CENTRO UNIVERSITÁRIO DO DISTRITO FEDERAL

RAPHAEL ROSA NUNES VIEIRA DE PAIVA

CRIMES VIRTUAIS

BRASÍLIA

2012

RAPHAEL ROSA NUNES VIEIRA DE PAIVA

CRIMES VIRTUAIS

Monografia de Conclusão de Curso apresentada à Coordenação de Direito do Centro Universitário do Distrito Federal – UDF. Instituto de Ciências Sociais, para obtenção do título de Bacharel em Direito.

Orientador. Profº.Valdinei Coimbra

Brasília

2012

RAPHAEL ROSA NUNES VIEIRA DE PAIVA

CRIMES VIRTUAIS

Monografia de Conclusão de Curso apresentada à Coordenação de Direito do Centro Universitário do Distrito Federal – UDF. Instituto de Ciências Sociais, para obtenção do título de Bacharel em Direito.

Nota de Aprovação:_____

Brasília, _____ de _____ de 2012.

Banca Examinadora

_____
Valdinei Cordeiro Coimbra
Orientador
Centro Universitário do Distrito Federal

_____
Professor (a) Examinador (a)
Centro Universitário do Distrito Federal

_____
Professor (a) Examinador (a)
Centro Universitário do Distrito Federal

Dedico este trabalho à minha mãe, meus irmãos, e, minha esposa, a vocês, meu muito obrigado, fica aqui registrada minha eterna gratidão pelo apoio nos momentos em que as palavras de vocês fizeram meus passos se tornarem firmes.

AGRADECIMENTO

Professor Valdinei Coimbra, meus sinceros agradecimentos, pela atenção, pelas orientações e pelo tempo compartilhado.

SUMÁRIO

RESUMO

O direito está ligado a evolução da sociedade, conforme a sociedade se desenvolve o direito vai se adequando aos anseios da mesma, novas normas são elaboradas para se regular a convivência, sendo assim, com o avanço da tecnologia e sua inserção no cotidiano das pessoas, é que se fez a necessidade do direito regular as relações que passaram a serem desenvolvidas em ambiente virtual, o presente trabalho versa sobre estas questões, mais precisamente sobre os crimes virtuais, ou seja, os crimes que passaram a ser perpetuados em ambiente virtual, se busca verificar as formas de se analisar um crime virtual, a busca de sua autoria, suas peculiaridades, e o que a legislação nacional e internacional já versa sobre o assunto, e o que existe hoje de projetos de lei sobre o assunto. Ao longo do trabalho utilizaremos alguns termos que são típicos de usuários já familiarizados com o ambiente cibernético, o uso é proposital, pois assim busca-se familiarizar o leitor com os termos deste mundo digital.

Palavras-chave: Direito. Crimes Virtuais. Ambiente Virtual. Tecnologia.

ABSTRACT

The right is on the evolution of society, as society develops the right will be fitting the same expectations of new standards are designed to regulate coexistence, so with the advance of technology and its integration into the daily to be developed in a virtual environment, this paper discusses these issues, specifically about cyber-crime, or crimes that came to be perpetuated in a virtual environment, if seeks to verify the ways of analyzing a virtual crime, the pursuit of his own, peculiarities, and that the national and international legislation already deals with the subject, and what exists today of bills on the subject. Throughout the paper we use some terms that are typical for users already familiar with the cyber environment, the use is deliberate, as well seek to familiarize the reader with the terms of this digital world.

Keywords: Right. Virtual Crimes. Virtual Environment. Technology.

INTRODUÇÃO

O mundo globalizado e a crescente evolução tecnológica fez com que as distancias fossem encurtadas, e as relações entre as pessoas passassem a serem feitas na maior parte das vezes utilizando equipamentos eletrônicos conectados a internet, culturas diferentes passaram a se encontrar na rede mundial de computadores, novas relações sociais passaram a surgir nesta Era digital, razão pela qual o Direito deve se moldar a esta nova realidade, caminhar junto com a Segurança da Informação, para que esta nova sociedade digital não se torne uma sociedade a margem do controle Estatal.

O presente trabalho foi objeto de uma pesquisa frente aos principais autores que discorrem sobre a relação do Direito Penal com os crimes que ocorrem em ambientes virtuais, utilizando para tanto o método dedutivo, sendo que foi feita uma pesquisa bibliográfica a partir de um material que já versava sobre o assunto, constituído de livros e artigos disponíveis em sítios na internet.

O trabalho foi desenvolvido em sete capítulos, o qual se buscou responder a problemática de quais os principais crimes praticados na internet? como o ordenamento jurídico pátrio e o de outros países trata sobre os crimes perpetuados na internet? O que já vem sendo feito no nosso ordenamento jurídico para abranger os crimes virtuais? No primeiro capitulo buscou-se demonstrar a evolução do direito digital, desde o surgimento da primeira maquina a vapor até o nascimento do primeiro computador, sendo que posteriormente mostrou-se a definição do que é ou não um delito virtual, ou crime virtual.

No segundo capitulo foi feita a classificação dos crimes virtuais, de acordo com a doutrina que versa sobre o assunto, e, a classificação dos crimes de acordo com a conduta do agente.

O terceiro capítulo foi destinado a analisar algumas condutas criminosas que são realizadas com o uso de equipamentos eletrônicos, e muitas das vezes tendo a Internet como caminho para execução destes crimes,

no quarto e no quinto capítulo foi feito um apanhado da legislação nacional frente aos crimes virtuais, o que a atual legislação abarca para reprimir as condutas dos criminosos, os projetos de lei existentes, as propostas que já existem no Congresso Nacional a respeito do tema, e, uma analise de algumas legislações internacionais que versam sobre o assunto.

No sexto e sétimo capítulo, foi realizada uma pesquisa nos principais doutrinadores que dominam o assunto concernente aos crimes virtuais, a qual se buscou demonstrar a dificuldade em se apurar um crime que se desenrola em ambiente virtual, visto que não há fronteira entre os usuários que se relacionam na internet, e, qual é a lei que deve ser aplicada quando se realiza um crime em ambiente virtual.

1 SURGIMENTO DOS CRIMES VIRTUAIS

Os computadores surgiram para facilitar nosso dia a dia, as tarefas que antes eram realizadas em espaços de tempo muito longos, passaram a ser realizadas quase de forma instantânea, o computador é uma maquina que armazena e transforma informações, sob o controle de instruções predeterminadas.[1]

1.1 HISTÓRICO

Desde os primórdios até os dias atuais, o homem vem buscando desenvolver novas máquinas e ferramentas que lhe torne as atividades do dia a dia mais fáceis e de certa forma mais prazerosas.

Uma alteração significativa que o mundo experimentou foi a Revolução Industrial, a qual modificou as feições do mundo moderno, alterou o modo de vida da população mundial, e, trouxe avanço significativo na mudança do homem do campo para as cidades, iniciou primeiramente no Reino Unido, por volta do século XVIII, talvez porque a Inglaterra possuísse grandes reservas de carvão mineral em seu subsolo, a principal fonte de energia para que as máquinas daquele período[2].

As maquinas começaram a surgir em larga escala, as cidades começaram a se desenvolver, os trabalhadores que antes trabalhavam de forma artesanal passaram a controlar máquinas, as fábricas passaram a produzir cada vez mais, e as novas invenções, navios e locomotivas a vapor, fizeram com que a circulação das mercadorias se tornasse cada vez mais rápido, fazendo com que as matérias primas chegassem mais rapidamente as pessoas, e começaram a surgir de forma mais expressiva os inventores que viriam a mudar a maneira que vemos o mundo.

---

[1] **FRAGOMENI**, Ana Helena. **Dicionário Enciclopédico de Informática**. Vol.I. Rio de Janeiro: Campus, 1987, p.125

[2] **SUAPESQUISA – Formulários e Pesquisas Online**. Revolução Industrial, História da Revolução Industrial, pioneirismo inglês, invenções de máquinas, passagem da manufatura para a maquinofatura, a vida nas fábricas, origem dos sindicatos. Disponível em: <http://www.suapesquisa.com/industrial>. Acesso em: 24 abr. 2012.

Podemos citar grandes invenções, como por exemplo, a Fotografia (1839), Telefone (1876), Luz Elétrica (1879), Televisão (1924), dentre outras tantas invenções que alteraram a forma como as pessoas viviam na época em que surgiram estes inventos, e de certa forma, o modo o qual vivemos hoje[3].

O primeiro computador digital eletrônico foi o ENIAC, desenvolvido em 1946, o qual a sigla significa *Eletronic Numerical Integrator and Calculator*, o qual o desenvolvimento foi todo por parte do exército norte-americano o equipamento pesava por volta de 30 toneladas, e media cerca de 140 metros quadrados[4].

O primeiro computador com mouse e interface gráfica é lançado pela Xerox, em 1981; já no ano seguinte, a Intel produz o primeiro computador pessoal 286, desde o surgimento do primeiro computador até os dias atuais a sociedade vive em constante mudança, mudamos dos escritos nas cavernas para o papel, do uso da pena com tinta ao código Morse, do e-mail para a videoconferência[5].

No meio desta onda de transformações surgiu a internet, por volta da década de 60, aproximadamente no ano de 1996, algumas universidades se uniram para desenvolver a ARPANET (*Advanced Research Projects Administration* – Administração de Projetos e Pesquisas Avançados) primeiramente o surgimento da internet se deu por uma necessidade militar, pois naquela época estava retratado o cenário da Guerra Fria[6].

Conforme definição de Zanellato[7], “A Internet é um suporte (ou meio) que permite trocar correspondências, arquivos, idéias, comunicar em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos”.

A Internet é uma Rede de computadores, integrada por outras Redes menores, comunicando entre si, os computadores se comunicam

---

[3] **SUPERDICAS** - Invenções que mudaram o mundo e sobreviveram ao tempo. Disponível em: <http://www.superdicas.com.br/almanaque/almanaque.asp?u_action=display&u_log=254>. Acesso em: 24 abr. 2012.
[4] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.30.
[5] **PECK**, Patrícia. **Direito digital**. São Paulo: Saraiva, 2002.p.13.
[6] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.30.
[7] **ZANELLATO**, Marco Antonio. **Condutas Ilícitas na sociedade digital**, Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet, n. IV, Julho de 2002.p. 173.

através de um endereço lógico, chamado de *endereço IP*, onde uma gama de informações são trocadas, surgindo ai o problema, existe uma quantidade enorme de informações pessoais disponíveis na rede, ficando a disposição de milhares de pessoas que possuem acesso à internet, e quando não disponíveis pelo próprio usuário, são procuradas por outros usuários que buscam na rede o cometimento de crimes, os denominados *Crimes Virtuais*[8].

