

EDERLEI NORBERTO MAJOLO

INFORMÁTICA E CRIME

CURITIBA

2006

EDERLEI NORBERTO MAJOLO

INFORMÁTICA E CRIME

Monografia apresentada ao Curso de Direito do Setor de Ciências Jurídicas da Universidade Federal do Paraná, como pré-requisito para a obtenção do Título de Bacharel em Direito.

Professor Orientador: Rolf Koerner Jr.

CURITIBA

2006

TERMO DE APROVAÇÃO

EDERLEI NORBERTO MAJOLO

INFORMÁTICA E CRIME

Monografia aprovada como pré-requisito para a obtenção do título de Bacharel em Direito do Curso de Direito do Setor de Ciências Jurídicas da Universidade Federal do Paraná, pela seguinte banca examinadora:

Orientador: -1)

-2)

-3)

Curitiba, 29 de setembro de 2006

SUMÁRIO

RESUMO	iv
1 INTRODUÇÃO	1
2 HISTÓRICO	3
3 SISTEMA DE INFORMAÇÃO	5
4 A INFORMÁTICA E O DIREITO	7
4.1 INFORMÁTICA JURÍDICA	9
4.2 DIREITO DA INFORMÁTICA	10
5 DIREITO PENAL E INFORMÁTICA	12
6 DELITOS INFORMÁTICOS	14
7 CLASSIFICAÇÃO DOS DELITOS INFORMÁTICOS	16
7.1 DELITO INFORMÁTICO PRÓPRIO	16
7.2 DELITO INFORMÁTICO IMPRÓPRIO	16
7.3 DELITO INFORMÁTICO MISTO	17
7.4 DELITO INFORMÁTICO MEDIATO	17
8 LEGISLAÇÃO BRASILEIRA SOBRE O ASSUNTO	18
8.1 DELITOS INFORMÁTICOS IMPRÓPRIOS.....	19
8.2 DELITOS INFORMÁTICOS PRÓPRIOS.....	21
9 BEM JURÍDICO PROTEGIDO	23
10 DIREITO ESTRANGEIRO	25
11 PERFIL DO CRIMINOSO DIGITAL	27
12 DETERMINAÇÃO DA AUTORIA, LOCAL E TEMPO	29
13 PROJETOS DE LEI EM ANDAMENTO	31
14 DA TIPIFICAÇÃO FRENTE A UMA ÉPOCA DE DESCRIMINALIZAÇÃO	34
15 CONCLUSÃO	36
REFERÊNCIA	38
ANEXO I	40
ANEXO II	46
ANEXO III	52

RESUMO

Os delitos informáticos tornam-se cada vez mais presentes na nossa realidade. A monografia aqui apresentada tem o objetivo de discorrer sobre os crimes cometidos através da Informática e contra a Informática, trazendo argumentos e posicionamentos, favoráveis e contrários, a uma legislação específica para combater infrações desta natureza. A partir de algumas reflexões acerca da importância da Informática e a sua relação com o Direito, procura-se mostrar como o Direito Penal aborda o tema, utilizando-se da doutrina, da legislação adotada para tratar destes delitos, quando existente, dos projetos de lei sobre o tema e do direito estrangeiro.

Palavras-chave: Informática; crime; delito.

1 INTRODUÇÃO

Com o advento da Revolução Informática, novos conceitos e valores invadiram a vida de uma grande parte dos cidadãos brasileiros que, no curto espaço de pouco mais de uma década viram suas vidas adaptadas, talvez de modo involuntário, com equipamentos de tratamento automático de informações

O surgimento do computador e de todos os aparatos que envolvem o seu funcionamento, tanto em um ambiente doméstico como em outro mais amplo, permitiram que o homem moderno pudesse estar conectado de várias formas com o seu semelhante. Tudo isso gerou também uma intrincada rede de relações que, por sua vez, acarretou em outras variantes que influem nas atividades comerciais e afins na sociedade moderna.

Vários elementos que surgiram com a revolução informática trouxeram grandes avanços e comodidades, e permitiram o rápido desenvolvimento das atividades humanas no decorrer da metade final do século XX, bem como nos primeiros anos do século vigente. Porém, como já sabido, no decorrer da história das relações humanas, inovações trazem consigo novos elementos de convivência que por vezes necessitam de regras para o seu devido aproveitamento.

Os problemas trazidos pela informática e pela sua principal derivada, a Internet, estão bem aquém dos seus benefícios. Contudo, esse argumento não pode servir para que sejam ignorados tantos atos socialmente reprováveis que são praticados nesse meio.

Essas entidades que não configuram algo real, no fato de não serem percebidas por todos os sentidos humanos, representam um conjunto de novas tecnologias e formas de negócios que muitos ainda não estão habituados em lidar e, em muitos casos, de dominar, sendo assim vítimas fáceis de pessoas que estão alheias à ordem das regras que regem o bom andamento das relações humanas - o Direito - e que se aproveitam disso para agir em proveito próprio em detrimento dos demais.

A Internet proporciona grandes e úteis formas de relacionamento entre os seus usuários que podem se estender também aos demais que não se utilizam dela diretamente, e que, pela sua natureza de ser algo de amplitude global, permite que várias formas de “crimes” venham por intermédio dela serem praticados. Nessas

elementos se baseia o objetivo da presente monografia, demonstrando a importância do tema “Informática e crime”, no que tange aos direitos de todos os cidadãos em relação a um “instrumento” que carrega na sua origem a vantagem de poder ser usado por todos de forma construtiva e segura, mas que possui uma faceta que pode representar perigo.

Faz-se mister o estudo do Direito Penal em face das modernas ferramentas tecnológicas que influenciaram as relações humanas nos últimos anos. Com o uso massivo da Internet por uma importante parcela da sociedade, incluindo aí grandes corporações econômicas (com destaque para as instituições bancárias), percebeu-se que a informática vinha sendo utilizada como instrumento criminoso em diversos casos. O que se indaga atualmente é se a estrutura do Direito Penal é compatível com as mudanças tecnológicas que se apresentam e se os tipos penais já existentes podem ser utilizados nas diversas hipóteses de crimes que o uso da informática permite.

2 HISTÓRICO

É possível, sem cair em lugar comum, afirmar que as relações humanas nunca mais serão as mesmas após o surgimento do computador e da ciência – computação - da qual o mesmo deriva e é produto. O termo computador provém do latim *computare* que significa *contar*.

Os primeiros indicativos do surgimento de instrumentos que permitissem uma maior agilidade dos afazeres do homem, já datam do período anterior a Cristo, pelo uso do ábaco e similares por várias civilizações.

Na época Moderna, tem-se com *John Napier* a possibilidade de realização de cálculos simples por intermédio da conhecida “*Tábua de Napier*”, sendo seguido pelas idéias de *Charles Babbage* que em 1835 desenvolveu um instrumento de calcular que funcionaria por intermédio de uma série de “cartões perfurados”¹.

Já no século XX, surge uma grande enxurrada de equipamentos de calcular que modificaram de forma indelével o cotidiano de várias empresas e atividades governamentais, pois facilitaram procedimentos que envolviam cálculos que custavam meses e até mesmo anos de trabalho para serem realizados².

Foi com o advento da Segunda Guerra Mundial - MARK I, primeira máquina de calcular automática em 1944 - e no período que se seguiu após ela - *Electronic Numerical Integrator and Calculator* (ENIAC), primeiro computador eletrônico em 1946, que realmente ocorreram inovações tecnológicas muito importantes e que resultaram nas bases concretas dos equipamentos que hoje existem, e que facilitam de forma bastante notória a vida do homem moderno.

O período da Guerra Fria foi um delimitador de águas entre a individualização e a integração dos computadores que existiam até então, pois a Corrida Armamentista e a Corrida Espacial foram grandes e eficazes catalisadores para o seu desenvolvimento e concretização.

No ambiente de pesquisas que se desenvolveu no período acima citado e que consumiu grande soma de recursos, surgiu uma “rede” onde várias instituições militares, de ensino e pesquisa norte-americanas se uniram umas as outras de forma

¹ A perfuração ou não dos pontos do cartão determinavam a seqüência a ser executada.

² O recenseamento americano da década de 1880 levou sete anos para ser concluído com o trabalho de 500 funcionários, sendo que para o mesmo trabalho de 1890, utilizaram-se calculadoras de cartão perfurado que consumiram 1 ano com o serviço de apenas 43 funcionários.

a compartilhar informações e tecnologias: a *Advance Research Projects Agency* (ARPANET). Essa rede, posteriormente a seu aprimoramento, foi chamada de Internet, tornando-se pública em 1993 pelo Centro Europeu de Investigação Nuclear (CERN), trazendo grande versatilidade.

3 SISTEMA DE INFORMAÇÃO

O Sistema de Informação é uma entidade de natureza complexa e variada, porém é possível defini-lo de forma simples como sendo o processo onde se permite receber informações, armazená-la e, quando necessário, alterá-la e enviar a mesma para destinos onde será de valia.

Como informação é de grande valor nos dias atuais, pois configura poder³, pode-se intuir o seu grau de importância dentro das relações humanas em todas as áreas.

O elemento básico da informação armazenada nos sistemas operacionais existentes é o dado. Dado por definição é a representação da informação de forma processável pela máquina chamada aqui de computador. Para essa máquina, de forma simplificada, somente a existência e a inexistência de energia elétrica é que pode ser entendida e transformada em dados que por sua vez representarão, como já afirmado, a informação que se deseja armazenar. Então, dados surgem como entidades que se fazem necessárias quando da transformação do mundo das idéias (mente humana) para o mundo concreto (relações humanas - informações) onde os mesmos poderão ser trabalhados e analisados.

Assim, a existência de equipamentos que permitam a manipulação dessa grande quantidade de dados de forma ágil e segura, e de forma lógica, exigiu o surgimento de novas entidades distintas que permitissem de forma conjunta essa manipulação - *hardware e software*.

A união desses elementos é representada pelo computador. O teclado, monitor, disco rígido, memória, etc, cujo conjunto representa o *Hardware*. O segundo item a ser citado consiste nos programas que fazem com que o computador funcione de acordo com a intenção do seu usuário e são chamados em seu conjunto de *software*, que por sua vez também é formado por dados, sendo de grande importância esse fato para a delimitação do problema aqui proposto.

Um elemento que permite bem exemplificar a complexidade de um Sistema de Informação é o fato do mesmo sofrer o fenômeno da retroalimentação ou *feedback*, ou seja, a sua existência está diretamente relacionada ao processamento

³ BARROS, Lucivaldo Vasconcelos. O crime na era da inform@ção. **Jus Navigandi**. Teresina. Ano 7, nº 61. Jan. 2003. Pg. 5.

dos dados, seu envio e seu retorno, sem sair do ambiente que forma o referido sistema.

