FACULDADES INTEGRADAS
"ANTÔNIO EUFRÁSIO DE TOLEDO"
FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE

CRIMES NA INTERNET: UMA REALIDADE NA SOCIEDADE DE INFORMAÇÃO

Wesley Almeida Andrade

Presidente Prudente/SP
2006

FACULDADES INTEGRADAS
"ANTÔNIO EUFRÁSIO DE TOLEDO"
FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE

CRIMES NA INTERNET: UMA REALIDADE NA SOCIEDADE DE INFORMAÇÃO

Wesley Almeida Andrade

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do Grau de Bacharel em Direito, sob orientação do Professor Jurandir José dos Santos.

Presidente Prudente/SP
2006

CRIMES NA INTERNET: UMA REALIDADE NA SOCIEDADE DE INFORMAÇÃO

Trabalho de Conclusão de Curso aprovado como requisito parcial para obtenção do Grau de Bacharel em Direito.

_____
Jurandir José dos Santos

_____
Carlos Schelini César

_____
Marcus Vinícius Feltrim Aquotti

Presidente Prudente/SP, 30 de novembro de 2006.

E digo-vos amigos meus: Não temais os que matam o corpo, e depois não têm mais que fazer. Mas eu vos mostrarei a quem deveis temer; temei aquele que, depois de matar, tem poder para lançar no inferno; sim, vos digo, a esse temei.

São Lucas, capítulo 12, versos 4-5.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ter me emprestado o dom da vida e ter permitido que eu chegasse até o presente momento, sendo superada mais uma fase de minha vida.

Aos meus pais, por terem me ensinado os grandes fundamentos dessa vida, ensinamentos que espero carregar por todo o sempre a fim de repassar para os meus filhos.

Ao Professor Jurandir José dos Santos, pessoa que com grande presteza aceitou ser meu orientador, sendo que seus ensinamentos foram essenciais para a conclusão deste humilde trabalho de conclusão de curso.

Eu não poderia deixar de agradecer ao Doutor Carlos Schelini César, Promotor de Justiça, que com muita dedicação e paciência me acolheu como seu estagiário, nunca deixando de ser uma pessoa atenciosa e preocupada com o nosso progresso na área Jurídica.

Agradeço ao Rômulo, sujeito que durante esse período de Faculdade foi sem dúvida um grande irmão para mim e que, sem dúvida, continuará sendo no decorrer dos dias.

Enfim, agradeço a todos aqueles que direta ou indiretamente contribuíram para a conclusão desse trabalho.

RESUMO

O presente trabalho pretende ilustrar as peculiaridades dos crimes praticados através da Informática e as dificuldades existentes na persecução criminal. Através de um método histórico e indutivo, procurou-se demonstrar que o avanço tecnológico propiciou um campo vasto para a atuação dos agentes denominados “hackers”, sujeitos que possuem profundo conhecimento de informática. De início, foi abordada a evolução histórica do computador e da Internet e as classificações doutrinárias referentes ao tema. O trabalho buscou discutir as questões processuais que dificultam a responsabilização dos autores dos crimes virtuais, questões essas referentes à “autoria”, “maioridade penal”, “produção de prova” e “competência em razão do lugar”. Tratou, ainda, dos crimes informáticos próprios e impróprios que representam relativa importância no âmbito da Internet. Houve discussão a respeito da falta de legislação específica e a conseqüente existência de inúmeras condutas atípicas. Sobre este aspecto, ficou demonstrada a existência de argumentos comumente utilizados pela defesa para o fim de isentar o acusado de responsabilidade. A título de comparação, foi abordada a legislação de outros países, concernente ao tema da informática e da Internet. Por fim, concluiu-se pela extrema necessidade em se obter novas leis específicas e equipamentos técnicos adequados para a investigação. Entretanto, embora o Brasil não possua legislação e estrutura técnica suficiente para a ideal responsabilização dos agentes, tudo indica que as Autoridades Policiais e Judiciárias estão com atuando com seriedade, fazendo o possível para superar as dificuldades existentes.

Palavras-chave: História do computador. História da Internet. Internet. Crimes de informática. Crimes de Internet. Direito Penal da Informática.

ABSTRACT

The present work intends to illustrate the peculiarities of the crimes practiced throughout the information tecnology and the difficulties existent in the criminal persecuttion. Throughout a historical and inductive method, it was tried to demonstrate that the technological progress propitiated a vast field for the agents'performance denominated "hackers ", persons that have deep knowledge in information tecnology. At the beginning, was approached the historical evolution of the computer and Internet, and the doctrines classifications referring to the theme. The work looked to discuss the processual questions that hinder the responsability of the virtual crimes' authors, questions that refer to "authorship", "penal majority", "proof production", and "competence in place's reason". It treated, nevertheless, about the proper and inappropriate crimes in information tecnology that represents relative importance in the Internet ambit. There was discussion regarding the lack of specific legislation and the consequent existence of countless atypical conducts. On this aspect, it was demonstrated the existence of arguments commonly used by the defense with the purpose of exempting the accused of this responsibility. In the comparison merit, the legislation of another countries was approached, regarding the theme of the information tecnology and Internet. Finally, it was concluded by the extreme need in obtaining new specific laws and technical equipments adapted for the investigation. However, although Brazil doesn't have legislation and enough technique structures for the ideal agents' responsability, everything indicates that the Police and Judiciary Authorities are acting with seriousness, making the possible to overcome the existent difficulties.

Word-key: Computer's history. Internet's history. Internet. Information tecnology's crimes. Crimes inside Internet. Penal right of the information tecnology.

SUMÁRIO

INTRODUÇÃO

O presente trabalho procurou abordar as conseqüências do avanço tecnológico no âmbito criminal, dando-se ênfase ao despreparo tecnológico das autoridades para a devida responsabilização dos agentes e à falta de legislação específica sobre o assunto.

Para uma devida abordagem do tema, foi necessário traçar alguns comentários sobre a evolução histórica do computador e da Internet. Logo em seguida, foram apresentadas algumas classificações doutrinárias envolvendo a sistemática da informática.

Superada a fase predominantemente teórica, enfocou-se de maneira concentrada as principais questões de ordem técnica, que comumente dificultam a persecução criminal, tais como a questão da dificuldade em seu identificar o autor dos delitos virtuais, da competência em razão do local, da maioridade penal e a produção de prova.

Posteriormente, o trabalho abordou os crimes mais importantes no mundo virtual, assim como algumas condutas ainda tidas como atípicas.

Por fim, foram indicadas as legislações de diversos países, pretendendo fazer uma análise comparativa com a legislação brasileira no que se refere ao tema da Informática e Internet.

Tudo isso levou à conclusão da importância do tema proposto, levando em consideração o avanço da tecnologia nos dias atuais. Contudo, o tema não vem sendo tratado com a importância que lhe é devida, fato esse cabalmente demonstrado com a carência de discussão doutrinária. Essa circunstância foi sem dúvida o maior desafio para a realização do trabalho.

1. HISTÓRICO

Ao contrário do que se imagina, o surgimento do computador não se deu nos dias atuais, existindo registro de seu aparecimento há milhares de anos. Não se pode identificar o computador como sendo somente os aparelhos eletrônicos modernos, considerando que no passado não recente, surgiu o ábaco, instrumento capaz de efetuar habilmente operações de adição e de subtração.

No decorrer dos dias, os instrumentos foram evoluindo gradativamente, chegando até os atuais e modernos computadores eletrônicos, criados no ano de 1946 para atender as necessidades militares.

Inicialmente, os computadores tinham finalidade preponderantemente matemática, utilizados pelo homem com o intuito de livrar-se de trabalhos repetitivos. Hoje, o computador exerce funções praticamente ilimitadas, propiciando ao usuário comodidade exorbitante.

Após essa pequena explanação a respeito da história do computador, é importante traçar alguns conceitos. Modernamente o conceito de computador está a compreender, invariavelmente, segundo Alexandre Pimentel (2000, p. 21), “a constituição de uma máquina eletrônica composta de elementos físicos e lógicos, capaz de efetuar, em linguagem natural, uma notável multiplicidade de tarefas unindo os pressupostos da velocidade aos da precisão operacional”.

Carla Rodrigues (2003, p. 1) conceitua o computador como sendo “um processador de dados que pode efetuar cálculos importantes, incluindo numerosas operações aritméticas e lógicas, sem a intervenção do operador humano durante a execução [...]”

Cumpre agora fazer um resumo da evolução histórica da Internet, essa sim com surgimento recente, o que não implica dizer em menor importância, quando comparado ao computador.

A Internet é definida como sendo uma grande rede de comunicação mundial, onde estão interligados milhões de computadores, sejam eles militares, comerciais, científicos ou pessoais, todos interconectados. É uma rede de redes,

que pode ser conectada por linhas telefônicas, satélites, ligações por microondas ou por fibra ótica (CARLA RODRIGUES, 2003, p. 2).

Há registros de que a Internet teria surgido no ano de 1969 como uma experiência do governo dos Estados Unidos, mais precisamente no Departamento de Defesa deste País. Tinha a finalidade de interconectar os computadores, permitindo que os pesquisadores acessassem centros de computação para compartilhar recursos de *hardware* e *software*. Dessa forma, criou-se o que se denominava Advanced Research Projects Agency (ARPA), que traduzido significa Agência de Projetos de Desenvolvimento Avançado.

É interessante o fato dessa sistemática ter sido criada com o objetivo de evitar que um ataque nuclear fosse capaz de aniquilar todas as informações contidas nos chamados *mainframes*, que armazenavam conteúdos importantes para a inteligência americana. Segundo Alfred e Emily Glossbrenner (1994) *apud* Alexandre Pimentel (2000, p. 45):

> A descentralização foi um aspecto crucial do ARPAnet desde então e, além de facilitar assuntos de defesa interligando o Pentágono, controladores de defesa e universidades de pesquisa, o ARPAnet oferecia a esperança de que pelo menos alguma parte da rede sobreviveria a um ataque nuclear. Ao explodir uma 'estrela do mar' você coloca o sistema inteiro fora do ar, mas explodindo uma rede você está meramente removendo alguns nós. A rede propriamente dita continua a funcionar.

Percebe-se que o intuito era descentralizar as informações, evitando que tudo ficasse armazenado em um único computador. E isso só se tornou possível através do ARPAnet, haja vista que a interconexão dos computadores propiciava o compartilhamento de informações.

Com o fim da Guerra Fria, a denominada rede, agora com o nome de Internet, passou a ser disponibilizada ao público em geral, surgindo a Web (Word Wide Web). A *"Word Wibe Web"* foi criada em Genebra no ano de 1988, sendo formada por hipertextos, o que facilitou a navegação.

A Internet surgiu precisamente no Brasil em 1988, com as comunidades acadêmicas de São Paulo e do Rio de Janeiro. Em 1989, O Ministério de Ciência e Tecnologia criou a Rede Nacional de Pesquisa, tendo a finalidade de

disponibilizar os serviços de acesso à Internet. Somente no ano de 1994 foi iniciada a exploração comercial da Internet neste País.

