UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS – UNIPAC
FACULDADEDE CIÊNCIAS JURÍDICAS E SOCIAIS DE BARBACENA – FABI
CURSO DE GRADUAÇÃO EM DIREITO

JÉSSICA CAMPOS SILVEIRA

CRIMES VIRTUAIS

BARBACENA
2015

JÉSSICA CAMPOS SILVEIRA

CIRMES VIRTUAIS

Monografia apresentada ao Curso de Graduação em Direito da Universidade Presidente Antônio Carlos – UNIPAC, como requisito parcial para obtenção de Bacharel em Direito

Orientador: Profª. Geisa Rosignoli Neiva

BARBACENA
2015

JÉSSICA CAMPOS SILVEIRA

CRIMES VIRTUAIS

Monografia apresentada ao Curso de Graduação em Direito da Universidade Presidente Antônio Carlos – UNIPAC, como requisito parcial para obtenção de Bacharel em Direito

Orientador: Profª. Geisa Rosignoli Neiva

Aprovada em ___/___/___

BANCA EXAMINADORA

_____

Profª. Geisa Rosignoli Neiva
Universidade Presidente Antônio Carlos - UNIPAC

_____

Profª. Josilene Nascimento Oliveira
Universidade residente Antônio Carlos – UNIPAC

_____

Prof. Fernando Antônio Mont'alvao do Prado
Universidade Presidente Antônio Carlos - UNIPAC

Dedico aos meus pais e irmã, por me ajudar a realizar mais uma etapa da minha vida; aos meus familiares e amigos pelo apoio e paciência que tiveram comigo nessa caminha.

AGRADECIMENTO

Agradeço primeiramente, a Deus, por ter me concebido o dom da vida, sempre guiando meus passos e iluminando meu caminho, permitindo que eu chegasse até aqui.

Minha eterna gratidão aos meus pais Cesar e Maria Aparecida, por acreditarem e lutarem comigo, para que eu pudesse realizar esse sonho, a minha irmã por estar comigo em todas as horas que eu sempre precisei.

A minha família que inclui meus avós, tios (as), primos (as) e claro meus amigos, por trilharem comigo e me poiarem em todas as formas possíveis. Desculpa pelas ausências mas foram essências para chegar aqui.

Aos docentes da Universidade Presidente Antônio Carlos, que muito me ensinaram dentro e fora da sala de aula, deixando seu melhor em mim.

Agradeço é claro a aqueles que confiaram em mim e me deram a oportunidade de aprenderem com eles.

SUMÁRIO

RESUMO

Este trabalho tem o objetivo de mostrar o histórico sobre a internet e os crimes virtuais mais cometidos, por *hackers* e *crackers*, até os dias atuais. Apresenta de forma direta e sucinta todos os assuntos relativos aos cibercrimes e a maneira com que os transgressores agem para fraudar suas vítimas. Versa sobre sua aplicação penal e os incontáveis prejuízos causados à sociedade. Também apresentaremos as dificuldades apresentadas pelas autoridades ao coletar as informações necessárias para a busca e o enquadramento da pena ao autor 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: Crimes Virtuais. Ambiente Virtual. Internet. Violação. Punição.

ABSTRACT

This work alms to sohw a historic about the internet and the cybercrimes more committed by hackers, till presente day. Intriduce directty and succinctly all matters relating to cybercrimes And the way the trangressors act to depraud their victims. Traverse about your criminal enforcement and the coumtless losses caused to society. Also presentes the difficulties of authorities to gather impormation for the search and proming of pen to author and what exists today of law's projects about the topic. Thoroughout the study will use some terms typical of users already familiar with the cyber ambience, the use is purposeful, because is sought to familiarize the reader with the terso f this digital wordl.

KEYWORDS: Virtual Crimes. Virtual environment. Internet. Violation. Punishment.

INTRODUÇÃO

O direito está presente em toda parte, em cada momento da vida dos indivíduos. Ele é o responsável para dar soluções aos conflitos interpessoais e institucionais que vem de uma sociedade moderna, que avança muito rápido, devido a inúmeras descobertas e avanços tecnológicos e científicos que dão facilidade e agilidade ao dia a dia de todos nós cidadãos. Com isso fez com que a distância fosse encurtada e a relação entre pessoas passasse a ser feita na maior parte por aparelhos eletrônicos conectados à rede.

O objetivo principal deste trabalho é analisar a investigação dos crimes contra a honra, contra a liberdade individual, contra o patrimônio e contra os costumes que com o avanço repentino da tecnologia, vêm sendo realizado, não mais de forma pessoal, mas sim de forma anônima, através do uso da rede de computadores como a internet.

O possível anonimato faz com que os indivíduos tenham uma ilusão de segurança muito pregaria, sendo que toda vez que a um computador ao conectar-se na rede mundial de computadores, faz com que a mesma tenha um endereçamento que permite que haja uma comunicação sem conflitos e choque de transmissão de dados. Este endereço chamado IP (internet protocol), é responsável pela recepção e transmissão de dados entre as maquinas sem que tenha perda das informações, devido à distribuição de servidores que identifica cada máquina conectada à rede.

Com esta identificação de cada máquina na rede, nós usuários de cada máquina, estamos seguramente identificados nos servidores, onde armazenamos a localidade e o usuário que ali está conectado, possibilitando assim que àqueles usuários que por ventura use a internet para a prática dos crimes através da internet.

No primeiro capítulo se demostra a evolução do direito digital, desde o surgimento do primeiro computador até os dias de hoje, no segundo falamos da definição do que é ou não um delito virtual, ou crime virtual.

No terceiro capítulo procurou demostrar as condutas danosas praticadas pelos criminosos, no quarto foi feito uma classificação dos crimes virtuais, e a classificação dos crimes de acordo com a conduta do agente.

No quinto é destinado a analisar algumas das condutas criminosas que são realizadas com o uso de equipamentos eletrônicos, e muitas das vezes tendo o caminho para execução destes crimes a Internet, no sexto capítulo foi feito um apanhado da legislação nacional frente aos crimes.

No sétimo e oitavo capítulo foi feita uma pesquisa no doutrinadores principais que dominam o assunto dos crimes virtuais, a qual buscou demonstrar a dificuldade em se apurar um crime que se desenrola no ambiente virtual, visto que não há barreira entre os usuários da Internet, e, qual é alei que deve ser aplicada quando se realiza um crime em ambiente virtual.

