*Ensaio Jurídico*. Patos de Minas: UNIPAM, (1):257-276, 2010 | ISSN 2179-1945

# Crimes eletrônicos: responsabilização criminal dos gerenciadores dos meios de facilitação e necessidade de tipificação penal específica para estes delitos

## *Electronic crimes: criminal responsibility of managers of facilitation means and the necessity of specific penal typication for these crimes*

***Raquel Bessa Teixeira da Cunha Vilela***
Bacharel em Ciências Militares pela Academia de Polícia Militar de Minas Gerais.
Aluna do 10.º Período do Curso de Direito do Centro Universitário de Patos de Minas.
e-mail: raquelbtc@yahoo.com.br

***Resumo*:** O presente trabalho teve o propósito de sensibilizar aqueles que se utilizam de diversos serviços oferecidos pela rede mundial de computadores, sobre as mais diversas possibilidades de serem vitimados pelas práticas delituosas impetradas pelo meio eletrônico, vindo a fomentar ainda a discussão a respeito dos tipos de crimes praticados nesse meio, além das responsabilidades por tais práticas daqueles entes que com ela possam contribuir, sejam eles administradores ou gerenciadores de sistemas, redes ou até mesmo estabelecimentos de uso de computadores. Chegou-se à conclusão de que não há necessidade da criação de novas leis para regulamentar o assunto, bastando, para tanto, aplicar as já existentes.
***Palavras-chave*:** Computadores. Crimes. Responsabilidades. Entes. Leis.

***Abstract***: The present work intended to move those who use the many services offered by the world web wide about the possibilities to be victimized by the criminal practices impetrated by the electronic medium. It also promotes the discussion about the kinds of crimes practiced in this means, besides the responsibilities for such practices by those who may contribute with it, be it administrators or system managers, webs or even organizations of computer use. We came to the conclusion that it is not necessary to create new laws to regulate the matter, for the existing laws are enough.
***Keywords***: Computers. Crimes. Responsibilities. Beings. Laws.

## *1. Introdução*

O desenvolvimento contínuo das formas e meios de comunicações está, indiscutivelmente, presente nas sociedades, tendo sido a internet o meio mais rápido e globalizado de comunicação já existente em todo o mundo, conectando em tempo real milhões de pessoas, causando uma difusão quase instantânea de informações e acontecimentos.

A acessibilidade à internet, bem como a possibilidade de não se identificar na rede, tornam-se fatores que estimulam a prática dos delitos, conhecidos como "eletrônicos" ou "virtuais", os quais, em grande parte das vezes, estão associados à ofensa à honra e/ou à sexualidade do indivíduo, ou à prática de fraudes financeiras.

Neste limiar, entra o nosso ordenamento jurídico que, tendo leis já um tanto quanto antigas, não fazia previsões específicas quanto ao assunto, por questões óbvias e lógicas, carecendo, portanto, de uma adequação de normas que visem a coibir e definir de forma específica os delitos cometidos por meios eletrônicos, em especial pela internet, além de punir com severidade os autores dos mencionados delitos, afim de regulamentar um mundo ainda sem regras, que é o mundo "virtual".

Desta forma, diante da ausência de legislação específica sobre delitos eletrônicos, e buscando-se discutir também a responsabilidade jurídica dos controladores dos meios virtuais frente a tais delitos, o presente trabalho vem expor tais inferências, buscando nos referenciais teóricos fundamentações para as devidas responsabilizações, além de definições dos crimes virtuais.

## *2. Conceitos*

### *2.1. Internet*

A Internet[1], conforme pesquisa realizada é:

> É um conglomerado de redes em escala mundial de milhões de computadores interligados pelo Protocolo de Internet que permite o acesso a informações e todo tipo de transferência de dados. A Internet é a principal das novas tecnologias de informação e comunicaçãos e refere-se ao sistema de informação global que é logicamente ligado por um endereço único global baseado no Internet Protocol (IP) ou suas subseqüentes extensões (<http://pt.wikipedia.org/wiki/Internet>, acesso em: 27 out. 2008).

### *2.2. IP*

*Internet Protocol*[2]. IP, conforme pesquisa realizada, é um acrônimo para a expressão inglesa "*Internet Protocol*" (ou *Protocolo de Internet*), que é um protocolo usado entre duas ou mais máquinas em rede para encaminhamento dos dados.

[1] Disponível em: < http://pt.wikipedia.org/wiki/Internet>. Acesso em: 27 out. 2008.

[2] Disponível em: < http://pt.wikipedia.org/wiki/Internet_protocol>. Acesso em: 27 out. 2008.

### *2.3. Provedor*[3]

Conforme pesquisa realizada a respeito do provedor, vê-se que

> o fornecedor de acesso à Internet (em inglês *Internet Service Provider*, ISP) oferece principalmente serviço de acesso à Internet, agregando a ele outros serviços relacionados, tais como "e-mail", "hospedagem de sites" ou blogs, entre outros. Inicialmente como um serviço cobrado, com o tempo passou a ser oferecido também como serviço gratuito, por empresas que estruturaram um outro modelo de negócio (<http://pt.wikipedia.org/wiki/Provedor>, acesso em: 27 out. 2008).