Em suma, o Sistema de Informação é bem definido nas palavras de LAUDON *apud* SILVA⁴: “...um conjunto de componentes inter-relacionados trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir informação com o objetivo de facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório em empresas e outras organizações.”

Já estabelecido o conceito de Sistema de Informação, é importante que se faça a menção também de outro elemento que de uma forma muito direta está relacionada ao mesmo que é a Informática.

A informática tem uma definição bastante ampla e também complexa, sendo interessante resumi-la em uma citação de KANAAN *apud* SILVA⁵: “...é a ciência do tratamento racional e automático da informação, considerada como suporte dos conhecimentos e comunicações, principalmente por meio de sistemas eletrônicos denominados computadores.”

⁴ SILVA, Rita de Cássia Lopes. **DIREITO PENAL E SISTEMA INFORMÁTICO**. Ciência do Direito Penal Contemporâneo, Vol. 4. São Paulo: Ed. Revista dos Tribunais, 2003. Pg. 29.

⁵ SILVA, Rita de Cássia Lopes. *Op. Cit.* Pg. 35.

4 A INFORMÁTICA E O DIREITO

Conforme PIMENTEL *apud* VIANNA, o termo informática deriva da união de dois outros vocábulos “informação” e “automática”, sendo produto do francês *Philippe Dreyfus*⁶.

Como qualquer ferramenta que possibilita a relação entre seres humanos distintos em conceitos e também culturalmente, há a necessidade de que vários elementos que constituem a Informática sejam regidos e também protegidos através de instrumentos legais.

Todos os elementos que no decorrer da história da humanidade trouxeram vantagens a ela, envolveram aspectos na esfera da ética, da cultura, dos valores econômicos e da sociedade como um todo, destacando-se que todos esses aspectos são mutáveis no decorrer da evolução da sociedade, algo que é natural.

Fatos que passaram despercebidos durante a rápida evolução da informática são as possibilidades da existência de crimes que podem ser perpetrados no ambiente virtual que corporifica a Internet. Para que esses crimes sejam coibidos, faz-se necessário a ação do Direito que “como ciência responsável pela regulação da sadia convivência entre os homens, é chamado para impor regras que resultem em harmonias e paz social” (DELGADO *apud* BARROS)⁷.

A informática também está diretamente relacionada ao Direito e a todas as áreas a ele ligadas, sendo muitas vezes de grande importância operacional para o funcionamento das mesmas. A informatização de grande quantidade de dados que permitem o funcionamento da máquina jurídica, permitiu uma grande variedade de novas ferramentas que proporcionaram uma rápida evolução e resolução de elementos que são de grande utilidade para o andamento do Direito.

Assim pode-se verificar que a informática veio como uma ferramenta que tem um alcance muito grande, atingindo várias áreas do conhecimento humano, como vários setores da economia, ciência e elementos que pertencem ao dia-a-dia de todos de forma direta e indireta. Assim, a informática é considerada uma

⁶ VIANNA, Túlio Lima. FUNDAMENTOS DE DIREITO PENAL INFORMÁTICO. DO ACESSO NÃO AUTORIZADO A SISTEMAS COMPUTACIONAIS. Rio de Janeiro: Ed. Forense, 2003. Pg. 10.

⁷ BARROS, Lucivaldo Vasconcelos. *Op. Cit.* Pg. 12.

evolução de grande benefício para a estruturação do cotidiano de todas as relações humanas em todas as áreas.

Essa ciência permitiu a “virtualização” da informação, ou seja, aquilo que existe no mundo real e que pode ser sentida pelo homem através da visão, tato e etc, passa para uma esfera onde tudo é transformado em dado que não pode ser sentido, apenas idealizado. Um exemplo bastante útil é o do dinheiro de um investidor que é aplicado em um banco. Esse valor é transformado em dados que representam o dinheiro investido, sendo representado no sistema de informação do banco como uma cifra, que agora não pode ser palpável como o é o dinheiro, porém não deixou de existir fisicamente, apenas foi introduzido em um outro ambiente, o virtual⁸.

No mundo virtual os limites não são como no mundo real, sendo neste produzidos pelas leis naturais e naquele produzidos apenas pela vontade humana, como bem define SILVA⁹: “...o virtual, ao contrário **(do real)**¹⁰, é uma criação humana, é uma construção inteiramente artificial, nele tudo se realiza por vontade e impulso humano.”

Para tanto, faz-se necessário a participação do Direito como um catalisador e organizador desses limites de forma harmônica, uma vez que neste ambiente virtual se exigem regras e códigos de conduta, pois nele interagem elementos de um grupo social.

Assim, SILVA¹¹ afirma: “O Direito deve buscar respostas adequadas para facilitar a transição entre o meio físico e o virtual. Um dos caminhos a ser seguido é exatamente incorporar aquelas normas que nasceram no ambiente virtual de forma que a resposta jurídica do mundo real seja um reflexo da resposta adequada e exigida no meio virtual, evitando efeitos legais divergentes.”

Também é oportuno analisar que a informação mesmo na forma de dados virtuais, de forma bastante lógica, continua a existir também no mundo real, pois sendo uma informação, ela está armazenada no *hardware* de algum banco de dados de alguma instituição ou de algum computador.

⁸ Que não existe como realidade física, mas sim como potência ou faculdade mental.

⁹ SILVA, Rita de Cássia Lopes. *Op. Cit.* Pg. 36.

¹⁰ Anotação e grifo nossos.

¹¹ SILVA, Rita de Cássia Lopes. *Op. Cit.* Pg. 37.

Torna-se importante agora diferenciar a Informática Jurídica do Direito da Informática.

4.1 INFORMÁTICA JURÍDICA

A Informática Jurídica trata da automatização do funcionamento dos órgãos do Poder Judiciário, procurando efetivar a informatização dos processos ou, como salienta FINKELSTEIN¹², “é a ciência que estuda a utilização de elementos físicos, como o computador e seus aparatos no Direito, disponibilizando conteúdo de natureza jurídica.”

Quando se analisa a realidade brasileira em relação a falta de mobilidade e rapidez dos processos jurídicos, verifica-se a grande utilidade da informática como uma ferramenta que poderá - e já é utilizada em algumas áreas - modificar de forma positiva o universo jurídico.

Um elemento negativo do judiciário brasileiro é a morosidade da maior parte dos processos que o corporificam, o mesmo pode ser comparado como uma máquina que necessita de agilidade e que cada vez mais é cobrada pela sociedade.

Um diferencial entre alguns mecanismos jurídicos estrangeiros e os brasileiros está refletido no alto grau de informatização dos dados que pertencem ao sistema jurídico daqueles, permitindo uma rápida consulta de elementos essenciais ao bom andamento de todos os processos.

No Brasil existe uma carência muito grande de instrumentos que permitam uma maior agilidade na consulta e transferência de dados que possam desta forma proporcionar uma qualidade maior de resoluções de processos que estão parados. Dessa forma vários criminosos têm a sua punição postergada; soluções que na ordem jurídica podem produzir grandes e vantajosos resultados em várias estruturas tanto administrativas, bem como na vida do cidadão comum que necessita das benesses jurídicas, não são produzidas.

Em última análise, pode-se verificar a grande autonomia que a informatização de dados relacionados ao campo jurídico produz, podendo assim

¹² FINKELSTEIN, Maria Eugênia. **Aspectos jurídicos do comércio eletrônico**. Porto Alegre: Síntese, 2004. Pg. 29.

permitir que o Direito venha gerar resultados rápidos para as áreas que dele necessitam e onde a Informática já se faz realidade.

Então, em relação ao exposto, vem ao encontro dessa idéia as palavras de SILVA¹³: “Está evidente a influência da informática nas atividades desenvolvidas pelo homem. No Direito identifica-se sua utilização da várias formas. Seja favorecendo a atuação criminosa, seja propiciando a informatização da documentação, ou, ainda a informatização dos procedimentos administrativos e processuais; é uma realidade que exige adequação.”

4.2 DIREITO DA INFORMATICA

O Direito da Informática busca sua autonomia dentro do mundo jurídico. As crescentes necessidades de regulamentação para as atividades desenvolvidas com o auxílio de computadores, envolvendo conceitos próprios, faz com que ao menos uma autonomia didática seja dada a esta matéria. Pode ser definido como um conjunto de normas e instituições jurídicas que buscam regular as relações humanas com os sistemas de computador e com a Internet, a criação, uso, modificação, alteração e reprodução de programas e o comércio eletrônico.¹⁴

A Informática demonstra uma evolução definitiva na vida de todos, sendo o seu alcance - considerado por muitos - ilimitado no sentido que, inclui dados que podem ser transmitidos para qualquer lugar em relação às fronteiras dos países, permitindo que vários elementos culturais e costumes influenciem em locais onde os mesmos não são comuns. Para tanto se fazem necessários instrumentos que permitam a regulação da informática e de seus efeitos sobre as sociedades onde ela influa.

O Direito da Informática é uma área de difícil delimitação, pois transcende o território nacional. A rede mundial de computadores, ou apenas Internet, não possui limites geográficos para a sua atuação. Neste campo, o Direito não é apenas relativo a um país em específico, pois como já falado a Internet é um patrimônio da humanidade, no que se refere ao fato de todos no globo terrestre utilizarem seus

¹³ SILVA, Rita de Cássia Lopes. *Op. Cit.* Pg. 45.

¹⁴ FINKELSTEIN, Maria Eugênia. *Op. Cit.* Pg. 30.

recursos, colocando em seu ambiente virtual uma miríade de pensamentos, idéias em liberdade total.

A informática permitiu uma série de novos focos de interesse que não estão de forma unânimes regulamentadas em todos os países.

No campo comercial, as transações nele existentes revelam a dificuldade para a regulamentação dela, pois é notório o grande volume de negócios que são realizados pela Internet, sendo muitas vezes realizados entre países distintos e com leis para a área comercial também distintas. Mesmo em território nacional, as transações comerciais realizadas na Internet requerem regras mais acuradas para o bom funcionamento delas, envolvendo direitos do consumidor, cobrança de impostos sobre produtos comercializados e regras de boa convivência comercial. Para tanto foi cunhado o termo *e-commerce*.

O campo tributário também exige uma análise que determine como muitos mecanismos de tributação poderão ser colocados em prática. A sonegação é um fato concreto, e se não existir mecanismo que a iniba de forma eficaz, a Internet tem todas as características que permitiria a sua livre prática, como exemplos o anonimato e o comércio transnacional.

Um outro campo que merece destaque como salienta SILVA¹⁵, é o que se refere às práticas trabalhistas, destacando que há indagações que surgiriam nas relações entre empregado e trabalhador no ambiente da Internet, como exemplos a assinatura de Contrato de Trabalho, pagamento de serviços realizados e horas-extras bem como demais características que identificam o vínculo empregatício.