Lévy[9], em sua obra *Cyberdémocracie: Essai de Philosophie Politique,* já havia identificado um crescente aumento por parte das pessoas que utilizavam a internet, e já previa um aumento substancial, tendo em vista o desenvolvimento de novas tecnologias, interfaces de comunicação sem fios, e o uso integrado de dispositivos portáteis.

Lévy estava certo, hoje a internet está disponível em vários dispositivos portáteis, das mais diferentes formas, milhares de pessoas permanecem por vezes mais tempo navegando na internet do que vivendo o mundo real, mídias sociais, leitura de livros, videoconferências, em fim, a rede mundial de computadores é acima de tudo uma rede mundial de Indivíduos, onde existem relações jurídicas fluindo, o Direito deve trazer soluções para os litígios que venham a ocorrer dentro deste ambiente virtual, o Direito é uma solução prática de planejamento e estratégia que só pode ser feita em equipe, num contato direto com as demandas e a própria evolução da sociedade, o Direito deve adaptar-se as demandas, os anseios da sociedade, onde as transformações são cada vez mais rápidas[10].

Os primeiros crimes de informática começaram a ocorrer na década de 70[11], na maioria das vezes era praticado por especialistas em informática, o qual o objetivo era driblar os sistemas de seguranças das empresas, com um foco principal nas instituições financeiras. Atualmente o perfil das pessoas que praticam crimes de informática já não são as mesmas da década de 70, os usuários mudaram, hoje em dia qualquer pessoa que tenha um conhecimento

---

[8] **INELLAS**, Gabriel Cesar Zaccaria. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004.p.3.
[9] **LEMOS**, André/LÉVY, Pierre. **O futuro da Internet: em direção a uma ciberdemocracia**. São Paulo: Paulus, 2010.p.10.
[10] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.44 e 45.
[11] **CERT.BR** - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <http://www.cert.br>. Acesso em: 10 mar. 2012.

não tão aprofundado, mas que tenha acesso à internet pode praticar algum crime de informática, o usuário doméstico hoje já tem um conhecimento bem maior sobre o uso de computadores e tecnologia voltada para internet.

1.2 CONCEITOS DE CRIMES DE INFORMÁTICA

Os crimes de informática são aqueles perpetrados através dos computadores, contra os mesmos, ou através dele. A maioria dos crimes são praticados através da internet, e o meio usualmente utilizado é o computador[12].

Podemos conceituar o termo computador[13] como:

> Máquina capaz de receber, armazenar e enviar dados, e de efetuar, sobre estes, seqüências previamente programadas de operações aritméticas (como cálculos) e lógicas (como comparações), com o objetivo de resolver problemas.

Os Crimes digitais podem ser conceituados como sendo às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros[14].

As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia, crimes de computação, delitos de informática, abuso de computador, fraude informática, em fim, os conceitos ainda não abarcam todos os crimes ligados à tecnologia, e, portanto, deve-se ficar atento quando se conceitua determinado crime, tendo em vista que existem muitas situações complexas no ambiente virtual[15].

---

[12] **CASTRO**, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003, p.9.
[13] **HOLANDA FERREIRA**, Aurélio Buarque de. **Novo dicionário da língua portuguesa**. 2ª Ed. Rio de Janeiro: Nova Fronteira, 2000.p.1016
[14] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.46
[15] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.48

Embora existam as divergências doutrinárias quanto a conceituar os crimes praticados em meio eletrônico, há uma grande leva de doutrinadores que os conceitua como “crimes digitais”.

A verdade é que a denominação dos delitos deve ser feita de acordo com o bem jurídico protegido, conforme diz Fragoso[16]:

> A Classificação dos crimes na parte especial do código é questão ativa, e é feita com base no bem jurídico tutelado pela lei penal, ou seja, a objetividade jurídica dos vários delitos ou das diversas classes de intenções.

Portanto, ao analisar um crime como sendo de informática, é necessário uma analise inicial, primeiramente para verificar se o mesmo é um *cibercrime* ou não, e depois aplicar o tipo penal correspondente, tendo em vista o bem jurídico tutelado.

[16] **FRAGOSO**, Heleno Cláudio. **Lições de direito penal**: parte especial: arts. 121 a 212 do CP. Rio de Janeiro: Forense, 1983.p.5

2 DOS CRIMES DE INFORMÁTICA E SUAS CATEGORIAS

Hoje a cada dia cresce o numero de pessoas que acessam a internet, existem mais de 800 mil *websites* na internet, e a cada dia são criadas mais de mil *homepages* por dia[17], na internet hoje se encontra basicamente tudo, desde comprar um eletrônico qualquer, até mesmo concluir um curso universitário pela internet, o que acontece é que os usuários que ali se encontram estão sujeitos aos mais variados crimes, estes, que não encontram barreiras para se perpetuarem por toda a rede, deixando estragos imensos na vida dos internautas de boa fé.

A constatação de um crime digital e sua posterior classificação não é uma tarefa fácil, tendo em vista que ainda existem poucas conclusões a respeito, e até porque a tecnologia evolui a passos largos, e ano após ano a opinião dos doutrinadores também muda conforme segue a evolução tecnológica.

Existem condutas que utilizam os computadores como meio para o cometimento dos delitos, e há casos em que sem o uso do sistema informático não seria possível a consumação de determinados crimes.

Tiedemann formulou em 1980 a seguinte Classificação dos delitos informáticos[18]:

a) Manipulações: podem afetar o *input (*entrada), o *output* (saída) ou mesmo o processamento de dados;
b) Espionagem: subtração de informações arquivadas abarcando-se, ainda, o furto ou emprego indevido de *software;*
c) Sabotagem: destruição total ou parcial de programas;
d) Furto de tempo: utilização indevida de instalações de computadores por empregados desleais ou estranhos.

Um conceito mais amplo na classificação foi feita por um doutrinador estrangeiro Rovira Del Canto, o qual subdividiu os delitos em Infrações à

[17] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.65.
[18] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.60

intimidade; ilícitos econômicos; ilícitos de comunicação pela emissão ou difusão de conteúdos ilegais ou perigosos; e, outros ilícitos[19].

Greco Filho[20] adota a seguinte divisão: condutas perpetradas contra um sistema informático, e, condutas perpetradas contra outros bens jurídicos, segue observação do autor.

> Focalizando-se a *Internet,* há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da *internet* e crimes ou ações que merecem incriminação praticados contra a *Internet,* enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou.

O Dr. Vladimir Aras[21] tem sua classificação da seguinte forma:

> a) uma primeira, onde estão substancialmente unidos pela circunstância que o computador constitui a necessária ferramenta de realização pela qual o agente alcança o resultado legal;
> b) a segunda categoria de crimes do computador, poderia incluir todos aqueles comportamentos ilegítimos que contestam os computadores, ou mais precisamente, seus programas;
> c) a última categoria deveria juntar todas as possíveis violações da reserva sobre a máquina. aqui entram em consideração as habilidades de colheita e elaboração de todo tipo de dados.

Em todas as classificações há distinções a considerar e pontos em comum, algumas posições atribuem os meios eletrônicos como objeto protegido (bem jurídico) e meios eletrônicos como meio/instrumento de se lesionar outros bens, está classificação torna-se umas das mais oportunas, tendo em vista que abarca mais opções acerca das práticas[22].

---

[19] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.61 e 62.

[20] **GRECO FILHO**, Vicente. **Algumas observações sobre o direito penal e a internet**. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

[21] **ARAS**, Vladimir. **Crimes de informática. Uma nova criminalidade**. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2250>. Acesso em: 18 mar. 2012.

[22] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.63

3 CRIMES POR MEIO DO COMPUTADOR E INTERNET

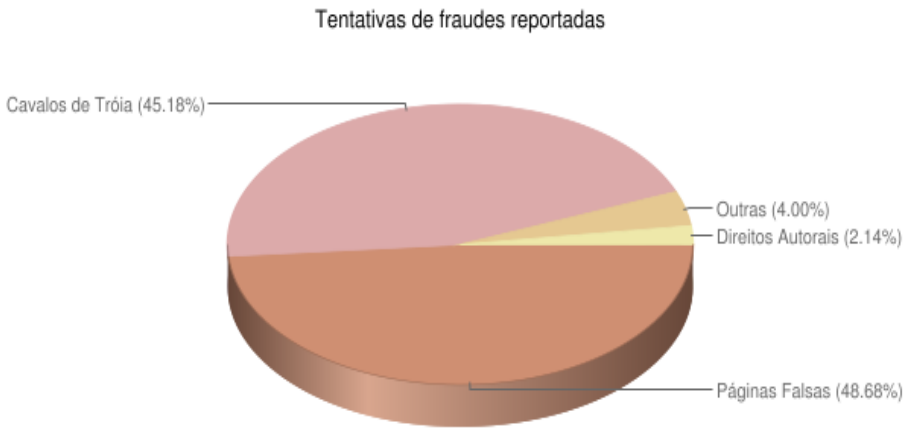
É uma tarefa árdua e delicada analisar as condutas criminosas que se alastram pela internet, uma vez que é extremamente difícil verificar onde o agente que praticou o crime se encontra, tendo em vista que os crimes digitais não encontram barreiras na internet e se perpetuam livremente pela rede.

A maioria dos crimes que ocorrem na rede também existem no mundo real, o que ocorre é que existem alguns crimes com algumas peculariedades, o que faz com que seja necessário uma adequação quanto ao seu tipo penal, abaixo analisaremos alguns crimes da era Digital e outros já existentes que passaram a ser executados virtualmente[23].

3.1 FRAUDES VIRTUAIS

Antes de adentrarmos no assunto Fraudes Virtuais, cabe analisar um dado importante sobre a quantidade de fraudes no Brasil, dados obtidos pela CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil[24].

Incidentes Reportados ao CERT.br - Janeiro a Dezembro de 2011



[23] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.294 e 295.
[24] **CERT.BR** - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2011. Disponível em: <http://www.cert.br/stats/incidentes/2011-jan-dec/fraude.html>. Acesso em: 31 mar. 2012.

Legenda:

- Cavalos de Tróia: Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia.
- Páginas Falsas: Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas.
- Direitos Autorais: Notificações de eventuais violações de direitos autorais.
- Outras: Outras tentativas de fraude.