E no último capítulo falamos da que a lei brasileira é avançada em alguns casos, e limitada ao que diz respeito aos crimes virtuais. No ano de 2012, a atriz Carolina Dieckmann, teve divulgação de suas imagens intimas em diversos sites eletrônicos da rede mundial de computadores, que tomou grande popularidade, fazendo com que a legislação pátria até então vigente, que não tinha um regulamento a respeito a esses delitos. Após o ocorrido com a atriz tomar grande proporção, foi aprovada a Lei de nº 12.373 e a 12.735, ambas entraram em vigência depois de decorrido 120 (cento e vinte dias) dias de sua publicação.

As leis referidas têm um objetivo que é acabar com os crimes virtuais. Portanto, o que vale ressaltar é que mesmo com a vigência destas leis, são poucos os estados no Brasil, que podemos dizer que tem estrutura para combater esse tipo de crimes.

1- EVOLUÇÃO HISTÓRICA

A informática teve início na II Guerra Mundial, quando surgiram os primeiros computadores. Ao longo do século XX, os computadores sofreram muitas notificações, chegando a atual 5º geração, tendo a internet como a sua principal função.

Em 1969, quando a subdivisão do Departamento de Defesa dos Estados Unidos, ARPA, criou a ARPANET, sua finalidade era espalhar informações para vários departamentos, evitando que o ataque a um deles provocasse perda das informações. Com o fim da Guerra Fria, a ARPANET deixou de ser uso exclusivo dos militares, sendo liberada para as universidades, possibilitando uma rápida troca de informações (PINHEIRO, 2006)

Em 1987, foi liberada para uso comercial, sendo "o grande marco para o desenvolvimento desta tecnologia" (COSTA, 2011, p.23), pois, motivou o fim das operações da ARPANET em 1990, sendo substituída por sistemas mais rápidos. Já em 1993, com o desenvolvimento do WWW (World Wide Web), a internet popularizou-se.

No Brasil, os primeiros passos foram em 1988, quando a Rede Nacional de Pesquisa (RNP) e o Ministério da Ciência e Tecnologia começou a investir na tecnologia. Em 1992, os primeiros pontos foram instalados em algumas universidades, já em 1995, for liberada para uso comercial. (COSTA, 2011)

Atualmente pode-se acessar a internet por microcomputadores, celulares, videogames e até geladeira. A conexão pode ser através de linhas telefônicas fixas e moveis, por cabo, satélite, radio e infravermelho.

2- CONCEITO DOS CRIMES VIRTUAIS

Ao lado de todos os benefícios trazidos, com a disseminação dos computadores e do acesso à internet, surgiram novas formas de violação de bens jurídicos protegidos os quais passaram a ser realizados não mais no plano físico, mas sim, no virtual.

Conforme Colli (2009, p.07): "apesar de internet facilitar e ampliar a inter comunicabilidade entre as pessoas, ela pode ter sua finalidade transformada em um meio para a pratica e a organização de infrações penais. Dentre estas despontam os chamados crimes informáticos [...]". Ressalta, que a internet pode ser tanto ambiente para consumação de crimes, quanto para realização de atos preparatórios, como rixas entre torcidas organizadas.

O conceito de crime virtual tem despertado controvérsias, trazemos alguns conceitos de estudiosos no assunto.

Para Ramalho Terceiro:

> [...] os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas.

Segundo Augusto Rossini:

> [...] o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

A Organização para a Cooperação Econômica e desenvolvimento da ONU, conceitua "crime de informática" como qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento de dados e/ou transmissão de dados.

O crime virtual em outras palavras é ação típica, antijurídica e culpável cometida contra ou utilização de processamento automático de dados ou sua transmissão em que o computador conectado à internet, seja o objeto de delito ou o instrumento.

Tem alguns autores que classificam os crimes em puros e impuros ou mistos. Os puros seriam aqueles no qual o infrator visa especificamente ao sistema de informática dos dados e sistemas e dos meios de armazenamento (crimes da dano e acesso não autorizado); e os impuros ou mistos é o sistema informático utilizado é mera ferramenta para a infração de outros bens jurídicos (estelionato, ameaça, etc).

Percebe-se que não há consenso sobre o que é considerado crimes virtuais, e muito menos uma denominação aceita.

Não há atualmente uma legislação específica para o é crime na rede, eventuais condenações são baseadas no Código Penal de 1984, antes da existência da Internet.

3- CONDUTAS DANOSAS DA INTERNET

Estima-se que cerca de 54,4% de brasileiros acessam a internet, e não para de crescer esse número (IBGE - 2014). Segundo estudos realizados pelo site alemão Alldas.de, o Brasil atualmente tem o maior trupe de *hackers* no mundo, entre os feitos desse grupo, se registra invasões contra a IBM Americam, Péntagono e a Microsoft.

Os criminosos passavam muita das vezes impunes, devido a não existir previsão legal que defina aquele delito como crime, conforme artigo primeiro do Código de Processo Civil (Princípio da Legalidade). A finalidade desde princípio é limitar o poder punitivo do estado, pois o crime para se configurar necessita de tipificação, uma conduta comissiva ou omissiva e esteja valido para provocar efeitos.

Dos condutas danosas praticadas podemos citar as mais corriqueiras:

Crimes contra a honra: São os crimes de calúnia (artigo 138), difamação (artigo 139) e injúria (artigo 140). Os crimes podem ocorrer em chats, blogs, pelo envio de spams, através de publicações em homepages, dentre outros meios de postagem eletrônica, os criminosos são incentivados pelo anonimato, estes crimes devem contar com a agravante no inciso III, do artigo 141, do Código Penal, pela facilidade de divulgação proporcionada pela Internet. Além das dificuldades de investigação inerentes à Internet, a polícia também esbarra na questão territorialidade, pois se o site está hospedado em um provedor estrangeiro, de um país como os Estados Unidos da América, onde é totalmente livre qualquer tipo de manifestação de opinião, então não é possível exigir a retirada do site ou das mensagens, nem mesmo processar o autor do crime.

Crimes contra a liberdade individual: São os crimes de ameaça (artigo 147), inviolabilidade de correspondência (artigos 151 e 152), divulgação de segredos (artigos 153 e 154), divulgação de segredos contidos ou não em sistemas de informação ou bancos de dados da Administração Pública (artigo 153, § 1º-A).