### *2.4. Orkut*

O orkut[4], conforme conceito pesquisado,

> é uma rede social filiada ao Google, criada em 19 de Janeiro de 2004 com o objetivo de ajudar seus membros a criar novas amizades e manter relacionamentos. Seu nome é originado no projetista chefe, Orkut Büyükkokten, engenheiro turco do Google. Tais sistemas, como esse adotado pelo projetista, também são chamados de rede social (<http://pt.wikipedia.org/wiki/Orkut>, acesso em: 27 out. 2008).

### *2.5. Lan House*

Lan House[5] conforme consulta realizada,

> É um estabelecimento comercial onde, à semelhança de um cyber café, as pessoas podem pagar para utilizar um computador com acesso à internet e a uma rede local, com o principal fim de acesso à informação rápida pela rede e entretenimento através dos jogos em rede ou online (<http://pt.wikipedia.org/wiki/Lan_house>, acesso em: 27 out. 2008).

## *3. Internet: seu principal ponto de partida*

A internet se desenvolve com muita ênfase, no auge do processo de barateamento das comunicações, no final da década de 80, sendo hoje vista como um meio de

[3] Disponível em: < http://pt.wikipedia.org/wiki/Provedor>. Acesso em: 27 out. 2008.

[4] Disponível em: < http://pt.wikipedia.org/wiki/Orkut>. Acesso em: 27 out. 2008

[5] Disponível em: < http://pt.wikipedia.org/wiki/Lan_house>. Acesso em: 27 out. 2008.

comunicação que interliga o mundo todo com milhões de computadores e permite o acesso a uma quantidade de informações praticamente inesgotáveis, anulando toda distância de tempo e lugar.

O mais importante elemento impulsor desse desenvolvimento todo, que permitiu à internet transformar-se num instrumento de comunicação de massa, nasceu no ano de 1989, no Laboratório Europeu de Física, de altas energias, com sede em Genebra, sob o comando de T. Berners-Lee e R. Cailliau, e era composto por hipertextos, ou seja, documentos cujo texto, imagem e sons seriam evidenciados de forma particular e poderiam ser relacionados com outros documentos, permitindo que, com um simples clique no *mouse,* o usuário pudesse ter acesso aos mais variados serviços e informações, sem necessidade de conhecer os inúmeros protocolos de acesso.

Se, por um lado, incontestável é o avanço e os benefícios que o uso ético da internet trouxe para a propagação da informação, desenvolvimento das tecnologias modernas em todas as áreas do conhecimento, com benefícios incalculáveis em sua divulgação, por outro, tem-se os riscos inerentes à tecnologia da informatização, notadamente os crimes informáticos.

## *4. Crimes informáticos: conceituações*

Em vários documentários e textos atuais, vemos a importância da internet em nossas vidas de modo que se tornaria impossível viver sem o uso desta ferramenta tão importante em todas as atividades. Porém como todo instrumento de uso do homem está fadado a ser utilizado para outras condutas de forma ilícita, a internet não é exceção. Assim, fazendo uma retrospectiva:

> O surgimento dos crimes informáticos remonta, no entender de Ulrich Sieber, da Universidade de Würzburg, à década de 1960, época em que apareceram na imprensa e na literatura científica os primeiros casos de uso do computador para a prática de delitos, constituídos, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados em matérias jornalísticas. Somente na década seguinte é que se iniciariam os estudos sistemáticos e científicos sobre essa matéria, com emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial (FERREIRA, 2000, p. 83).

Várias ações criminosas passaram a incidir através dos meios eletrônicos, em especial pela internet, citando-se a pirataria de programas de computadores, abusos nas telecomunicações, extorsão virtual, estelionatos etc., revelando vulnerabilidade que os criadores do processo não haviam previsto.

Entre os piores delitos cometidos através da internet podemos citar o delito de pornografia infantil na rede, muito difundido e praticado por milhares de pessoas pelos *websites* da rede mundial de computadores.

Tal criminalidade avassaladora conta com as mesmas características da informatização global:

> Transnacionalidade – todos os países fazem uso da informatização (qualquer que seja o seu desenvolvimento econômico, social ou cultural); logo, a delinqüência correspondente, ainda que em graus distintos, também está presente em todos os continentes; universalidade – integrantes de vários níveis sociais e econômicos já têm acesso aos produtos 69 R. CEJ, Brasília, n. 20, p. 67-73, jan./mar. 2003 informatizados (que estão se popularizando cada vez mais); ubiqüidade – a informatização está presente em todos os setores (públicos e privados) e em todos os lugares (GOMES, 2007, p. 76).

Nesse contexto, torna-se possível observar que a informática permite não só o cometimento de novos delitos, como potencializa alguns outros tradicionais, como o estelionato, por exemplo. Há, assim, crimes cometidos com o computador e os cometidos contra o computador, isto é, contra as informações e programas nele contidos.

Poderiam ser descritos os crimes digitais, como sendo todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar.

Outra corrente a ser analisada é a defendida por Pinheiro (2002), que classifica crimes informáticos ou cibernéticos em virtuais puros, mistos e comuns.