Existe no Brasil um Órgão responsável pela administração da Internet. Este Órgão denomina-se Comitê Gestor de Internet, criado para fomentar o desenvolvimento de serviços na Internet, recomendar padrões e procedimentos técnicos e operacionais para a Internet, coordenar a atribuição de endereços na Internet, o registro de nomes de domínios, a interconexão de espinhas dorsais e, por fim, coletar, organizar e disseminar informações sobre os serviços da Internet.

Feita essa introdução histórica, resta dizer que o avanço da tecnologia no âmbito da informática influenciou a relação entre todas as pessoas no mundo inteiro. Ninguém dúvida que o computador e a Internet transformaram a vida moderna, podendo ser dito que o ser humano de hoje vive a “Era da Informática”.

2. CLASSIFICAÇÃO

Antes de adentrarmos ao estudo dos crimes e suas peculiaridades, é de suma importância a referência de algumas classificações que guardam estreita relação com o tema aqui discutido.

Aliás, percebe-se que a doutrina não é unânime quanto à classificação, existindo inúmeras denominações para cada espécie, embora o conteúdo seja idêntico. Por não existir um critério rígido, a classificação exposta a seguir está baseada no grau de importância, isto é, naquilo que realmente interessa.

2.1. Direito de Informática e informática Jurídica

Cumpre ressaltar, primeiramente, que o significado dos dois termos não se assemelha. Trata-se de dois institutos diversos, cada qual com seu objeto de atuação.

Os doutrinadores procuraram conceituar "informática jurídica" levando em consideração as diversas espécies do aludido instituto. Alexandre Freire Pimentel (2000, p. 144) subdividiu a *infomática jurídica*: de gestão ou operacional, de registros ou documental, de decisão ou metadocumental, e, por fim, de ajuda à decisão.

Contudo, procurando não se estender demasiadamente com essa classificação, será mencionada apenas a essência e a finalidade da denominada "informática jurídica".

É comumente discutida a morosidade do Poder Judiciário no Brasil. Isto se dá em razão da desproporção existente entre o número dos processos e a quantidade de servidores do Judiciário e magistrados. Grosso modo, o número existente de Juízes, Desembargadores, servidores, e etc., é insuficiente em relação à quantidade de processos que deverão ser apreciados pelo Poder Judiciário.

Para amenizar essa situação, os operadores do direito passaram a utilizar a informática como um instrumento de trabalho, o que sem dúvida lhes proporcionaram uma maior comodidade. A própria sistemática dos Tribunais se adequou à era da informática. É a informática a serviço do direito, que se traduz em “avanços tecnológicos tendentes à automação das tarefas rotineiras da vida prática do direito, verificadas em qualquer ambiente jurídico como tribunais, juízos, escritórios, etc.” (Pimentel, 2000, p. 145).

Com efeito, a Informática Jurídica seria a ciência que estuda a aplicação dos princípios informáticos no âmbito do direito. Nas palavras de Perez Luño (1996) *apud* Pimentel (2000, p. 144):

> [...] a informática jurídica é uma disciplina bifronte, na qual se entrecruzam uma metodologia tecnológica com seu objeto jurídico, que por sua vez, condiciona as próprias possibilidades ou modalidades da aplicação dos recursos tecnológicos ao direito.

Direito de informática seria um ramo especializado do direito, assim como o Direito Penal, Direito Civil, e entre outros. Tem como objeto a tecnologia informática.

Os autores o classificam com um direito interdisciplinar, pois é aplicado em conjunto com outros ramos do direito.

É um direito especializado, levando em consideração o seu objeto de atuação. E, por fim, é universal, pois está presente em todos os países que utilizam a tecnologia computacional.

Discute-se muito se o direito de informática se caracteriza como ramo do direito privado ou público, tema que não tem relevância para o presente trabalho.

Não se discute que o Direito Informático tem significativa importância na esfera jurídica, embora não seja tratado com o destaque que merece. Com o aumento da influência da informática na vida das pessoas, da Internet mais precisamente, os operadores do direito terão que se especializar no Direito Informático, pois conforme será visto a seguir, é uma área com suas peculiaridades e complicações.

2.2. Classificação dos crimes de informática

Os crimes de informática são classificados como próprios e impróprios. Os primeiros são aqueles que só podem ser praticados através da informática. São os típicos crimes do mundo virtual, tendo em vista que existem única e exclusivamente em razão da informática (Carla Rodrigues, 2003, p. 10).

São esses crimes os que causam maiores problemas para os usuários do computador e operadores do direito, pois a grande parcela dos fatos são considerados atípicos. No máximo, as condutas dos chamados *hackers* se enquadram em um tipo penal comum. Exemplos: violação de e-mail, pirataria de *software* e vandalismo na rede.

Os impróprios são aqueles crimes que podem ser praticados de qualquer forma. O agente utiliza a informática para praticar um crime, mas dispunha de outros meios para atingir o fim criminoso. Não deixam de ter importância, mas quase sempre são punidos adequadamente de acordo com a legislação comum. Exemplos: furto, pedofilia, calúnia e estelionato.

Vários outros autores definem outras classificações, que no conteúdo não se diferem da que foi apresentada. De acordo com Marco Aurélio Rodrigues da Costa (1995) *apud* Carla Rodrigues (2003, p. 11), os crimes são divididos em crimes de informática puros, crimes de informática misto e crime de informática comum.

Para o citado autor, os crimes de informática puros seriam aqueles que atingem especificadamente o sistema de informática. Os mistos se consubstanciam nas condutas que lesão bens jurídicos diversos da área da informática, mas para que o fim seja alcançado, é necessário utilizar o sistema de informática. Por fim, os crimes de informática comum são aqueles que podem ser praticados com qualquer meio, inclusive o sistema de informática.

3. A PROBLEMÁTICA DA CRIMINALIDADE ATRAVÉS DA INTERNET

O presente capítulo visa discutir as peculiaridades dos crimes praticados por intermédio da Internet. Serão discutidos os aspectos processuais relacionados com a autoria, a maioridade penal, a competência em razão do lugar e da produção de provas.

3.1 O problema da autoria

A identificação dos autores dos *cyber crimes* é um dos grandes desafios para as autoridades na *persecutio criminis*. Essa realidade não é restrita apenas no Brasil, mas em todos os países onde a tecnologia está presente.

Um sujeito que se encontra na cidade de Porto Alegre/RS, por exemplo, pode enviar um e-mail com vírus para um computador localizado na cidade de Manaus. Caso o vírus cause danos significativos no aludido computador, presume-se que o seu proprietário irá a uma Delegacia de Polícia para noticiar esse fato. A partir daí é que se inicia a dificuldade, pois sem meios tecnológicos, não saberá sequer de onde partiu o e-mail contendo vírus.

O exemplo proposto é apenas uma ilustração da difícil missão de se identificar os autores desses crimes.

Através de um recurso denominado *Internet Protocol,* é possível identificar o computador que deu origem ao comando criminoso. Contudo, isso não é suficiente para resolver o problema.

A começar pela característica dos agentes que praticam os crimes desse gênero. Geralmente, esses indivíduos possuem elevado conhecimento a respeito da informática e, por tal motivo, procuram agir sem levantar suspeitas.

Somente a título de exemplo, os *hackers* costumam utilizar celulares clonados para ter acesso à Internet, inviabilizando a identificação do local da chamada e de seu autor, mediante rastreamento de sinal (Vladimir, 2002).

Além disso, esses agentes comumente praticam crimes em lugares públicos, isto é, lugares onde o acesso ao computador é destinado a um grande número de pessoas. Não adiantaria identificar o computador nestes casos, pois inúmeros são os seus usuários. É o que ocorre, por exemplo, nos denominados *"Cyber Café's"*.

Com efeito, não se dúvida que a identificação dos autores dos crimes cibernéticos é um grande desafio para as autoridades responsáveis pela investigação. Contudo, tudo indica que esses problemas serão minimizados ou até mesmo solucionados futuramente. No Brasil, já é possível verificar alguns avanços, no sentido de existirem Delegacias e Promotorias especializadas nesta seara de crimes.

Não raramente surgem notícias de casos envolvendo crimes praticados através da Internet, onde os componentes das quadrilhas especializadas nesses crimes são identificados. Uma atitude que vem sendo utilizada é a quebra de sigilo bancário dos suspeitos, prática eficaz nos crimes que envolvem questão patrimonial.

A tendência é que surjam instrumentos tecnológicos capazes de identificar os usuários, mesmo se estiverem em lugares públicos. Técnicas biológicas, como a impressão digital, a análise de pupila, ou até mesmo o uso de assinaturas digitais, criptografia por chaves assimétricas, etc., poderão ser utilizadas no combate à impunidade. De acordo com Vladimir Aras (2002):

> [...] O único método realmente seguro de atribuição de autoria em crimes informáticos é o que se funda no exame da atuação do responsável penal, quando este se tenha valido de elementos corporais para obter acesso a redes ou computadores. Há mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. As formas mais comuns são a análise do fundo do olho do usuário ou a leitura eletrônica de impressão digital, ou, ainda, a análise da voz do usuário.

O citado autor complementa dizendo:

> [...] Como dito, somente os mecanismos de assinatura eletrônica e certificação digital e de análise biométrica podem conferir algum grau de

> certeza quanto à autoria da mensagem, da informação, ou da transmissão, se considerado o problema no prisma penal.

Apesar de todos os problemas, a sociedade é esperançosa no sentido de surgirem novos mecanismos para o combate dos crimes informáticos. Mesmo sem os precisos mecanismos, os operadores do direito continuarão lutando em busca da solução dos inúmeros problemas, apesar das “incontáveis dificuldades”.

3.2 O problema da maioridade penal

Inicialmente, é importante ser ressaltado que o presente trabalho não visa defender a necessidade da redução da maioridade penal. O fim precípuo é expor as circunstâncias e conseqüências dos atos infracionais praticados pelos menores.

É sabido que o microcomputador está presente em parcela razoável nas casas brasileiras. Se não está nas residências, o computador pode ser encontrado nas escolas, nas lanchonetes, nos *Cyber's*, etc. Diante disto, pode ser afirmado que a criança e o adolescente não encontram grandes dificuldades para ter acesso ao computador e, conseqüentemente, à Internet.

Levando isso em consideração, não é forçoso concluir que o adolescente pode facilmente ser autor de atos infracionais praticados através da internet. Caso isto ocorra, e tendo indícios que o adolescente foi o autor, deverá ser instaurado procedimento apuratório para eventual aplicação de medida sócio-educativa. Tudo isso em consonância com o Estatuto da Criança e do Adolescente. Quando o infrator é criança, ou seja, pessoa menor de 12 anos, será aplicado as regras do artigo 101, do ECA.

Contudo, em se tratando de atos infracionais praticados pela Internet, cada caso deverá ser analisado de acordo com as suas particularidades. Em algumas hipóteses deverá ser levada em consideração a personalidade do adolescente, as circunstâncias do fato, bem como suas conseqüências.