O crime do artigo 151, crime de violação de correspondência, é um tipo aplicável a conduta de interceptação de *e-mail* e sua violação, se equipararmos a correspondência eletrônica à correspondência tradicional – o que é possível uma vez que comunicação telegráfica ou radioelétrica dirigida a terceiro, assim como conversação telefônica entre pessoas também são tuteladas pelo artigo 151, em seu § 1º, e a Internet, neste aspecto, é apenas uma evolução dos meios de comunicação –, pois o bem jurídico que visa proteger é o sigilo das informações, a liberdade de comunicar-se e se expressar através de correspondência. O sigilo das informações de uma correspondência é garantia fundamental, e está prevista no artigo 5º, XII, da Constituição Federal a proibição da sua violação.

Os crimes previstos nos artigos 153, 153, § 1º-A, e 154, recebe o mesmo tratamento que o crime de violação de correspondência, pois é necessário equiparar o documento eletrônico ao tradicional, o que não apresenta dificuldades pois o documento eletrônico é formado por *bits* que o computador traduz em símbolos gráficos que representam letras, ao passo que o tradicional é composto de símbolos também – letras ou imagens.

Crimes contra o patrimônio: Compreende os crimes de furto (artigo 155), extorsão (artigo 158), dano (artigo 163) e estelionato (artigo 171).

Nos tipos de furto e roubo o bem jurídico protegido é o patrimônio, então a criação de outro tipo penal é desnecessária somente para discriminar o meio de execução do delito que costuma ser através de manipulação de dados - fraude por manipulação de um computador contra um sistema de processamento de dados - para modificação de depósitos bancários e obtenção de vantagem econômica, ou, ainda, a obtenção de dados como senhas para manipular contas bancárias e obter vantagem financeira.

Para alguns a criação de um tipo para lidar com o que chamamos de furto virtual é necessária, dentre eles está Ramalho Terceiro que coloca o problema na diminuição do patrimônio, pois não haverá a diminuição do patrimônio da vítima se o criminoso só copiar arquivos ou informação de banco de dados.

Dados estatísticos mostram que 400 milhões de computadores no mundo todo estão infectados por vírus. E o Brasil é o sexto país mais afetado, até o ano de 2014.[1]

Quanto ao estelionato, para se configurar se faz necessário induzir ou manter alguém ao erro mediante ardil (ao menos uma determinada pessoa e não um sistema eletrônico), é necessário uma relação psicológica entre autor e vítima, que deve se sentir iludida.

É nesse lugar que os criminosos utilizam de suas maiores artimanhas, através de cavalos-de-tróia, clonando sites e utilizando a engenharia social.

Crimes contra os costumes: São os crimes de favorecimento à prostituição (artigo 228), de escrito ou objeto obsceno (artigo 234) e a pedofilia (artigo 241, da Lei 8.069/90). É muito comum encontrar sites (paginas) de pornografia e de prostituição, aliás, é muito difícil fazer uma pesquisa em um site de busca, sobre qualquer tema, em que não apareça pelo menos um resultado indicando um link sobre pornografia.

Nos últimos anos intensificou-se o movimento mundial contra a pedofilia, tendo a Convenção de Budapeste, também conhecida como Convenção sobre Crimes Virtuais, dado ênfase à proteção da criança e do adolescente.

Bem lembrado por Felipe Cardoso Moreira de Oliveira que:

> Um usuário da web que em sua home page publique fotografias ou filmes pornográficos, envolvendo crianças ou adolescentes, certamente terá de responder pelo delito previsto no referido artigo. Não basta, porém, para a configuração, a simples colocação de links capazes de proporcionar o acesso a outras páginas que contenham esse material; o administrador da página remota não é o usuário em questão; não lhe pode ser atribuída a responsabilidade sobre a conduta de terceiro.

[1] http://g1.globo.com/fantastico/noticia/2014/04/virus-infectam-cerca-de-400-milhoes-de-computadores-no-mundo.html

Além dos citados crimes, podem ocorrer na Internet crimes de lavagem de dinheiro e invasões de privacidade, pichações em sites oficiais do governo, vandalismo, sabotagem, crimes contra a paz pública, a pirataria em geral, espionagem, lesões a direitos humanos - terrorismo, crimes de ódio, racismo, etc -, destruição de informações, jogos ilegais, falsificação do selo ou sinal público, falsidade ideológica, modificação ou alteração não autorizada de sistema de informação, violação de sigilo funcional, fraude em concorrência pública, dentre muitos outros.

Todas as condutas acima citadas utilizam a Internet como meio para a conduta, o fim é obter vantagem do usuário do computador alvo, ou, ainda, atacar a honra deste.

Para alguns dos autores, o verdadeiro crime virtual, ou seja, a conduta lesiva que necessita de legislação, por não encontrar amparo na lei penal vigente é o crime de *hacking*, denominação proposta por Marcelo Baeta Neves Miranda, consistente no acesso a um determinado sistema por particular sem autorização. Conforme o autor, em outros países já existem leis que visam coibir o ataque dos *hackers*, quais sejam: a) Copyright, Designs and PatentsAct (Inglaterra-1988); b) Computer Fraudand Abuse Act (E.U.A. - 1986) e c) Communication DecencyAct (E.U.A. – 1996).

Mas, se toda conceituação e classificação de condutas passa pela identificação do bem jurídico, então, até o momento presente, não há nenhuma conduta que necessite da criação de um novo tipo penal.

4- DOS CRIMES DE INFORMÁTICA E SUAS CATEGORIAS

Hoje a cada dia o número de pessoas que acessa a internet só cresce, existem muitos websites na internet, e a cada dia mais homepages são criadas, hoje se encontra basicamente tudo na internet, desde de compras de qualquer eletrônico, até mesmo concluir um curso universitário, o que acontece é que os usuários estão sujeitos aos mais variados crimes, 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 classificação não é uma tarefa fácil, tendo que ainda existem poucas conclusões a respeito, porque a tecnologia evolui a passos largos, e a opinião dos doutrinadores também muda conforme segue a evolução tecnológica de ano a ano.

Em determinados crimes não seria possível a consumação sem o uso do sistema informático, várias condutas utilizam os computadores como meio para o cometimento dos delitos.

Tiedemann formulou em 1980 a seguinte Classificação dos delitos informáticos:

> 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.