> O crime virtual puro seria toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas.
>
> Crime virtual misto seria aquele em que o uso da internet é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático, como, por exemplo, as transferências ilícitas de valores em uma *homebanking* ou no chamado *salamislacing*, onde o *cracker* retira de milhares de contas correntes, diariamente, pequenas quantias que correspondem a centavos e as transfere para uma única conta. Embora

> esses valores sejam ínfimos para o correntista, que, na maioria das vezes, nem se dá conta do furto, representam para o cibercriminoso uma expressiva quantia em seu montante.
>
> Por derradeiro, crime virtual comum seria utilizar a internet apenas como instrumento para a realização de um delito já tipificado pela lei penal (PINHEIRO, 2002, p. 62).

Assim, a Rede Mundial de Computadores acaba por ser apenas mais um meio para a realização de uma conduta delituosa. Se antes, por exemplo, o crime como o de pornografia infantil (art. 241 do ECA) era instrumentalizado por meio de vídeos ou revistas, atualmente, dá-se por salas de bate-papo, Orkut, como também pela troca de fotos por *e-mail* entre pedófilos e divulgação em *sites*.

Mudou a forma, mas a essência do crime permanece a mesma. De forma abrangente, o crime de informática pode ser definido como sendo, segundo Pinheiro (2002, p. 42), "toda ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão".

O Professor Viana (2003, p. 13-26) apresenta a seguinte classificação dos crimes informáticos:

1. *Delitos Informáticos Impróprios*, para esclarecê-los como "aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico nem inviolabilidade da informação automatizada";
2. *Delitos Informáticos Próprios*, para fixá-los como "aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)";
3. *Delitos Informáticos Mistos*, para explicá-los como "crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa";
4. *Delitos Informáticos Mediatos ou Indiretos*, definindo-os como "delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação".

Indo ao encontro dos fatores ligados à criminalidade, a definição exposta pelo professor Vianna nos dá uma clara noção do que venha a ser os delitos informáticos, observando-se que os delitos informáticos próprios estão mais suscetíveis de serem cometidos, tendo em vista que o criminoso usa o computador para perpetrar o crime informacional, violando informações automatizadas.

Para Ferreira, outra é a classificação, e para ele os crimes de informática se distinguem em duas categorias:

> 1) os atos dirigidos contra um sistema de informática, por qualquer motivo, verdadeiro núcleo da criminalidade informática, por se tratarem de ações que atentem contra o próprio material informático (suportes lógicos ou dados dos computadores);
> 2) os atos que atentem contra outros valores sociais ou outros bens jurídicos, cometidos através de um sistema de informática, que compreenderiam todas as espécies de infrações previstas em lei penal (FERREIRA , 2006, p. 54).

O nosso ordenamento jurídico não prevê tipificações específicas para os crimes eletrônicos, contudo a Constituição Federal dispõe no Art. 5.º, inciso X, que a privacidade das pessoas é um bem jurídico fundamental. Dessa maneira, Vianna diz que "*a* inviolabilidade das informações é decorrência natural do direito a privacidade, devendo, portanto, ser reconhecida como bem jurídico". E mais:

> Como corolário desta afirmação, a inviolabilidade das informações automatizadas, ou seja, daquelas armazenadas e processadas em sistemas computacionais, surgirá então como um novo bem jurídico a ser tutelado pelo Direito Penal, de forma a se garantir a privacidade e a integridade dos dados informáticos.
> Reconhecida, pois, a existência de um bem jurídico a se proteger, tem-se que há crime sobre o aspecto material, sendo que a simples omissão normativa não é suficiente para descaracterizá-lo como objeto de estudo do Direito Penal, já que este reconhece sua existência sob o aspecto material (VIANNA, 2003, p. 9-10).

Na prática o que ocorre para a imputação de um crime informático a uma pessoa é o seu enquadramento em nossa legislação penal, que apesar de não prevê-los de forma específica, molda-os perfeitamente aos tipos penais previstos.

Em uma abordagem sobre ilícitos informáticos que violam a privacidade na *web*, cita-se, dentre outras condutas:

> *a)* ***spamming****, como forma de envio não-consentido de mensagens publicitárias por correio eletrônico* a uma massa finita de usuários da rede, conduta esta não oficialmente criminal, mas antiética; A partir de 1980, ressalta a autora o aumento de ações criminosas que passaram a incidir em manipulações de caixas bancárias, pirataria de programas de computador, abusos nas telecomunicações etc., revelando vulnerabilidade que os cria-

dores do processo não haviam previsto. Acrescente-se, ainda, o delito de pornografia infantil na rede, igualmente difundido na época. 70 R. CEJ, Brasília, n. 20, p. 67-73, jan./mar. 2003.