Como bem advertido por Carla Rodrigues (2003, p. 134), o mesmo tratamento não pode ser dado ao menor que subtrai uma bolsa de outrem e ao

que publica fotos de crianças e adolescentes para satisfazer sua curiosidade e de seus amigos da mesma idade. No primeiro caso, o menor sabe o que está fazendo e tem a vontade de provocar o resultado. Conforme exposto, tudo dependerá do caso concreto.

Regra geral, os menores infratores terão tratamento adequado ao fato por ele cometido. Nos casos em que causar dano a outrem deverá ser compelido a reparar o dano.

Segundo Milano Filho *apud* Carla Rodrigues (2003, p. 135):

> [...] estas medidas implicam em responsabilização com conscientização do adolescente infrator, com reflexos de natureza civil, tornando necessária a instauração de processo contraditório, apurando-se o ato infracional e, na medida do possível, os prejuízos a serem recompostos.

Em decorrência da dificuldade existente para se apurar os autores desses crimes, os menores poderão ser responsabilizados por atos infracionais que não cometeram. Isso acontece quando um agente imputável pratica o ilícito penal, mas ao ser descoberto, atribui os fatos ao adolescente ou menor.

Imagine um sujeito portador de maus antecedentes, reincidente, que com o uso do computador subtrai milhões de reais de diversas contas bancárias. Caso ele seja descoberto, poderá cumprir pena em regime fechado por vários anos, além do dever de reparar o dano causado.

Nesta mesma situação, o aludido sujeito poderá conluiar com um adolescente, dizendo para ele se responsabilizar pelo furto. Se o adolescente nunca se envolveu em outro ato infracional, dificilmente será imposta a medida sócio-educativa de internação e, dependendo do caso, a reparação do dano será muito mais difícil. Percebe-se que as conseqüências para o sujeito maior são mais rígidas quando comparadas às medidas socioeducativas.

É evidente que as autoridades terão que utilizar os meios adequados (indicados no item anterior) para se chegar aos reais responsáveis pelos crimes, punindo também os menores que tiveram participação. Infelizmente isso não ocorrerá na maioria das vezes, o que ocasionará a absolvição dos agentes, sejam eles imputáveis ou inimputáveis.

3.3 O problema da produção de prova

Ao tomar ciência de um crime, a Autoridade Policial deverá instaurar o inquérito policial com o fim de colher elementos para eventual propositura de ação penal. Iniciado o processo, o acusado será interrogado, serão ouvidas as testemunhas e, no final, o Magistrado proferirá sentença, fundamentando-se no contexto probatório existente.

Obedecendo ao princípio do *in dúbio pro reo,* o Juiz somente condenará se o contexto probatório indicar de forma satisfatória que o acusado foi o autor do crime. Caso contrário, ou seja, caso as provas colhidas durante a investigação e a instrução sejam frágeis, o Juiz decidirá favoravelmente ao réu, absolvendo-o com fundamento no inciso VI, do artigo 386, do Código de Processo Penal.

Com efeito, é fácil concluir que a investigação nos crimes praticados através da Internet deverá ser especializada, sustentada em meios tecnológicos precisos.

Sabe-se que os internautas criminosos são pessoas capacitadas, especialistas no meio tecnológico. Por certo, eles procuram atuar sem deixar vestígios, visando evidentemente não serem identificados. Em razão disso, os responsáveis pela investigação terão muitas dificuldades para encontrar indícios que conduzam à autoria. Diga-se “dificuldade para indicar a autoria”, tendo em vista que a materialidade na maioria dos casos estará comprovada.

Para dificultar, a grande maioria dos Delegados de Polícia, membros do Ministério Público e até mesmo dos Magistrados não têm conhecimento tecnológico suficiente, sendo dependentes dos pareceres dos peritos.

Reiterando o que foi dito no subcapítulo referente à autoria, o avanço tecnológico será fundamental para solucionar os crimes cibernéticos, propiciando um contexto probatório suficiente para o decreto condenatório. Caso contrário, valerá aquela máxima onde “é melhor absolver um culpado do que condenar um inocente”.

3.4 O problema da competência em razão do lugar

Antes de ser discutida a questão da competência, é necessário fazer uma breve consideração a respeito do lugar do crime.

Como bem asseverado pelo doutrinador Damásio (2003, p. 129), o Código Penal Brasileiro, em seu artigo 6º, adotou a teoria da ubiqüidade, que indica como lugar do crime "aquele em que se realizou qualquer dos momentos do *iter*, seja da prática dos atos executórios, seja da consumação".

Para ilustrar aludida teoria, Damásio cita um exemplo: "na fronteira Brasil-Bolívia um cidadão brasileiro, que se encontra em território nacional, atira em outro, em solo boliviano, vindo este a falecer". Pela teoria da ubiqüidade, considera-se praticado o crime tanto no Brasil quanto na Bolívia.

Nas palavras de Hungria (1977) *apud* Damásio (2003, p. 129), "imprescindível é que o crime haja tocado o território nacional".

Além disso, existem as regras da extraterritorialidade, previstas no artigo 5º do Código Penal, casos onde a lei brasileira deverá ser aplicada.

Após essa breve explanação a respeito do "lugar do crime", passará a ser discutido o tema referente à competência.

É fato que uma pessoa pode se interligar no mundo todo através da Internet, necessitando apenas de um microcomputador, uma linha telefônica e um provedor de Internet. Devido a esse caráter internacional da rede, os juristas encontram grandes problemas ao se trabalhar com o conceito de jurisdição e territorialidade na Internet.

Como bem entendido por Celso Valin (1978) *apud* Vladimir Aras (2002), na Internet não existem fronteiras e, portanto, algo que nela esteja publicado estará em todo o mundo. Como, então, determinar o juízo competente para analisar um caso referente a um crime ocorrido na rede?

É induvidoso que o autor Celso Valin quis se referir a determinados grupos de crimes, como por exemplo, os crimes praticados contra a honra. Uma

declaração caluniosa publicada na rede poderá ser lida por todos aqueles que acessarem a rede mundial de computadores. Qual seria o foro da culpa?

Como era de se esperar, os doutrinadores não são unânimes quanto a essa matéria.

No ponto de vista de Carla Rodrigues (2003, p. 107), a competência deverá ser determinada de acordo com o artigo 70, do Código de Processo Penal, que dispõe o seguinte: “A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução”.

Para a aplicação desse artigo, Carla Rodrigues ressalta que é de suma importância a identificação do lugar da infração, situação não muito fácil de acontecer nos crimes praticados através da Internet.

Quando não for possível identificar o lugar da infração, deverá ser aplicada a regra subsidiária de fixação de competência, regra essa prevista no artigo 72, do Código de Processo Penal. Dessa forma, “não sendo conhecido o lugar da infração, a competência regular-se-á pelo domicílio ou residência do réu”. Caso o réu tenha mais de uma residência, a competência será determinada pela prevenção. Por fim, se o réu não tiver residência ou for ignorado seu paradeiro, será competente o Juízo que primeiro tomar conhecimento do fato.

Percebe-se que a respeitável autora não apresentou soluções para o caso da infração se consumar se em várias localidades, situações que ensejariam conflito de competência.

Vladimir Aras (2002), por sua vez, defende a aplicação, por equiparação, da Lei n. 5.250/67 (Lei de Imprensa), que através do artigo 42, considera competente para o processo e julgamento o foro do local onde for impresso o jornal.

> Artigo 42: Lugar do delito, para a determinação da competência territorial, será aquele em que for impresso o jornal ou periódico, e do local do estúdio do permissionário ou concessionário do serviço de radiodifusão, bem como o da administração principal da agência noticiosa.

De acordo com este entendimento, o provedor de acesso à Internet seria equiparado à empresa jornalística. Dessa forma, estariam resolvidos os conflitos de competência que eventualmente surgiriam.

Com efeito, para efeito de competência, seria considerado como local do fato aquele onde estiver hospedado o *site* com conteúdo ofensivo.

Como alternativa a essa solução, Vladimir sugere a aplicação do artigo 72 do Código de Processo Penal, naqueles casos em que não for conhecido o lugar da infração. Nas hipóteses dos "crimes a distância", poderá ser utilizado a regra prescrita no artigo 6º, do Código Penal, já tratado acima.

Por fim, ele termina seu raciocínio defendendo a aplicação do artigo 70, do Código de Processo Penal, nos crimes plurilocais, atentando-se para a teoria do resultado. Além disso, devem ser respeitadas regras da extraterritorialidade e a competência da Justiça Federal para processar e julgar crimes previstos em Tratados ou Convenções.

Como se percebe, há uma grande variedade de soluções para a firmação de competência. O que não se pode deixar de lado é o fim principal do processo, que é o de solucionar o conflito de interesses da forma mais justa. E tal fim só será atingido se a "verdade real" for realmente encontrada. Para que isso ocorra, o Juízo competente deverá ser fixado de acordo com a comodidade processual, devendo evidentemente ser observado as normas processuais.

4. DOS CRIMES EM ESPÉCIE

A partir deste capítulo, passaremos a estudar os crimes que representam maior relevância no contexto “virtual”. Inicialmente, é importante ser ressaltado que o estudo será restrito aos aspectos referentes à Internet, não sendo viável traçar uma classificação doutrinária profunda.

É claro que nos crimes informáticos impróprios não há muito a inovar, utilizando-se geralmente as lições apresentadas pela doutrina comum.

Será dado enfoque às peculiaridades e conseqüências dos crimes cometidos através da informática. Como será visto, não só os crimes próprios de informática representam importância, mas também os que são praticados por outros meios que não seja o virtual.

4.1 Dos crimes contra a honra

Os crimes contra a honra estão previstos nos artigos 138 ao 141, do Código Penal. Segundo Damásio (2003, p. 201), tais tipos penais visam proteger a honra, que consiste em “conjunto de atributos morais, físicos, intelectuais e demais dotes do cidadão, que o fazem merecedor de apreço no convívio social”.

Os crimes contra a honra são elencados em calúnia, difamação e injúria. O crime de calúnia ocorre quando o sujeito atribui falsamente a terceiro a prática de delito. Já o crime de difamação consiste na imputação de fato ofensivo à reputação da vítima.

Esses dois delitos incidem sobre a honra objetiva da vítima, ou seja, estão relacionadas com a reputação da pessoa atingida pela ofensa. Essa circunstância será fundamental para a configuração desses crimes quando praticados através da Internet.

Por fim, injúria consiste na ofensa à honra-dignidade ou à honra-decoro da vítima, onde o sujeito atribui à alguém qualidade negativa. Diferentemente da

calúnia e da difamação, a injúria ofende a honra subjetiva, consubstanciada na honra-dignidade e honra-decoro (Damásio, 2003, p. 202).

Esses conceitos básicos são essenciais para o estudo dos crimes contra a honra praticados por intermédio da Internet.

No âmbito virtual, os delitos ofensivos à honra costumam ocorrer durante conversas instantâneas em salas de "bate-papo", na criação de *homepages* e no envio de *e-mails*. É comum a utilização de um programa denominado "*messenger",* que propicia conversa instantânea entre diversas pessoas.

