáveis a todos os agentes, somente o funcionário público seria punido, não recaindo nenhuma punição sob quem acessou o banco de dados ou o sistema de informações.

Já o inciso II do parágrafo 1º do artigo 325 do Código Penal procura punir o funcionário que dotado de autorização para acessar informações ou para realizar atividades de cunho restrito no sistema informático, arbitrariamente extrapola os limites de sua autorização, acessando dados não permitidos ou praticando atividades indevidas.

Os exemplos colacionados demonstram que apesar do surgimento de legislação correlacionada com a matéria, a regulamentação existente é esparsa e extremamente específica aplicando-se a determinados temas. Em conseqüência disto uma gama de condutas ilícitas encontram-se carentes de punição em face da ausência de normas legais atinentes ao assunto como um todo. Deve-se então elaborar diploma legal que trate a matéria de forma técnica, criminalizando as condutas que atentem contra os sistemas informáticos e seus dados independentemente do seu proprietário, não importando se ente público ou privado, se a Administração Pública ou particular, ressaltando-se que uma vez escalonado os graus de importância dos mais variados sistemas informáticos se deve

estipular algumas qualificadoras para condutas que atentem contra os mais importantes.

Logo, em virtude do vácuo normativo existente ocasionador da falta de sanção a um conjunto de novos atos ilícitos, se deve com urgência elaborar diploma legal regulador do tema.

Conclusão

O espírito humano sempre inovador e ávido por novas descobertas fez com que a espécime humana adquirisse patamares de evolução únicos no seu habitat natural, a Terra. Em um curto período de tempo geológico o homem abandonou as trevas, as antigas cavernas e a selvageria típica da raça animal para conquistar não só o mundo em que vive mas também o espaço sideral. Um novo desafio surge, buscando abrandar a chama da inovação, que crestalhe a alma, o homem busca agora colonizar uma nova era, um novo mundo fruto não da benevolência de Deus, mas de sua criação intelectual, um espaço não real e intangível, o mundo virtual.

O fogo, a roda, a escrita, a pólvora, a energia elétrica, a moeda, as máquinas de calcular, o computador. A evolução do conhecimento humano fez com que a cada nova descoberta a sociedade sofresse transformações nem sempre benéficas. A realidade social pós industrial parecia estagnada quando o evoluir de um aparelho que simplesmente fazia cálculos modificou de forma profunda e irreversível a vida humana.

Os sistemas informáticos, anteriormente simples coadjuvantes das atividades humanas hoje assumem papel imprescindível na vida em sociedade moderna, pois está presente de forma direta ou indireta em todas as atividades humanas.

Dentre os impactos causados pela evolução da informática, o surgimento e o desenvolvimento da Internet alterou sensivelmente as relações econômicas, e humanas, quebrando as barreiras geográficas e temporais.

Contudo, como tudo que está no domínio do saber e da convivência humana o uso dos sistemas informáticos sofreram deturpações. Surgiu uma nova espécie de criminalidade que aproveitando-se do período de deslumbramento do homem com o novo universo que se abria a sua frente começou a procurar meios de obter vantagens ilícitas peculiares a essa nova realidade. Surgiu a criminalidade informática. Aproveitando-se da ausência de regulamentação jurídica aplicável a essas novas condutas, a prática de crimes informáticos se proliferou de modo frenético, atingindo patamares que colocam em risco os níveis de desenvolvimento alcançados.

Ao se analisar a questão dos Crimes Informáticos e seu tratamento legal no ordenamento jurídico brasileiro conclui-se que a inexistência de normas penais incriminadoras tipificando condutas lesivas a bens computacionais contribui de forma ímpar para a disseminação da criminalidade de informática. O vácuo normativo existente permite a prática de inúmeros atos que atentam contra os sistemas informáticos e aos dados neles contidos.

A norma penal incriminadora possui duas finalidades básicas, a primeira é coibir a prática de ato lesivo ao bem jurídico tutelado, o segundo é punir a prática desse ato danoso. Logo dentre as funções precípuas da norma penal estão a prevenção e a punição de condutas danosas a interesses jurídicos importantes para a vida em sociedade.

No atual estado de desenvolvimento da sociedade humana o atrelamento do ser humano aos sistemas computacionais é de tal monta que o mesmo se torna indispensável para a mantença das atividades cotidianas, demonstrando-se assim a importância dos sistemas computacionais para a sociedade.

A ausência de diplomas normativos que delimitam os crimes de informática tornam a situação insustentável, uma vez que a medida que o nível de informatização das atividades humanas é cada vez mais crescente, mais surgem situações suscetíveis de lesão por crimes informáticos, pois a criminalidade também tende a se informatizar.