b) ***cookies***, a quem chama "biscoitinhos da *web*", *pequenos arquivos de textos que são gravados no computador do usuário pelo* browser *quando ele visita determinados* sites *de comércio eletrônico*, de forma a identificar o computador com um número único, e obter informações para reconhecer quem está acessando o *site*, de onde vem, com que periodicidade costuma voltar e outros dados de interesse do portal;

c) ***spywares***, como *programas espiões que enviam informações do computador do usuário da rede para desconhecidos*, de maneira que até o que é teclado é monitorado como informação, sendo que alguns *spywares* têm mecanismos que acessam o servidor assim que usuário fica *on-line* e outros enviam informações por *e-mail*;

d) ***hoaxes***, como sendo *emails que possuem conteúdos alarmantes e falsos, geralmente apontando como remetentes empresas importantes ou órgãos governamentais*, como as correntes ou pirâmides, *hoaxes* típicos que caracterizam crime contra a economia popular, podendo, ainda, estar acompanhadas de vírus;

e) ***sniffers***, programas espiões, assemelhados aos *spywares*, que, introduzidos no disco rígido, visam a rastrear e reconhecer *e-mails* que circundam na rede, de forma a permitir o seu controle e leitura;

f) ***trojan horses*** ou cavalos de tróia, que, uma vez instalados nos computadores, abrem suas portas, tornando possível a subtração de informações, como senhas, arquivos etc (ROSSINI, 2006, p. 56).

Sobre o cavalo de tróia, o autor complementa que

embora o usuário possa recebê-lo de várias maneiras, na maioria das vezes ele vem anexado a algum e-mail. Este vem acompanhado de mensagens bonitas que prometem mil maravilhas se o arquivo anexado for aberto. Uma vez aberto o arquivo, o trojan horse se instala no computador do usuário. Na maioria das vezes, tal programa ilícito vai possibilitar aos hackers o controle total da sua máquina. Poderá ver e copiar todos os arquivos do usuário, descobrir todas as senhas que ele digitar, formatar seu disco rígido, ver a sua tela e até mesmo ouvir sua voz se o computador tiver um microfone instalado.

Considerando-se que boa parte dos computadores é dotada de microfones ou câmaras de áudio e vídeo, observa-se que o cavalo de tróia permite a possibilidade de se fazer escuta ambiente clandestina, arma poderosa nas mãos de criminosos que visam à captura de segredos industriais (ROSSINI, 2006, p. 56).

Para vários doutrinadores não há uma definição de caráter universal própria de delito informático, apesar dos esforços dos *experts* que têm se ocupado do tema, e, enquanto não existe a concepção universal, foram formulados conceitos funcionais atendendo a realidades nacionais concretas.

A rede mundial de computadores notadamente modificou hábitos e costumes de toda a sociedade, combinando comportamentos tradicionais com o acesso à informação e cultura, tornando-se motivo de inquietude, uma vasta área para as mais variadas atividades ilícitas, criminalidade esta caracterizada pela dificuldade de investigação, prova e aplicação da lei penal, pelo caráter transnacional e ilimitado dessas condutas, o que pode gerar conflitos de Direito Internacional, em decorrência da competência da jurisdição sancionadora.

## *5. Alguns tipos de crimes eletrônicos e suas configurações*

### *5.1. Furto*

O Código Penal Brasileiro, em seu artigo 155 prevê as seguintes disposições:

> 155 – Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena: reclusão de 1 a 4 anos e multa.
> § 1.º – a pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
> § 2.º – se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
> § 3.º – equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.
> Furto qualificado
> § 4.º – a pena é de reclusão de dois a oito anos e multa se o crime é cometido:
> I – com destruição ou rompimento de obstáculo à subtração da coisa;
> II – com abuso de confiança, ou mediante fraude, escalada ou destreza;
> III – com emprego de chave falsa;
> IV – mediante o concurso de duas ou mais pessoas.
> § 5.º – a pena é de reclusão de três a oito anos, se a subtração for de veículo automotor que venha a ser transportado para outro Estado ou para o exterior.

Várias são as condutas estipuladas pelo artigo 155 do Código Penal Brasileiro e uma destas condutas necessariamente abrange os delitos de furtos cometidos pela internet.

Para Greco, furto é

> subtração patrimonial não violenta para si ou para outrem de coisa alheia móvel. Percebe-se, portanto, que o mencionado tipo penal é composto por vários elementos, a saber: o núcleo *subtrair;* o especial fim de agir caracterizado pela expressão *para si ou para outrem*; bem como pelo objeto da subtração, ou seja, a coisa alheia móvel (GRECO, 2007, p. 59).

A principal característica dos crimes eletrônicos cometidos por meio da internet é a facilidade de se penetrar em bancos de informações de usuários. O crime de furto através da internet vem se alastrando a cada dia por ser de fácil manipulação os mais diversos sistemas de senhas eletrônicas e operacionais.

Como exemplo do crime de furto ocorrido pela internet, podemos citar o furto em contas correntes bancárias ocorridos em detrimento de envios de SPAMs, em que os infratores utilizam desta ferramenta, enviando mensagens com assuntos do tipo "veja você na foto da turma de 2000', ou "você lembra de mim, sou o fulano", ou mensagens de operadoras de telefonia móvel, da receita federal pedindo atualização de dados, entre outras. Desta forma os infratores conseguem as senhas bancárias eletrônicas, sendo que por meio delas fazem transferências de valores monetários para outras contas, às quais eles já têm acesso. Assim delito já se encontrara configurado.