Através destes instrumentos de comunicação, uma pessoa pode perfeitamente proferir ofensas. Dependendo da espécie do crime e das circunstâncias, o crime atingirá sua consumação ou não.

Como bem asseverado por Carla Rodrigues (2003, p. 16), os crimes de calúnia e difamação se consumam se terceira pessoa tomar conhecimento do fato. Isto é explicado pelo fato dos aludidos crimes atingirem a honra objetiva. Caso somente a vítima tome conhecimento dos fatos imputados pelo autor, a sua reputação não será prejudicada.

É a hipótese da pessoa que recebe um e-mail contendo ofensas, mas acaba deletando após a sua leitura. Se as ofensas estiverem relacionadas à honra objetiva, o crime não se consumou.

Por outro lado, as ofensas poderão ser proferidas em salas de bate-papo, onde diversos usuários presenciaram os fatos. Neste caso, a reputação da vítima foi lesionada, consumando-se o delito.

No crime de injúria, não interessa para sua configuração se terceiras pessoas tomaram conhecimento do fato, tendo em vista que neste caso se protege a honra subjetiva da vítima, isto é, os atributos morais, físicos e intelectuais do cidadão.

Na visão de Carla Rodrigues (2003, p. 17):

> No crime de injúria, o agente não imputa à vítima a prática de um fato, como na calúnia e na difamação, mas sim uma característica, qualidade, enfim, o conceito que o agente tem sobre a vítima. Exemplo: Tiago diz que Renata é preguiçosa e malandra.

E são esses os motivos da diferenciação. Não importa se alguém presenciou os fatos, pois a vítima foi ofendida internamente.

É cediço que a Internet é utilizada atualmente com o fim de informação, função correspondente aos jornais e revistas. São os denominados portais de informação.

Não se duvida também que as informações veiculadas por tais portais possam conter conteúdos ofensivos a honra de determinadas pessoas. Nestes casos, conforme ensina a doutrina, deverá ser aplicado a legislação atinente à imprensa.

Os artigos 20, 21 e 22, da Lei n. 5.250/67, tipificam os crimes de calúnia, difamação e injúria, praticados através de jornais, publicações periódicas, serviços de radiodifusão e noticiosos.

Nas lições de Márcio Coimbra *apud* Carla Rodrigues (2003, p. 18):

> Além dos periódicos veiculados na Internet, algumas outras empresas passaram a divulgar informações de caráter jornalístico na rede. Aí se encontram os portais de informações. Esses endereços são grandes centros de informação na rede, e seu conteúdo é geralmente produzido por jornalistas e contam com respaldo de grandes empresas de comunicação... a divulgação de fatos pela Internet da forma noticiosa é simplesmente uma evolução, uma nova forma de transmitir as informações para as pessoas... Portanto, as leis e princípios atinentes às empresas de comunicação e mídia tradicionais são plenamente aplicáveis às empresas de comunicação via Internet.

Em se tratando de crime de imprensa, será competente o Juízo do local onde se encontra a sede da empresa responsável pela divulgação, podendo ser a empresa construtora do *site* ou a que presta manutenção (Carla Rodrigues, 2003, p. 19).

Outro aspecto que representa relevância concernente aos crimes contra a honra é a utilização do site de relacionamentos “Orkut”. Quem utiliza o “Orkut”, percebe a existência de milhares de comunidades tratando dos mais variados assuntos.

As referidas comunidades indicam na maioria das vezes gostos e preferências, que de certa forma não apresentam qualquer potencialidade delitiva.

O que tem chamado a atenção das autoridades é a existência de comunidades relacionadas ao aspecto racial, isto é, comunidades de pessoas que manifestam o menosprezo por determinada raça, sejam elas relacionadas à religião, cor, etc.

Conforme bem preceitua Carolina de Aguiar (2006), tudo que uma pessoa escreve no Orkut poderá ser utilizado contra a sua pessoa. Dessa forma, todos aqueles que fazem parte dessas comunidades racistas poderão ser responsabilizados pela prática dos crimes previstos nos artigos 138 e sequintes, do Código Penal.

É evidente que estamos diante de crime cuja ação penal somente se inicia mediante a propositura de queixa-crime. Aquela pessoa que se sentir ofendida com as ofensas praticadas no *site* relacionamento, poderá intentar ação penal.

Não se deve deixar de lado as peculiaridades desses crimes praticados através da Internet. Embora se saiba que uma mensagem partiu de um usuário, não significa que foi ele o emitente. Só para lembrar, uma pessoa estranha pode facilmente utilizar uma conta ou um e-mail de outra pessoa.

Além dessas ofensas racistas, o "*Orkut"* vem sendo utilizado para ofender a honra de artistas e, evidentemente, de pessoas comuns. Em relação à ofensa aos artistas, vejamos o tratamento já dado pela Justiça (Carolina de Aguiar, 2006):

> Os membros da comunidade, então, começaram a espelhar mensagens de ofensa à honra da artista, o que fez com que Neusa ... entrasse com pedido formal na Justiça, fundamentado na Lei de Direitos Autorais. Assim decidiu liminarmente o Juiz Rodrigo de Silveira Cardoso pela retirada dos desenhos do Orkut. A multa imposta ao *website* pelo descumprimento da decisão foi de R$ 500,00 por dia.

Essa decisão serve para ilustrar que em muitos casos os administradores do site de relacionamento "*Orkut"* são responsabilizados por alguns atos. E a tendência é que isso aconteça.

Conforme se verifica, já é possível ter uma idéia dos problemas que a Internet pode causar a uma pessoa.

Por fim, concernente às provas e competência, aplica-se as regras já debatidas.

4.2 Furto

O crime de furto está previsto no artigo 155, e seus parágrafos, do Código Penal, sendo que a sua forma simples consiste em “subtrair, para si ou para outrem, coisa alheia móvel”.

Tal figura delitiva é classificada como crime de informática impróprio, pois pode ser praticado por outros meios alheios à informática.

Costuma-se fazer uma distinção entre crime de informática praticado contra o sistema de informática ou através deste. Quando o agente furta o computador ou um de seus acessórios, o crime é contra o sistema de informática. Exemplo: furto de um disquete. Por outro lado, se o agente utiliza o computador para praticar a subtração, ele utiliza a informática como instrumento do crime. São os casos de subtração de valores de conta bancária (Carla Rodrigues, 2003, p. 26).

É evidente que esta diferenciação não traz importância prática, tendo em vista que tanto um quanto outro tem enquadramento fático no artigo 155, do Código Penal. O que mais interessa para o tema aqui proposto são os crimes praticados através da Internet.

A subtração de valores de contas bancárias praticados através da Internet tem preocupado as Instituições Financeiras de todo o Mundo, fazendo com que eles invistam cada vez mais em tecnologia.

Quase não se vê notícias desses furtos em Instituições Bancárias, o que não significa inocorrência desses fatos. Como bem exposto por Carla Rodrigues (2003, p. 26), os Bancos não costumam divulgar os furtos em contas correntes de seus clientes, pois preferem arcar com o prejuízo a tornar pública a vulnerabilidade de seu sistema tecnológico.

Para praticarem o crime, os agentes violam o sistema de informática de um Banco e transferem valores para suas contas-correntes. É comum de ocorrer também a hipótese do agente conseguir a senha do correntista, através de *spans* ou e-mails, e invadir a própria conta bancária dela, subtraindo valores.

Ao praticar subtração de valores de uma conta corrente através da Internet, o sujeito incorrerá nos preceitos do artigo 155, do Código Penal, conforme o entendimento de Alexandre Jean (2001):

> [...] a inovação está no *modus operandi*. O resultado alcançado com a conduta independe da abrangência jurídica atribuída a *res* ... O dinheiro rapinado de uma conta corrente via Internet é furto como outro qualquer, diferenciando-se apenas quanto a maneira e quanto ao agente que pratica o delito.

Discute-se a aplicação dos parágrafos do artigo 155, do Código Penal, nesses casos. Como regra geral, o que não for incompatível será aplicado nos furtos cometidos através da Internet.

A causa de aumento de pena prevista no § 1º, do artigo 155, do Código Penal, não tem aplicação, eis que o fundamento da qualificadora reside na circunstância da maior facilidade que pode ter o sujeito quando pratica o furto em altas horas da noite (Damásio, 2003, p. 314). Ora, tanto faz para o *hacker* agir durante o período diurno ou noturno, pois a dificuldade será a mesma.

De outro lado, nada impede que o privilégio do § 2º, do artigo supra seja aplicado, desde que o criminoso seja primário e o valor da coisa furtada seja de pequeno valor (Carla, 2003, p. 26).

Em relação às qualificadoras do § 4º, é facilmente perceptível que os incisos I (destruição ou rompimento de obstáculo) e III (emprego de chave falsa) não terão relevância para os *cybercrimes*. Nada impede que a qualificadora relativa ao abuso de confiança e mediante fraude tenha aplicabilidade (Carla, 2003, p. 26). Exclui-se a qualificadora referente à escalada e destreza.

Por fim, dois agentes podem agir em conluio para praticar subtrações em contas bancárias por intermédio da informática. Estaria caracterizada a qualificadora de concurso de agentes.

É importante ser ressaltado que as discussões acima se referem apenas aos furtos cometidos por internautas com o uso do computador. Concernente aos crimes contra o sistema de informática, em nada se difere dos casos comuns.

4.3 Estelionato

É estranho imaginar que o estelionato pode ser praticado através da Internet. Quando se fala em estelionato, imagina-se um sujeito que tem enorme facilidade em persuadir uma pessoa através da conversa pessoal, induzindo ou mantendo-a em erro com uso de meio fraudulento.

Ao contrário do que se pensa, essa figura delitiva pode ocorrer perfeitamente no mundo da informática. Segundo Guilherme Guimarães (2001, p. 75), "a conduta consiste em o sujeito ativo empregar o meio informático para induzir ou manter a vítima em erro, obtendo com isso a vantagem ilícita para si ou para outrem".

Apresentando correlação com a conversa pessoal, os agentes utilizam salas de bate papo, *homepages* e até mesmo os e-mails para ludibriar a vítima.

A fraude, segundo Eduardo Valadares de Brito *apud* Carla Rodrigues (2003, 32), costuma ocorrer:

> [...]quando o indivíduo ao comprar, vender ou investir via Internet é enganado de alguma forma. O vendedor pode descrever produtos ou serviços de maneira enganosa ou pode, ainda, receber o pedido e o dinheiro, mas não entregar o bem o qual estava obrigado.

Obedecendo a tipificação legal, o agente pode empregar artifício, ardil ou qualquer outro meio fraudulento. Para Damásio (2003, p. 436), "artifício é o engodo empregado por intermédio de aparato material, encenação", enquanto que "ardil é o engano praticado por intermédio de insídia, como a mentirosa qualificação profissional". No final, o preceito normativo utiliza uma fórmula genérica, onde estará caracterizado o crime de estelionato quando o agente utiliza qualquer meio fraudulento capaz de induzir ou manter uma pessoa em erro.