O doutrinador estrangeiro Rovira Del Canto, deu uma classificação mais ampla no conceito, a qual subdividiu os delitos em Infrações à intimidade; ilícitos econômicos; ilícitos de comunicação pela emissão ou difusão de conteúdos ilegais ou perigosos; e, outros ilícitos

Greco Filho 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 Vladimir Aras tem sua classificação da seguinte forma:

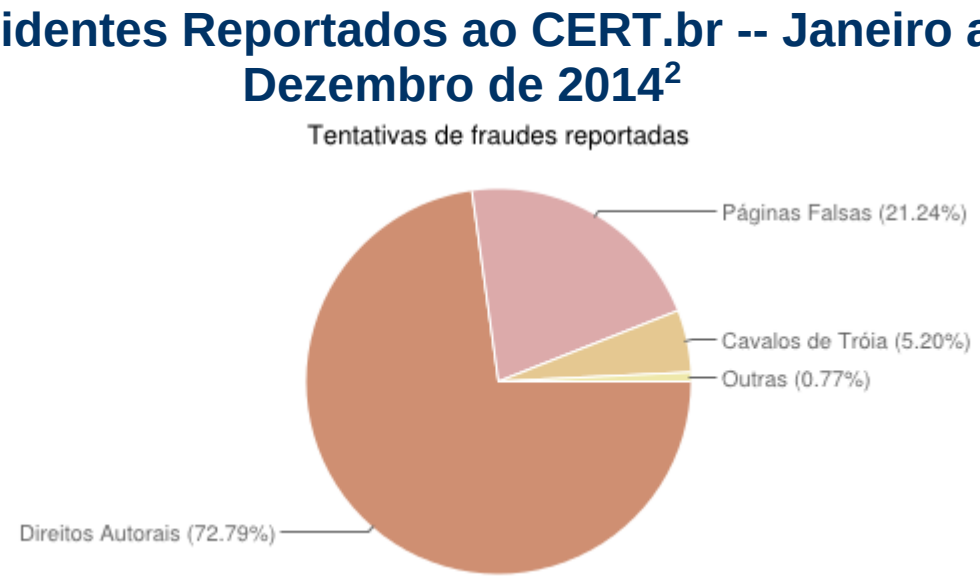
> a) uma primeira, onde estão substancialmente unidos pela circunstância que o computador constitui a necessária ferramenta de realização pela qual o agente alcança o resultado legal;
> b) a segunda categoria de crimes do computador, poderia incluir todos aqueles comportamentos ilegítimos que contestam 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 a cima há pontos em comum e distinções, alguns doutrinadores 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 mais opções acerca das práticas.

5- CRIMES POR MEIO DO COMPUTADOR E INTERNET

É uma tarefa delicada e difícil de analisar as condutas criminosas que se espalham pela internet, uma vez que é muito difícil verificar onde o agente que praticou o crime se encontra, tendo em vista que os crimes virtuais não encontram barreiras na internet e se perpetuam livremente pela rede. A maioria dos crimes que ocorrem na rede existe no mundo real, o que ocorre é que existem alguns crimes com algumas peculiaridades, o que faz com que seja necessário uma adaptação quanto ao seu tipo penal, logo analisaremos alguns crimes da era Digital e outros já existentes que passaram a ser executados virtualmente.

5.1- FRAUDES VIRTUAIS



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 crime virtual é definido como sendo Fraude Virtual, onde o agente pratica uma conduta de invasão, alteração ou modificação, ou qualquer outra adulteração em um sistema de processamento de dados.

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

---

[2]CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2014. Disponível em: http://www.cert.br/stats/incidentes/2011-jan-dec/fraude.html. Acesso em: 06 dez. 2015.

> 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.

As fraudes eletrônicas vêm crescendo muito rápido nos últimos anos, principalmente no que diz respeito à modalidade de furto mediante fraude - art. 155 do Código Penal -, a qual é caracterizado pelo envio de um e-mail falso para um usuário, e lá é capturado dados de sua conta bancária, dados pessoais, mediante a instalação de um programa em seu equipamento de acesso à internet.

As fraudes virtuais 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.

O usuário é induzido a fornecer seus dados pessoais e financeiros nas fraudes, na maioria das vezes por trás de páginas duvidosas, o qual o usuário e encaminhado para páginas fraudulentas, muitas vezes os eles utilizam as mídias sociais.

O 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 vem discutido, é se poderia enquadrar o furto de dados como sendo o furto deste artigo, tendo que poderia o mesmo não se enquadrar no tipo legal, visto que na conduta o agente pode levar os dados da empresa e apagá-los, sendo que não haveria a indisponibilidade do bem, no caso para configurar a subtração.

5.2- ESTELIONATO

No nosso ordenamento jurídico o estelionatário é o agente ativo, entendido como sendo qualquer pessoa que cometa o crime de estelionato de forma dolosa, pela livre e consciente vontade. A figura do estelionato em ambiente virtual é novo, alguns autores divide as condutas delituosas em face dos computadores, e contra os dados os quais se encontram neles, já que a Internet vem atingindo e adquirindo milhares de usuários novos a cada dia, merece atenção especial.

O artigo 171 do Código Penal versa 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.

Ainda que o Código Penal Brasileiro faça menção do estelionato em seu texto, a conduta descrita diz respeito ao delito praticado de forma direta pelo infrator, de induzir ou manter a vítima em erro, e com isso, obtendo vantagem elícita, para si ou para outrem. Várias são as condutas dos estelionatários na Internet, a questão é tipifica-las como estelionato, o legislador previu, como meio executório a fraude com o objetivo de obter consentimento da vítima, iludi-la para que entregue o bem voluntariamente, enganando, levando a vítima a erro.

Uma das condutas típicas do estelionato virtual baseia-se na conduta do agente de encaminhar e-mails com conteúdo falso, induzindo a clicar em links disponíveis no e-mail, em que várias vezes leva o usuário para sites falsos onde lá digita informações pessoais ao agente que formulou a página falsa, essas informações são enviadas por meio da Internet, que após de se apoderar de seus dados bancários, transfere os valores disponíveis em conta para seu domínio.

A maneira de tentar se livrar desses e-mails é a instalação de antivírus, o qual deve ser configurado para excluir e-mails falsos, tidos como ataques ao computador, à exclusão pode ser feita antes mesmo dos e-mails serem recebidos, ou, efetuar a configuração de segurança do Firewall.

O obstáculo surge quando a tipificação do estelionato na legislação penal, que se mostra inativo quanto ao uso. Nota-se que a Constituição Federal traz no inciso 39 do artigo 5º o Princípio da Legalidade, que encontra-se no primeiro artigo do CPB, in verbis:

> “Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.”

Com esse princípio exposto acima, qualquer indivíduo que comete crime deverá ser punido com base neste inciso, o fato deve se adequar na legalidade da lei, não podendo ser reprovável sem que cumpra os requisitos de validade, para que o processo penal tenha seu curso normal e previsto.