No tipo de crime definido como Fraude Virtual, o agente pratica uma conduta de invasão, alteração ou modificação, pagamento ou supressão de dados eletrônicos ou programas, ou qualquer outra adulteração em um sistema de processamento de dados[25].

Segundo o CERT-BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil)[26], a Fraude Eletrônica se define como:

> A fraude eletrônica consiste em uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, esse tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

No entendimento de Paulo Marco[27], o mesmo define as fraudes virtuais como:

> *Fraudes eletrônicas* – invasão de sistemas computadorizados e posterior modificação de dados, com o intuito da obtenção de vantagem sobre bens, físicos ou não, por exemplo, a adulteração de depósitos bancários, aprovações em universidades, resultados de balanços financeiros, pesquisas eleitorais, entre outros.

As fraudes eletrônicas têm crescido assustadoramente nos últimos anos, especialmente o que diz respeito à modalidade de furto mediante fraude

---

[25] **LIMA**, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas, SP: Ed. Millennium, 2005.p.134.

[26] **CERT.BR** - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha. Disponível em: <http://cartilhacert.br/glossario>. Acesso em: 31 mar. 2012.

[27] **LIMA**, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas, SP: Ed. Millennium, 2005.p.60.

(art. 155 do Código Penal), a qual se caracteriza pelo envio de um e-mail falso (*phishing)* para um usuário, e são capturados dados de sua conta bancária, mediante a instalação de um programa em seu equipamento de acesso à internet.

Antonio Loureiro Gil[28] conceitua as fraudes informatizadas como:

> Ação intencional e prejudicial a um ativo intangível causada por procedimentos e informações (software e bancos de dados), de propriedade de pessoa física, ou jurídica, com o objetivo de alcançar benefício, ou satisfação psicológica, financeira e material.

As fraudes por meio de computadores possuem dois tipos de origens: a) interna – quando são praticadas por empregado ou terceiro que se encontram dentro do local a ser fraudado; e b) externa – o fraudador não possui vínculo com o local que será fraudado, mas isso não significa que o agente da fraude não possa um dia ter tido relação com a vítima[29].

Nas fraudes o usuário é induzido a fornecer seus dados pessoais e financeiros, na maioria das vezes mascarada por trás de páginas duvidosas, o qual o usuário e encaminhado para páginas fraudulentas, na maioria das vezes os fraudadores utilizam as mídias sociais, e tentam de todas as maneiras persuadir o usuário a fornecer seus dados pessoais[30].

Um crime que acontece diariamente é o chamado furto de dados, onde o Código Penal conceitua furto em seu Art. 155 como sendo “subtrair, para si ou para outrem, coisa alheia móvel”, a questão que se tem discutido, é se poderia enquadrar o furto de dados como sendo o furto do art. 155 do CP, tendo em vista que poderia o mesmo não se enquadrar no tipo legal, visto que na conduta do agente o mesmo pode levar os dados da empresa e apagá-los, ou também pode levar os mesmos mediante cópia e não eliminá-los, sendo que nesta ocasião não haveria o quesito de indisponibilidade do bem, no caso para configurar a subtração[31].

---

[28] **GIL**, Antônio de Loureiro. **Fraudes Informatizadas**. 2 ed. São Paulo: Atlas, 1999.p. 15.
[29] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.311.
[30] **CERT.BR** - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Cartilha. Disponível em: <http://cartilha.cert.br/fraudes/sec2.html#sec2>. Acesso em: 18 mar. 2012.
[31] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.313.

3.2 ESTELIONATO

O ramo do Direito Digital é uma sistemática nova, alguns autores separam as condutas delituosas em face dos computadores, como elemento físico, e contra os dados os quais se encontram neles.

As condutas variam conforme o uso que o agente faz dos meios eletrônicos disponíveis, com o fim de atingir um objetivo, um dos crimes mais populares tanto na Internet quanto fora dela é o estelionato, o Código Penal[32] em seu art. 171, *caput,* reza que:

> 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.

Ademais, em seu § 3º, o artigo estabelece que a pena será aumentada de um terço, na situação em que o crime for cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

No caso da aplicação do estelionato no meio informático, a conduta do agente será de induzir ou manter a vítima em erro, e com isso, obtendo vantagem ilícita, para si ou para outrem. Diversas são as condutas dos estelionatários na internet, a questão é tipificá-las como estelionato, o legislador previu, como meio executório a fraude com o objetivo de obter consentimento da vítima, iludi-la para que voluntariamente entregue o bem, o agente leva a vítima a erro, enganando a mesma, mantendo-a em erro.

Uma das condutas típicas do estelionato pela Internet consiste na conduta do agente encaminhar e-mails com conteúdo falso ao usuário, induzindo o mesmo a clicar em links disponíveis no corpo do e-mail, em que muita das vezes direciona o usuário para um site falso onde o mesmo digita informações pessoais ao agente que formulou a pagina falsa, estas informações são enviadas ao agente por meio da internet, que após apropriar-

[32] **VADE MECUM**. 11ª Ed. São Paulo. Saraiva, 2011.p.171 e 172.

se dos seus dados bancários, transfere os valores disponíveis em conta[33] para o seu domínio.

Uma maneira de tentar se livrar destes e-mails indesejáveis é a instalação de antivírus, o qual pode ser configurado para excluir os e-mails tidos como possíveis ataques ao computador, à exclusão pode ser feita antes mesmo dos e-mails serem recebidos no computador, ou, efetuar a configuração de segurança do *Firewall*[34], o qual servirá como uma barreira para possíveis intrusos, o *Firewall* e o antivírus irão monitorar as portas de entrada e saída de pacotes que são transmitidos pelo computador, fazendo com que as regras de transferência de documentos pela rede sejam realizadas de forma controlada.

3.3 INVASÃO DE PRIVACIDADE

Com o avanço dos acessos na rede mundial de computadores, as pessoas passaram a disponibilizar um número quase ilimitado de informações na rede, desde informações que são lançadas em cadastros em sites de e-commerce[35] até informações de preenchimento de perfis nas redes sociais.

As pessoas que utilizam a rede mundial de computadores para acesso a informações diversas, ou para compra de produtos, em fim, para um numero por vezes ilimitado de situações onde a internet possibilita se realizar inúmeras questões, o que ocorre, e que as informações que estão disponibilizadas ou não na internet, podem trazer uma penalidade as pessoas, física ou jurídica, que as utilizam sem autorização, ou seja, o direito à privacidade constitui um limite natural ao direito à informação[36].

O que se procura na verdade é resguardar o cidadão com relação aos seus dados que estão disponibilizados na rede, sejam aqueles disponíveis

---

[33] **INELLAS**, Gabriel Cesar Zaccaria de. Editora Juarez de Oliveira. São Paulo, 2004.p.44

[34]**TECMUNDO**, Disponível em: <http://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.html>. Acesso em: 18 mar. 2012.

[35]**EDUCACIONAL**. Vida Inteligente o computador no dia-a-dia. Disponível em: <http://www.educacional.com.br/vidainteligente/clickdigital02/e-commerce.asp>. Acesso em: 01 abr. 2012.

[36] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.85

em órgãos públicos, seja em entes privados, mesmo porque os dados pessoais dos cidadãos não podem ser tratados como mercadoria, tendo em vista que se devem considerar seus aspectos subjetivos, o Estado deve garantir os direitos da pessoa, tutelar sua identidade, e o cidadão deve exigir das empresas que armazenam seus dados que as mesmas se preocupem com a segurança dos mesmos, e os utilizem somente para aquele fim especifico[37].

3.4 CRIMES CONTRA A HONRA

Os crimes contra a honra estão previstos nos arts. 138, 139 e 140 do Código Penal, sendo que os mesmos são crimes comuns na internet, tendo em vista o alto numero de usuários que navegam diariamente na rede.

Honra são as qualidades de um individuo físicas, morais e intelectuais, fazendo-a respeitada no meio social onde se convive, a qual diz respeito ainda à sua autoestima. A honra é um patrimônio que a pessoa possui, sendo que o mesmo deve ser protegido, tendo em vista que os seus atributos como pessoa em sociedade irá definir a sua aceitação ou não para conviver em um determinado grupo social[38].

Um dos crimes contra a honra e o crime de Difamação, o qual se encontra definido no art. 139 do Código Penal: “Difamar alguém, imputando-lhe fato ofensivo à sua reputação”, este crime afeta a honra objetiva da pessoa, algo perpetuado por um terceiro que venha a macular a reputação da pessoa[39].

O crime de Difamação e praticado na internet nas suas mais diversas formas, seja na perpetuação de e-mails enviados a pessoas diversas da vitima, imputando à esta, algum fato que ofenda sua honra objetiva, ou publicando em redes sociais as mesmas ofensas. No crime de Difamação a pessoa Jurídica não pode ser sujeito passivo, tendo em vista que no art. 139 do CP a norma é dirigida à pessoa humana, mas, quando o crime for praticado por

---

[37] **LIMBERGER**, Têmis. **O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais**. Porto Alegre: Livraria do Advogado Editora, 2007.p.58, 59 e 60.

[38] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.90.

[39] **INELLAS**, Gabriel Cesar Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004. p.49.

meio da imprensa, pode-se aplicar a Lei nº 5.250/67 – Lei de Imprensa.[40].

Na Difamação a lei não exige que a atribuição seja falsa, basta somente à perpetuação de algo que venha a ofender a reputação do agente perante a sociedade, o crime irá se consumir no momento em que o terceiro tomar conhecimento do fato, em ambiente virtual o crime irá se consumir, por exemplo, quando alguém espalhar um ato ofensivo a uma pessoa pelas redes sociais, e os usuários presentes fizeram a leitura do fato ofensivo[41].

O Crime de Calúnia esta descrito no art. 138 do Código Penal, o qual versa: “Caluniar alguém, imputando-lhe falsamente fato definido como crime”.

No crime de Calúnia a honra objetiva da vítima é abalada, ou seja, o agente atribui à vítima a prática de fato definido como crime, sabendo que a imputação é falsa, abalando assim, sua reputação perante a sociedade.

O crime de injúria consiste na propagação de qualidade negativa da vítima por um terceiro, qualidade esta que diga respeito aos seus atributos morais, intelectuais ou físicos, afetando de forma significativa a honra subjetiva da vítima, o tipo penal está previsto no art. 140 do Código Penal: “Injuriar alguém, ofendendo-lhe a dignidade ou o decoro”.