Aplica-se aqui o que foi falado no crime de furto concernente a aplicação dos parágrafos e incisos do artigo 171, do Código Penal. Tudo aquilo que não for incompatível se aplica aos estelionatos aplicados por intermédio da Internet.

No campo prático, os criminosos possuem um campo vasto para atuar. Aumenta-se a cada dia os negócios realizados pelo meio virtual, o que facilita a atuação dos estelionatários.

O despreparo técnico dos usuários e até mesmo a fragilidade dos sistemas tecnológicos utilizados pelas empresas que comercializam na rede, são as grandes responsáveis pela ocorrência de fraudes na Internet.

4.4 Inserção de dados falsos em Sistema de Informações e Modificação ou Alteração não autorizada de Sistema de Informações

Trata-se de dois tipos penais inseridos no Código Penal através da Lei nº 9.983/00, caracterizando-se como crimes praticados por funcionário público contra a Administração Pública.

Vejamos as redações dos dois artigos:

> Artigo 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou banco 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. Modificar ou alterar, o funcionário, sistema de informações ou programas de informática sem autorização ou solicitação da autoridade competente.
>
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.
>
> Parágrafo único: As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

É perfeitamente perceptível que os referidos tipos penais visam tutelar a probidade da Administração Pública e o sistema de informação por ele utilizado.

Conforme o entendimento de Guilherme Guimarães (2001, p. 104), os crimes definidos nos artigos 313-A e 313-B são próprios, tendo em vista que são praticados necessariamente por funcionário público. Refere-se também a crimes "informáticos próprios", eis que somente podem ser praticados por intermédio da informática.

Guilherme Guimarães (2001, p. 105) define com precisão a forma de atuação dos agentes:

> Em ambos os casos, o sujeito manipula o objeto tecnológico informático ("sistema informatizado", "banco de dados", "sistema de informações", "programa de informática"), sendo tais os objetos sobre os quais incidem as condutas puníveis, assumem foros de objeto material dos delitos, com razoável ineditismo, pela nota da exclusividade típica (o tipo não rende ensanchas à compreensão de outros objetos materiais que não o informático).

Como se pode verificar, os crimes aqui discutidos são profundamente relacionados à informática, sendo que as suas tipificações são compostas por vários termos técnicos. Isso significa que o Magistrado, ao decidir, poderá pedir auxílio a um perito especialista no campo da informática a fim de descrever o "modus operandi" e as conseqüências materiais dos crimes.

É significativa a inovação trazida pelos dois dispositivos tratando de crimes informáticos, embora se saiba que os fatos estão restringidos à Administração Pública.

4.5 Envio de Vírus ou Similares

O envio de vírus ou similares caracteriza-se como sendo uma conduta tipicamente ligada ao meio informático e, como tal, é classificado como crime próprio de informática.

Por óbvio, o vírus só poderá ser enviado através do meio informático, sendo inadmissível situação diversa.

De acordo com a conceituação oferecida por Guilherme Guimarães (2001, p. 73), vírus é o "programa que se reproduz ao entrar em contato com outros programas e contamina arquivos de computador". Em outra definição trazida pelo aludido doutrinador, vírus significa "programa desenvolvido para destruir outros programas. O objetivo dos vírus de computador é prejudicar o funcionamento normal do computador".

Desde que se tem notícias da existência dos vírus, várias espécies foram surgindo, apresentando cada qual a sua característica própria. São classificados em vírus de programa, vírus de "boot" e vírus de macro (Guilherme Guimarães, 2001, p. 73).

Os "vírus de programa" são aqueles que infestam afetam arquivos de programa, que são os de extensões .COM, .EXE, .SYS, .DLL, .OVL ou .SCR. Os denominados "vírus de *boot*" contaminam as *nonfile áreas* do disco rígido e de disquetes, que consistem em espaços não ocupados por arquivos. Essa espécie é bastante eficaz, pois propicia de forma eficiente a disseminação de vírus de máquina para máquina. Por fim, os "vírus de macro" são aqueles que afetam os arquivos-documento do tipo ".DOC" e ".DOT". Esses vírus contêm um conjunto de instruções para realizar comandos sob nome abreviado. A título de exemplo, tais espécies são usadas para afetar os programas "Word" e o "Excel", que acabam sendo afetados a partir de documentos infectados compartilhados em rede ou baixados a partir de *sites* da Internet (Guilherme Feliciano, 2001, p. 73).

Os vírus costumam atuar de forma que prejudique o normal processamento do computador, ou até mesmo destruindo o funcionamento em sua integralidade. Neste último caso, não significa que o computador passa a não existir mais, mas torna irrecuperáveis os arquivos e programas afetados. Caso todos os arquivos e programas sejam atingidos, o computador não terá mais utilidade prática.

Referente ao tema, Francisco de Assis Rodrigues (2003), manifestou da seguinte forma:

> Trata-se aqui de hipóteses nas quais a pessoa já possui acesso autorizado ao sistema e dolosamente o danifica ou ainda de *hackers* que invadem o sistema e depois o danifica. Cabe nesta conduta a ação dos vírus de computador, que danificam arquivos essenciais ao sistema. Essas condutas afetam diretamente a integridade do sistema, fazendo-o funcionar de forma indevida ou ainda levando-o à total perda.

O envio de vírus ou similares pode ser praticado à distância, com o uso da Internet, ou com a ação direta e pessoal do agente sobre o computador lesado, situação que se verifica, por exemplo, no caso de utilização de disquete (Carla Rodrigues, 2003, p. 28).

Atualmente, não existe no Brasil legislação penal específica tratando da emissão de vírus. Diante dos prejuízos que o vírus pode causar, percebe-se que o artigo 163, do Código Penal, poderá ser aplicado para eventual punição do agente.

É evidente que a incursão do agente no artigo que trata do crime de dano não corresponde aos anseios da sociedade. O mais adequado seria a existência de legislação penal que tratasse do assunto, situação que eventualmente intimidaria os *hackers.*

Mas enquanto essa lei não surge, o artigo 163, do Código Penal, deverá ser aplicado nos casos onde o envio de vírus cause algum dano. É essencial que haja efetivo prejuízo econômico, pois caso contrário não estará configurado o crime. Logo, se o vírus destrói apenas *e-mails* que tratam de sentimentos ou amizade, não haverá crime de dano (Carla Rodrigues, 2003, p. 28).

Em relação ao dano qualificado, os incisos I (violência à pessoa ou grave ameaça) e II (emprego de substância inflamável ou explosiva), parágrafo único, do artigo 163, do CP, não terão aplicabilidade nos crimes virtuais, eis que são incompatíveis. Já as qualificadoras previstas nos incisos III (patrimônio pertencente à União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista) e IV (motivo egoístico ou prejuízo considerável para a vítima), terão aplicabilidade (Carla, 2003, p. 29).

Na dosimetria da pena, o Juiz deverá se atentar com ênfase ao artigo 59, do Código Penal, visualizando principalmente a culpabilidade, as circunstâncias e conseqüências do crime.

O doutrinador Guilherme Guimarães (2001, p. 75) tratou sobre o assunto:

> Caberá ao magistrado, no entanto, dosar a pena, em sua primeira fase (artigo 68, do Código Penal), com particular atenção para as conseqüências do delito (artigo 59, do Código Penal); assim dar-se-á tratamento diverso àquele que deu ensejo à destruição de arquivos valiosos de uma empresa com posição estratégica de mercado e àquele que apenas interferiu, por meio do vírus, no ambiente gráfico do programa de um usuário doméstico. Atentará, igualmente, para a culpabilidade e aos motivos do agente.

Em continuação o referido autor apresentou interessante posicionamento (2001, p. 75):

> Em hipóteses fronteiriças, optará pela absolvição, ora recorrendo ao princípio da insignificância penal, registrado alhures, ora refutando a subsunção ao tipo subjetivo (e.g., *hacker* que, com *animus jocandi*, contaminou rede restrita com vírus que apenas lança no vídeo palavras de baixo calão).

Trata-se de ação penal privada quando a conduta do agente recair no *caput* ou no inciso IV, parágrafo único, do artigo 163, e ação penal pública incondicionada em se tratando dos demais incisos do aludido parágrafo único.

Uma outra atitude a ser tomada pela vítima, caso o autor do fato seja identificado, é propor ação cível buscando a reparação dos danos.

4.6 Violação dos Direitos Autorais

Esta é outra conduta muito praticada na Internet, qual seja a de violar os diretos autorais. Nas palavras de Eduardo Faria (2005), “o direito autoral existe para resguardar o escritor, artista, ou compositor de modo a que possam gozar, usar e dispor dos produtos resultantes de suas criações”.

Além disso, continua o autor, o direito autoral serve “para estimular a produção intelectual, de forma a fazer com que o criador possa usufruir as

benesses de sua criação". Para ele, a coletividade poderá desfrutar dessa proteção dada ao direito autoral.

Existiria dessa forma o interesse do indivíduo em obter algum proveito econômico de seu trabalho e o interesse da coletividade em utilizar a obra daquele.

Ocorre que nem sempre o interesse do dono do "trabalho" é respeitado, significando que ele deixará de obter o proveito econômico.

Antes de tudo, para que a criação tenha proteção legal, deverá ser constituída de tal forma a ser original e sensível. Em relação à originalidade, sustenta-se que não haverá obra se não houver espírito criador, enquanto que a sensibilidade está ligada a concretização do pensamento ou sentimento de forma inteligível, fisicamente perceptível à visão, à audição ou ao tato (Eduardo Faria, 2005).

O direito autoral poderá estar ligado a obras literárias, musicais, programas de computador, entre outras invenções suscetíveis de proteção.

É interessante notar que o direito autoral é protegido constitucionalmente nos incisos XXVII e XXVIII, do artigo 5º, da Carta Magna, que prescrevem:

> XXVII – aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar;
>
> XXVIII – são assegurados, nos termos da lei:
>
> a) a proteção às participações individuais em obras coletivas e à reprodução da imagem e voz humanas, inclusive nas atividades desportivas;
>
> b) o direito de fiscalização do aproveitamento econômico das obras que criarem ou de que participarem aos criadores, aos intérpretes e às respectivas representações sindicais e associativas;

Concernente a legislação ordinária, o artigo 184, e seus parágrafos, do Código Penal, trata dos crimes contra a propriedade intelectual. Na figura do

caput, aquele que “violar direitos de autor e os que lhe são conexos”, estará sujeito a uma pena de 3 (três) meses a 1 (um) ano, ou multa.

O § 1º, do citado artigo, refere-se à “reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, ou de quem os represente”. Neste caso, a pena será de 2 (dois) a 4 (quatro) anos, e multa.

Em relação ao § 2º, do artigo 184, do Estatuto Penal, incorrerá nas mesmas penas do parágrafo anterior quem, “com o intuito de lucro direto ou indireto, por qualquer meio ou processo, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante...”.

Por fim, a violação aos direitos autorais do § 3º, está ligada ao “oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção de obra ou produção para recebê-la em tempo e lugar previamente determinados por quem o formula a demanda, com intuito de lucro direto ou indireto...”. A pena também é de 2 (dois) a 4 (quatro) anos, e multa.