Neste caso, Cesar Roberto Bitencourt, comprova:

> "O princípio da legalidade ou da reserva legal constitui efetiva limitação ao poder punitivo estatal. Feuerbach, no início do século XIX, consagrou o princípio da reserva legal por meio da fórmula latina nullumcrimen, nullapoenasine lege. O princípio da reserva legal é um imperativo que não admite desvios nem exceções e

> representa uma conquista da consciência jurídica que obedece a exigências de justiça; somente os regimes totalitários o têm negado".

Diante disto, conclui que para a pratica do estelionato na Internet e de qualquer outro crime é necessário a presença de três requisitos essenciais que compõem o fato típico, que sem eles seriam impossível a imputação de penalidade do agente.

O primeiro requisito fala da tipificação expressa do crime em lei, ou seja, sua denominação legal e precisa do ato volitivo contributivo do infrator para o resultado final. Se não houver tal tipificação, a materialidade para o delito irá desaparecer, o tornando atípico e não punível pela legislação jurídica penal brasileira.

O próximo requisito fundamental que se encaixa ao delito é a conduta do autor, que pode se dar de forma comissiva ou omissiva, dolosa ou culposa. A conduta comissiva se alega em uma ação positiva desencadeada pelo transgressor, ocorrendo quando a ação for proibida por lei, como por exemplo, matar alguém, contrariando o que diz o artigo 121 do CPB.

Já na hipótese de ato omissivo, o indivíduo age negativamente, deixando de praticar algo que era devido por obrigação ou que poderia fazer para amenizar a consequência derradeira, como a inércia de pedido de socorro em ocorrências de acidente automobilístico com vítimas, caracterizando a omissão de socorro.

O estelionato virtual ou real não admite a modalidade culposa, valendo-se do preceito que o estelionatário sempre irá proceder com a vontade de induzir ou manter a vítima em erro, criando situações que se furtam, não advindo à situação negligência, imprudência ou imperícia. Portanto, toda fraude classificada como estelionato será sempre dolosa, onde o autor age livre e consciente de praticar a conduta inserida na norma penal incriminadora.

A prática do estelionato virtual é operado na maioria das vezes por pessoas com notável conhecimento sobre internet e tecnologia de informação, que possa agir de outra maneira, mas prefere se investir no mundo virtual do crime para prejudicar pessoas, obtendo algum tipo de vantagem com isso. A única diferença entre o estelionato virtual e o estelionato real está no *modus operandi* empregado, onde, é realizado pela internet, enquanto aquele no mundo físico.

Os usuários com conhecimento avançado da informática e que comete crimes e outras ações maldosas, são chamados de *crackers*, que na definição de Fabrízio Rosa, ensina que:

> "*Cracker* é o mesmo que *hacker*. A diferença entre um e outro está em utilizar o seu conhecimento para o mal. Destruir e roubar são suas palavras de ordem. Assim, o *cracker* usa os seus conhecimentos para ganhar algo, rouba informações sigilosas para fins próprios e destrói sistemas para exibir".

O *cracker* utiliza o avançado conhecimento que possui para praticar crimes ou danificar sistemas, e no caso do estelionato, ele é o protagonista principal, haja vista a grande maioria dos crimes serem praticados por estes usuários maliciosos. No entanto, muitos usuários comuns também cometem crimes, haja vista a facilidade que a internet proporciona para isto.

Permanecendo na matéria, tem o personagem pouco conhecido do *loser*, que é um operador de internet novo e sem muita experiência técnica, entretanto, é atraído intimamente pelo mundo virtual e quer adquirir cada vez mais novos conhecimentos. É correto dizer que o *loser* é um *hacker* em potencial, pois seu maior desejo é um dia se tornar um, e não mede esforços em estudar e perguntar para outras pessoas como proceder nas mais diversas situações.

O perito judicial na área de informática Pedro Augusto Zaniolo classifica o *loser* da seguinte maneira:

> "*Loser* é a união *loser* (perdedor) e *user* (usuário) e denota aquele que não quer aprender nada útil, objetivando apenas saber o mínimo necessário para operar o computador e terminar suas tarefas o mais rápido possível."

A ausência de legislação específica acaba por induzir os criminosos a cometer esta modalidade de infração, pois eles acreditam que não haverá punição devido à falta de lei. Muitos são os problemas que rondeiam o estelionato virtual, dentre os quais: a dificuldade de identificação dos autores, a delimitação do local do crime e a competência do juízo.

A grande problema de identificar os autores é que a rede mundial de computadores interliga pessoas do mundo inteiro, e em alguns casos é praticamente impossível localizar onde foi gerado o ato ilícito, sabendo que o criminoso pode-se ter inúmeros computadores e locais diferentes de acesso para gerar o fato. Devido ao computador e a internet serem objetos móveis, muitas vezes um único crime cometido por apenas um autor "passa" por diversos lugares, impossibilitando o trabalho de identificação de autoria.

Segundo o Código Penal Brasileiro, o seu artigo 6º, diz que o lugar do crime é aquele local onde ocorreu a ação ou a omissão por artefato do agente, ainda que em parte, bem como onde se produziu ou deveria ser produzido o resultado. Esta regra é de uso obrigatório quando da ocorrência de crimes reais, contudo, no caso de crimes eletrônicos ou virtuais, isto se distorce um pouco. A teoria adotada pelo CPB a respeito da aplicação da lei penal no espaço recebe o nome de teoria mista ou da ubiquidade.

5.3- INVASÃO DE PRIVACIDADE

As pessoas que utilizam a rede mundial de computadores para acesso a informações diversas, ou para compra de produtos, enfim, para um número por vezes ilimitado de situações onde a internet possibilita se realizar inúmeras questões, o que ocorre, e que as informações que estão disponíveis ou não na internet, pode 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.

O que se procura na verdade é resguardar o cidadão em relação aos seus dados que estão disponibilizados na rede, sejam aqueles disponíveis em órgãos públicos, ou em entes privados, mesmo porque os dados pessoais não podem ser tratados como mercadoria, tendo em vista que se deve considerar seus aspectos subjetivos, o Estado deve garantir os direitos da pessoa, de 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.

5.4- CRIMES CONTRA A HONRA

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

Honra são as qualidades de um indivíduo 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.

Um dos crimes contra a honra é a Calunia, que está tipificado no Art. 138 que diz: “Caluniar alguém imputando-lhe falsamente fato definido como crime.”. Neste crime a honra objetiva da vítima é abalada, ou seja, o agente atribui à vítima a prática de fato, sabendo que a imputação é falsa, abalando assim, sua reputação perante a sociedade.