### *5.2. Estelionato*

O estelionato é outro tipo de crime que ocorre muito pela internet, e que também está previsto no Código Penal Brasileiro, em específico no artigo 171, que diz:

> Art. 171 – Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.
> § 1.º – Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.
> § 2.º – Nas mesmas penas incorre quem:

***Disposição de coisa alheia como própria***

I – vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;

***Alienação ou oneração fraudulenta de coisa própria***

II – vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;

***Defraudação de penhor***

III – defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;

*Fraude na entrega de coisa*

IV – defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;

***Fraude para recebimento de indenização ou valor de seguro***

V – destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as conseqüências da lesão ou doença, com o intuito de haver indenização ou valor de seguro;

***Fraude no pagamento por meio de cheque***

VI – emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento.

§ 3º – A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

Para Greco,

> o crime de estelionato é regido pelo binômio vantagem ilícita/prejuízo alheio. A conduta do agente, portanto deve ser dirigida a obter vantagem ilícita, em prejuízo alheio. Ilícita é a vantagem que não encontra amparo no ordenamento jurídico, sendo, na verdade, contrária a ele. Além da vantagem ilícita obtida pelo agente com o seu comportamento, a vítima sofre prejuízo, também de natureza econômica. Assim poderá tanto perder aquilo que já possuía, ou mesmo deixar de ganhar o que lhe era devido (GRECO, 2007, p. 87).

Geralmente os crimes de estelionato via internet são direcionados para a aquisição de mercadoria sem o respectivo pagamento, bem como para a simulação do encaminhamento da mercadoria, após o pagamento prévio feito pela vítima. O estelionato

praticado na Internet se expandiu muito após a criação de sites conhecidos como "balcão de negócios". Podemos citar o mercado livre, em que os usuários anunciam diretamente as mercadorias na internet, como se fossem pessoas físicas.

Ressalta-se que todas as condutas, apesar de não termos legislação específica, podem perfeitamente serem amoldadas aos tipos penais existentes.

### *5.3. Crimes contra a honra*

A internet é um meio eletrônico de fácil manuseio e acessado por milhões de pessoas todos os dias. As correspondências escritas no papel têm sido deixadas de lado e, portanto, o meio instrumental pelo computador passa a ser muito usado na troca de mensagens das mais variadas.

Dentro deste limiar, os crimes contra a honra tomam evidência na medida em que as pessoas imputam às outras condutas ou comportamentos que por vezes eles não fazem, cometendo aquelas algum tipo penal especificado como crime, seja a calúnia, a injúria ou a difamação. O Código Penal Brasileiro, sobre os crimes contra a honra, em seu Capítulo V, nos artigos 138, 139 e 140, traz em seu bojo o seguinte:

> Art. 138 – Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena – detenção, de 6 (seis) meses a 2 (dois) anos, e multa.
> § 1.º – Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2.º – É punível a calúnia contra os mortos.
> *Exceção da verdade*
> § 3º – Admite-se a prova da verdade, salvo:
> I – se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
> II – se o fato é imputado a qualquer das pessoas indicadas no n.º I do art. 141;
> III – se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.
> **Art. 139 –** Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
> *Exceção da verdade*
> 38 § 3.º acrescentado pela Lei n.º 8.069, 13.07.90.
> Parágrafo único – A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.
> *Injúria*

**Art. 140** – Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

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

§ 1.º - O juiz pode deixar de aplicar a pena:

I – quando o ofendido, de forma reprovável, provocou diretamente a injúria;

II – no caso de retorsão imediata, que consista em outra injúria.

§ 2.º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:

Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa, além da pena correspondente à violência.

§ 3.º – Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência.

Pena – reclusão de 1 (um) a 3 (três) anos e multa".

Segundo Greco (2007, p. 37), "a honra é um bem constitucionalmente inviolável, amparado pelo inciso X, do art. 5.º da Constituição Federal. É um conceito que se constrói durante toda uma vida e que pode, em virtude de apenas uma única acusação leviana, ruir imediatamente".

Como se vê, a honra é um dos bens jurídicos mais sutis e mais difíceis de se apreender. A existência de um ataque à honra engloba diversos fatores, dentre eles a situação dos sujeitos ativo e passivo, o tipo de relação mantida entre eles, as circunstâncias em que se deram os fatos, a cultura intelectual dos envolvidos, entre outros.

Assim, tais delitos ocorrem com muita frequência pela internet, seja pelo Orkut, quando o agente utiliza a imagem da vítima em perfis falsos e que denigram a honra pessoal dessa vítima; ou inserindo comentários inverídicos ou indecorosos sobre alguém ou divulgando imagens da vítima de que tenha o poder, em decorrência de algum tipo de relacionamento que manteve ou ainda mantém com essa vítima.