Devido a um grande número de problemas jurídicos gerados com o advento da Informática, faz-se necessário restringir a análise. O foco será o Direito Penal, com especial atenção a necessidade de novos tipos penais para determinados delitos informáticos. Não será estudado aqui o Direito Privado, o Direito do Trabalho e o Direito Tributário, muito embora a importância destes seja inquestionável.

¹⁵ SILVA, Rita de Cássia Lopes. *Op. Cit.* Pg. 48.

5 DIREITO PENAL E INFORMÁTICA

No estudo do Direito Penal Brasileiro, estudiosos das relações existentes dentro do universo da Informática, variam em vários elementos pertinentes a capacidade de julgamento dos crimes que lá ocorrem pelos mecanismos existentes dentro da Legislação Penal.

Para COSTA¹⁶ o Código Penal Brasileiro contem elementos que servem para coibir crimes identificados na Internet, sendo porém necessários avanços em direção a uma melhor adequação dos elementos penais já existentes em relação aos novos meios de práticas delitivas.

BARROS¹⁷ afirma que o Código Penal Brasileiro não é suficiente para inibir e punir os crimes praticados através da Internet, sendo necessária a adequação e o surgimento de novas leis que contemplem novos tipos de delito, porém o autor afirma que só a criação de novos instrumentos legais não será suficiente para solucionar o problema, necessitando assim de uma ação política e social que seja efetiva contra os crimes que estão surgindo no ambiente informático.

Como bem afirma SILVA¹⁸: “O crescimento desenfreado da informática está obrigando o homem a uma adaptação forçada, pois, em âmbito legislativo, as adaptações não ocorrem no mesmo ritmo.”

A mesma autora também salienta que é necessário, em alguns casos específicos, o surgimento de novas leis para poder ser aplicado o Princípio da Legalidade, pois nos casos em que não se encontra tipificação para determinada conduta, o Sistema Jurídico Brasileiro não permite analogias para incriminá-la.

A Informática trouxe consigo vários elementos que facilitam o cotidiano das pessoas, porém propiciou também o surgimento de práticas que aperfeiçoaram atividades que podem trazer em sua estrutura grande desconforto social.

Em opinião contrária da criação de novos tipos está GRECO FILHO¹⁹

¹⁶ COSTA, Marco Aurélio Rodrigues da. Crimes de Informática. **Jus Navigandi**. Teresina. Ano 1, nº 12. Mai. 1997. Pg. 3.

¹⁷ BARROS, Lucivaldo Vasconcelos. *Op. Cit.*

¹⁸ SILVA, Rita de Cássia Lopes. *Op. Cit.* Pg. 48.

¹⁹ GRECO FILHO, Vicente. Algumas Observações Sobre o Direito Penal e a Internet. **Boletim IBCRIM**. Ano 8. N° 95. Pg. 3.

afirmando que todos os elementos criminais que podem estar envolvidos nos crimes informáticos já se encontram tipificados nas leis existentes, não sendo necessário chamar holofotes sobre o mundo virtual da informática.

O objetivo aqui proposto é o de que: sim, há crimes de informática que exigem a criação de novos tipos criminais que ainda não existem no Código Penal Brasileiro, contrariando a opinião de GRECO FILHO²⁰ e encontrando respaldo no pensamento de VIANNA²¹.

Para VIANNA²², no Direito Penal Brasileiro o acesso não autorizado a Sistemas de Informação é uma conduta atípica, pois não é considerado crime, e para tanto, é necessário que essa conduta seja tipificada para que a mesma torne-se um delito e possa dessa forma ser combatida. Por dedução, se faz necessário também que a informação - dados - seja um bem jurídico protegido, levando em consideração o valor que à mesma é atribuído.

²⁰ GRECO FILHO, Vicente. *Op. Cit.* Pg. 3.

²¹ VIANNA, Túlio Lima, *Op. Cit.*

²² VIANNA, Túlio Lima, *Op. Cit.* Pg. 01.

6 DELITOS INFORMÁTICOS

Os delitos informáticos são aqueles em que houve dano a um bem jurídico protegido - dados, programas, inviolabilidade, honra, etc - através da utilização de um computador para a sua perpetração.

Também, salientam-se algumas definições de outros autores sobre delitos informáticos. Em seu livro SILVA²³ cita a definição da Organização para a Cooperação Econômica e Desenvolvimento (OECD) como sendo “...qualquer conduta ilegal, não ética, ou não autorizada, que envolva processamento automático de dados e ou a transmissão de dados.”

Já para FERREIRA²⁴, crime de informática é “toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão.”

Importante salientar que o crescimento dos crimes digitais no Brasil tem sido expressivo nos últimos anos. Já em 2003, uma reportagem do jornal norte-americano *The New York Times* apontou o país como a “base mais ativa de delito cibernético”²⁵, devido a uma boa colaboração dos *crackers*²⁶ entre si, aliada a impunidade deste tipo de delito.

Segundo especialistas da área de segurança digital, as principais ameaças aos sistemas digitais são as invasões, as transações fraudulentas e a difusão ilegal de materiais²⁷. No primeiro caso, ocorre o acesso não autorizado a outro computador com o objetivo de furtar dados. A simples invasão, atualmente, não constitui crime no Brasil. Apenas poder-se-ia incriminar o invasor se este fizesse uso do que acessou, alterasse indevidamente o conteúdo dos dados lá encontrados ou danificasse o computador invadido.

As transações fraudulentas ocorrem com a criação de endereços de Internet falsos, visando confundir a vítima e conseguir senhas e números de cartões de

²³ SILVA, Rita de Cássia Lopes. *Op. Cit.* Pg. 55.

²⁴ FERREIRA, Ivette Senise. *Direito & Internet – aspectos jurídicos relevantes.* Bauru: Edipro, 2000. Pg. 210.

²⁵ Criminosos Virtuais na Mira da Lei. **Revista RT Informa**, nº 38, Julho/Agosto 2005 Ed. Revista dos Tribunais. Pg. 4.

²⁶ Denominação dada ao criminoso virtual.

²⁷ Criminosos Virtuais na Mira da Lei. **Revista RT Informa**, nº 38, Julho/Agosto 2005.. Ed. Revistas dos Tribunais. Pg. 4.

crédito; ocorrem também com o envio de correio eletrônico solicitando informações confidenciais como se fossem instituições reconhecidas.

A difusão ilegal ocorre com o envio de *spam* ou com mensagens que prejudiquem a reputação de uma pessoa.

7 CLASSIFICAÇÃO DOS DELITOS INFORMÁTICOS

Para o objetivo aqui proposto, foram encontradas na literatura pesquisada, várias classificações para os delitos informáticos.

Essas classificações não são unânimes entre os autores devido à divergências conceituais existentes entre os mesmos, porém, a que mais corresponde a uma compilação de todas elas é a de VIANNA²⁸, que aqui será apresentada por ser também abrangente e de fácil entendimento.

VIANNA²⁹ classifica os delitos informáticos em quatro tipos: próprios, impróprios, mistos e mediatos.

7.1 DELITO INFORMÁTICO PRÓPRIO

São aqueles que se utilizam de um Sistema Informático objetivando danificar ou atingir elementos pertencentes a outro Sistema Informático: a saber, dados, *software* e *hardware*.

SILVA³⁰ em suas palavras também define esses delitos nos quais o “sistema informático serve como meio e fim almejado pelo agente...”.

Como exemplo se pode citar o acesso não autorizado a um Sistema Informático através de um computador.

7.2 DELITO INFORMÁTICO IMPRÓPRIO

São aqueles que são cometidos contra elementos jurídicos protegidos, já definidos assim na legislação vigente, utilizando-se o computador como ferramenta que permite a sua prática, sem, no entanto, violar o bem jurídico protegido³¹ denominado dado³².

²⁸ VIANNA, Túlio Lima, *Op. Cit.*

²⁹ VIANNA, Túlio Lima, *Op. Cit.* Pg. 13-26.

³⁰ SILVA, Rita de Cássia Lopes. *Op. Cit.* Pg. 60.

³¹ Enfrentaremos mais a frente a discussão sobre a necessidade de se considerar o dado com um bem jurídico protegido.

³² VIANNA, Túlio Lima, *Op. Cit.* Pg. 14.

Como exemplo um delito contra a honra - calúnia (artigo 138 do Código Penal) através do envio de um *e-mail* por intermédio de um computador que será mero instrumento para tal fim.

7.3 DELITO INFORMÁTICO MISTO

Nas palavras de VIANNA³³ são aqueles “...derivados do acesso não autorizado a Sistemas Computacionais que ganharam *status* de delitos *sui generis* dada a importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos.”

Como o mesmo autor exemplifica, é o caso do acesso não autorizado ao Sistema de Informação Eleitoral para adulterar a apuração da contagem dos votos. Este delito encontra-se tipificado na Lei nº 9.504/97, em seu art. 72, I.³⁴

7.4 DELITO INFORMÁTICO MEDIATO

Aqui VIANNA³⁵ salienta, em suas palavras, o delito onde: “... se alguém acessa sem autorização o sistema computacional de um banco e transfere indevidamente dinheiro para a sua conta, estará cometendo dois delitos distintos: o acesso não autorizado a sistemas computacionais e o furto; o primeiro, crime informático, o segundo, patrimonial.”

Em outras palavras o crime de informática será o delito-meio para praticar o furto que seria então o delito-fim. Pune-se apenas o último delito, pelo Princípio da Consumação.

³³ VIANNA, Túlio Lima, *Op. Cit.* Pg. 23.

³⁴ “Art 72. Constituem crimes, puníveis com reclusão de 5(cinco) a 10 (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;...”

³⁵ VIANNA, Túlio Lima, *Op. Cit.* Pg. 25.

8 LEGISLAÇÃO BRASILEIRA SOBRE O ASSUNTO

No âmbito nacional as opiniões variam, não havendo unanimidade entre os formadores de opinião no universo do direito a respeito de como deve proceder o corpo jurídico.

Para BARROS³⁶ as leis existentes no Código Penal e Código Civil são suficientes e eficazes quando se analisam os delitos que podem ser praticados pela Internet, sendo, portanto, desnecessário uma legislação à parte para tratar do assunto “delito informático”³⁷, necessitando apenas de ajustes e adequações.

Este é também o pensamento de SARDAS, para quem “o direito penal, em geral, está perfeitamente aparelhado na missão de coibir condutas lesivas, quer sejam praticadas pela ou contra a internet.”³⁸ Na mesma linha de pensamento, a autora expõe que: “A criação de novos tipos legais de crimes para as ações ou omissões praticadas pela internet ou contra a internet, é erro grave e perigoso na política penal.”³⁹

Em lado oposto está ROSA⁴⁰, que salienta que as leis existentes não comportam em seu bojo todos os mecanismos regulatórios que se fazem necessários para o bom funcionamento e andamento das relações que se realizam no ambiente virtual onde os delitos informáticos são cometidos. Também afirma que ao ser construída uma legislação específica, atrairia a atenção de vários setores da sociedade, como a indústria e o mundo acadêmico, e assim se faria um debate amplo acerca do problema.