O crime de Difamação que esta tipificado no Art. 139 que diz: “Difamar alguém imputando-lhe fato ofensivo à sua reputação”. O crime é praticado na internet nas suas mais diversas formas, seja na reprodução de e-mails enviados a pessoas diversas da vítima,

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 artigo a norma é dirigida à pessoa humana, mas, quando o crime for praticado por meio da imprensa, pode-se aplicar a Lei nº 5.250/67 – Lei de Imprensa.

O crime de Injuria está tipificado no Art. 140 que diz: "Injuriar alguém ofendendo lhe a dignidade ou o decoro.". 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.

5.5- ESPIONAGEM ELETRÔNICA

Existe vários tipos de espionagem eletrônica, mas podemos destacar esta, por ser a mais comum, é chamada de Sigint (signalsintelligence), a qual teve sua origem na interceptação, tradução e análise de mensagens por um terceiro, além do emissor e do destinatário. Antes se imaginava que a espionagem seria praticada por empresas, as quais iriam tentar falsificar o sistema de segurança das concorrentes com o fim de se apropriar de informações privilegiadas do mercado concorrente, mas o que ocorre na maioria dos casos é o contrário, pessoas de dentro da empresa são envolvidas para permitir o acesso ao ambiente, ou agir para coletar ou apagar as informações as quais o espião tem interesse.

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

O funcionário que praticar a conduta poderá ter o seu contrato rescindido por justa causa, tendo o que versa o art. 482, "g" da CLT:

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

As empresas deve investir em segurança no ambiente laboral, fazer uso de diferentes ações e equipamentos para monitorar tudo o que ocorre na empresa, tendo que as ameaças internas são mais difíceis de serem descobertas, uma vez que o agente que a exerce é

normalmente um usuário legítimo, é o mesmo quando exerce a espionagem e apaga o registro de logs e não deixa qualquer rastro pra que venha a ser descoberto.

A Patrícia Peck diz 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 frequência 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 monitoramento 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 das condutas visa um controle mais eficaz para que o Insider reduza sua capacidade de exercer sua conduta de espionagem, e que aumenta a probabilidade de pegar o infrator, seja por meio de um número maior de evidencias como logs, ou pelo uso da perícia digital, por exemplo.

5.6- CRIMES CONTRA A PROPRIEDADE INTELECTUAL

Neste crime, 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, de territorialidade, o que oferece 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 respaldo aos seus direitos como autor da obra que está sendo replicada.

O Art. 184 do Código Penal versa:

> 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:
> 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.

O Código Penal não mencionam a violação de programas de computadores, limita-se a obras fonográficas e cópia de obras intelectuais, além disso, o art. 12, caput, da Lei n. 9.609/98, diz 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 Softwares Livres, que são aqueles em que os usuários pode redistribuir cópias, efetuar modificações, caso o mesmo tenha acesso ao código-fonte, ou seja, o usuário é livre para fazer o que desejar. Os Softwares que não são livres, o usuário não tem acesso ao código-fonte, e não pode copiá-lo, ou efetuar a distribuição, para que a distribuição ocorra, deve ter uma contraprestação, ou seja, ônus para que ocorra a distribuição.

Uma das formas mais comuns de crime de violação de direito autoral é a pirataria dos softwares, que consiste na cópia não autorizada, seja por usuários finais, seja por empresas que adquire alguma licença e efetua cópias adicionais para comercialização, a seguir conceituaremos alguns tipos de pirataria.

Venda não autorizada – Outra forma de pirataria que é muito significativa acontece através de algumas Revendas, que copiam integralmente o software e o vendem a preços reduzidos, ou gravam cópias ilegais nos discos rígidos dos computadores, oferecendo este software pirata como uma "gentileza" na compra do hardware.

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.

Pirataria pela Internet – Esta forma de pirataria ocorre quando o software é transferido para os usuários conectados, através de modem, a uma BBS pública ou semiprivada, ou à Internet, sem a autorização expressa do proprietário dos direitos autorais do software. Esta forma não deve ser confundida com a partilha de software de domínio público ou com o "shareware" disponibilizado. O *shareware* é software que pode ter ou não direitos de autor, mas na generalidade é oferecido a baixo custo ou gratuitamente pelo editor, para utilização livre, incluindo a cópia e partilha com outros utilizadores. Qualquer software não autorizado, disponível através de uma BBS, deverá ser considerado ilegal.

Cracking – Estes sim, são os "hackers maus". São os que invadem computadores com a pura intenção de devastar e os que quebram os códigos de proteção de programas para distribuir na Rede.

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

> 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 ideia de produção ou, mais precisamente, sobre a ideia 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.

Pode entender que o direito de propriedade intelectual, sendo o conjunto de prerrogativas, conferidas por lei, ao indivíduo que criou determinada obra, para que o mesmo goze de todos os benefícios resultantes da exploração da sua criação.

Atualmente ainda se tem a ideia do que está publicado na Internet é público, e não tem problema algum em se apropriar do mesmo, está questão impõe um enorme desafio aos operadores do Direito, tendo em vista que se deve repensar o modelo econômico de exploração da propriedade intelectual.

5.7- DANO INFORMÁTICO

Este crime 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 falar do 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 a "coisa" vem a ser algo tangível, material, e o legislador não levou em consideração a conduta do dano à época da elaboração deste artigo, é o problema que ocorre hoje ao se aplicar o 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, enfim, equipamentos de informática, pois o artigo 163 falados danos causados a estes, mas falamos sobre os danos causados aos dados disponíveis em CDs-ROM, disquetes, pen drives, quando não há deterioração dos equipamentos, mas sim dos dados contidos neles.

Não se pode falar em uma interpretação analógica, tendo em vista que seria *in malam partem*, o que não poderia ser feito, tendo em vista o princípio da legalidade, que proíbe a utilização de analogia no Direito Penal em situações que traz prejuízo ao agente da conduta. Não se pode 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 penas do Código Penal, será responsabilizado somente no que dispõe a legislação Cível.

5.8- PORNOGRAFIA INFANTIL

A Pornografia Infantil no mundo movimenta mais de R$ 5 Bilhões por ano, e dados da Interpol mostram que o Brasil é o 4º colocado no ranking de países que exploraram o

mercado. Antes de começarmos a falar da Pornografia Infantil, é importante comentar o art. 234 do Código Penal, o qual diz:

> 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 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 é o dolo, o qual a finalidade do agente é de expor ao público, ou comercializar o objeto material do crime, não é necessário que alguém tenha 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.

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.