## *6. Responsabilidade dos entes*

Com base em tudo que aqui foi exposto, um assunto intrigante e ao mesmo tempo valoroso, é o modo pelo qual os entes administram os canais de relacionamento pela internet. Os provedores, os sites de relacionamentos, os sites de gerenciamentos de contas de e-mails e sites de intermediação de compra e venda, não exigem dos usuários muitas informações quando do acesso e cadastro desses nos sites referidos. Não ocorre, como, por exemplo, quando se efetua uma compra diretamente na loja ou se

abre uma conta em um banco, quando inúmeros dados e informações pessoais do comprador são exigidos. Em alguns casos, há, inclusive, a solicitação de referências pessoais que possam informar sobre a pessoa daquele que pretende realizar a compra.

Os provedores e gerenciadores chegam até mesmo a inserir nas informações do cadastro do usuário que todos os dados prestados são de inteira responsabilidade do usuário, não cabendo qualquer tipo de responsabilidade por parte dos provedores e dos gerenciadores.

Não obstante os provedores, gerenciadores e administradores furtarem-se de sua responsabilidade perante sua ineficácia em exigir dados e informações dos usuários e checar a veracidade de tais dados e informações, entende-se que esses entes possuem responsabilidades diante da ocorrência de delitos e prejuízos causados às vítimas dos crimes eletrônicos.

Nos casos da prática de fatos típicos, pode-se considerar a responsabilidade dos entes citados (provedores, administradores e gerenciadores de rede), no sentido de coautoria ou participação nos delitos, conforme art. 29 do Código Penal Brasileiro, que diz o seguinte:

> **Art. 29 -** Quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida de sua culpabilidade.
> § 1.º – Se a participação for de menor importância, a pena pode ser diminuída de um sexto a um terço.
> § 2.º – Se algum dos concorrentes quis participar de crime menos grave, ser-lhe-á aplicada a pena deste; essa pena será aumentada até metade, na hipótese de ter sido previsível o resultado mais grave.

No entendimento de Welzel (1987, apud Greco, 2007), a respeito da coautoria, revela-se o seguinte:

> A co-autoria é autoria; sua particularidade consiste em que o domínio do fato unitário é comum a várias pessoas. Co-autor é quem possuindo as qualidades pessoais de autor é portador da decisão comum a respeito do fato e em virtude disso toma parte na execução do delito.

Sobre a coautoria:

> São conhecidos como participes aqueles que atuam como coadjuvantes na história do

> crime. O autor é o protagonista na infração penal, quem exerce o papel principal. Contudo, não raras as vezes, o protagonista pode receber o auxílio daqueles que, embora não desenvolvendo as atividades principais, exercem papéis secundários, mas que influenciam na prática da infração penal (GRECO, 2007, p. 42).

Desta forma conclui-se perfeitamente cabível a coautoria ou a participação dos provedores e gerenciadores de sistemas e redes nos chamados delitos eletrônicos, uma vez que suas condutas omissivas, no sentido do baixo controle que exercem sobre os dados e informações dos usuários, constituem, em não raras vezes, fator preponderante para a facilitação do cometimento de delitos pela internet.

Ainda há a possibilidade da responsabilidade objetiva dos provedores e gerenciadores, nos casos em que as ações praticadas pelos infratores que se utilizam da internet para a consecução de suas condutas reprováveis acarretarem algum tipo de demanda ou pleito na área cível, como por exemplo, na reparação de danos morais.

Neste sentido:

> A lei impõe, a certas pessoas, em determinadas situações, a reparação de um dano cometido sem culpa. Quando isto acontece, diz-se que a responsabilidade é legal ou objetiva, porque prescinde da culpa e se satisfaz apenas com o dano e o nexo de causalidade. Esta teoria, dita objetiva ou do risco, tem como postulado que todo dano é indenizável, e deve ser reparado por quem a ele se liga por um nexo de causalidade, independentemente de culpa. Nos casos de responsabilidade objetiva não se exige prova de culpa do agente para que seja obrigado a reparar o dano (GONÇALVES, 2006, p. 63).

Nesse entendimento, apesar de, na grande maioria dos casos, não ser a intenção do provedor ou gerente promover ou facilitar a promoção de dano aos direitos e bens jurídicos tutelados das pessoas que se utilizam da internet, sua conduta, no sentido de pouco exigir e de pouco fiscalizar os dados e informações de pessoas que fazem usos de seus serviços, liga-se, por nexo de causalidade, ao resultado de dano praticado, sendo, portanto, objetiva a sua responsabilidade.

Ainda na discussão sobre a responsabilidade, cível e penal, de entes ou pessoas que possam facilitar a prática de delitos ou condutas diversas reprováveis pelo ambiente da internet, há que se ressaltar a figura dos proprietários ou administradores das conhecidas *lan houses*.

Aqueles que são proprietários ou responsáveis por este tipo de comércio de-

vem primar pelo controle das informações referentes às pessoas que desse serviço fazem uso. Tal controle deve ser feito de forma a verificar, confirmar e controlar os dados pessoais das pessoas que frequentam esse tipo de estabelecimento comercial.

No caso de um delito praticado na internet, identificando-se o número do IP da máquina utilizada para a prática do crime, é possível atribuir sua responsabilidade ao proprietário ou usuário da máquina. Nesse sentido, com o controle das informações pessoais e horários de utilização, mesmo os delitos praticados no ambiente das *lan houses*, será possível a identificação do autor.