Aplica-se aqui o que foi falado anteriormente nos itens anteriores, condizente à aplicação dessas figuras naquilo que for compatível ao meio informático. Quando o artigo prevê que a violação do direito autoral poderá acontecer por “qualquer meio ou processo”, ou ainda “qualquer outro sistema”, inclui-se o uso da Internet.

E é justamente a Internet o que causa maiores problemas às gravadoras, artistas, estúdios e editoras. Antigamente, a gravação de um disco rendia uma cópia ruim em fita cassete, sendo que essa fita só podia dar origem a cópias ainda piores. Com o advento da Internet, um “CD” pode dar origem a arquivos de qualidade em formato “mp3”, que podem ser transmitidos facilmente pela rede mundial de computadores (Eduardo Faria, 2005).

Eduardo Faria (2005) faz alusão ao *software* denominado “Napster”, como sendo um dos grandes responsáveis pela violação dos direitos autorais. O “Napster” funcionava da seguinte maneira, segundo o aludido autor:

> O princípio foi a tecnologia peer-to-peer (P2P), que possibilita a conexão direta entre dois computadores ligados à Internet. Os usuários do Napster conectavam-se com o sistema de busca de um computador central, capaz de listar diversos computadores de outros usuários comuns que possuíam a música desejada e conectá-los com o computador de outro usuário.

Em virtude da constante intervenção das grandes gravadoras, o programa “Napster” foi extinto. Isso só foi possível porque o referido programa utilizava uma base de dados como índice num local fixo, o que possibilitava a identificação do sujeito que violava o direito autoral (Eduardo, 2005).

A Lei n. 9.609/98 faz alusão à propriedade intelectual do programa de computador. O artigo 12 e seguintes, da mencionada Lei, trata das infrações e penalidades relacionadas à violação dos direitos de autor de programa de computador.

As condutas descritas no artigo 12, e seus parágrafos, apresentam estreita relação com aquelas previstas no artigo 184, do Código Penal.

Embora essa lei não esteja relacionada especificadamente a crimes praticados através da Internet, não se duvida que os direitos de autor de programa de computador poderão ser violados com o uso da Internet. Aliás, Carla Rodrigues (2003, p. 65) destaca que:

> A Internet é uma grande aliada da pirataria de *software*, pois facilita a distribuição de programas dos programas pirateados, propiciando ao agente do crime a comodidade de praticar a conduta sem sair de casa. A rede é usada para divulgação e distribuição, ao mesmo tempo que encobre a autoria do delito. Saliente-se que muitos “piratas” divulgam as cópias gratuitamente, restando para o usuário simplesmente fazer um *download* dos arquivos que lhe interessarem.

4.7 Pedofilia

Dentre todos os crimes praticados através da Internet, esse é o que causa maior repugnância na sociedade. Com previsão no artigo 241, do Estatuto da Criança e do Adolescente (Lei nº. 8.069/90), a pedofilia consiste em "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 ou adolescente" (grifo nosso).

É interessante notar que a redação original do ECA não fazia menção à "rede mundial de computadores" e à "Internet", levando em consideração que a aludida Lei passou a vigorar no ano de 1990. Com o advento da Lei nº. 10.764/03, o artigo 241, do ECA, passou a ter a redação descrita acima. Houve mudança também na fixação da pena, que inicialmente era de reclusão de 1 (um) a 4 (quatro) anos, alterando para reclusão de 2 (dois) a 6 (seis) anos.

Essas alterações representam indubitavelmente uma reação da sociedade a essas atitudes consistentes em divulgar imagens pornográficas de crianças e adolescentes. Sem contar que essas alterações surgiram para suprir a lacuna existente, visto que em 1.990 não se falava em Internet aqui no Brasil.

E os números são assustadores, dados informados por Demócrito Reinaldo (2004):

> [...] em maio deste ano, a Interpol, sediada em Madri, fez chegar à Polícia Federal brasileira a indicação de 272 sites, com origem no Brasil, onde eram exibidas fotografias de adultos explorando sexualmente crianças e adolescentes. Um convênio (protocolo de cooperação técnica) entre o MP do Rio Grande do Sul, o MPF, a Interpol, a PF e outros organismos revelou que, em 2002, houve 1.245 denúncias de páginas na Internet contendo material de pornografia infantil. De janeiro a 31 de maio do ano passado, houve 401 denúncias de páginas contendo esse tipo de material.

Para Demócrito, a Internet tem servido como instrumento para proliferação da pornografia e, de um modo ainda mais sensível, para a disseminação da

“pedofilia”. Salienta que os pedófilos trocam fotos e imagens que descrevam práticas sexuais com menores pré-púberes, método que serve não somente para extravasar suas fantasias sexuais, mas também para difundir uma espécie de “filosofia pedófila”.

Segundo Carla Rodrigues (2003, p. 46), a pedofilia é tratada como crime formal, bastando que as imagens ou fotografias sejam publicadas na Internet de forma a permitir que os usuários tenham pleno acesso. Mesmo que ninguém conheça o seu conteúdo, a infração estará consumada com a simples publicação.

Por outro lado, não haverá crime, por exemplo, quando o sujeito envia um e-mail contendo uma foto anexada. Neste caso, as imagens não caíram no domínio público, motivo que torna o fato atípico penalmente. Percebe-se que é dado o mesmo tratamento conferido aos crimes de difamação e calúnia.

Não se exige também que a divulgação dos vídeos ou das fotos venha trazer dano real à imagem da criança e do adolescente. Presume-se que o menor sofreu prejuízo psicológico com o ato de produzir as imagens com conteúdo sexual (Damásio e Gianpaolo *apud* Carla Rodrigues, 2003, p. 47). E não restam dúvidas de que o menor poderá sofrer abalos psicológicos irreparáveis, pois a pedofilia atinge diretamente toda sua infância e, conseqüentemente, a “inocência”.

Muito se discute a respeito da necessidade ou desnecessidade de se identificar o menor envolvido na pedofilia. O posicionamento de Carla Rodrigues parece ser o mais correto, no sentido de não ser necessário conhecer e identificar a criança ou o adolescente que teve sua foto divulgada na Internet (2003, p. 47). Seria um absurdo isentar um sujeito de responsabilidade pelo simples fato de não se identificar o menor. É certo que a não identificação do menor poderá trazer algumas conseqüências práticas, conforme será visto a seguir.

Como é comum de ocorrer nos crimes perpetrados através da Internet, existe uma certa dificuldade em se descobrir o autor desse crime. Se descoberto, alguns argumentos poderão ser utilizados pela defesa a fim de ser obtida uma absolvição no processo criminal.

Carla Rodrigues (2003, p. 46), apresenta determinadas teses que dificultam a condenação do sujeito. Dentre elas, existe aquela em que se alega

desconhecimento da idade da pessoa ou, até mesmo, hipóteses em que o menor declara ser maior de idade. Estaria ausente, portanto, o elemento subjetivo do tipo.

Esses casos costumam ocorrer quando o menor possuiu compleição física avançada, aparentando realmente ser pessoa com idade superior a 18 anos. Por uma questão de lógica, não se admite que uma criança seja confundida com uma pessoa adulta. Nos casos envolvendo os adolescentes, a acusação poderá afastar a tese apresentada acima, dizendo que o autor agiu com dolo eventual. Isto porque o pedófilo, diante dessas situações, deveria ter a cautela em verificar a idade do adolescente, analisando, por exemplo, a cédula de identidade.

Há menção até de imagens virtuais, isto é, situações onde os menores não existem no mundo concreto, representando uma invenção tecnológica. Como a legislação não faz qualquer previsão a esse respeito, não poderá ser dada uma interpretação extensiva para prejudicar o réu.

Em diverso caso, o autor alega que adquiriu as imagens por intermédio da Internet. Logo, não era possível conhecer a idade da pessoa envolvida nas publicações de cunho sexual. Restaria para a acusação apenas a tese de dolo eventual.

Por fim, no caso da não identificação do adolescente, poderá ser alegado que a pessoa presente nas imagens é maior de idade, circunstância que tornaria o fato atípico.

Conforme se verifica, como se não bastasse a dificuldade em se identificar o autor das publicações das imagens, inúmeros obstáculos poderão surgir durante a instrução criminal, a ponto do sujeito ser absolvido. Nas mais diversas vezes, o Magistrado terá que utilizar o bom senso na hora de julgar, evitando-se assim a impunidade.

Um outro ponto importante a ser discutido é a questão da competência nos casos de crimes praticados no exterior. Como bem asseverado por Carla Rodrigues (2003, p. 47), “se a criança é estrangeira, foi fotografada no exterior e o agente divulgou as fotos fora de nosso território, a Justiça brasileira não será competente, ainda que algumas imagens tenham chegado até aqui”.

Enfim, por tudo isso, conclui-se que o Brasil está fazendo a sua parte a fim de coibir esse crime tão bárbaro e repugnante. O certo é que o Estado tem interesse na repressão da pedofilia, haja vista que pesquisas demonstram que a divulgação de "pornografia infantil" contribui para o aumento de crimes sexuais contra menores (Demócrito Reinaldo, 2003).

E pode ser dito com veemência que as mudanças introduzidas no artigo 241, do ECA, contribuirão em muito na coibição da pedofilia. Um exemplo a ser citado é a responsabilização daquele que assegura, por qualquer meio, o acesso, na rede mundial de computadores ou Internet, das fotografias, cenas ou imagens produzidas na forma do *caput* do artigo 241, do ECA. Por este dispositivo, o provedor de serviço de hospedagem de página Web e o de serviço de acesso à Internet serão responsabilizados caso contribuam para a disseminação de pornografia infantil. É o que vem ocorrendo com os administradores do "Orkut".

Vejamos a dissertação de Demócrito (2004) sobre o assunto:

> Não somente o praticante direto do ato, mas também aquele que fornece os meios técnicos para sua realização incorre no mesmo tipo penal. Assim, por exemplo, quando um provedor sabidamente fornece os meios para a transmissão de uma mensagem de e-mail contendo pornografia infantil pratica conduta típica (descrita no inciso III do § 1º). O mesmo ocorre quando hospeda conscientemente página web contendo esse tipo de material (inciso II do § 1º).

O referido autor traçou uma sábia observação a respeito da aplicabilidade do inciso III, parágrafo 1º, do artigo 241. No seu ponto de vista, essa modalidade de crime somente se configura quando o provedor tem conhecimento da natureza do material que ele está transportando ou hospedando. De acordo com esse raciocínio, o provedor não poderá ser responsabilizado caso ele desconheça a existência de uma página eletrônica, com cenas de pornografia infantil, hospedada em seu sistema informático.

O sujeito passaria a ter responsabilidade a partir do momento em que toma conhecimento da existência do material ilícito hospedado em seu sistema e não impede o acesso ao material pornográfico ou a transmissão das mensagens,

deixando até de comunicar os fatos às autoridades competentes (Demócrito, 2004).

Para desfecho do tema, vejamos o interessante conceito apresentado por Carla Rodrigues (2003, p. 46), concernente à pedofilia: “A pedofilia consiste num distúrbio de conduta sexual, no qual o indivíduo adulto sente desejo compulsivo por crianças ou pré-adolescentes, podendo ter caráter homossexual ou heterossexual”.