3.5 ESPIONAGEM ELETRÔNICA

Tendo em vista o crescente uso da tecnologia por pessoas, e o uso dependente de software diversos pelas empresas, o que faz com permanecemos mais tempos conectados a rede de computadores, e ao lançamento maciço de informações pessoais e estratégicas nos servidores empresarias, essa realidade faz com que necessitamos cada vez mais de um hábito de segurança das informações, seja prevenindo, seja monitorando.

---

[40] **INELLAS**, Gabriel Cesar Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004. p.51

[41] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.91.

Existem vários tipos de espionagem eletrônica, mas a que podemos destacar, por ser a mais comum, é chamada de Sigint[42] (signals intelligence), a qual teve sua origem na interceptação, decodificação, tradução e análise de mensagens por um terceiro, além do emissor é do destinatário. No passado imaginava-se que a espionagem seria praticada por empresas, as quais iriam tentar burlar o sistema de segurança das concorrentes com o fim de apropriar-se de informações privilegiadas do mercado concorrencial, mas o que ocorre na maioria dos casos e o contrario, pessoas de dentro da empresa são envolvidas a permitirem o acesso ao ambiente, ou agirem para coletar ou apagar as informações as quais o espião tem interesse[43].

Não existe um tipo penal especifico que venha a especificar o crime de espionagem eletrônica, sendo que a conduta está definida no Código Penal em seus art. 154 e 184 – crime de violação de segredo profissional[44] e crime de violação de direito autoral:

> Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena – detenção, de três meses a um ano, ou multa.
>
> Violar direitos de autor e os que lhe são conexos: pena de detenção, de três meses a um ano, ou multa.

Aquele funcionário que praticar a conduta poderá ter o seu contrato rescindido por justa causa, tendo em vista o que versa o art. 482, “g” da CLT[45]:

> Constituem justa causa para rescisão do contrato de trabalho pelo empregador:
>
> g) violação de segredo da empresa

As empresas devem investir em segurança no ambiente laboral, fazer uso de diferentes ações e equipamentos para monitoramente de tudo que ocorra na empresa, tendo em vista que as ameaças internas são mais difíceis de serem apanhadas, uma vez que o agente que exerce a conduta e normalmente é um usuário legítimo, e o mesmo quando exerce a espionagem

---

[42] **ABRAIC – Associação Brasileira dos Analistas de Inteligência Competitiva**. Glossário de IC. Disponivel em: <http://www.abraic.org.br/V2/glossario.asp?letra=I>. Acesso em: 01 mar. 2012.
[43] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.381, 382 e 383.
[44] **VADE MECUM**. 11ª Ed. São Paulo. Saraiva, 2011.p.597 e 601.
[45] **VADE MECUM**. 11ª Ed. São Paulo. Saraiva, 2011.p.974.

apaga o registro de logs e não deixa qualquer rastro pra que venha a ser apanhado[46].

Patrícia Peck[47] salienta que para combater a espionagem é essencial aplicar medidas em três níveis: Físico, Lógico e Comportamental, e devem-se considerar os seguintes pontos:

a) Criação de controles mais rígidos na área de Recursos Humanos, pois a maioria dos Insiders possui um histórico de violação a políticas corporativas e/ou prática de crimes, mas há também informações sobre atividades extratrabalho, como família e mesmo Orkut e Blog da pessoa que revelam muitas vezes o que está acontecendo;
b) Fazer segregação de função, mas rever com freqüência os acessos e, se possível, amarrar não apenas o login do usuário com uma senha, mas também a uma identidade de máquina;
c) Criação de equipes com atividades especificas, a fim de que determinada tarefa que envolva confidencialidade ou risco não fique atrelada a somente um indivíduo, e sim a um grupo, a fim de cada um exerça uma fiscalização sobre o outro;
d) Uso de software de monitoramente eletrônico, pois vigiar é essencial;
e) Desenvolvimento e aplicação de Políticas de segurança da Informação;
f) Regulamentação do uso de dispositivos móveis, com bloqueio de portas USB, por exemplo, restrições de uso de determinadas mídias;
g) Execução de ações de conscientização que englobem todos os funcionários, terceirizados e gestores (de nada adianta chefes não serem conscientizados, pois cabe a eles dar o exemplo;
h) Criação de um canal de denúncia anônimo;
i) Preparar o terreno para a adequada coleta das provas. Nesse sentido, é fundamental guardar os logs da rede, guardar os e-mails originais (eletrônicos), dados de acesso entre outros;
j) Seguir o “princípio do menor privilégio”, ou seja, garantir acesso ao que é estritamente necessário;
k) Ter classificação da informação bem definida e aplicada;
l) Realizar testes de vulnerabilidade e simulações de Black bag.

O conjunto de condutas visa um controle mais eficaz para que o Insider tenha reduzida sua capacidade de exercer sua conduta de espionagem, e que se aumenta a probabilidade de pegar o infrator, seja por meio de um numero maior de evidencias como logs, por exemplo, ou pelo uso da perícia digital[48].

---

[46] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.385 - 386.
[47] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.387 - 388.
[48]**TECMUNDO** – Disponível em: <http://www.tecmundo.com.br/o-que-e/3615-perito-digital-o-que-ele-faz-e-como-consegue-recuperar-informacoes-perdidas.htm>. Acesso em: 01 abr. 2012.

3.6 CRIMES CONTRA A PROPRIEDADE INTELECTUAL

No crime contra a Propriedade Intelectual, o bem jurídico que procura ser preservado é o direito autoral, e, os reflexos que a obra irá gerar, ou seja, os direitos conexos à mesma.

No âmbito da Internet há uma ausência de fiscalização, ausência de territorialidade, o que propicia uma rapidez na circulação de informações, e que permite também que cópias de materiais disponibilizados sejam feitas de maneira desordenada, onde muitas das vezes o criador é desrespeitado, tendo em vista que não há qualquer respaldo aos seus direitos como autor da obra que está sendo replicada[49].

O Art. 184 do Código Penal versa[50]:

> Art. 184 - Violar direitos de autor e os que lhe são conexos:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa.
> § 1º - Se a violação consistir em 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, conforme o caso, ou de quem os represente:
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 2º - Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, 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 ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
> § 3º - Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto.
> Art. 186 - Procede-se mediante:

---

[49] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.134.

[50] **BRASIL**. Código Penal. Decreto Lei n. 2.848/40. Disponível em <http://www.dji.com.br/codigos/1940_dl_002848_cp/cp184a186.htm>. Acesso em: 10 abr. 2012.

> I – queixa, nos crimes previstos no caput do art. 184;
> II – ação penal pública incondicionada, nos crimes previstos nos §§ 1º e 2º do art. 184;
> III – ação penal pública incondicionada, nos crimes cometidos em desfavor de entidades de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo Poder Público;
> IV – ação penal pública condicionada à representação, nos crimes previstos no § 3º do art. 184.

Os artigos do Código Penal não mencionam a violação de programas de computadores, limita-se a obras fonográficas e cópia de obras intelectuais, ademais, o art. 12, *caput,* da Lei n. 9.609/98, versa que:

> Art. 12. Violar direitos de autor de programa de computador:
> Pena - Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
> Pena - Reclusão de um a quatro anos e multa.
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
> § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
> I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
> II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.
> § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

Existem os Softwares Livres, que são aqueles em que os usuários podem redistribuir cópias, efetuar modificações (caso o mesmo tenha acesso ao código-fonte[51], ou seja, o usuário é livre para fazer o que desejar do mesmo.

Os Softwares que não são livres, o usuário não tem acesso ao código-fonte, e não pode copiá-lo, ou efetuar distribuição do mesmo, para que ocorra a distribuição, deve haver uma contraprestação, ou seja, ônus para que ocorra a distribuição[52].

Uma das formas mais comuns de Crimes de violação de direito autoral é a pirataria de softwares, que consiste basicamente na cópia não autorizada de softwares, seja por usuários finais, seja por empresas que

---

[51] **FOLHA.COM**, Entenda o que é o código-fonte de um programa. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u7618.shtml>. Acesso em: 10 abr. 2012.

[52] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.160.

adquirem algumas licenças e efetuam cópias adicionais para comercialização, abaixo conceituaremos alguns tipos de pirataria[53].

Pirataria de Usuário Final – cópias adicionais de software sem autorização, cópias eventuais muitas das vezes efetuadas por indivíduos que realizam cópias dos softwares comprados pelas empresas onde laboram.

Venda não autorizada – ocorre quando revendedores distribuem cópias de um único pacote para clientes diferentes, ou quando efetuam cópias não autorizadas de softwares originais, alterando o documento original que deveria acompanhar o mesmo.

Pirataria pela Internet – Sites piratas disponibilizam download gratuito de software, oferecem cópias falsas, ou desviadas.

Cracking – ocorre quando se consegue quebrar o acesso de determinados softwares protegidos.

A propriedade intelectual é um valor, e deve ser objeto de proteção, tendo em vista o conjunto de direitos que estão embutidos no objeto do intelecto, Denis Borges Barbosa e Mauro Fernando Maria Arruda conceituam a propriedade intelectual[54]:

> A partir do momento em que a tecnologia passou a permitir a reprodução em série de produtos a serem comercializados. Além da propriedade sobre o produto, a economia passou a reconhecer direitos exclusivos sobre a idéia de produção ou, mais precisamente, sobre a idéia de que permite a reprodução de um produto. A estes direitos, que resultam sempre numa espécie de qualquer exclusividade de reprodução de um produto (ou serviço) dá-se o nome de propriedade intelectual.

Sendo assim, pode-se entender o direito de propriedade intelectual como sendo o conjunto de prerrogativas, conferidas por lei, ao individuo que criou determinada obra intelectual, para que o mesmo goze de todos os benefícios resultantes da exploração de sua criação[55].

Nos dias atuais ainda se tem a ideia do que está publicado na Internet é público, e não tem problema algum em se apropriar do mesmo, está

---

[53] **BORLAND. A Micro Focus Company**. O que é a Pirataria de Softwares. Disponível em: <http://www.borland.com/br/piracy/what_is_piracy.aspx>. Acesso em: 10 abr. 2012.

[54] **BARBOSA**, Denis Borges; ARRUDA. Mauro Fernando Maria. **Sobre a Propriedade Intelectual**. Rio de Janeiro: Campinas, 1990. p. 10

[55] **ECAD – Escritório Central de Arrecadação e Distribuição**. O que é Direito Autoral. Disponível em: <http://www.ecad.org.br/viewcontroller/publico/conteudo.aspx?codigo=48>. Acesso em: 10 abr. 2012.

questão impõe um enorme desafio aos operadores do Direito, tendo em vista que se deve repensar o modelo econômico de exploração da propriedade intelectual[56].