Considerando-se ainda a responsabilidade dos proprietários ou administradores de *lan house,* deve-se considerar o crime disposto no artigo 241 da lei 8069/90, que trata do Estatuto da Criança e do Adolescente, observando-se as proibições referentes à utilização dos computadores por crianças e/ou adolescentes para o acesso a sites considerados de cunho pornográfico, bem como a propagação de imagens desta natureza, que envolvam crianças e/ou adolescentes. Prevê esse dispositivo legal:

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente: (Redação dada pela Lei n.º 10.764, de 12.11.2003)
> Pena – reclusão de 2 (dois) a 6 (seis) anos, e multa.
> §1.º Incorre na mesma pena quem: (Incluído pela Lei n.º 10.764, de 12.11.2003)
> I – agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;
> II – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do caput deste artigo;
> III – assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do caput deste artigo.
> § 2.º A pena é de reclusão de 3 (três) a 8 (oito) anos: (Incluído pela Lei nº 10.764, de 12.11.2003)
> I – se o agente comete o crime prevalecendo-se do exercício de cargo ou função;
> II – se o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial.

Conclui-se assim, na mesma linha de raciocínio referente aos provedores e gerenciadores de rede, que o proprietário e o administrador dos estabelecimentos denominados *lan house* são também responsáveis pelo controle e fiscalização das pessoas

que se utilizam de seus computadores para a prática de delitos eletrônicos, ainda sujeitos a prática de outras condutas, também típicas e puníveis, de várias outras formas, como, por exemplo, o citado no Estatuto da Criança e do Adolescente.

## *7. Conclusão*

Conclui-se com este trabalho que a internet é uma ferramenta mundial de grande utilidade e eficácia para as sociedades de todo o mundo atual, considerando-se o contexto globalizado em que vivemos. A velocidade, a comodidade e a praticidade proporcionada pelos serviços disponíveis na rede mundial tornam mais viáveis as comunicações entre pessoas, setores, instituições e até mesmo entre países em todo o mundo, proporcionando uma economia de tempo na vida de uma sociedade, bem como quebrando barreiras até então intransponíveis.

Não pode, porém, um meio tão moderno e com alto grau de tecnologia ser utilizado como meio tão rápido para a prática de atos delituosos, proporcionando tamanho anonimato aos detratores da lei.

As pessoas que desse meio de comunicação se utilizam não podem empreender-se do conceito de que, ao praticar um crime ou ato lesivo a outra pessoa utilizando-se, para isto, o meio virtual, estão simplesmente fazendo algo errado. Devem incutir-se de que estão ferindo gravemente um ou vários direitos e bens jurídicos de outrem. Sua conduta é tão lesiva quanto a de quem pratica condutas da mesma natureza pelos meios convencionais já utilizados, com o agravante de serem revestidos da figura reprovável do anonimato e da facilidade de não deixarem quaisquer indícios capazes de identificar sua autoria.

Apesar de os crimes eletrônicos constituírem temas centrais de discussões recentes, percebe-se que é possível a análise das condutas típicas praticadas no meio eletrônico embasando-se nos dispositivos legais já existentes no ordenamento jurídico pátrio. Não se faz, portanto, necessária a criação de nova legislação que trate dos chamados crimes eletrônicos, uma vez que se pode recorrer aos tipos penais e legislações esparsas já existentes ao analisar as condutas criminosas praticadas na rede mundial.

Há que se ressaltar, porém, que a sociedade hoje vive em constantes mudanças e evoluções, as quais nem sempre ocorrem no sentido de proporcionar melhoria e progresso. Os crimes também se modificam e evoluem, não sendo possível prever meios para se praticar um delito daqui a alguns anos, por exemplo. Assim, futuramente e em

decorrência do surgimento de novas tecnologias, poder-se-á deparar com a necessidade de criação de legislação que regule o assunto. Hoje, já há que se falar em algumas interpretações por analogia, quando se recorre à legislação existente para a análise da prática dos crimes eletrônicos.

Conclui-se, ainda, a inegável responsabilidade, civil e penal, dos entes que proporcionam a funcionalidade do ambiente da rede, bem como daqueles que de alguma forma contribuem para facilitação da prática de crimes eletrônicos. Desta forma, são responsáveis, tanto quanto os autores dos delitos praticados, os provedores e gerenciadores de rede, proprietários e administradores dos estabelecimentos denominados *lan house*, quando, devido a sua conduta omissiva e inerte perante a consecução e a fiscalização de dados e informações pessoais dos usuários, acabam por propiciar aos agentes meios eficazes e garantidores do anonimato na prática de delitos.

Assim, pretendeu este trabalho sensibilizar aqueles que se utilizam de diversos serviços oferecidos pela rede mundial de computadores, sobre a possibilidade de serem vitimados pelas condutas delituosas praticadas no meio eletrônico. Ainda, buscou-se fomentar a discussão a respeito dos tipos de crimes praticados nesse meio, além da responsabilidade por tais práticas, daqueles que com ela possam contribuir.