A dificuldade encontrada na falta de uma legislação específica, está no princípio de que, na inexistência de lei não há crime (*nullum crimen sine lege*).

8.1 DELITOS INFORMÁTICOS IMPRÓPRIOS

³⁶ BARROS, Lucivaldo Vasconcelos. *Op. Cit.* Pg. 13.

³⁷ Termo cunhado pelo autor.

³⁸ SARDAS, Letícia de Faria. Novos Rumos do Direito Penal: Os Tipos Penais e a Internet. **Revista da EMERJ**. Vol. 7, Nº 25. Rio de Janeiro: 2004. Pg. 94.

³⁹ SARDAS, Letícia de Faria. *Op. Cit.* Pg. 95.

⁴⁰ ROSA, Fabrizioo. **Crimes de informática**. 2ª ed. Campinas: Bookseller, 2005. Pg. 49.

Para ROSSINI, infrações informáticas impróprias seriam aquelas em que o computador é uma simples ferramenta com a qual se ofende outros bens jurídicos, não necessariamente pertencentes a um Sistema Informático. É o caso do estelionato, a ameaça e os crimes contra a honra ou, até mesmo, homicídio pela internet (alterações em rotas de aviões ou acesso a um sistema informático de um hospital para alterar um medicamento que está sendo dado a um paciente).⁴¹

Vários criminosos utilizam-se dos Sistemas Informáticos para a prática dos seus atos ilícitos, sendo que muitos deles já estão tipificados no Sistema Penal Brasileiro. Entre os crimes mais comuns e conhecidos pela sociedade estão a pedofilia, a injúria, a calúnia e a difamação.

Dentre os vários elementos pertinentes a esse tema, um ambiente virtual que se tornou uma verdadeira mania brasileira é o ORKUT, como principal representante dos sites de relacionamento.

No ambiente virtual do ORKUT existem várias comunidades onde os seus participantes se unem devido a afinidades de pensamento e perfil psicológico, sendo, porém, em alguns casos, comunidades que aglutinam manifestação de idéias que são penalmente tipificadas, como o racismo, a pedofilia e críticas contra determinados grupos étnicos.

Em seu estudo sobre o tema ORKUT, MIRANDA⁴² salienta a possibilidade de invasão do computador dos usuários por vírus transmitidos através do *site*, a possibilidade do delito de falsidade ideológica, crimes contra a honra e o estabelecimento de grupos de crime organizado.

Vários elementos pertencentes a este *site* onde os usuários se expõem de forma ampla, permitem que vários criminosos possam usar dados dos participantes de forma aleatória, podendo até mesmo os usuários serem expostos em situações que denigram a sua imagem, bem distante talvez do que imaginaram ao se cadastrarem⁴³.

⁴¹ ROSSINI, Augusto Eduardo de Souza. Do necessário estudo do direito penal ante a informática e a telemática. **Revista Brasileira de Ciências Criminais**. Vol. 12, Nº 49. São Paulo: jul./ago. de 2004. Pg. 42.

⁴² MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via Internet. **Jus Navigandi**. Teresina. Ano 4, nº 37. Dez. 1999.

⁴³ MENDES, Carolina Aguiar Teixeira. Perfil: Orkut. **Jus Navigandi**. Ano 10, nº 883. Dez. 2005.

Um crime que tem aumentado é o de pedofilia, que está devidamente tipificado no Estatuto da Criança e do Adolescente⁴⁴ (Lei nº8.069 de 13-7-1990). De forma pouco efetiva o combate a este crime tem se intensificado, porém os criminosos encontram no ambiente virtual um local propício para a sua não identificação, favorecendo o envio de material pornográfico a todos os locais onde existam acessos a Internet.

O estelionato está plenamente tipificado no artigo 171 do Código Penal e, no comentário de COSTA⁴⁵, o artigo prevê "...substancialmente muitas condutas desenvolvidas contra o computador e os seus sistemas."

Os crimes contra a honra são bastante freqüentes na Internet, devido a grande facilidade de envio de *e-mail* e sua vinculação e distribuição. Esse crime é bastante freqüente no ambiente do ORKUT. Segundo MENDES⁴⁶:

Os crimes contra a honra são: calúnia, difamação e injúria. Calúnia é a falsa imputação a alguém (mesmo se este alguém já morreu) de fato definido como crime, também cometendo o mesmo delito aquele que, sabendo da falsidade, propala ou divulga a informação; difamar uma pessoa é imputar fato ofensivo à sua reputação; e, injuriar é ofender-lhe a dignidade ou decoro.

A lista de crimes praticados com o auxílio da Informática e da Internet é extensa. No entanto, entende-se que todos os crimes mencionados acima estão devidamente regulados pelo Direito pátrio, não havendo a necessidade de uma legislação específica para tipificá-los. Os delitos informáticos impróprios utilizam o Sistema Informático como meio e atingem bens jurídicos já tutelados. O que entende-se ser importante é uma legislação que regule os procedimentos de averiguação desses delitos, determinando como a investigação deve proceder, quais meios utilizar e como chegar a autoria do crime.

8.2 DELITOS INFORMÁTICOS PRÓPRIOS

⁴⁴ "Art 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores, ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança e adolescente: Pena – reclusão de 2 (dois) a 6 (seis) anos, e multa."

⁴⁵ COSTA, Marco Aurélio Rodrigues da. *Op. Cit.* Pg. 5.

⁴⁶ MENDES, Carolina Aguiar Teixeira. *Op. Cit.* Pg. 3.

Existem dentro da Legislação Brasileira leis já aprovadas e que caracterizam o delito informático próprio, porém limitadas a pontos específicos: Lei nº 9.609, de janeiro de 1998 que protege a Propriedade Intelectual, ou seja, coíbe a cópia sem autorização de programas de computadores e a Lei nº 9.983⁴⁷, de 14 de julho de 2000, que tipifica o delito cometido por funcionário público que no exercício de sua função interfira em dados informatizados. Note-se, apenas funcionário público.

A interceptação ilegal é também um crime de informática próprio, no qual os dados são capturados quando estão sendo transferidos de um sistema computacional para outro, não havendo aí acesso direto ao computador da vítima, mas apenas interceptação dos dados em trânsito⁴⁸. Encontramos a tipificação para esta conduta na Lei nº 9.296⁴⁹ de 24 de julho de 1996.

SILVA⁵⁰ lista outras leis brasileiras que de forma direta estão relacionadas ao tema quando se analisam mecanismos em vigor para proteção de bens jurídicos relacionados a Sistemas Informáticos: Lei nº 9.610 de 1998 - Lei dos Direitos Autorais e a Lei nº 8.137, a qual torna crime a utilização de programas de computador que forneçam acesso a dados que pertençam a Fazenda Pública.

Encontra-se, no entanto, dificuldades para punir a criação e divulgação de programas de computadores destrutivos, sendo seu principal representante o vírus informático. Não há na legislação brasileira um tipo penal que reprima a propagação de tais programas. A única maneira de se punir tal conduta seria através do crime de dano, artigo 163⁵¹ do Código Penal. Porém, alguns juristas entendem que os dados não podem ser considerados como coisas.

⁴⁷ “Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão de 2 (dois) a 12 (doze) anos, e multa.”

“Art 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.”

“Parágrafo único. As penas são aumentadas de 1/3 (um terço) até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.”

⁴⁸ VIANNA, Túlio Lima, *Op. Cit.* Pg. 19.

⁴⁹ “Art 10°. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de 2 (dois) a 4 (quatro) anos, e multa.”

⁵⁰ SILVA, Rita de Cássia Lopes. *Op. Cit.*

⁵¹ “Art 163. Destruir, inutilizar ou deteriorar coisa alheia: Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa.”

Para FERREIRA⁵² *apud* VIANNA: “...coisa é tudo aquilo que existe ou pode existir. Se os dados existem, são coisas”. Portanto, o problema acima não existiria. Já para RAHAL e GARCIA⁵³, o vírus causa deterioração de programa ou dado, mas não há qualquer alteração no maquinário, no *hardware*. Assim, se não há modificação física palpável, não configura crime de dano. Os mesmos autores citam a definição de MIRABETE⁵⁴, onde “...coisa é toda substância corpórea, material, ainda que não tangível, suscetível de apreensão e transporte”. Buscam suporte também na obra de HUNGRIA⁵⁵, para quem o “...objeto material do dano é a coisa móvel, devendo tratar-se, obviamente, de coisa corpórea ou no sentido realístico, pois somente esta pode ser danificada por ação física”.

Em razão da controvérsia, elenca-se a criação e divulgação de programas de computadores destrutivos como um delito informático próprio que necessita de uma adequada tipificação, sendo um dos objetos de estudo daqui para a frente.

O outro delito informático próprio que necessita de um tratamento legislativo adequado é o acesso não autorizado a Sistemas Informáticos. Parece, no entanto, incongruente falar-se de um delito que não é tipificado. Porém, VIANNA⁵⁶ utiliza-se do conceito material de crime “...que elege a afetação de um bem jurídico como base da ação típica”. As palavras de FRAGOSO⁵⁷ elucidam melhor esta questão:

Sob o aspecto material, é o crime um desvalor da vida social, ou seja, uma ação ou omissão que se proíbe e se procura evitar, ameaçando-a com pena, porque constitui ofensa (dano ou perigo) a um bem, ou a um valor da vida social”. Tentaremos, mais adiante, mostrar que os dados possuem valor social relevante e precisam ser tratados como bens jurídicos protegidos.

O objeto de estudo, à partir de agora, concentrar-se-á na necessidade de tipificação desses dois últimos delitos abordados.

⁵² VIANNA, Túlio Lima, *Op. Cit.* Pg. 22.

⁵³ RAHAL, Flávia; GARCIA, Roberto Soares. Vírus, direito à intimidade e a tutela penal da Internet. **Revista do Advogado**. Vol. 23, Nº 69. São Paulo: mai. De 2003. Pg. 26.

⁵⁴ RAHAL, Flávia; GARCIA, Roberto Soares. *Op. Cit.* Pg. 27.

⁵⁵ RAHAL, Flávia; GARCIA, Roberto Soares. *Op. Cit.* Pg. 27.

⁵⁶ VIANNA, Túlio Lima, *Op. Cit.* Pg. 2.

⁵⁷ VIANNA, Túlio Lima, *Op. Cit.* Pg. 2.

9 BEM JURÍDICO PROTEGIDO

Toda sociedade possui valores que são de grande valia para o seu funcionamento harmônico, sendo também imprescindíveis para a convivência social, como a vida, o patrimônio, a honra, a liberdade, a privacidade, etc.

Alguns desses elementos são denominados de bens jurídicos e devido a seu grande valor para a sociedade, devem receber proteção pela legislação de cada país.