A Lei 8.069/9062 - Estatuto da Criança e do Adolescente, estabelece algumas penalidades para o Pedófilo e aquele que divulga ou comercializa as imagens e 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.

Para que encontre o agente que praticou algumas das condutas citados nos artigos acima, é necessária muitas das vezes a quebra do sigilo, em vista que será preciso rastrear aquele que praticou o crime, e após conseguir localizar o culpado, é muita das vezes necessário que seja as provas eletrônicas analisadas por uma perícia técnica rigorosa, para que sejam aceitas em processos.

6- LEGISLAÇÃO NACIONAL EM RELAÇÃO AOS CRIMES VIRTUAIS

O atual Código Penal está de certa forma eficiente em punir condutas praticadas com o uso da internet, e outras, onde a conduta do agente afeta bens jurídicos relativos à Sociedade da Informação, como dados de sistemas, passa então a exigir uma intervenção legislativa para elaborar novos instrumentos normativos de punição. O Direito Penal está ligado inteiramente a Internet, sendo que as relações que ali firmadas é entre indivíduos, e, devem ter suas condutas disciplinadas, cabendo ao Direito disciplinar e regulamentar as condutas entre os membros desta sociedade digital.

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

A primeira legislação veio ocorrer com a criação do Plano Nacional de Informática e Automação (Conin), Lei n. 7.232/84, o qual abordava sobre as diretrizes no âmbito da informática no solo Brasileiro, depois veio a Lei n. 7.646/87, mas foi revogada pela Lei n. 9.609/98, sendo que foi o primeiro ordenamento a descrever as infrações de informática, vejamos 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.
> § 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.

Algumas normas do Código de Defesa do Consumidor – Lei 8.078/11.

> 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.

Cabe um resumo das condutas que já estão tipificadas no ordenamento jurídico, 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.
> § 1 o Nas mesmas penas deste artigo incorre quem:
> I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a 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 projetos atualmente de Lei em andamento que trata 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 vários artigos, apenas seis artigos iniciais que recebeu várias emendas que o ampliam, dentre as alterações que este projeto de lei trará a legislação, podemos citar algumas.

> 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 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 fazer um comentário ao art. 16, que o mesmo define como sendo dispositivos de comunicação, um pen-drive, disco rígido, CD, DVD, por exemplo, o que não contradiz 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 proveem 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.

Quando se faz uma análise detalhada dos artigos do citado projeto de lei, se nota, que embora ele alcance condutas até então não criminalizadas, em certos momentos nota-se que não cria regras rígidas de responsabilização, as empresas exercem o papel de provedoras do serviço de acesso à internet, o que faz que de certa forma o usuário que age de má-fé, tenha um caminho livre para que venham a praticar suas condutas antijurídicas, sob o prisma que para que o mesmo venha a ser responsabilizado.

Outro projeto que vem caminhando lentamente é o PLC n. 89/2003, o qual dispõe também de crimes cometidos na internet, e que também vai abranger vários crimes que cometidos por meio de computadores e/ou instrumentos de acesso à internet ou no cenário digital, o qual podemos citar alguns pontos importantes deste projeto.

NOVA CONDUTA NOVA	TIPIFICAÇÃO DO CRIME
Disseminar *phishingscam* (e-mails fraudulentos contendo*malwares* e outros códigos maliciosos).	Estelionato Eletrônico
Roubar senhas bancárias por meio de *phishingscam.*	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 danos.	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	Ataques a redes e invasões

pública.	
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.

7- 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:

> 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, desde que, a parte contra quem forem exibidos, não lhes impugnar a exatidão.

Já 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".

O art. 332 do Código de Processo Civil versa que:

> 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 aceita também 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 o art. 232 que preleciona "consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares".

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

> "Art. 1°: fica instituída a Infraestrutura de Chaves Públicas Brasileiras – 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 verifique que o documento eletrônico não tenha sido assinado, ou o certificado não esteja vinculado ao ICP-Brasil, pode realizar uma perícia no computador para que verifique a autenticidade da documentação. O credenciamento serve como um selo de

qualidade técnica e não é preponderante na avaliação da prova, uma vez que, o juiz dispõe do livre convencimento motivado.

Segundo o CERT-BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) 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.

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, sendo que, sem os mesmos, fica impossível fazer a quebra de sigilo dos dados.

Como bem lembra Pinheiro após a localização do provedor, deve-se requerer ao juiz o pedido de quebra do sigilo de dados telemáticos 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.

8- COMPETÊNCIA PARA PROCESSAR E JULGAR

No momento em que ocorre um determinado crime na internet o que se deve observar, é onde se deu o mesmo, em qual território a ação se concretizou. 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. O direito deve intervir para proteger os litígios que eventualmente vier acontecer.

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

Na atualidade existe diversos princípios para se determinar qual será a lei aplicável a cada caso. Há o princípio 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, etc.

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, veja-se:

> "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 verifica, o ordenamento jurídico pátrio adotou a teoria da ubiquidade, conforme versa o art. 6° do Código Penal, sendo que os delitos que são praticados por brasileiros, 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, que sujeita a lei brasileira a alguns crimes praticados no estrangeiro.

9- LEI N. 12.737/2012 – LEI CAROLINA DIECKMANN

Antes do ano de 2012, a falta de lei específica tornava difícil a apuração dos crimes virtuais, uma vez que a legislação até então vigente havia sido direcionada aos crimes de forma geral, independentemente do meio utilizado para a sua prática. Nesse sentido, podemos citar, dentre outros, o Código Penal (CP), o Estatuto da Criança e do Adolescente (Lei n. 8.069/90) e Lei dos crimes de software (ou lei antipirataria, Lei n. 9.609/98) e a Lei de Segurança Nacional (Lei nº 7.170/83).

Mas então, no ano de 2012 no mês de maio, foi notícia na mídia a divulgação de imagens da intimidade da atriz Carolina Dieckmann em diversos sites eletrônicos da rede mundial, o que causou uma grande comoção social, o que abriu campo para a Lei n. 12.737, de 30/11/2012, publicada no DOU de 03/12/2012, com *vacatio legis* de 120 (cento e vinte) dias, apelidada de "Lei Carolina Dieckmann", que, dentre outras providências, dispôs sobre a tipificação criminal dos delitos informáticos, introduzindo os arts. 154-A, 154-B, e alterando os arts. 266 e 298, todos do Código Penal.