3.6 DANO INFORMÁTICO

O crime de Dano está previsto no Código Penal em seu art. 163: Destruir, inutilizar ou deteriorar coisa alheia: Pena – detenção, de um a seis meses, ou multa.

O legislador ao abarcar o crime de Dano no Código Penal o fez dirigido a proteger o dano a "coisa", seja ela móvel ou não, o que ocorre é que "coisa" vem a ser algo tangível, material, e o legislador não levou em consideração a conduta do dano informático à época da elaboração do art. 163 do CP, e o problema que ocorre hoje ao se aplicar o citado artigo a conduta do agente quando efetua o dano informático, é que o mesmo não pode ser entendido como algo tangível, material, não no que diz respeito ao dano a computadores, impressoras, em fim, equipamentos de informática, pois o art. 163 abarca os danos causados a estes, mas falamos sobre os danos causados aos dados disponíveis em CDs-ROM, disquetes, pen drives, hard disks, quando não há deterioração dos equipamentos, mas sim dos dados neles contidos[57].

Não se pode aqui falar em uma interpretação analógica, tendo em vista que a mesma seria *in malam partem*, o que não poderia ser feito, tendo em vista o princípio da legalidade[58], que proíbe a utilização de analogia no Direito Penal em situações que tragam prejuízos ao agente da conduta.

Não se pode simplesmente atribuir como material algo que é imaterial, o que ocorre é que se hoje alguém praticar um dano a dados informáticos de um terceiro, mesmo que de forma dolosa, não estará sujeito as

---

[56] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.132.
[57] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.71,72 e 73.
[58] Art. 1° do CP e art. 5°, XXXIX, da CF.

penas do Código Penal, será responsabilizado somente no que dispõe a legislação Cível.

Existe atualmente o Projeto de Lei 84/99, o qual se aprovado, o art. 163 do Código Penal passará a ter a seguinte redação:

> Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio.
>
> Parágrafo único. Nas mesmas penas incorre quem apaga, altera ou suprime os dados eletrônicos alheios sem autorização ou em desacordo com aquela fornecida pelo legítimo titular.

Nota-se que o legislador buscou separar as coisas tangíveis das não tangíveis, o que irá resolver a questão no que diz respeito a lacuna jurídica que se verifica hoje na legislação atual, com o fim de se criminalizar as condutas com o viés de destruir dados eletrônicos, que cada vez mais são valorados, tendo em vista o armazenamento em massa de um número quase ilimitado de informações.

3.7 PORNOGRAFIA INFANTIL

O mercado de Pornografia Infantil no mundo movimenta mais de R$ 4 Bilhões por ano[59], e dados da Interpol mostram que o Brasil é o 4º colocado no ranking de países que exploraram o mercado. Antes de adentrarmos no assunto da Pornografia Infantil, é de importância comentar o art. 234 do Código Penal[60], o qual versa:

> Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno:
>
> Pena – detenção, de 6 (seis) meses a 2 (dois) anos, ou multa.
>
> Parágrafo único. Incorre na mesma pena quem:
>
> I – vende, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo;
>
> II – realiza, em lugar público ou acessível ao público, representação teatral, ou exibição cinematográfica de caráter

[59] **TERRA**. Carnaval 2012 – Pornografia infantil movimenta R$ 4 bilhões. Disponível em: <http://diversao.terra.com.br/carnaval/2012/videos/0,,196577.html>. Acesso em: 01 abr. 2012.
[60] **VADE MECUM**. 11ª Ed. São Paulo. Saraiva, 2011.p.606

> obsceno, ou qualquer outro espetáculo, que tenha o mesmo caráter;
>
> III – realiza, em lugar público ou acessível ao público, ou pelo rádio, audição ou recitação de caráter obsceno.

O elemento subjetivo do tipo é o dolo, o qual o agente tem a finalidade de expor ao público, ou comercializar o objeto material do crime, não é necessário que alguém venha a ter acesso ao material para que o crime venha a se consumir, basta somente a disponibilização do material e a possibilidade de que alguém venha a ter acesso ao mesmo.

Há que se fazer uma distinção entre a Pedofilia e a Pornografia Infantil, naquela, há uma perversão sexual, a qual o adulto experimenta sentimentos eróticos com crianças e adolescentes, já na Pornografia Infantil não é necessário a ocorrência da relação sexual entre adultos e crianças, mas sim, a comercialização de fotografias eróticas ou pornográficas envolvendo crianças e adolescentes[61].

O Estatuto da Criança e do Adolescente, Lei 8.069/90[62], estabelece algumas penalidades para o Pedófilo e aquele que divulga ou comercializa imagens, vídeos envolvendo crianças em cena de sexo, ou seja, Pornografia Infantil, vejamos.

> Art. 240 – Produzir ou dirigir representação teatral, televisiva ou película cinematográfica, utilizando-se de criança ou adolescente em cena de sexo explícito ou pornográfica:
>
> Pena – reclusão de 1 (um) a 4 (quatro) anos, e multa.
>
> Parágrafo único. Incorre na mesma pena que, nas condições referidas neste artigo, contracena com criança ou adolescente.
>
> Art. 241 – Fotografar ou publicar cena e sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão de 1 (um) a 4 (quatro) anos.

A norma que tipifica o crime previsto no art. 241 é entendida como *norma aberta,* e o Supremo Federal já entende que sua aplicação se dá também para os crimes que são perpetrados pela Internet, tendo em vista que

---

[61] **INELLAS**, Gabriel Cesar Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004. p.46

[62] **VADE MECUM**. 11ª Ed. São Paulo. Saraiva, 2011.p.1.106.

o crime caracteriza-se pela simples publicação, a qual independe do meio que foi utilizado, basta a divulgação e o delito está consumado, vejamos o entendimento da Colenda Primeira Turma do STF[63]:

> ESTATUTO DA CRIANÇA E DO ADOLESCENTE – Art. 241 – Inserção de cenas de sexo explícito em rede de computadores (*Internet)* – Crime caracterizado – Prova pericial necessária para apuração da autoria. "Crime de computador"; publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/*Internet* de computadores atribuída a menores – Tipicidade – Prova pericial necessária à demonstração da autoria – *Habeas Corpus* deferido em parte.
>
> 1. O tipo cogitado – na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma normal aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/*Internet* de computador.
> 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta incriminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da Lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.
> 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada do conhecimento do homem comum, impõe-se a realização de prova pericial.

Para que se encontre o agente que praticou uma das condutas previstas nos citados artigos, muitas das vezes é necessária a quebra de sigilo[64], tendo em vista que será preciso rastrear aquele que praticou o ilícito, e após conseguir localizar o culpado, é necessário muitas das vezes que sejam as provas eletrônicas analisadas por uma perícia técnica rigorosa, para que sejam aceitas em processos[65].

---

[63] **BRASIL**. Supremo Tribunal Federal – RHC n. 76.689-0 – Pernambuco – Primeira Turma – Relator: Ministro Sepúlveda Pertence, DJU de 6.11.1998, p.03.

[64] **FOLHA.COM**. CPI aprova quebra de sigilo de 18 mil páginas do Orkut. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u418514.shtml>. Acesso em: 01 abr. 2012.

[65] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.300 e 301.

4 LEGISLAÇÃO NACIONAL EM RELAÇÃO AOS CRIMES VIRTUAIS

O Direito Penal esta inteiramente ligado a Internet, tendo em vista que as relações que ali são firmadas são entre indivíduos, e estes, devem ter suas condutas disciplinadas, sendo que cabe ao Direito disciplinar e regulamentar as condutas entre os membros desta sociedade digital. O atual Código Penal já é de certa forma eficiente em punir algumas condutas praticadas com o uso da tecnologia, e outras, onde a conduta do agente afeta bens jurídicos relativos à Sociedade da Informação, como dados de sistemas, por exemplo, ai passa a exigir uma intervenção legislativa para elaboração de novos instrumentos normativos de punição[66].

A Constituição Federal versa em seu art. 5º, XXXIX que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal", ou seja, para que se venha a punir os crimes que são praticados no meio digital, é necessário que o tipo penal venha a se adequar nas normas já existentes, e as lacunas que por ventura ainda existem, devem ser preenchidas, sendo que hoje é extremamente necessária a incorporação dos conceitos de informática à legislação vigente[67].

As primeiras manobras legislativas vieram a ocorrer com o advento do Plano Nacional de Informática e Automação (Conin), Lei n. 7.232/84, o qual versava sobre as diretrizes no âmbito da informática em solo Brasileiro, depois veio a Lei n. 7.646/87, a qual foi revogada pela Lei n. 9.609/98, sendo que esta foi o primeiro ordenamento a descrever as infrações de informática, a qual podemos citar alguns artigos:

> Art. 12. Violar direitos de autor de programa de computador:
> Pena – Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
> Pena – Reclusão de um a quatro anos e multa.
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

---

[66] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.161 e 162.
[67] **LIMA**, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas, SP: Ed. Millennium, 2005.p.157.

> § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
> I – quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
> II – quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.
> § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

Podemos citar algumas normas do Código de Defesa do Consumidor – Lei 8.078/11[68].

> Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
>
> Pena – Detenção de seis meses a um ano ou multa.
>
> Art. 73. Deixar de corrigir imediatamente informações sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata:
>
> Pena – Detenção de um a seis meses ou multa.

Ademais, cabe um resumo das condutas que já estão tipificadas no ordenamento jurídico pátrio, e que são criminalizadas.

> Art. 153, § 1° - A do Código Penal – Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública.
> Pena – detenção de 1 a 4 anos, e multa.
> Art. 313 – A do Código Penal – Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.
> Art. 313 – B do Código Penal – Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.
> Pena – detenção de 3 (três) meses a 2 (dois) anos, e multa.
> Art. 325, § 1°, incisos I e II - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação:
> Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.
> § 1º Nas mesmas penas deste artigo incorre quem:

[68] **VADE MECUM**. 11ª Ed. São Paulo. Saraiva, 2011.p.855.

> I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública;
> II – se utiliza, indevidamente, do acesso restrito.
> Art. 2°, V – Lei n. 8.137/90 – utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública.
> Art. 72 da Lei n. 9.504/97 – Constituem crimes, puníveis com reclusão, de cinco a dez anos:
>
> I – obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;
>
> II – desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;
>
> III – causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

Existem atualmente projetos de Lei em andamento que tratam do tema de delitos tecnológicos, dentre os projetos de maior relevância destaca-se o PL n. 84/99, o qual ao longo dos anos já foi incorporado inúmeros artigos, dos seus apenas seis artigos iniciais, sendo que recebeu inúmeras emendas que o ampliaram, dentre as alterações que este projeto de lei trará a legislação, podemos citar algumas[69].