Para que algo receba a denominação de bem jurídico protegido, faz-se necessário inicialmente o reconhecimento de sua existência e após o reconhecimento de seu valor dentro de uma sociedade onde o mesmo está presente e é necessário.

No campo da informática, podem-se identificar elementos que receberiam o título de bem jurídico protegido, como os dados armazenados - aqui se inclui também os programas informáticos - e a inviolabilidade dos mesmos, devido a sua importância para a sociedade moderna, sendo que a inviolabilidade é decorrência natural do direito à privacidade⁵⁸.

Nas palavras de PRADO *apud* VIANNA⁵⁹:

Não há delito sem que haja lesão ou perigo de lesão (princípio da lesividade ou ofensividade) a um bem jurídico determinado. Sob esta perspectiva, a tutela penal só é legítima quando socialmente necessária (princípio da necessidade), imprescindível para assegurar as condições de vida, o desenvolvimento e a paz social, tendo em conta os ditames superiores da dignidade e da liberdade da pessoa humana.

Perante tal afirmação se pode intuir que os dados armazenados em um Sistema Informático são bens jurídicos que devem ser protegidos, bem como a inviolabilidade dos mesmos. Diante de tal conceito pode-se agora classificar que uma conduta não legítima em relação a dados armazenados e a sua inviolabilidade são crimes e sua "...simples omissão normativa não é suficiente para descaracterizá-

⁵⁸ VIANNA, Túlio Lima, *Op. Cit.* Pg. 3.

⁵⁹ VIANNA, Túlio Lima, *Op. Cit.* Pg. 2.

lo como objeto de estudo do Direito Penal, já que este reconhece sua existência sob o aspecto material.”⁶⁰

Outros bens jurídicos protegidos já citados como a honra, a liberdade, o patrimônio, etc, também podem ser atingidos por intermédio do computador e também constituem crimes, porém já estão tipificados e a legislação existente consegue abrangê-los.

⁶⁰ VIANNA, Túlio Lima, *Op. Cit.* Pg. 03.

10 DIREITO ESTRANGEIRO

Os delitos informáticos próprios que não possuem tratamento no Direito Brasileiro já estão tipificados em algumas legislações estrangeiras, variando quanto a amplitude e interpretações dos mesmos.

A primeira tentativa de tipificação de um delito informático ocorreu nos Estados Unidos da América em 1977, sendo o projeto de lei do Senador americano *Ribikoff* rejeitado. Atualmente nesse país está em vigor o *Computer Fraud and Abuse Act* que surgiu em 1986.

No Código Penal italiano⁶¹, encontra-se as alterações trazidas pela Lei n° 547/1993, com o objetivo de punir aquele que abusivamente acessa um Sistema Informático, ou que se mantém nele contra a vontade de quem tem o direito de excluí-lo⁶². Pune-se também aquele a propagação de vírus de computador, danificando um Sistema Informático.⁶³

Na França⁶⁴ também se encontra a punição contra o acesso obtido de forma fraudulenta a um sistema de tratamento automático de dados, salientando-se que até mesmo a tentativa é punida com a mesma pena. A supressão ou modificação dos dados qualifica o delito.

⁶¹ “Art. 615 ter Accesso abusivo ad un sistema informatico o telematico. Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, é punito con la reclusione fino a tre anni”.

⁶² VIANNA, Túlio Lima, *Op. Cit.* Pg. 38.

⁶³ Art. 615 quinquies *Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.*

Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, é punito con la reclusione sino a due anni e con la multa sino a lire venti milioni.”

⁶⁴ “ Article 323-1. Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 F d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 200 000 F d'amende.

Article 323-7. La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.”

No Reino Unido, Suécia, Suíça, Bélgica e Áustria também são encontradas leis que procuram proteger Sistemas Informáticos, dados e programas, cada uma com suas peculiaridades como salientam VIANNA⁶⁵ e ROSA⁶⁶.

Em Portugal⁶⁷ como salienta COLARES⁶⁸, já existe legislação própria com a Chamada Lei de Criminalidade Informática de 1991⁶⁹. Essa lei tipificou o acesso não autorizado a sistema ou rede informáticos e também tornou crime a sabotagem eletrônica, punindo-se assim a introdução de vírus, com a intenção de entrar ou perturbar, um Sistema Informático alheio.

Na América do Sul, o Chile tipificou o acesso não autorizado a sistemas computacionais através da Lei 19.223⁷⁰ de 1993.

Os canadenses também já desfrutam de lei que os protege, bem como na China que possui uma peculiaridade, pois lá só é crime os delitos informáticos contra dados sobre assuntos estatais.

Um exemplo bastante importante sobre esse tipo de delito e seu combate de forma incisiva é a aprovação em 2001 do *Draft Convention of Cybercrime* pelo Comitê Europeu para Problemas Delitivos, o primeiro tratado internacional sobre a criminalidade informática⁷¹.

⁶⁵ VIANNA, Túlio Lima, *Op. Cit.* Pg. 41-42.

⁶⁶ ROSA, Fabrizio. *Op. Cit.* Pg. 83.

⁶⁷ “ Art 7 Acesso Ilegítimo. Quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos será punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

Art 6. Falsidade Informática. Quem introduzir, alterar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir em sistema informático, actuando com intenção de entrar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distância, será punido com pena de prisão até 5 anos ou com pena de multa até 600 dias”.

⁶⁸ COLARES, Rodrigo Guimarães. Cybercrimes: os crimes na era da informática. **Jus Navigandi**. Teresina. Ano 6, nº 59. Out. 2002. Pg. 2.

⁶⁹ Lei nº 109/91.

⁷⁰ “Artículo 2º - El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.”

⁷¹ VIANNA, Túlio Lima, *Op. Cit.* Pg. 44.

11 PERFIL DO CRIMINOSO DIGITAL

Conforme afirma MIRANDA⁷², o perfil daqueles que cometem crimes através dos Sistemas Informáticos está definido em pesquisas empíricas por vários estudiosos desse fenômeno no mundo criminal. Segundo o autor, em geral são pessoas do sexo masculino, com inteligência acima da média, educados, entre 15 e 32 anos.

Geralmente também são aficionadas em jogos eletrônicos, audaciosos, gosto por desafios, aventureiros e movidos por motivos de auto-superação. Esses criminosos são definidos também como autodidatas, pois o aprendizado dos processos necessários para a efetivação do delito se faz quase que exclusivamente por intermédio da aprendizagem solitária, podendo haver casos onde um criminoso agencia novos “alunos” para a transmissão de seus conhecimentos. VIANNA⁷³ salienta também que o prestígio entre pessoas com esse perfil, está baseado no montante do conhecimento que cada um possui em sua “sub-cultura”, ou seja, o prestígio está diretamente relacionado à suas proezas ilegais.

Vários dos criminosos digitais que foram surpreendidos em seus atos ilícitos, alegaram que não estavam cometendo crimes, apenas estavam procurando ultrapassar seus limites; tudo estava sendo feito em caráter de “teste” e “brincadeira”, sendo também importante salientar que seus valores e normas de conduta divergem significativamente dos valores sociais predominantes.

Outros afirmam que invadem Sistemas Informáticos porque os donos desses sistemas “mereceram” sofrer a invasão, pois não cuidaram da sua segurança de forma efetiva, conforme afirma VIANNA⁷⁴.

Por fim podem ser salientadas as seguintes características que conforme afirmam SYKES e MATZA *apud* VIANNA⁷⁵, predominam no perfil desse tipo de criminoso como tentativa de justificar os seus atos: “exclusão da própria responsabilidade” - não podem controlar o seus impulsos; “negação de ilicitude” - a sua conduta é apenas proibida, mas não imoral ou danosa; “negação da vitimização” - a vítima mereceu a invasão pois não tomou os devidos cuidados com a segurança

⁷² MIRANDA, Marcelo Baeta Neves. *Op. Cit.* Pg. 4.

⁷³ VIANNA, Túlio Lima, *Op. Cit.* Pg. 29.

⁷⁴ VIANNA, Túlio Lima, *Op. Cit.* Pg. 30.

⁷⁵ VIANNA, Túlio Lima, *Op. Cit.* Pg. 30.

de seus sistemas; “condenação dos que condenam” - a sociedade é hipócrita - e “respeito a hierarquia” - obediência ao código de “ética” do grupo a qual pertencem.

Há de se atentar para os aspectos criminológicos para tentar-se delinear os sujeitos ativos deste tipo de infração, “...preocupando-se não só com o campo puramente normativo, mas também com as causas do fenômeno criminal” (HANS WELZEL *apud* ROSSINI)⁷⁶. Assim, importante se faz o estudo da “...origem social, os novos paradigmas de acesso ao conhecimento criminoso, a indiferença da idade penal, o oportunismo, a proximidade eletrônica ou a ausência da distância e anonimato...”⁷⁷.

⁷⁶ ROSSINI, Augusto Eduardo de Souza. *Op. Cit.* Pg. 45.

⁷⁷ ROSSINI, Augusto Eduardo de Souza. *Op. Cit.* Pg. 45.

12 DETERMINAÇÃO DA AUTORIA, LOCAL E TEMPO

Entre as características dos delitos realizados pela Internet, está o anonimato; aqui está inserida a maior dificuldade de caracterizar o autor do delito, bem como pela instantaneidade dos crimes.

O Direito Penal Brasileiro não permite a condenação por presunção de culpa, ou seja, é necessário que existam provas reais para que alguém possa ser punido efetivamente. No ambiente virtual os entes reais que mais próximo se encontram da responsabilidade dos crimes cometidos, de forma não direta, seriam os provedores de acesso, pois são por intermédio deles que se tornam possíveis as interligações das redes.

Elementos que também merecem análise são o local onde é praticado o crime de informática e o tempo de sua ocorrência.

Em relação ao primeiro item citado, realça-se a importância quanto a extensão dos crimes de informática no que se refere a jurisdição quanto a aplicação da lei sobre crimes de informática quando praticados em territórios soberanos distintos. Para tal elemento faz-se necessária atuação conjunta de nações amigas que tenham como características em suas legislações o combate e esse tipo de crime, sendo que o mesmo deve estar tipificado de forma conjunta em ambas as legislações, sendo aqui importante tratados internacionais de cooperação.

Em relação ao tempo do crime, conforme VIANNA⁷⁸, é importante a sua determinação "...na aplicação da norma penal para a solução de conflito temporal de normas, aferição da imputabilidade do agente, aplicação da anistia e da prescrição e análise das circunstâncias do crime."

Quanto a autoria se configura um dos elementos mais difíceis de serem resolvidos, pois devido a grande facilidade do anonimato do agente ativo do crime, torna-se de forma quase hercúlea a tentativa de identificá-lo. Métodos de rastreamento do *Internet Protocol* (IP), endereço único que identifica cada um dos computadores interconectados em qualquer Sistema Informático, podem ser

⁷⁸ VIANNA, Túlio Lima, *Op. Cit.* Pg. 61.

instrumentos eficazes⁷⁹. Então seria dessa forma possível identificar a origem e local do ato criminoso, bem como, de uma forma não direta o autor.