## *8. Referências*

BICUDO, Hélio. *Direitos Humanos e sua Proteção*. São Paulo: FDT, 1998.

BITENCOURT, Cezar Roberto. *Código Penal Comentado.* São Paulo: Saraiva, 2002.

BOBBIO, Norberto. *Liberalismo e Democracia*. São Paulo: Brasiliense, 1988.

BRASIL. *Constituição da República Federativa do Brasil***.** 1988. Coleção Saraiva de Legislação. 40 ed. São Paulo: Saraiva, 2007, 447p.

BRASIL. Decreto Estadual nº 43.778/04, de 12/04.04. Dispõe sobre ações de integração entre as instituições policiais do Estado de Minas Gerais. Publicado no Minas Gerais - Diário do Executivo, Belo Horizonte, no dia 13/04/2004, na pág. 01, coluna 01.

BRASIL. Lei 8069 (Estatuto da Criança e do Adolescente). 1992. Coleção saraiva de Legislação. 40 ed. São Paulo: Saraiva, 2007.

CAPEZ, Fernando. *Curso de Processo Penal*. 13 ed. rev. e atual. São Paulo: Saraiva, 2006.

FERREIRA, Ivette Senise. *A criminalidade informática***,** in: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). *Direito e internet:* aspectos jurídicos relevantes. Bauru: Edipro, 2000, p. 207-237.

FOUCAULT, Michael. *Vigiar e Punir*. Petrópolis: Vozes, 1977.

FRANCO, Alberto Silva e STOCO; Rui. *Código Penal e sua Interpretação Jurisprudencial*. Parte Especial. 7 ed. rev. e atual. e ampl. São Paulo: Revista dos Tribunais, 2001. v. 2.

GOMES, Flávio Luiz. *Crimes informáticos*. Disponível em: <www.direitocriminal.com.br>. Acesso em 26 out. 2008.

GONÇALVES, Victor Eduardo Rios. *Dos Crimes contra a Pessoa.* 8 ed. rev. e atual. São Paulo: Saraiva, 2006, v. 8.

GRECO, Rogério. *Curso Direito Penal: parte especial*. 4 ed. Niterói: Impetus, 2007.

JANE MORSE. *EUA intensificam esforços pela liberdade na internet no mundo todo.* Disponível em: http://embaixadaamericana.org.br/index.php?action=materia&id=5069&submenu=padr>. Acesso em: 24 out. 2008.

MAGALHÃES, José Luiz Quadros de. *Direito Constitucional, tomo I.* Belo Horizonte: Mandamentos, 2002.

MUNIZ, Jacqueline Proença Jr, Domício Diniz. *Uso da Força e Ostensividade na Ação Policial. Conjuntura Política:* Boletim de Análise do Departamento de Política da UFMG: Belo Horizonte, (Editora UFMG?), 1999.

PIOVESAN, Flávia Xavier; GOMES, Luiz Flávio. *O Sistema Interamericano de Proteção dos Direitos Humanos e o Direito Brasileiro.* São Paulo: RT, 2000.

PINHEIRO, Reginaldo César. *Os crimes virtuais na esfera jurídica brasileira.* São Paulo: IBCCrim, v. 101, p. 18-19, abr. 2001(separata).

ROSSINI, Augusto Eduardo de Souza. *Brevíssimas considerações sobre delitos informáticos.* São Paulo: ESMP, jul. 2002, p. 140 (Caderno Jurídico, ano 02, n. 04).

SOARES, Luiz Eduardo. *Meu Casaco de General*: Quinhentos dias no front da Segurança Pública do Rio de Janeiro. São Paulo: Cia das Letras, 2000.

S*obre o CGI.BR – Quem somos*. Disponível em: <http://www.cgi.br/sobre-cg/indez.htm>. Acesso em: 24 out. 2008.

*Sobre a internet*. Disponível em: < http://pt.wikipedia.org/wiki/Internet>. Acesso em: 27 out. 2008.

*Sobre a lan house*. Disponível em: < http://pt.wikipedia.org/wiki/Lan_house>. Acesso em: 27 out. 2008.

*Sobre a internet protocol*. Disponível em: <http://pt.wikipedia.org/wiki/Internet_protocol>. Acesso em: 27 out. 2008.

*Sobre o Orkut*. Disponível em: < http://pt.wikipedia.org/wiki/Orkut>. Acesso em: 27 out. 2008.

*Sobre o provedor*. Disponível em: <http://pt.wikipedia.org/wiki/Provedor>. Acesso em: 27 out. 2008

VELHO, Gilberto. *Desvio e Divergência:* uma crítica da Patologia Social. Rio de Janeiro: Editora Jorge Zahar, 1974.

VIANA, Túlio Lima. *Fundamentos do Direito Penal Informático*: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.

WACQUANT, Loic. *Punir os Pobres. A Nova Gestão da Miséria nos Estados Unidos*. 2 ed. Rio de Janeiro: Revan, 2003.

ZAFFARONI, Eugenio Raúl. *Globalização, Sistema Penal e Ameaças ao Estado Democrático de Direito.* Rio de Janeiro: Lumen Júris Ed. 2005.