> a) O art. 2° prevê a inclusão do Capítulo IV do Título VIII, da Parte Especial do Código Penal, com a redação dos arts. 285-A (acesso não autorizado a sistemas informáticos), 285-B (obtenção e transferência ilegal de dados) e 285-C (ação penal);
> b) O art. 3° prevê a inclusão do art. 154-A no Título I, Capítulo VI, Seção IV, que trata da divulgação ou utilização indevida de informações e dados pessoais;
> c) O art. 4° trata da alteração do art. 163, inserido no Título II, Capítulo IV, para que inclua no crime de dano a destruição, inutilização ou deterioração de dado alheio.
> d) O art. 5° trata da inclusão do art. 163-A no mesmo Título II, Capítulo IV, que incrimina a disseminação de vírus computacional;
> e) O art. 6° altera o crime de estelionato para que conste no art. 171, § 2°, VII, a difusão de vírus que vise destruir, copiar, alterar, facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado, para obter vantagem econômica para si ou para outrem, em detrimento de outrem;
> f) O art. 7° altera os crimes dos arts. 265 e 266 do Código Penal para que constem como crime contra a segurança dos

[69] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.164 a 169.

serviços de utilidade pública os de informação e telecomunicações;

g) O art. 8° altera o art. 297 do Código Penal para que dentre as falsificações de documentos públicos incluam-se os dados;
h) O art. 9° altera o art. 298 do Código Penal para que dentre as falsificações de documentos particulares incluam-se os dados;
i) O art. 10 muda o Código Penal Militar para que o art. 251 do Capítulo IV, do Título V da Parte Especial do Livro I do Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), passe a vigorar acrescido do inciso VI ao seu § 1°, e do § 4°, incriminando-se o estelionato eletrônico;
j) O art. 11 altera o *caput* do art. 259 e o *caput* do art. 262 do Capítulo VII, do Título V, da Parte Especial do Livro I do Decreto-Lei n. 1001, de 21 de outubro de 1969 (Código Penal Militar), para que deles conste destruição a dados sob administração militar;
k) O art. 12 altera o Capítulo VII, do Título V, da Parte Especial do Livro I do Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), que fica acrescido do art. 262-A, prevendo a disseminação de vírus em sistemas militares;
l) O art. 13 altera o Título VII da Parte Especial do Livro I do Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), que fica acrescido do Capítulo VII-A, que prevê crimes contra a segurança dos sistemas informatizados;
m) O art. 14 altera o *caput* do art. 311 do Capítulo V, do Título VII, do Livro I da Parte Especial do Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), para que a falsificação de documentos inclua os dados;
n) O art. 15 altera os incisos II e III do art. 356, do Capítulo I, do Título I, do Livro II da Parte Especial do Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), para que conste do crime de favorecer o inimigo a entrega de dados;
o) O art. 16, um dos mais polêmicos, traz definições do que devem ser considerados dispositivo de comunicação, sistema informatizado, rede de computadores, código malicioso, dados informáticos e dados de tráfego;

Cabe tecer um comentário quanto ao art. 16, sendo que o mesmo define como sendo dispositivos de comunicação, por exemplo, um pen-drive, disco rígido, CD, DVD, o que não condiz com a realidade, por isso a polemica deste artigo.

p) O art. 17, cuja supressão da redação é recomendada pela proposta do substitutivo, dispõe que para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado;
q) O art. 18 estabelece que os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializados no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado;
r) O art. 19 altera a redação do inciso II do § 3º do art. 20 da Lei n. 7.716, de 5 de janeiro de 1989 (crimes de racismo e preconceito), para permitir a cessação de transmissões

radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio de condutas descritas na lei;

s) O art. 20 prevê que o *caput* do art. 241 da Lei n. 8.069, de 13 de julho de 1990, tenha redação que coíba o recebimento e o armazenamento de imagens e fotos com conteúdo de pornografia infantil;

t) O art. 21 pretende alterar a Lei n. 10.446/02, que dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme, para os fins do disposto no inciso I do § 1° do art. 144 da Constituição, para que os crimes digitais sejam da competência da Justiça Federal;

u) O art. 22 obriga os que provêem o acesso a rede de computadores mundial, comercial ou do setor público, e também as prestadoras de serviço de conteúdo, sejam obrigados a diversas condutas, que dizem respeito, por exemplo, que as responsáveis pelo provimento, deverão manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, destino hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória e ao Ministério Público mediante requisição. Este artigo tende a ser o mais polêmico de todos os citados do Projeto de Lei.

O que se nota quando se faz uma analise detalhada dos artigos do citado projeto de lei, é que embora ele abarque condutas até então não criminalizadas, em certos momentos pode-se notar que não cria regras rígidas de responsabilização ás empresas que exercem o papel de provedoras do serviço de acesso à internet, o que faz com que de certa forma o usuário de má-fé, tenha um caminho livre para que venha a praticar suas condutas antijurídicas, sob o prisma que para que o mesmo venha a ser responsabilizado, o ambiente de provas ainda é deficitário.

Outro projeto que vem caminhando lentamente é o PLC n. 89/2003, de iniciativa do Senador Eduardo Azeredo, o qual também dispõe de crimes cometidos no meio informático, e que também irá abarcar vários crimes que são cometidos por meio de computadores e/ou instrumentos de acesso a internet ou no cenário digital, o qual podemos citar alguns pontos importantes deste projeto[70].

NOVA CONDUTA	NOVA TIPIFICAÇÃO DO CRIME
Disseminar *phishing scam (e-mails* fraudulentos contendo *malwares* e outros códigos maliciosos).	Estelionato Eletrônico

[70] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.295.

Roubar senhas bancárias por meio de *phishing scam.*	Estelionato Eletrônico
Falsificar cartão de crédito	Falsificação de dado eletrônico ou documento particular
Destruir, inutilizar ou deteriorar dado eletrônico alheio.	Dano
Inserir ou difundir códigos maliciosos em dispositivos de comunicação, redes, sistemas, causando dano.	Inserção ou difusão de código malicioso seguido de dano
Inserir ou difundir códigos maliciosos (vírus, *worms, trojans,* etc.) em dispositivos de comunicação, redes, sistemas.	Inserção ou difusão de código malicioso
Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida.	Acesso não autorizado
Obter ou transferir dado ou informação sem autorização (ou em desconformidade à autorização).	Obtenção não autorizada de informação
Divulgar, sem autorização, informações pessoais disponíveis em banco de dados.	Divulgação não autorizada de informações pessoais
Atentado contra a segurança de serviço de utilidade pública.	Ataques a redes e invasões
Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistemas informatizados.	Ataques a redes e invasões
Falsificação de dado eletrônico ou documento público.	Falsa identidade, falsidade ideológica digital, fraude.
Falsificação de dado eletrônico ou documento particular	Falsa identidade, falsidade ideológica digital, fraude.
Preconceito.	Preconceito digital
Pedofilia.	Pedofilia digital.

O que se pode verificar da analise do citado projeto, é que o mesmo não é muito técnico, não faz menção a poucos institutos que os especialistas da área de informática estão acostumados a se debaterem no seu cotidiano, era de se esperar, até porque o mesmo foi colocado em discussão para a sociedade apenas depois de a proposta de lei ser aprovada pela Câmara dos Deputados, e o que se observa hoje é a falta de uma equipe de profissionais da área de Informática para auxiliar na ordenação dos artigos que fazem parte do Projeto, tendo em vista que o instituto é de alta complexidade até para profissionais mais experientes da área.

5 LEGISLAÇÃO INTERNACIONAL EM RELAÇÃO AOS CRIMES VIRTUAIS

A preocupação com os problemas relacionados com a criminalidade informática e sua tipificação no ordenamento jurídico é uma questão que vem sendo analisada há vários anos. Os Estados Unidos foi o primeiro país a tipificar e punir penalmente os entraves oriundos dos crimes perpetuados pelo uso da informática.

Em 1978 foi proposto o “Ribicoff Bill”, o qual não foi aprovado, mas serviu como modelo para elaboração de legislações posteriores.

Abaixo abordaremos as principais questões que estão sendo discutidas sobre a criminalidade informática no mundo.

OCDE – Organização para a Cooperação e Desenvolvimento Econômico[71] - entidade que reúne países comprometidos em apoiar o crescimento econômico sustentável, qualidade de vida, e contribuem para o crescimento do comércio mundial.

Em 1986 a OCDE, por meio de seus países membros, realizou um inventário sobre a capacidade das legislações nacionais frente ao combate da criminalidade informática, e foram delineados alguns tipos de abusos informáticos[72]:

a) Fraude informática;
b) Falsificação informática;
c) Sabotagem informática;
d) Cópia ilegal de programas informáticos;
e) Acesso ilegal a sistemas informáticos;
f) Introdução, alteração, destruição e/ou supressão de dados informáticos e/ou programas de computador, realizadas intencionalmente como forma de se praticar falso;

---

[71] **OCDE – Organisation de Coopération ET de Développemente Economiques**. Disponível em: <http://www.oecd.org/home/0,3675,fr_2649_201185_1_1_1_1_1,00.html>. Acesso em: 10 abr. 2012.

[72] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.120 a 121.

g) Introdução, alteração, destruição e/ou supressão de dados informáticos e/ou programas de computador ou qualquer outra interferência em sistemas informáticos, realizadas com o fim de obstaculizar o funcionamento do sistema informático ou de telecomunicações;
h) Transgressão de direito exclusivo de propriedade de programa informático protegido, com o fim de explorá-lo comercialmente, introduzindo-o no mercado;
i) Acesso ou interceptação não autorizados a sistema informático ou de telecomunicações, com finalidade fraudulenta ou danosa.

O que se nota, é que na época foi feita uma analise dos países que fazem parte do OCDE, tendo sido apresentado os possíveis critérios para uma cooperação internacional frente aos crimes de informática, os quais eram definidos como abuso informático.

Faremos uma análise da legislação de alguns países quanto à criminalidade informática[73].

Conselho da Europa – O conselho da Europa é composto por 47 países-membros, tendo como língua oficial o inglês e o francês, este conselho não ficou indiferente frente aos problemas relacionados aos crimes informáticos, sendo que em 1995 foi elaborada a Recomendação R(95), a qual versa sete princípios de atuação aos problemas de procedimentos penais frente a tecnologia da informação, sejam eles[74]:

a) Registro;
b) Vigilância técnica;
c) Obrigações de cooperação com autoridades investigadoras;
d) Prova eletrônica;
e) Uso de criptografia;
f) Buscas, estatísticas e treinamento;
g) Cooperação internacional.