⁷⁹ VIANNA, Túlio Lima, *Op. Cit.* Pg. 50.

13 PROJETOS DE LEI EM ANDAMENTO

A discussão sobre a necessidade ou não de uma legislação específica para os crimes de informática, com a criação de novos tipos penais, pode ser percebida no âmbito legislativo. Analisando os projetos de lei que tratam sobre o assunto, temos dois originados no Senado Federal (PLS 76/2000 e PLS 137/2000), e lá aguardando votação, e um originado na Câmara dos Deputados, já aprovado em 05 de Novembro de 2003, e aguardando votação também no Senado Federal (PLC 89/2003)⁸⁰.

No projeto de lei 137/2000, de autoria do Senador Leomar Quintanilha, observa-se um posicionamento contrário à novas tipificações. O art 1º do referido projeto⁸¹ expõe: “Os crimes cometidos contra a pessoa, o patrimonício, a propriedade imaterial e intelectual, contra os costumes, bem como contra a criança e o adolescente, com a utilização de meios de tecnologia de informação e telecomunicações terão, levando-se em conta a culpabilidade e as conseqüências do crime, as penas até o triplo.”

Na exposição dos motivos, destaca o mesmo Senador que o projeto parte do princípio de que não são necessários novos tipos penais para combater as infrações por meios de informática e telecomunicações, estando o nosso ordenamento jurídico já apto para isto.⁸²

Posicionamento contrário encontra-se no projeto de lei 76/2000, de autoria do Senador Renan Calheiros, tendo o projeto o intuito de definir e tipificar os delitos informáticos⁸³. Encontra-se na justificção deste projeto o posicionamento do Senador: “...entendemos que este projeto ao definir como conduta delituosa determinados procedimentos até agora não tipificados no nosso Direito Penal, pretende preencher uma lacuna existente no ordenamento jurídico, colocando nosso país em igualdade com outros tantos.”⁸⁴

⁸⁰ O projeto original do deputado Luiz Piauhyllino tinha o número 84/1999, recebendo a numeração PLC 89/2003 ao chegar ao Senado Federal.

⁸¹ Diário do Senado Federal, 12 de maio de 2000, Pg. 9750.

⁸² Diário do Senado Federal, 12 de maio de 2000, Pg. 9751.

⁸³ Diário do Senado Federal, 28 de março de 2000, Pg. 5404.

⁸⁴ Diário do Senado Federal, 28 de março de 2000, Pg. 5406.

Destaca também o mesmo Senador que delitos informáticos devem ser tipificados urgentemente por todos os países⁸⁵.

O projeto de lei 89/2003, por já ter sido aprovado na Câmara dos Deputados, parece ser o mais próximo de adentrar em nosso ordenamento jurídico. O projeto foi aprovado por unanimidade pela referida Casa Legislativa, com substitutivos, sendo rejeitados outros três projetos sobre o tema.

Destaca-se a posicionamento do Deputado Luiz Piauhyllino, na justificação do referido projeto: “Não podemos permitir que pela falta de lei, que regule os crimes de informática, pessoas inescrupulosas continuem usando computadores e suas redes para propósitos escusos e criminosos. Daí a necessidade de uma lei que defina os crimes cometidos na rede de informática e suas respectivas penas”⁸⁶.

ROSA⁸⁷ na apresentação de seu livro salienta que vários delitos informáticos são, desde muito, considerados crimes pela Organização das Nações Unidas (ONU) e é necessário que seus países membros definam em suas legislações vários tipos penais e métodos de investigação.

É notório o grande número de atitudes que podem ser consideradas delitos informáticos e que vêm acontecendo em vários países, sendo o Brasil um possível alvo desses crimes em amplitude global. Assim sendo, a tipificação pela legislação brasileira dessa espécie de delito faz-se necessária, pois através dela será definida punição que servirá como um método eficaz para desincentivar o seu cometimento.

No projeto do Deputado Luiz Piauhyllino estão tipificados crimes de acesso indevido ou não autorizado a dados armazenados e confidenciais, alteração de senha, dados e informações, danos através de vírus e demais elementos de crimes dessa natureza.

Este projeto conforme a opinião de COLARES⁸⁸, veio ao encontro da necessidade de uma lei que fosse específica à este tipo de delito.

Também ROSA⁸⁹ analisa o projeto como sendo de grande importância, pois vem preencher uma lacuna que existe na legislação brasileira, quando tipifica

⁸⁵ Diário do Senado Federal, 28 de março de 2000, Pg. 5405.

⁸⁶ VIANNA, Túlio Lima, *Op. Cit.* Pg. 106.

⁸⁷ ROSA, Fabrizio. *Op. Cit.*

⁸⁸ COLARES, Rodrigo Guimarães. *Op. Cit.* Pg. 2.

⁸⁹ ROSA, Fabrizio. *Op. Cit.* Pg. 91.

condutas delituosas não presentes no Código Penal, deixando o Brasil em pé de igualdade com outros países.

O Projeto de Lei mencionado acima busca trazer para o Direito Penal Brasileiro a tipificação de delitos informáticos próprios, sendo que alguns não encontram atualmente punições regulamentadas contra as suas práticas. Esses delitos só são apreendidos pelo nosso Sistema Penal quando afetam um bem jurídico já tipificado.

Para GOMES⁹⁰, esta lei é bem-vinda, pois além de trazer a tipificação mais adequada de alguns crimes já previstos no ordenamento jurídico brasileiro, a evolução tecnológica traz a necessidade de combater crimes antes inexistentes, que serão tipificados por esta lei.

Como já exposto, os delitos informáticos podem ser impróprios ou comuns, quando não afetam o Sistema Informático em si, mas outros bens jurídicos. Neste caso o computador torna-se um instrumento para a execução da conduta criminosa. Estes acabam sendo os crimes mais comuns e difundidos, pois a rede de informática, que inunda o planeta com dados e informações que são transmitidas em velocidade muito grande, permite em sua estrutura a existência de vários crimes que, como já definidos, estão já tipificados através do Código Penal.

Nesse ambiente virtual, vários interesses estão envolvidos e tantos outros elementos que são oferecidos por empresas de alcance global - grande soma em dinheiro está envolvida - permitem a existência de um ambiente bastante propício para a prática de muitos delitos no âmbito financeiro, sendo o Brasil palco de grande número de exemplos. Portanto, o seu combate e punição realizados de uma forma mais rápida e eficaz, são muito importantes.

A atuação policial para a punição desses crimes, porém, fica a desejar, pois como afirma MIRANDA⁹¹, existem pouquíssimos profissionais de polícia preparados para a investigação desse tipo de delito, mesmo sendo ele tipificado.

⁹⁰ GOMES, Luis Flávio. Criminosos virtuais na mira da lei. RT Informa. Ano VI, nº 38. Jul/ago, 2005. Ed. Revista dos Tribunais. Pg. 4.

⁹¹ MIRANDA, Marcelo Baeta Neves. *Op. Cit.* Pg. 2.

14 DA TIPIIFICAÇÃO FRENTE A UMA ÉPOCA DE DESCRIMINALIZAÇÃO

Os homens, que inicialmente viviam isolados, uniram-se para enfrentar as vicissitudes da vida, formando as primeiras sociedades. Esta união atendeu as necessidades básicas de sobrevivências mas exigiu a criação de normas de conduta para a manutenção das sociedades. Essas regras, inicialmente orais, converteram-se em normas escritas e o conjunto destas normas foi denominado Direito.

Como cada pessoa da sociedade quer submeter a vontade alheia à sua, as normas para o convívio em sociedade acabavam sendo desrespeitadas, o que gerou a necessidade de se estabelecer sanções àqueles que as infringiam. “O que aconteceu posteriormente foi uma evolução das normas penais, restringindo a liberdade individual, na defesa do conjunto harmônico da sociedade.”⁹²

Para o professor COSTA *apud* SARDAS: “O Direito Penal tem ou utiliza diferentes técnicas de construção do tipo legal de crime e ao empregar diversos modos de fabricar o crime está a assumir uma escolha. Está a decidir sobre as margens da punibilidade. Está, em síntese, a operar uma decisão político-legislativo”.⁹³

O direito penal é a forma mais drástica de intervenção na vida social, gerando grande desconforto. Há defensores de uma neocriminalização, com a definição de comportamentos proibidos e a criação de novos tipos penais e, defensores da descriminalização, onde o legislador tira do mundo jurídico-penal uma determinada infração. Indaga-se, atualmente, se há a necessidade ou não da criação de novos tipos penais para abranger comportamentos provenientes da sociedade da informação.

Para DELL' ORTO *apud* SARDAS:

As novas concepções de bem jurídico não devem gerar o aumento da quantidade de comportamentos humanos incriminados e sim a formulação de uma nova Teoria do Estado, onde o Direito Penal representaria um novo papel, utilizando o mecanismo de valorização da pessoa, num mundo massificado, ao invés da simples aplicação de sanções punitivas.⁹⁴

⁹² SARDAS, Letícia de Farias. *Op. Cit.* Pg. 80.

⁹³ SARDAS, Letícia de Farias. *Op. Cit.* Pg. 81.

⁹⁴ SARDAS, Letícia de Farias. *Op. Cit.* Pg. 85.

Para ZAFFARONI *apud* SARDAS:

...o segundo milênio foi o do sistema penal e o terceiro milênio será o da quebra do discurso punitivo e do sistema penal. Não estamos falando em termos de um otimismo irresponsável. No terceiro milênio, a humanidade vai sobreviver, e para isso terá que acabar com o sistema penal, vai ter que acabar com o discurso punitivo e achar soluções reais para os problemas, não ilusões para solucioná-lo.⁹⁵

⁹⁵ SARDAS, Letícia de Farias. *Op. Cit.* Pg. 87.

15 CONCLUSÃO

A informática tornou-se crucial para a execução das mais diversas atividades do homem contemporâneo. Seja no trabalho ou no entretenimento, lá está o computador e as suas inúmeras possibilidades de uso. Os investimentos em Tecnologia da Informação crescem anualmente exigindo que equipamentos sejam substituídos corriqueiramente para não restarem ultrapassados.

Nesse trabalho, observou-se o conceito de Sistema da Informação e a importância do dado, como representante da informação dentro do Sistema Informático.

Diferenciou-se a Informática Jurídica do Direito da Informática. A primeira como o tratamento automático de dados relacionados ao Direito e o último como o conjunto de regras e conceitos que abrangem a Informática.

Ao analisar-se a relação da Informática com o Direito Penal, há autores que defendem uma legislação específica para os delitos praticados com o auxílio da Informática, seja contra ela mesma ou contra qualquer outro bem jurídico. Por outro lado, há autores que salientam que a atual legislação penal é suficiente para abranger os delitos trazidos pelo advento da informática, sendo esta apenas um meio.