5. FATOS ATÍPICOS

A existência de inúmeras condutas tidas como atípicas penalmente representa uma realidade incontestável no mundo virtual, embora tais condutas demonstram relativa gravidade e importância no âmbito penal.

Como é cediço, isso só ocorre em razão da ausência de legislação específica tratando dos crimes denominados virtuais. Conforme será observado, existem fatos que se adequam às normas penais comuns, maiormente quando existir dano material. Contudo, essas ditas normas não punem os criminosos de forma adequada, haja vista que servem apenas, a grosso modo, como "tapa buracos".

Essa situação traz certa insegurança àquelas pessoas que utilizam a Internet, seja como um meio de trabalho ou de entretenimento. Essa insegurança é ilustrada com propriedade por Mário Antônio Lobato de Paiva (2004):

> [...] demonstra o perigo que estamos passando e a falta de estabilidade legal em que vivemos, levando o cidadão à total insegurança e desproteção jurídica, que pode levar a sociedade a ter sérios prejuízos, sem falar na intranqüilidade permanente que pode ser e está sendo gerada pela falta de legislação. Uma das questões que mais provocam perplexidade é, justamente, a que diz respeito à punição dos delitos cometidos pela via eletrônica. A leitura de alguns artigos e livros sobre o assunto refletem a imaturidade intelectual em que nos encontramos, pois nem sequer sabemos se há possibilidade de punir ou não esse tipo de crime.

Nesta esfera de discussão, há até quem entenda que as normas penais comuns não poderão ser aplicadas aos fatos provenientes do meio informático. Um dos fundamentos utilizados pelos defensores deste pensamento consiste na aplicabilidade do princípio da reserva legal, onde não há crime sem lei que o defina.

Surge ainda uma outra doutrina, defendendo a tese de que não é possível a construção de interpretações extensivas e analógicas (salvo exceção), maiormente considerada quando algum prejuízo surgir no julgamento do acusado. Para esta corrente doutrinária, a analogia seria aceita apenas *in bonam partem* e,

mesmo assim, com as restrições feitas pela doutrina e jurisprudência, obedecendo ao disposto no art. 3º, do Código de Processo Penal (Mário Antônio, 2004).

Esses argumentos são os principais responsáveis pelo reconhecimento da atipicidade de diversos fatos comumente praticados na Internet, o que implica na inaplicabilidade da legislação penal vigente.

Em contrapartida, há o entendimento no sentido de que certos crimes praticados pela via eletrônica são os mesmos tratados pelo Código Penal e legislações esparsas, com a peculiaridade de serem apenas versões modernas dos tipos. O único diferencial residiria apenas no *modus operandi*, fator que não tem o condão de impedir a adequação da conduta a um tipo penal comum (Mário Antônio, 2004).

Nada obstante os sábios argumentos utilizados por esta última corrente doutrinária, percebe-se que as correntes mais benéficas ao acusado atendem perfeitamente os princípios que norteiam o sistema penal brasileiro. Os acusados não poderão ser responsabilizados por condutas que não se enquadram em qualquer tipo penal, cabendo unicamente ao legislador a obrigação de elaborar leis específicas sobre o assunto.

Isso não significa que tudo aquilo que foi discutido no capítulo anterior não tem validade, pois esses argumentos estão restritos a determinados casos onde não há a perfeita adequação entre a conduta e o fato típico.

O doutrinador Guilherme Guimarães elencou algumas condutas tidas ainda como atípicas (2001, p. 122):

- *Spam* inábil à provocação de dano.
- Invasão, pela ação de *hackers*, de IP (Protocolo Internet), sem prejuízo sensível.
- Alteração indevida, pela ação de *hackers*, de *web pages* mantidas por terceiros, sem prejuízo sensível.

- Interceptação ou escuta do fluxo de dados fora de tráfego típico de serviço de telecomunicações.
- Violação, sonegação ou destruição de e-mail.
- Uso de nome alheio em domínio próprio para extorsão.

Essas são algumas dentre outras muitas condutas que não admitem punição criminal. E essa situação ficará ainda pior se levado em consideração o avanço desenfreado da tecnologia, onde surgirão brechas para a atuação dos denominados *hackers.*

6. DIREITO COMPARADO

Diante de tudo o que já foi exposto, fica claro que o Brasil não dispõe ainda de uma legislação adequada concernente ao meio da informática, nada obstante existam algumas inovações e projetos de lei a serem apreciados pelo Congresso Nacional.

Diferente do Brasil, outros países já possuem leis específicas, tratando não só dos crimes, mas também de outros assuntos relacionados à informática e à Internet.

Para ilustrar as diferenças existentes entre a legislação brasileira com a dos outros países, é interessante traçar comentários sobre as leis específicas de determinados países.

6.1 Portugal

Portugal possui ampla legislação no que diz respeito aos crimes praticados por meio da Internet, havendo previsões tanto no Código Penal quanto em leis esparsas.

No Código Penal do País, existem duas figuras delitivas, sendo que o primeiro, previsto no artigo 193º, está inserido no capítulo reservado aos crimes contra a reserva da vida privada e refere-se à devassa por meio da informática. O artigo 221º dispõe sobre a burla informática e nas comunicações, tratando-se de crime contra o patrimônio (Carla Rodrigues, 2003, p. 155).

De acordo com a autora mencionada, vigora em Portugal a Lei da Criminalidade Informática (Lei nº 109/91), que além de tipificar crimes, define alguns conceitos comumente restritos ao âmbito da informática. O legislador procurou dar suporte técnico ao operador do direito, que, na maioria das vezes, não possui conhecimento aprofundado em informática.

Aliás, é interessante notar que a aludida Lei da Criminalidade Informática vigora desde o ano de 1.991. Por certo, a Internet existe no país há muito tempo,

mas essa assertiva demonstra cabalmente a preocupação e a seriedade do legislador em relação ao tema.

Concernente aos delitos, há a previsão de seis tipos penais: falsidade informática, danos relativos a dados ou programas informáticos, sabotagem informática, acesso ilegítimo, interceptação ilegítima e reprodução ilegítima de programa protegido (Carla Rodrigues, 2003, p. 158).

6.2 Itália

Da mesma forma que Portugal, a Itália possui legislação avançada concernente ao tema da informática. Para se ter uma idéia, a Lei nº 547/93 acrescentou quinze figuras típicas, sendo seis figuras essenciais: sabotagem, acesso ilegal, violação de segredo informático e do sigilo, falsificações, fraude informática e violação dos direitos do autor concernentes ao *software* (Carla Rodrigues, 2003, 158).

Percebe-se que a Lei mencionada acima vigora na Itália há mais de treze anos, circunstância já destacada na legislação portuguesa.

O envio de vírus também é considerado crime na Itália, tendo tipificação própria. O artigo 615, do Código Penal Italiano prevê a conduta do agente que difunde, comunica ou entrega um programa informático com o intuito de provocar danos nos dado, programas informáticos ou telemáticos de computadores alheios ou interrompa, total ou parcialmente, seu funcionamento (Carla Rodrigues, 2003, p. 158).

Pela leitura do artigo 615, é tirada a conclusão de que basta o envio de vírus para que o crime se configure, não se exigindo a existência de dano material. Como visto anteriormente, aqui no Brasil, por não possuir legislação específica, só haverá crime caso o vírus provoque danos materiais ao destinatário.

Pune-se igualmente o sujeito que difunde, ilegalmente, os códigos de acesso, palavras chaves ou outros meios idôneos de acessar um sistema de

informática protegido por medida de segurança, tudo isso com fulcro no artigo 615, primeiro parágrafo, do Código Penal Italiano (Carla Rodrigues, 2003, p. 159).

6.3 Estados Unidos da América

Os Estados Unidos, titulados como grande potência mundial e detentores de elevado nível de modernização, não poderiam deixar de ter vasta legislação concernente à informática.

A Lei 18 U.S.C. 1030, disciplina a fraude e atividades relacionadas a computadores. Esta mesma lei tipifica algumas condutas e oferece conceitos de diversas expressões relacionadas à informática.

Dentre as condutas tipificadas, podemos citar aquela em que o agente acessa computador sem autorização ou excedendo autorização e com isso obtenha informação de registro financeiro de instituição financeira ou informações do departamento e agências dos Estados Unidos.

Na mesma esteira, comete crime quem acessa computador, sem autorização ou excedendo autorização, de uso exclusivo do Governo dos Estados Unidos ou computador não exclusivo, mas utilizado pelo Governo.

De outra banda, é punida a conduta de quem cause transmissão de um programa, informação, código ou comando e provoque dano para computador protegido ou quem, com o intento de extorquir dinheiro ou outra coisa de valor, ameace de causar dano a computador protegido de pessoa, firma, associação, instituição educacional, instituição financeira, entidade de governo ou outra entidade legal (Carla Rodrigues, 2003, p. 161).

Como se pode ver, os Estados Unidos procuraram dar ampla proteção ao sistema informático, prevendo condutas das mais variadas modalidades. Sem sombra de dúvidas, essa larga previsão de condutas dificulta em muito a atividade da defesa no processo criminal, levando em consideração a inexistência de “brechas”. A maioria dessas condutas não está prevista na legislação brasileira.

E não para por aí, eis que existem outras leis tratando do assunto: Lei 18 U.S.C. 1362, que protege as linhas de comunicações, estações e sistemas; Lei 18 U.S.C. 2551, que tutela as comunicações, tipificando como crime a conduta de quem intercepta ou revela comunicação, oral ou eletrônica, proibida; Lei 18 U.S.C. 2701, que tipifica o acesso ilícito de comunicações armazenadas; e, por fim, a Lei 18 U.S.C. 2702, que dispõe sobre a revelação de conteúdo (Carla Rodrigues, 2003, p. 161).

6.4 Inglaterra

A Inglaterra, por sua vez, no *Computer Minuse Act*, tratou de várias condutas criminosas relacionadas à informática.

Dentre as enumeradas, citemos aquela em que o agente obtém acesso não autorizado a programa ou informação. Dispõe, ainda, sobre a excludente de responsabilidade criminal, que incidirá quando o agente, sem ter conhecimento, obtém a informação, ou seja, não tinha a intenção de violar o sistema alheio.

O legislador inglês inovou ao punir o acesso quando utilizado como meio para execução de outro delito. Punem-se, dessa forma, os atos preparatórios de crimes mais graves que, por circunstâncias diversas, não chegam a se consumar (Carla Rodrigues, 2003, p. 162).

Existem outras condutas previstas, como aquela que o autor modifica as informações armazenadas em computadores.

É importante salientar a conduta do governo britânico em apresentar um projeto que prevê o rastreamento do tráfico de informações na Internet pelos serviços de segurança do país, onde os provedores de acesso à Internet seriam obrigados a permitir acesso irrestrito da polícia a uma grande quantidade de informações sobre seus usuários (Carla Rodrigues, 2003, p. 162).