Logo é de suma importância que os vazios normativos existentes em relação aos crimes informáticos sejam supridos. Contudo, isto deve ser feito de forma técnica, em face da extrema mutabilidade do mundo informático evitando-se assim excessos legislativos prejudicias a boa regulamentação do tema.

Ao término de todo o estudo realizado a cerca de Crimes Informáticos conclui-se que o ordenamento jurídico nacional apresenta enormes lacunas legais ocasionadoras da falta de punição a condutas lesivas a bens informáticos pois em face do disposto em nosso ordenamento jurídico um crime só existe e por conseqüência só poderá ser punido quando norma jurídica expressamente o delimite e imponha a sua punição. Em se tratando de crimes informáticos isso ainda não existe no Brasil. Urge a aprovação de diploma normativo jurídico que incrimine e estabeleça as sanções as condutas danosas a bens jurídicos computacionais, suprindo assim a lacuna existente em nosso ordenamento.

Referências

ANDREUCCI, Ricardo Antunes; BARRA, Rubens Preste (Coord.). *Estudos jurídicos.* São Paulo: Revista dos Tribunais, 1992.

ARAS, Vladimir. Crimes de informática: comentários ao substitutivo do deputado Pellegrino. *Consultor jurídico*. Disponível em: < http://www.conjur.com.br>. Acesso em: 10 jan. 2003.

ARAS, Vladimir. Crimes de informática**:** uma nova criminalidade. *Jus navigandi.* 51. ed. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2250>. Acesso em: 15 out. 2001.

BECCARIA, Cesare. *Dos delitos e das penas*. 2. ed. Tradução de Lucia Guidicini; Alessandro Berti Contessa. São Paulo: Martins Fontes, 1998.

BLUM, Renato Opice (Coord). *Direito eletrônico:* a internet e os tribunais. São Paulo: EDIPRO, 2001.

BRASIL, Angela Bittencourt. *Informática jurídica:* o ciber direito. Rio de Janeiro: Juris Doctor, 2000.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil.* 18. ed. São Paulo: Saraiva, 1998.

BRASIL. *Código civil:* lei nº 3.071, de 1 de janeiro de 1916*.* 49. ed. São Paulo: Saraiva, 1998.

BRASIL. *Código penal:* decreto-lei nº 2.848, de 7 de dezembro de 1940*.* 36. ed. São Paulo: Saraiva, 1998.

BRASIL. Lei nº 8.137, de 27 de dezembro de 1990. Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. Disponível em: <http://www.senado.gov.br>. Acesso em: 7 set. 2001.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: <http://www.senado.gov.br>. Acesso em: 7 set. 2001.

BRASIL. Lei nº 9.504, de 30 de setembro de 1997. Estabelece normas para as eleições. Disponível em: <http://www.senado.gov.br>. Acesso em: 7 set. 2001.

BRASIL. Lei nº 9.983, de 14 de julho de 2000. Altera o Decreto-lei n.º 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências. Disponível em: <http://www.senado.gov.br>. Acesso em: 7 set. 2001.

CASACUBERTA, David; MARTÍNS MÁS, José Luis. *Diccionario de ciberderechos*. Disponível em: <http://www.kriptopolis.com/dicc.html>. Acesso em: 5 jan. 2000.

ELIAS, Paulo Sá. A questão da reserva legal no direito penal e as condutas lesivas na área da informática e da tecnologia. *Jus Navigandi.* Disponível em: <http://www1.jus.com.br/texto.asp?id=2038 >. Acesso em: 15 nov. 2001.

JESUS, Damásio E. de. *Direito penal.* 20. ed. São Paulo: Saraiva, 1997. v. 1.

LANDRETH, B. *Out of the inner circle.* Redmond: Microsoft Books, 1985. Disponível em: <http://www.escape.ca/~mkr/hackerdoc.pdf>. Acesso em: 15 nov. 2001.

LUCCA, Newton de.; SIMÃO FILHO, Adalberto (Coord.). *Direito e internet:* aspectos jurídicos relevantes. São Paulo: Edipro, 2000.

PEREIRA, Ricardo Alcântara. Breve introdução ao mundo digital. In: BLUM, Renato Opice (Coord.). *Direito eletrônico*: a internet e os tribunais. São Paulo: Edipro, 2001.

REIS, Maria Helena Junqueira Reis. *Computer crimes:* a criminalidade na era dos computadores. Belo Horizonte: Del Rey, 1997.

VIANA, Tulio Lima. *Hackers:* um estudo criminólogico da subcultura cyberpunk. Disponível em: <http://www.infojur.ccj.ufsc.br>. Acesso em: 12 jan. 2003.