Procurou-se diferenciar os delitos informáticos em impróprios, próprios, mistos e mediatos. Os primeiros foram elencados de maneira exemplificativa, defendendo-se em seguida que não há a necessidade de uma lei que normatize essas condutas, pois as mesmas já estão tipificadas no Direito Brasileiro. Para exemplificar, seja pela internet, por carta ou oralmente, a calúnia será enquadrada pelo art. 138 do Código Penal. Para esses delitos, o que se faz necessário é uma regulamentação que ajude no combate a criminalidade praticada pela internet, dizendo como devem ser investigados, se os provedores devem ou não prestar as informações que ajudem na determinação da autoria, etc.

Quanto aos delitos informáticos próprios, mostrou-se alguns que já estão tipificados pelo Direito Brasileiro, porém limitados a pontos específicos. A criação de vírus de computador e sua inserção em Sistema Informático não possui regulamentação no país, sendo de difícil aplicação o crime de dano, art. 163 do Código Penal.

O acesso não autorizado a sistemas computacionais mostra-se como uma conduta socialmente reprovável mas que ainda não é coibida pela legislação penal. Procurou-se demonstrar a relevância social do dado para concluir que o mesmo deve ser considerado um bem jurídico protegido.

À partir da comparação da legislação estrangeira, percebeu-se como é o tratamento destas questões em outros países e como poderia ser adotado aqui.

Por fim, salientou-se que a criação de novos tipos penais contrariam uma tendência atual de discriminalização, já que o Direito Penal não tem sido o melhor dos meios para se evitar as condutas delituosas. Por isso, defendeu-se o cuidado em não exagerar-se, evitando assim uma inflação legislativa penal.

Conclui-se pela necessidade de uma legislação própria que trate das condutas reprováveis praticadas contra a informática. Os crimes contra a honra, presentes na Grande Rede Mundial, objeto de noticiários e de preocupação social, assim como o furto de senhas para a transferência ilegal de dinheiro de contas bancárias, já encontram guarida no ordenamento jurídico brasileiro. No entanto, a criação e posterior introdução de vírus no Sistema Informático e o acesso não autorizado a sistemas computacionais, são condutas sociais reprováveis mas de difícil tratamento pelo Direito Penal pátrio.

REFERÊNCIA

- 1 ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Jus Navigandi**. Teresina. Ano 5, nº 51. Out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/>. Acesso em: 20 de agosto de 2006.
- 2 BARROS, Lucivaldo Vasconcelos. O crime na era da iform@ção. **Jus Navigandi**. Teresina. Ano 7, nº 61. Jan. 2003. Disponível em: <http://jus2.uol.com.br/doutrina/>. Acesso em: 20 de agosto de 2006.
- 3 CHILE, *Ley nº 19.223 de 7 de Junio de 1993. Ley relativa a delitos informaticos*. Disponível em: <http://www.ads.cl/download/>. Acesso em: 10 de setembro de 2006.
- 4 COLARES, Rodrigo Guimarães. Cybercrimes: os crimes na era da informática. **Jus Navigandi**. Teresina. Ano 6, nº 59. Out. 2002. Disponível em :<http://jus2.uol.com.br/doutrina/>. Acesso em: 25 de março de 2006.
- 5 COSTA, Marco Aurélio Rodrigues da. Crimes de Informática. **Jus Navigandi**. Teresina. Ano 1, nº 12. Mai. 1997. Disponível em <http://jus2.uol.com.br/doutrina/>. Acesso em 10 de março de 2006.
- 6 Criminosos virtuais na mira da lei. **RT Informa**. Ano VI, nº 38. Jul/ago, 2005. Ed. Revista dos Tribunais. Pg. 4-5.
- 7 FERREIRA, Ivette Senise. **Direito & Internet – aspectos jurídicos relevantes**. Bauru: Edipro, 2000.
- 8 FINKELSTEIN, Maria Eugênia. **Aspectos jurídicos do comércio eletrônico**. Porto Alegre: Síntese, 2004.
- 9 FRANÇA, *Code Penal*. Disponível em: <http://www.legifrance.gouv.fr>. Acesso em: 10 de setembro de 2006.
- 10 GRECO FILHO, Vicente. Algumas Observações Sobre o Direito Penal e a Internet. **Boletim IBCRIM**. Ano 8. N° 95.
- 11 ITÁLIA, *Codice Penale*. Disponível em: <http://www.usl4.toscana.it/dp/>. Acesso em: 09 de setembro de 2006.

12 MENDES, Carolina Aguiar Teixeira. Perfil: Orkut. **Jus Navigandi**. Ano 10, nº 883. Dez. 2005. Disponível em: <http://jus2.uol.com.br/doutrina/>. Acesso em: 01 de agosto de 2006.

13 MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via Internet. **Jus Navigandi**. Teresina. Ano 4, nº 37. Dez. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/>. Acesso em: 10 de agosto de 2006.

14 PORTUGAL, Lei nº 109, de 17 de agosto de 1991. Criminalidade Informática. Disponível em: <http://www.icp.pt/>. Acesso em: 10 de setembro de 2006.

15 RAHAL, Flávia; GARCIA, Roberto Soares. Vírus, direito à intimidade e a tutela penal da Internet. **Revista do Advogado**. Vol. 23, Nº 69. São Paulo: mai. de 2003.

16 ROSA, Fabrizio. **Crimes de informática**. 2ª ed. Campinas: Bookseller, 2005.

17 ROSSINI, Augusto Eduardo de Souza. Do necessário estudo do direito penal ante a informática e a telemática. **Revista Brasileira de Ciências Criminais**. Vol. 12, Nº 49. São Paulo: jul./ago. de 2004.

18 SARDAS, Letícia de Faria. Novos Rumos do Direito Penal: Os Tipos Penais e a Internet. **Revista da EMERJ**. Vol. 7, Nº 25. Rio de Janeiro: 2004.

19 SILVA, Rita de Cássia Lopes. **DIREITO PENAL E SISTEMA INFORMÁTICO**. Ciência do Direito Penal Contemporâneo, Vol. 4. São Paulo: Ed. Revista dos Tribunais, 2003.

20 VIANNA, Túlio Lima. **FUNDAMENTOS DE DIREITO PENAL INFORMÁTICO. DO ACESSO NÃO AUTORIZADO A SISTEMAS COMPUTACIONAIS**. Rio de Janeiro: Ed. Forense, 2003.

21 www.senado.gov.br

22 www.camara.gov.br

ANEXO I
PROJETO DE LEI DA CÂMARA Nº 89, DE 2003

PROJETO DE LEI DA CÂMARA Nº 89, DE 2003 (nº 84/99, na Casa de Origem)

(altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e a Lei nº 9.296, de 24 de julho de 1996, e dá outras providências)

(em trâmite no Senado)

O Congresso Nacional decreta:

Art. 1º Esta Lei dispõe sobre os crimes de informática, e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar acrescido da seguinte Seção V do Capítulo VI do Título I:

SEÇÃO V

Dos crimes contra a inviolabilidade

Dos sistemas informatizados

Acesso indevido a meio eletrônico

Art. 154-A. Acessar, indevidamente ou sem autorização, meio eletrônico ou sistema informatizado:

Pena - detenção, de três meses a um ano, e multa.

§ 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a meio eletrônico ou sistema informatizado.

§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista.

Manipulação indevida de informação eletrônica

Art. 154-B. Manter ou fornecer, indevidamente ou sem autorização, dado ou informação obtida em meio eletrônico ou sistema informatizado:

Pena - detenção, de seis meses a um ano, e multa.

§ 1º Nas mesmas penas incorre quem transporta, por qualquer meio, indevidamente ou sem autorização, dado ou informação obtida em meio eletrônico ou sistema informatizado.

§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista.

Meio eletrônico e sistema informatizado

Art. 154-C. Para os efeitos penais, considera-se:

I - meio eletrônico: o computador, o processador de dados, o disquete, o CD-ROM ou qualquer outro meio capaz de armazenar ou transmitir dados magnética, óptica ou eletronicamente;

II - sistema informatizado: a rede de computadores, a base de dados, o programa de computador ou qualquer outro sistema capaz de armazenar ou transmitir dados eletronicamente."

Art. 3º O art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar com as seguintes alterações, renumerando-se o parágrafo único para § 1º:

"Art. 163.

§ 1º.....

Dano eletrônico

§ 2º Equipara-se à coisa:

I - o dado, a informação ou a base de dados presente em meio eletrônico ou sistema informatizado;

II - a senha ou qualquer meio de identificação que permita o acesso a meio eletrônico ou sistema informatizado.

Difusão de vírus eletrônico

§ 3º Nas mesmas penas do § 1º incorre quem cria, insere ou difunde dado ou informação em meio eletrônico ou sistema informatizado, indevidamente ou sem autorização, com a finalidade de destruí-lo, inutilizá-lo, modificá-lo ou dificultar-lhe o funcionamento."(NR)

Art. 4º O art. 167 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar com a seguinte redação:

"Art. 167. Nos casos do art. 163, § 1º, inciso IV, quando o dado ou informação não tiver potencial de propagação ou alastramento, e do art. 164, somente se procede mediante queixa." (NR)

Art. 5º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar acrescido do seguinte artigo:

"Pornografia infantil".

Art. 218-A. Fotografar, publicar ou divulgar, por qualquer meio, cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

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

§ 1º As penas são aumentadas de metade até dois terços se o crime é cometido por meio de rede de computadores ou outro meio de alta propagação.

§ 2º A ação penal é pública incondicionada."

Art. 6º Os arts. 265 e 266, ambos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com as seguintes alterações:

"Atentado contra a segurança de serviço de utilidade pública".

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor ou telecomunicação, ou qualquer outro de utilidade pública:

....." (NR)

"Interrupção ou perturbação de serviço telegráfico ou telefônico"

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento:

....." (NR)

Art. 7º O art. 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar acrescido do seguinte parágrafo único:

"Art. 298.

Falsificação de cartão de crédito

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito"
(NR)

Art. 8º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar acrescido do seguinte artigo:

"Falsificação de telefone celular ou meio de acesso a sistema eletrônico"

Art. 298-A. Criar ou copiar, indevidamente ou sem autorização, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de radiofrequência ou de telefonia celular ou qualquer instrumento que permita o acesso a meio eletrônico ou sistema informatizado:

Pena - reclusão, de um a cinco anos, e multa."

Art. 9º O art. 2º da Lei nº 9.296, de 24 de julho de 1996, passa a vigorar acrescido do § 2º, renumerando-se o parágrafo único para § 1º:

"Art. 2º.

.....

§ 1º

§ 2º O disposto no inciso III do caput não se aplica quando se tratar de interceptação do fluxo de comunicações em sistema de informática ou telemática. "(NR)

Art. 10. Os crimes previstos nesta lei quando praticados nas condições do inciso II, art. 90, do Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, serão de competência da Justiça Militar.