Esse mecanismo pretendido pela Inglaterra será eficiente na identificação dos autores dos crimes virtuais. E como tal, os demais países poderão tomar por

base esse modelo de investigação, o que certamente propiciará uma efetiva responsabilização dos *hackers*.

6.5 Outros países

Embora em outros países não seja dado enfoque consistente ao tema, alguns aspectos poderão ser salientados. Países como a Argentina, Canadá, Alemanha e China tratam do tema de maneira superficial, mas merecem destaque.

Na Argentina, através do Decreto 427/98, iniciou-se um programa de assinaturas digitais no âmbito da Administração Pública, para os atos internos que não produzam efeitos jurídicos.

Por outro lado, o Canadá, através da *Royal Canadian Mounted Police*, enumera os principais tipos de crimes: acesso não autorizado, danos a dados, furto de telecomunicações e violação de direito autoral de *software*.

A Alemanha, por seu turno, procurou dar um tratamento mais aprofundado sobre o tema. Por intermédio da Lei Federal de 1.997 (*Informations – und Kommunikationsdiense – Gesetzt)*, alterou várias leis existentes, além de introduzir novas figuras delitivas.

Vejamos algumas: disciplinou o uso de serviço de comunicações, a segurança e proteção de dados nos serviços de comunicações, a assinatura digital, modificou o Código Penal e a Lei das Contravenções Penais, alterou a lei sobre difusão de publicações atentatórias à juventude e a lei dos direitos autorais.

Além disso, a referida lei definiu a responsabilidade por transmissão de material pornográfico e previu a responsabilidade pela veiculação de material ilegal, fazendo distinção entre provedores de acesso e provedores de conteúdo (Carla Rodrigues, 2003, p. 163).

Por derradeiro, a China foi rigorosa ao divulgar normas de controle do conteúdo da Internet, pois entende que a rede mundial de computadores é

utilizada para filtrar segredos de Estado e difundir informações danosas. Como pena, é prevista multa de até US$ 1.800,00 (Carla Rodrigues, 2003, p. 163).

CONCLUSÃO

Diante de todo o exposto, não é forçoso concluir pela extrema importância do tema proposto, ainda mais se levado em conta a época em que vivemos, denominada de “Era da Informática”.

Nada obstante este grau de importância, restou evidenciado que os problemas relacionados à informática e à Internet não são tratados com o devido merecimento, notadamente aqui no Brasil.

É notória a falta de legislação a respeito do assunto, embora existam algumas raríssimas exceções. Aliás, em se tratando de Internet e informática, percebe-se a carência de discussões doutrinárias quanto às questões de cunho criminal.

Estes dois fatores conduzem a uma triste realidade no processo criminal, representada pela impunidade. Diante da falta de previsões legais, sobram teses defensivas, plenamente capazes de provocar uma absolvição.

Como se não bastasse, os problemas existem antes mesmo do início do processo. A começar pela identificação dos autores dos delitos virtuais, problema que certamente atribula as Autoridades encarregadas pela investigação. Isso é resultado da ausência de tecnologia adequada a disposição das Autoridades e do elevado nível de conhecimento técnico dos *hackers.* Aliada à dificuldade em se produzir prova, o problema da autoria é sem dúvida o grande obstáculo para a devida responsabilização dos agentes.

É incrível que todos esses problemas existem num País onde se conta mais de 5.000 decisões judiciais sobre casos envolvendo a Internet. País que possui o maior número de usuários do site de relacionamentos “Orkut”, representando 75% dos usuários.

Se isto serve de consolo, é oportuno dizer que existem 52 projetos de Lei tratando de assuntos relacionados à Internet, a exemplo do projeto de Lei n.º 84/99, de autoria do Deputado Luiz Piauhylino. Com base nesses números, é possível que num futuro próximo novas leis surjam, sanando de vez a carência na legislação brasileira.

Não poderia deixar de registrar a seriedade do Ministério Público no combate aos crimes virtuais. Não raras vezes é noticiada alguma atitude dos seus Membros na difícil missão de responsabilizar os sujeitos ativos dos crimes virtuais.

Como exemplo, a dura batalha judicial existente entre o Ministério Público Federal e o “Google”, empresa responsável pelo site “Orkut”. Em um dos casos, o Membro do Ministério Público Federal ajuizou uma ação civil com o intuito de obter a quebra de sigilo de dados de comunidades e perfis criminosos. Em caso de descumprimento da determinação judicial, a multa diária seria de pelo menos R$ 200.000,00 (duzentos mil reais). Há até a possibilidade da filial da “Google” do Brasil ser fechada.

É evidente que não só o Ministério Público tem atuado na repressão dos crimes virtuais. Órgãos como a Polícia Federal, Interpol, Congresso Nacional e Empresas de Serviço Virtual têm contribuído consideravelmente nos casos envolvendo a Rede Mundial de Computadores.

Entretanto, mesmo diante dessas circunstâncias favoráveis, o Brasil encontra-se em situação muito aquém de outros países, como por exemplo, os Estados Unidos da América. Não representa uma justificativa o fator do subdesenvolvimento, eis que os números demonstram o elevado grau de desenvolvimento do Brasil em se tratando de informática e Internet.

Pelo que parece, falta dedicação aos representantes dos Poderes Legislativo e Executivo, no sentido de criar alternativas para as autoridades encarregadas pela persecução criminal.

Muito embora isso aconteça, a sociedade espera ansiosamente por algumas mudanças, a fim de serem preservados os interesses e valores sociais predominantes. Neste mesmo sentido, espera-se que a repressão aos crimes virtuais tenha proporcional progressão com o constante e infinito avanço tecnológico.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade**. In: Jus Navigandi, n. 51. [Internet]. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2250>. Acesso em: 5 abr. 2006.

CAMPOS, Eduardo Faria de Oliveira. **Direito e Internet: direitos autorais e a tecnologia peer-2-peer**. In: Jus Navigandi, n. 613. [Internet]. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=6363>. Acesso em: 11 jun. 2006.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática**: e seus Aspectos Processuais. 2. ed. Rio de Janeiro: Lumem Júris, 2003. 236 p.

DAOUN, Alexandre Jean. **Os novos crimes de informática**. In: Avocati Locus. [Internet]. Disponível em: <http://www.advogado.com/internet/zip/novocrim.htm>. Acesso em: 2 jul. 2006.

FELICIANO, Guilherme Guimarães. **Informática e Criminalidade**: Primeiras Linhas. Ribeirão Preto: Nacional de Direito, 2001. 137 p.

JESUS, Damásio Evangelista. **Direito Penal**. 26 ed. São Paulo: Saraiva, 2003. 754 p. v. 1.

MENDES, Carolina de Aguiar Teixeira. **Perfil: Orkut**. In: Jus Navigandi, n. 883. [Internet]. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=7631>. Acesso em: 22 jul. 2006.

PAIVA, Mário Antônio Lobato de. A atipicidade dos delitos cometidos na Internet. **Revista Síntese de Direito Penal e Processual Penal**, [S.l.], n. 26, p. 155, jun. /jul. 2004.

PIMENTEL, Alexandre Freire. **O Direito Cibernético**: Um Enfoque Teórico e Lógico-Aplicativo. Rio de janeiro: Renovar, 2000. 267 p.

REINALDO FILHO, Demócrito. Crimes cometidos na Internet: Questões técnicas dificultam condenações. **Revista Síntese de Direito Penal e Processual Penal**, [S.l.], n. 26, p. 158, jun. /jul. 2004.

_____ . Pornografia Infantil Pela Internet: Divulgação – Breves Comentários à Lei Nº 10.764/03. **Revista Síntese de Direito Penal e Processual Penal**, [S.l.], n. 24, p. 40, fev. /mar. 2004.

GLOSSÁRIO

Chat – Modo de comunicação direta entre usuários de redes de informática. Compreende diálogo textual, em tempo real.

Ciberespaço – Termo que se aplica ao mundo virtual das redes de computadores; espaço virtual ou espaço artificial.

Cracker – São pessoas especializadas em quebrar senhas.

Domínio – Método utilizado para identificar os computadores na Internet. A utilização de domínios visa evitar que um mesmo nome seja dado por mais de um equipamento e descentralizar o cadastramento. São exemplos de domínios institucionais: “com”, destinadas às instituições com fins comerciais; “gov”, destinadas para instituições governamentais; “mil”, destinadas às instituições com fins militares.

Download – É a obtenção de uma cópia de arquivo através do computador e da Internet. Fazer um download significa baixar um arquivo.

E-mail – Correio eletrônico. É utilizado como endereço eletrônico.

FTP – *File Transfer Protocol*. Significa protocolo de comunicação para transferência de arquivo entre dois computadores. É o método mais comum de transferência de arquivos entre dois locais na Internet.

Hacker – Conhecido como pirata eletrônico. É a pessoa que possui conhecimento de informática acima da média e o utiliza para penetrar em sistemas de segurança de computadores alheios. O *Hacker* é um violador do sistema de computação, um intruso que acessa e controla uma máquina na rede, sem possuir autorização para tal.

Hardware – São os componentes físicos do computador e seus acessórios. Exemplos: teclado, mouse e monitor.

Homepage – É a página de entrada em um site na *Web*, ou de outro sistema de hipertexto ou de hipermídia que geralmente contém uma apresentação geral e um índice, com elos de hipertexto que remetem às principais seções do site, visando facilitar a navegação pelo sistema.

HTTP – *Hiper Text transport Protocol*. É o protocolo utilizado para transferência de páginas de hiper texto ou outros documentos na Internet. O servidor "www" fornece a informação, requerida e transferida para o cliente através do protocolo "http".

Internet – É a maior rede de computadores de âmbito mundial e de acesso público, possuindo o ciberespaço, mundo virtual, serviços, correio eletrônico, *chat* e a *Web.* Com a inicial maiúscula designa a "rede das redes", já com inicla minúscula significa uma coleção de redes locais e/ou de longa distância, interligadas.

Internet Protocol – Também conhecida como *IP* Address. Versão numérica do nome do hospedeiro. Todo computador de rede tem um endereço de *IP*.

Password – Consiste numa seqüência de caracteres de segurança que é requerida antes do acesso a um sistema, ou parte dele, e que deve ser requerida.

Server – Servidor, entidade que gera bases de dados ou um conjunto de dados e que permite, mediante determinadas condições, o respectivo acesso. É normalmente um computador central conector de vários computadores.

Site – É o conjunto de documentos apresentados ou disponibilizados na *Web* por um indivíduo, instituição ou empresa, e que pode ser fisicamente acessado por um computador e em endereço específico na rede.

Software – Qualquer programa ou um conjunto de programa e procedimentos referentes ao sistema de processamento de dados.

Virtual – Adjetivo utilizado para designar algo que não tem uma existência real, mas existe apenas em meios de informática e/ou redes de comunicações.

Web – É reconhecido pela sigla "www" (*Word Wide Web*). É o recurso ou serviço oferecido na Internet e que consiste num sistema distribuído de acesso às informações, as quais são apresentadas na forma de hipertexto, com elos entre documentos e outros objetos, localizados em pontos diversos da rede.