[73] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.122 a 155.
[74] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.125.

Espanha – No Código Penal espanhol, em seu art. 197, 1, há incriminação daquele que se apodera, sem autorização, de papeis, cartas, mensagens de correio eletrônico ou qualquer outro documento, com o intuito de descobrir segredo ou violar a intimidade de outrem, no inciso 2° do referido artigo há incriminação de interceptação de telecomunicações.

O art. 256 do Código Penal espanhol incrimina a utilização não autorizada de terminal de telecomunicação, e o art. 248, 2, incrimina a fraude informática e o estelionato tendo como meio o uso de tecnologia.

Portugal – Os crimes informáticos passaram a ser criminalizados com o advento da Lei n. 109/91, a qual repreende as seguintes condutas:

a) Art. 4° - Falsidade Informática – introdução, modificação ou supressão de dados ou programas informáticos, com o intuito de falsear a obtenção de dados eletrônicos;
b) Art. 5° - Dano a dados ou programas informáticos – destruição de dados eletrônicos ou de programas de computador, com o objetivo de dado ou, vantagem ilícita.
c) Art. 6° - Sabotagem Informática – apagar, alterar, introduzir ou suprimir dados ou programas informáticos, com o objetivo de perturbar o funcionamento informático ou de comunicação de dados à distância.
d) Art. 7° - Acesso Ilegítimo – invadir sistemas informáticos.
e) Art. 8° - Interceptação ilegítima – interceptações irregulares em ambiente computacional.
f) Art. 9° - Reprodução ilegítima de programa protegido – reprodução, divulgação ou a comunicação de software ao público sem autorização.

França – Em 1988 houve uma alteração no Código Penal Francês, o qual a Lei n. 88-19, introduziu capítulo especial o qual passou a reprimir atentados contra sistemas informáticos, foram feitas as alterações:

a) Acesso fraudulento a sistema de elaboração de dados, sendo considerados delitos tanto o acesso ao sistema, como nele manter-se ilegalmente.

b) Sabotagem informática, punindo quem apaga ou falseia o funcionamento de sistema eletrônico.
c) Destruição de dados, pune aquele que dolosamente introduz dados em sistema ou, suprime ou modifica dados.
d) Falsificação de sistemas informatizados, pune quem falsifica documentos informatizados, com intenção de prejuízo a terceiros.
e) Uso de documentos informatizados falsos, falsos retromencionados.

Itália – O Código Penal italiano desde 1993 trata de alguma forma dos delitos relacionados com a informática, vejamos:

a) Art. 615 – pune o acesso abusivo a sistema informático ou telemático.
b) Art. 617 – pune a instalação, interceptação, impedimento ou interrupção ilícita de comunicação informática ou telemática, e, ainda aquele que falsifica ou suprime conteúdo de comunicação informática ou telemática, quando o intuito é de lucrar ou causar prejuízo.
c) Art. 635 – pune aquele que causou destruição, deterioração ou inutilização a qualquer sistema informático.

Chile – o primeiro país da America Latina a incorporar a sua legislação alguns crimes digitais, a Lei n. 19.223/93, a qual em seu art. 1° pune aquele que destrua ou inutilize um sistema ou seus componentes; no art. 2° incimina-se a interceptação indevida em sistema; o art. 3° pune aquele que altera, danifica ou destrua os dados contidos em determinados sistemas.

Argentina – A Lei n. 26.388/08 alterou o Código Penal argentino, o qual passou a versar:

a) Art. 128 – incrimina aquele que armazena mensagens contendo pornografia de menores de 18 (dezoito) anos.
b) Art. 153 – pune aquele que abre ou se apropria sem autorização, de correspondência aberta ou fechada, ou comunicação eletrônica ou telegráfica.
c) Incrimina o acesso não autorizado a sistema informático.

d) Incrimina aquele que dá publicidade a informações, inclusive aquelas obtidas em mensagens eletrônicas, desde que possam causar prejuízo a outrem.

Japão – Em 1987 houve uma reforma na legislação penal que trouxe novas formas de tipificação quanto a manipulação e sabotagem informática, onde foi acrescentado a fraude com o uso de computador, e, a interferência em sistemas.

Estados Unidos – Cabe lembrar que nos EUA cada Estado pode criar seus estatutos penais, sendo que a intervenção Legislativa Federal tem um papel secundário.

A Principal Lei Federal que criminaliza ilícitos informáticos é a *Computer Fraud and Abuse Act – Lei de Fraude e Abuso Computacional,* a qual é datada de 1986, sendo que a mesma incrimina o acesso não autorizado a sistemas para obtenção de segredos nacionais ou para auferir vantagens financeiras.

6 DA DIFICULDADE DE OBTENÇÃO DE PROVAS NO MEIO ELETRÔNICO

No ordenamento jurídico pátrio, não há qualquer empecilho para a utilização de provas eletrônicas, conforme versa o art. 225 do Código Civil[75]:

> As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão.

Pedro Batista Martins conceitua prova como sendo "o conjunto de elementos de que se serve o juiz para formar a convicção sobre os fatos que se funda a demanda"[76]

Ademais, o art. 332 do Código de Processo Civil versa que[77]:

> Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa.

O Código de processo penal também aceita as provas eletrônicas, conforme versa o art. 231, "salvo os casos expressos em lei, as partes poderão apresentar documentos em qualquer fase do processo", e, ademais, o art. 232 também versa que "consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares".

Cabe citar também da Medida Provisória n° 2.200-1/2001, sendo que a mesma institui a Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, a qual já em seu art. 1º versa sobre sua finalidade[78].

> Art. 1° Fica Instituída a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Caso se verifique que o documento eletrônico não tenha sido assinado, ou o certificado não esteja vinculado ao ICP-Brasil, pode-se realizar

---

[75] **VADE MECUM**. 11ª Ed. São Paulo. Saraiva, 2011.p.180
[76] **MARTINS**, Pedro Batista. **Comentários ao Código de Processo Civil**. Forense, v.2, p. 383.
[77] **VADE MECUM**. 11ª Ed. São Paulo. Saraiva, 2011.p.442
[78] **BRASIL**. **PRESIDÊNCIA DA REPÚBLICA – Casa Civil – Subchefia para Assuntos Jurídicos** – Medida Provisória n° 2.200-1, de 27 de Julho de 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-1.htm>. Acesso em: 11 abr. 2012.

uma perícia no computador para que se verifique a autenticidade da documentação[79], o credenciamento serve como um selo de qualidade técnica, e não é preponderante na apreciação da prova, uma vez que o Juiz dispõe do Livre Convencimento Motivado, sendo que o mesmo apreciará livremente as provas.

Nos dias atuais as pessoas podem utilizar da assinatura digital e certificação digital, a certificação digital é um tipo de tecnologia de criptografia a qual se usa uma ferramenta de codificação usada para envio de mensagens seguras em redes eletrônicas[80].

A assinatura eletrônica é uma chave privada, um código pessoal que não pode ser reproduzido, a qual evita que o que se esta transmitindo seja lido somente por aquele receptor que possua a mesma chave e é reconhecida com a mesma validade da assinatura tradicional[81].

Os certificados digitais são excelentes instrumentos do mundo atual, pois propiciam autenticidade aos documentos virtuais, não deixando pairar duvidas sobre a origem dos mesmos.

Quando um usuário navega na internet, lhe é atribuído um numero de IP – *Internet Protocol é* esse numero que propicia a identificação do usuário na rede, ou a investigação de algum crime que tenha ocorrido, a questão é que este numero só é atribuído ao usuário no momento em que ele esta conectado, após este período, quando o mesmo desligar o modem, o endereço de IP será atribuído a outro usuário, caso o mesmo não tenha optado por um IP Fixo.

O IP quando solicitado ao provedor de acesso à internet, deve vir acompanhado de data, hora da conexão, e o fuso horário do sistema, sendo que esses dados são imprescindíveis, tendo em vista que sem os mesmos fica impossível fazer a quebra de sigilo dos dados.

---

[79] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.214

[80]**CERT.BR** - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Disponível em: <http:// http://cartilha.cert.br/conceitos/sec8.html>. Acesso em: 11 abr. 2012.

[81] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.216

Após a localização do provedor, deve-se requerer ao juiz o pedido de quebra do sigilo de dados telemáticos[82], para que o provedor de acesso informe quem estava vinculado ao endereço de IP naquele momento em que ocorreu o crime, ou seja, seu endereço físico.

[82]**INSTITUTO FEDERAL CEARÁ**, Tecnologia em Telemática. Disponível em: <http://www.ifce.edu.br/ensino/curso-de-pos-graduacao/185-tecnologia-em-telematica.html>. Acesso em: 12 abr. 2012.

7 COMPETÊNCIA PARA PROCESSAR E JULGAR

No momento em que ocorre um determinado crime na internet, o que se deve observar primeiramente, é onde se desenrolou o mesmo, em qual território a ação se deu.

O problema é que na internet fica muito difícil estabelecer uma demarcação de território, as relações jurídicas que existem podem ser entre pessoas de um país e outro, e entre diferentes culturas, as quais se comunicam o tempo todo, e o direito deve intervir para proteger os litígios que eventualmente vierem a acontecer[83].

Vários usuários registram sites na internet em outros países diferentes daquele em que estão sendo praticadas suas atividades, mas o que ocorre é que a internet não tem barreiras, e pessoas de vários outros países podem acessar um site registrado nos Estados Unidos, mas que as atividades estão sendo elaboradas no Brasil.

Na atualidade existem diversos princípios para se determinar qual será a lei aplicável a cada caso, há o principio do endereço eletrônico, o do local em que a conduta se realizou ou exerceu seus efeitos, o do domicílio do consumidor, da localidade do réu, o da eficácia na execução judicial[84].

No ordenamento jurídico Brasileiro, aplicam-se os artigos 5° e 6° do Código Penal Brasileiro, no que tange a competência para processar e julgar os crimes praticados na internet, sejam eles:

> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
>
> Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.

Como se pode verificar, o ordenamento jurídico pátrio adotou a teoria da ubiquidade, conforme versa o art. 6° do CP, sendo que os delitos que

---

[83] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.80
[84] **PINHEIRO**, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.82

são praticados por brasileiro, tanto no país quanto fora, ainda que transnacionais, será aplicado à lei brasileira, tendo em vista ainda o que dispõe o art. 7° do Código Penal, o qual sujeita a lei brasileira a alguns crimes praticados no estrangeiro[85].