Art. 11. As entidades que coletam, armazenam, processam, distribuem ou comercializam informações privadas, ou utilizam tais informações para fins comerciais ou para prestação de serviço de qualquer natureza, não poderão divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, a origem racial, opinião política, filosófica ou religiosa, crenças, ideologia, saúde física ou mental, vida sexual, registros policiais, assuntos familiares ou profissionais, e outras que a lei definir como sigilosas, salvo por ordem judicial ou com anuência expressa da pessoa a que se referem ou do seu representante legal.

Art. 12. Fica revogado o art. 241 da Lei nº 8.069, de 13 de julho de 1990.

Art. 13. Esta Lei entra em vigor na data de sua publicação.

Câmara dos Deputados, 11 de novembro de 2003.

Deputado *JOÃO PAULO CUNHA*

(Publicado no Diário do Senado Federal de sexta-feira, 14/11/03, página(s): 36938 - 36939)

ANEXO II
PROJETO DE LEI DO SENADO Nº 76, DE 2000

PROJETO DE LEI DO SENADO Nº 76, DE 2000

Define e tipifica os delitos informáticos, e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Constitui crime de uso indevido da informática:

§ 1º contra a inviolabilidade de dados e sua comunicação:

- I – a destruição de dados ou sistemas de computação, inclusive sua inutilização;
- II – a apropriação de dados alheios ou de um sistema de computação devidamente patenteados;
- III – o uso indevido de dados ou registros sem consentimento de seus titulares;
- IV – a modificação, a supressão de dados ou adulteração de seu conteúdo;
- V – a programação de instruções que produzam bloqueio geral no sistema ou que comprometam a sua confiabilidade.

Pena: detenção, de um a seis meses e multa.

§ 2º contra a propriedade e o patrimônio:

- I – a retirada de informação privada contida em base de dados;
- II – a alteração ou transferência de contas representativas de valores;

Pena: detenção, de um a dois anos e multa.

§ 3º contra a honra e a vida privada:

- I – difusão de material injurioso por meio de mecanismos virtuais;
- II – divulgação de informações sobre a intimidade das pessoas sem prévio consentimento;

Pena: detenção, de um a seis meses e multa.

§ 4º contra a vida e integridade física das pessoas:

- I – o uso de mecanismos da informática para ativação de artefatos explosivos, causando danos, lesões ou homicídios;

II – a elaboração de sistema de computador vinculado a equipamento mecânico, constituindo-se em artefatos explosivo;

Pena: reclusão, de um a seis anos e multa.

§ 5º contra o patrimônio fiscal:

I – alteração de base de dados habilitadas para registro de operações tributárias;

II – evasão de tributos ou taxas derivadas de transações “virtuais”;

Pena: detenção, de um a dois anos e multa.

§ 6º contra a moral pública e opção sexual:

I – a corrupção de menores de idade;

II – divulgação de material pornográfico;

III – divulgação pública de sons, imagens ou informação contrária aos bons costumes.

Pena: reclusão, de um a seis anos e multa.

§ 7º contra a segurança nacional:

I – a adulteração ou revelação de dados declarados como reservados por questões de segurança nacional;

II – a intervenção nos sistemas de computadores que controlam o uso ou ativação de armamentos;

III – a indução a atos de subversão;

IV – a difusão de informação atentatória a soberania nacional.

Pena: detenção, de um a dois anos e multa.

Art. 2º Os crimes tipificados nos §§ 1º a 3º são ações penais públicas condicionadas a representação e as demais ações penais incondicionadas.

Art. 3º Qualquer um desses crimes que venha a ser praticado contra empresa concessionária de serviços públicos, sociedades de economia mista ou sobre qualquer órgãos integrante da administração pública terão suas penas aumentadas para dois a seis meses e multa, nos casos os §§ 1º e 3º e de um ano e seis meses a dois anos e seis meses e multa nos demais casos.

Art. 4º Caso seja praticado qualquer um dos crimes tipificados nesta Lei como meio de realização ou facilitação de outro crime, fica caracterizada a circunstância agravante qualificadora, aumentando-se a pena de um terço até a metade.

Art. 5º Todos os crimes por uso indevido de computador estão sujeitos a multa igual ao valor do proveito pretendido ou do risco de prejuízo da vítima.

Art. 6º Esta lei entra em vigor na data de sua publicação.

Justificação

O espaço cibernético é um mundo virtual onde os defeitos e os atos ilícitos dos seres humanos se reproduzem com a mesma facilidade como as suas virtudes e suas atividades lícitas.

O uso da tecnologia e informática é um instrumento que facilita o desenvolvimento social e cultural da sociedade, permitindo que um número crescente de pessoas tenham acesso a esta tecnologia, utilizando-a nas suas diversas atividades, como educativos, comerciais, industriais e financeiras, entre outras.

Paralelamente a este avanço tecnológico surgiram novas formas de conduta antisocial fazendo dos equipamentos de informática, meios de de linqüência e de infrações.

Entre as condutas ilícitas mais comuns que constituem os chamados “delitos informáticos” estão: o acesso não autorizado a computadores e sistemas eletrônicos, a destruição e alteração das informações, a sabotagem por computadores, a intercessão de correio eletrônico, a fraude eletrônica e a transferência ilícita de fundos.

A Organização das Nações Unidas reconheceu que este tipo de delito é um sério problema, já que vários países não adequaram suas legislações mediante a criação de novos tipos penais e procedimentos de investigação. Países membros da União Européia tem uma regulamentação mais abrangente no campo da informática, incluindo a segurança de dados, as criações intelectuais relativas a

informática, de fraude informática, entre outros. Estabelecem como condição de acesso aos seus arquivos policiais que o país solicitante tenha legislação protetora da privacidade informática. A Alemanha, a França e a Áustria criaram uma lei específica para tal, enquanto que os Estados Unidos, a Argentina e a Espanha optaram por inclusão em seus Códigos Penais.

A tipificação desse tipo de delito pelas legislações de todos os países é medida urgente e que não pode esperar mais. Como afirmativa disso tivemos recentemente a invasão dos principais **sites** da rede mundial de computadores “Internet”, que sofreu ação dos chamados “hackers” ou piratas cibernéticos. Essa ação, embora não tenha chegado a atingir diretamente aos consumidores, impediu a oferta de serviços, pois tiraram os **sites** do ar. É difícil medir a dimensão de uma ação desta e de outras modalidades de ataque, como as realizadas por piratas chineses que invadiram páginas do Governo Americano para protestar contra o bombardeio da Embaixada da China em Belgrado, ou a suspensão das atividades do Lloyds em Londres ao descobrir invasão de hackers, e ainda a constatação da American Express e da Discover que vários números de seus cartões haviam sido descobertos e publicados ensejando sua substituição. Estes são exemplos recentes e é preciso que estejamos preparados para aplicar a punição de vida a este tipo de delito, desencorajando qualquer conduta incentivada por esses piratas cibernéticos, até agora de difícil identificação, mas não é, de forma alguma, tarefa impossível. Acresça-se ainda que, a tipificação desse delito, possibilitará, inclusive, a reparação de danos prevista no Direito Civil, pois é princípio fundamental do Direito Penal: “não há crime se não há lei que o defina”.

Uma questão tem sido suscitada em razão das características peculiares ao cometimento deste tipo de delito: a possibilidade de ser feito à distância, envolvendo diversos países, o que tem tido pelo qual surgem dificuldades vinculadas ao Direito Internacional, em especial no que diz respeito a quem compete investigar e punir tais ilícitos. Assim, há que se considerar sempre os princípios que determinam a jurisdição internacional para sua aplicação em nosso território.

Assim sendo, faz-se **necessária** a tipificação deste tipo de delito, bem como a sua punição, cuja penalidade deve ser estabelecida de forma a desincentivar o seu cometimento.

Procuramos tipificar cada delito, utilizando classificação similar àquela adotada pelo Código Penal Brasileiro, bem como para o critério básico de aplicação da pena, sempre sem prejuízo da punibilidade aplicável a cada caso, quando de sua utilização para cometimento de outros crimes já tipifica os pelo Código Penal.

Em razão do exposto, entendemos que este projeto ao definir como conduta delituosa determinados procedimentos até agora não tipificados no nosso Direito Penal, pretende preencher uma lacuna existente no ordenamento jurídico, colocando nosso país em igualdade com outros tantos.

Isto posto, é de suma importância contarmos com o apoio imprescindível dos nobres colegas na aprovação do presente projeto.

Sala das Sessões, 27 de março de 2000.

– Senador Renan Calheiros.

ANEXO III
PROJETO DE LEI DO SENADO Nº 137 DE 2000

PROJETO DE LEI DO SENADO Nº 137 DE 2000

Estabelece nova pena aos crimes cometidos com a utilização de meios de tecnologia de informação e telecomunicações.

O Congresso Nacional decreta:

Art. 1º Os crimes cometidos contra a pessoa, o patrimônio, a propriedade imaterial e intelectual, contra os costumes, bem como contra a criança e o adolescente, com a utilização de meios de tecnologia de informação e telecomunicações terão, levando-se em conta a culpabilidade e as conseqüências do crime, as penas até o triplo.

Art. 2º Esta lei entra em vigor na data de sua publicação.

Justificação

A evolução tecnológica tem trazido inúmeras inovações no cotidiano da sociedade. O advento da comunicação de dados, da internet e do comércio eletrônico tem a cada dia facilitado a vida de milhões de usuários de equipamentos de informática e de telecomunicações. Paradoxalmente, esses recursos tecnológicos têm propiciado e facilitado ações delituosas que vão desde a invasão de privacidade até crimes abomináveis como a divulgação de cenas de sexo explícito ou pornográfica envolvendo crianças ou adolescentes.

A sociedade tem se mostrado irredimível com a suposta imputabilidade desses agentes delituosos. Todavia, ao agente não deixa de ser imputável o resultado obtido por sua ação ou omissão. Basta a correspondência entre o fato e o tipo legal de crime.

O projeto de lei parte do princípio de que os crimes tipificados no nosso ordenamento jurídico já alcançam as ações dos usuários de meios de informática e telecomunicações, não havendo a necessidade de criação de novos tipos penais. O que se procura é rechaçar a utilização desse novo meio nas condutas criminais.

Dessa forma, o projeto dispõe que aos crimes praticados mediante a utilização de meios de tecnologia de informação e telecomunicações, as penas são

aumentadas até o triplo, levando-se em conta a culpabilidade do agente e as conseqüências produzidas. Diante da urgente necessidade de se inibir a utilização dos meios tecnológicos de informação e telecomunicações para a prática de ilícitos penais, acreditamos que a proposta, caso acatada nos moldes ora apresentada, constitua-se no instrumento capaz de inibir a sua ocorrência.

Sala das Sessões, 10 de maio de 2000 – Senador Leomar Quintanilha.