[85] **CRESPO**, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.118.

CONCLUSÃO

Na presente pesquisa procurou-se demonstrar a relação entre o Direito Penal e as novas relações que ocorrem entre os indivíduos em ambientes virtuais.

Foi feito um levantamento dos principais crimes que ocorrem na internet, sendo que ficou bastante claro que a cada dia crescer o numero de usuários que buscam no ambiente virtual propagar seus crimes de uma maneira desenfreada, seja aplicando golpes como estelionatários, iludindo a vitima, ou aplicando golpes fraudulentos, com o uso por exemplo de falsos sites, em que a vitima achando se encontrar no site de um determinado banco, digita todos os seus dados, senha, numero da conta, cartão de crédito, e todos os dados digitados são encaminhados aos bandidos.

Falamos também da pornografia infantil, um mal que assola não só o Brasil, pois o mundo todo compartilha deste infortúnio, sendo que com o surgimento da internet em grande parte do mundo, os criminosos passaram a ter mais facilidade para escolher suas vitimas, tendo em vista que podem se utilizar de sites de relacionamentos, redes sociais, em fim, a pornografia infantil aumentou muito com o advento da internet e a falta de fiscalização pelo poder público nas relações entre os diversos usuários na rede.

Outra questão que foi abordada foram os crimes contra a honra perpetuados na internet, que aumentaram significamente nos últimos anos, tendo em vista o crescente numero de usuários que utilizam a internet no seu dia a dia, e com o sentimento de impunidade dos usuários, pela falta de fiscalização do poder público.

Outro crime que merece destaque são os crimes contra a propriedade intelectual, os quais aumentaram muito, tendo em vista que com o advento da internet, os usuários passaram a ter acesso irrestrito a vários conteúdos que estão presentes na rede, mas que muitas das vezes não estão disponíveis para terceiros, que mesmo assim se apossam dos mesmos sem autorização, e efetuam cópias de softwares, trabalhos acadêmicos, em fim,

praticam os atos e não efetuam uma contraprestação por parte do titular dos conteúdos.

Outro crime que foi destaque trata-se do crime de invasão de privacidade, o qual a tendência é somente aumentar, caso o poder público não crie mecanismos que impeçam as empresas por exemplo, de divulgarem os dados constantes em seus bancos de dados de cadastros de clientes de serem repassados a um terceiro, e que estas empresas também criem mecanismos de segurança para que os dados não sejam copiados por pessoas não autorizadas.

Foi feito uma análise da legislação brasileira e de alguns países sobre a questão dos crimes virtuais, sendo que ficou constatado que no direito brasileiro algumas condutas conseguem ser abarcadas pela legislação atual, mas outras ainda não passam de projetos de lei, ou seja, o Direito deve acompanhar a evolução da sociedade para que as relações entre os indivíduos que utilizam meios eletrônicos no seu dia a dia, não sintam insegurança em suas relações com terceiros em ambientes virtuais.

No que tange as legislações de outros países, os mesmos ainda estão se adaptando a nova realidade sobre os crimes virtuais, mas ainda assim se mostram mais receptivos as novas realidades criminosas, sendo que em muitos ordenamentos já há previsão quanto as condutas mais atuais.

Foi elaborada uma análise ao processo probatório relacionado aos crimes perpetuados na rede, sendo que ficou demonstrado que ainda é muito difícil se extrair uma prova de um crime que ocorra com o uso de mecanismos tecnológicos, sendo que em muitas das vezes é necessário a intervenção de peritos especializados para se atestar a autenticidade de determinados documentos, ou para se extrair a prova de um computador, por exemplo, e em outras vezes a dificuldade esbarra na capacidade técnica dos criminosos, que se escondem atrás de terminais existentes em outros países.

No ultimo capítulo ficou claro que não há ainda qualquer problema quanto a competência para processar e julgar os crimes virtuais que venham a ocorrer por usuários que se encontrem no Brasil, conforme art. 5°, 6° e 7° do

Código Penal, não deixando margem de dúvida quanto a aplicação do ordenamento jurídico pátrio.

O que se busca com o presente trabalho de pesquisa é abrir os olhos aos profissionais do Direito quanto a importância de se adequarem a nova realidade no que concerne aos crimes que são perpetrados tendo como meio a internet, e, a necessidade do poder público aprovar os projetos já existentes em pauta, e aplicar mecanismos de maior rigor na apuração de ilícitos que venham a ocorrer em ambiente virtual, sendo que aos poucos a sociedade está migrando para uma sociedade cada vez mais digital.

REFERÊNCIAS

ABRAIC – Associação Brasileira dos Analistas de Inteligência Competitiva. Glossário de IC. Disponivel em: <http://www.abraic.org.br/V2/glossario.asp?letra=I>. Acesso em: 01 mar. 2012.

ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade**. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2250>. Acesso em: 18 mar. 2012.

BARBOSA, Denis Borges; ARRUDA. Mauro Fernando Maria. **Sobre a Propriedade Intelectual**. Rio de Janeiro: Campinas, 1990.

BRASIL. Código Penal. Decreto Lei n. 2.848/40. Disponível em <http://www.dji.com.br/codigos/1940_dl_002848_cp/cp184a186.htm>. Acesso em: 10 abr. 2012.

BRASIL. Supremo Tribunal Federal – RHC n. 76.689-0 – Pernambuco – Primeira Turma – Relator: Ministro Sepúlveda Pertence, DJU de 6.11.1998.

BRASIL. PRESIDÊNCIA DA REPÚBLICA – Casa Civil – Subchefia para Assuntos Jurídicos – Medida Provisória n° 2.200-1, de 27 de Julho de 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-1.htm>. Acesso em: 11 abr. 2012.

BORLAND. A Micro Focus Company. O que é a Pirataria de Softwares. Disponível em: <http://www.borland.com/br/piracy/what_is_piracy.aspx>. Acesso em: 10 abr. 2012.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

CERT.BR - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Disponível em: <http://www.cert.br>. Acesso em: 10 mar. 2012.

CERT.BR - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Disponível em: <http:// http://cartilha.cert.br/conceitos/sec8.html>. Acesso em: 11 abr. 2012.

CERT.BR - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**.Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2011. Disponível em: <http://www.cert.br/stats/incidentes/2011-jan-dec/fraude.html>. Acesso em: 31 mar. 2012.

CERT.BR - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Cartilha. Disponível em: <http://cartilhacert.br/glossario>. Acesso em: 31 mar. 2012.

CERT.BR - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Cartilha. Disponível em: <http://cartilha.cert.br/fraudes/sec2.html#sec2>. Acesso em: 18 mar. 2012.

ECAD – Escritório Central de Arrecadação e Distribuição. O que é Direito Autoral. Disponível em: <http://www.ecad.org.br/viewcontroller/publico/conteudo.aspx?codigo=48>. Acesso em: 10 abr. 2012.

EDUCACIONAL. Vida Inteligente o computador no dia-a-dia. Disponível em: <http://www.educacional.com.br/vidainteligente/clickdigital02/e-commerce.asp>. Acesso em: 01 abr. 2012.

FOLHA.COM, Entenda o que é o código-fonte de um programa. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u7618.shtml>. Acesso em: 10 abr. 2012.

FOLHA.COM. CPI aprova quebra de sigilo de 18 mil páginas do Orkut. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u418514.shtml>. Acesso em: 01 abr. 2012.

FRAGOMENI, Ana Helena. **Dicionário Enciclopédico de Informática**. Vol.I. Rio de Janeiro: Campus, 1987.

FRAGOSO, Heleno Cláudio. **Lições de direito penal: parte especial**: arts. 121 a 212 do CP. Rio de Janeiro: Forense, 1983.

GIL, Antônio de Loureiro. **Fraudes Informatizadas**. 2 ed. São Paulo: Atlas, 1999.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

HOLANDA FERREIRA, Aurélio Buarque de. **Novo dicionário da língua portuguesa**. 12ª Ed. Rio de Janeiro: Nova Fase, 2000.

INELLAS, Gabriel Cesar Zaccaria. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004.

INSTITUTO FEDERAL CEARÁ, Tecnologia em Telemática. Disponível em: <http://www.ifce.edu.br/ensino/curso-de-pos-graduacao/185-tecnologia-em-telematica.html>. Acesso em: 12 abr. 2012.

LEMOS, André/LÉVY, Pierre. **O futuro da Internet: em direção a uma ciberdemocracia**. São Paulo: Paulus, 2010.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas, SP: Ed. Millennium, 2005.

LIMBERGER, Têmis. **O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais**. Porto Alegre: Livraria do Advogado Editora, 2007.

MARTINS, Pedro Batista. **Comentários ao Código de Processo Civil**. Forense, v.2.

OCDE – Organisation de Coopération ET de Développemente Economiques. Disponível em: <http://www.oecd.org/home/0,3675,fr_2649_201185_1_1_1_1_1,00.html>. Acesso em: 10 abr. 2012.

PECK, Patrícia. **Direito digital**. São Paulo: Saraiva, 2002.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.

SUAPESQUISA – Formulários e Pesquisas Online. Revolução Industrial, História da Revolução Industrial, pioneirismo inglês, invenções de máquinas, passagem da manufatura para a maquinofatura, a vida nas fábricas, origem dos sindicatos. Disponível em: <http://www.suapesquisa.com/industrial>. Acesso em: 24 abr. 2012.

SUPERDICAS - Invenções que mudaram o mundo e sobreviveram ao tempo. Disponível em: <http://www.superdicas.com.br/almanaque/almanaque.asp?u_action=display&u_log=254>. Acesso em: 24 abr. 2012.

TECMUNDO – Disponível em: <http://www.tecmundo.com.br/o-que-e/3615-perito-digital-o-que-ele-faz-e-como-consegue-recuperar-informacoes-perdidas.htm>. Acesso em: 01 abr. 2012.

TECMUNDO, Disponível em: <http://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.html>. Acesso em: 18 MAR. 2012.

TERRA. Carnaval 2012 – Pornografia infantil movimenta R$ 4 bilhões. Disponível em: <http://diversao.terra.com.br/carnaval/2012/videos/0,,196577.html>. Acesso em: 01 abr. 2012.

VADE MECUM. 11ª Ed. São Paulo. Saraiva, 2011.

ZANELLATO, Marco Antonio. **Condutas Ilícitas na sociedade digital**, Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet, n. IV, Julho de 2002.