É importante destacar o art. 154-A do Código Penal, que trouxe para o ordenamento jurídico o crime novo de "Invasão de Dispositivo Informático", veja:

> Art. 154-A – Do Código Penal - Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

O crime falado é comum, o sujeito ativo pode ser qualquer pessoa (de direito público ou de direito privado, física ou jurídica), se dizendo em relação ao sujeito passivo, que pode

ser qualquer pessoa passível de sofrer dano moral ou material decorrente da violação do seu sistema de informática.

O tipo objetivo é o misto alternativo, sendo um crime de ação múltipla ou conteúdo variado, apresentando os verbos "invadir" e "instalar", podendo o agente praticar ambas as condutas e responder por um único crime, desde que num mesmo contexto.

A conduta criminosa do crime cibernético caracteriza-se somente pelo dolo, não havendo a previsão legal da conduta na forma culposa, quanto à culpabilidade.

Relativamente à consumação e tentativa, o crime do *caput* do art. 154-A é formal, se consuma com a invasão ou instalação de vírus, não sendo importante para a consumação a obtenção ou não da vantagem ilícita pelo agente. Já na forma qualificada (art. 154, § 3º, do CP), referida abaixo, o crime é material, pois exige para a consumação a efetiva obtenção de conteúdo ou o controle remoto não autorizado do dispositivo.

O art. 154-A, § 1º, do CP, prevê a forma equiparada do crime cibernético, incriminando com a mesma pena do "caput" a conduta de quem "produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput", sendo esse, também, um crime de ação múltipla que exige dolo específico, tal qual o *caput* do mesmo artigo.

O art. 154-A, § 2º, do CP, prevê causa de aumento de pena de um sexto a um terço, no caso da ocorrência de prejuízo de caráter econômico/financeiro para a vítima, sendo causa de aumento aplicável somente para a forma simples do delito, e não para a forma qualificada, prevista no parágrafo seguinte, em razão da topografia do dispositivo.

O art. 154-A, § 3º, do CP, prevê pena e regime prisional diferenciado de seis meses a 2 anos de reclusão e multa, para as hipóteses seguintes:

1) quando a invasão possibilitar a obtenção de conteúdo de comunicações eletrônicas privadas;

2) quando possibilitar a obtenção do conteúdo de segredos comerciais ou industriais;

3) quando possibilitar a obtenção do conteúdo de informações sigilosas, assim definidas em lei;

4) quando possibilitar o controle remoto não autorizado do dispositivo invadido.

Nota-se que as figuras qualificadas acima descritas configuram crime subsidiário, de subsidiariedade expressa, pois em seu preceito secundário prevê a norma que ela somente será aplicada "se a conduta não constitui crime mais grave".

Por fim, os parágrafos 4º e 5º, I a IV, do CP, preveem causas de aumento de pena, aplicáveis somente para a forma qualificada do delito (§ 3º, do art. 154-A, do CP).

A lei apresentada veio com certa demora. A sociedade reclamou da tutela penal da intimidade cibernética durante muito tempo. E com razão, muitas outras intimidades foram protegidas, tais como a inviolabilidade de domicílio, o sigilo epistolar, o sigilo das correspondências e das comunicações, sigilos das comunicações telefônicas, sigilo bancário e outros. E no mundo digitalizado há a mesma necessidade de se erguer muros protetores.

Conclui que ainda há tempo para combater o crescente número de crimes virtuais, com a consequente aplicação de punição a quem os pratica. Espera-se agora que seu efetivo cumprimento possa proporcionar mais segurança para a comunidade plugada em suas máquinas virtuais, lamentando-se, como é praxe na legislação penal, a tibieza da sanção penal.

CONCLUSÃO

O presente trabalho teve como objetivo falar sobre os crimes cometidos na internet, abordando os delitos que estão tipificados no ordenamento jurídico. Os crimes virtuais estão em crescimento o que preocupa a sociedade, mesmo tendo leis exigentes que se pode tipificar, antes não existia uma especifica até o ano de 2012 onde foi criada a Lei da Carolina Dieckann.

Enquanto a criminalidade virtual avança em passos largos, a legislação caminha calmamente aqui no Brasil, há apenas duas leis completamente dedicadas aos crimes virtuais atualmente em vigor. No entanto, o cometimento destes crimes só aumenta, violando direitos fundamentais e deixando a sociedade à margem de uma proteção efetiva. O crescimento deste delito provoca uma avalanche processual no judiciário, que sem uma legislação contemporânea e forte, precisa recorrer a outros meios jurídicos para tentar solucionar os casos da melhor forma possível.

Houve um levantamento feito dos principais crimes que ocorrem na internet, ficou bastante claro que a cada dia cresce o número de usuários que buscam na internet espalhar seus crimes de uma maneira avassaladora, seja aplicando golpes como estelionatários, iludindo a vítima, com o uso por exemplo de falsos sites, onde a vítima achando estar no site seguro, digita todos os seus dados, senha, número da conta, cartão de crédito, e todos os dados ali digitados são encaminhados aos bandidos.

Falamos da pornografia infantil, um mal que devasta não só o Brasil, mas o mundo todo, sendo que com o surgimento da internet em grande parte do mundo, os criminosos passaram a ter mais facilidade para escolher as vítimas. A pornografia infantil aumentou muito com o avanço da internet e a falta de fiscalização pelo poder público nas relações entre os diversos usuários na rede.

Ao concluirmos este trabalho constatamos que uma das várias dificuldades de resposta para este crime é que onde estes crimes ocorrem é muito rápido, não deixam pistas, mas causam danos a bens juridicamente protegidos. Além disso a Internet não tem território fixo, por ser uma rede mundial e virtual, necessitando do empenho global. A criação de agências reguladoras que possam fiscalizar o ambiente virtual pode ser uma opção viável, assim como a celebração de tratados internacionais que caibam as condutas criminosas no ambiente da Internet.

REFERÊNCIAS

BRITO, José Augusto Pereira. **Formas de Pirataria**. Disponível em: <http://meusite.mackenzie.com.br/brito/leis/formaspirataria.htm> Acesso em 10 nov. 2015.
CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <http://www.cert.br/stats/incidentes/2014-jan-dec/fraude.html> Acesso em 10 nov.2015.

DULLIUS, Aladio Anastacio; HIPLLER, Aldair; FRANCO, Elisa Lunardi. **Dos Crimes Praticados em Ambientes Virtuais**. Conteúdo Jurídico. Santa Rosa, ago. 2012. Disponível em: <http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html> Acesso em 15 set. 2015.

FANTÁSTICO, G1. **Vírus Infectam cerca de 400 milhões de computadores no mundo**. São Paulo, 13 abr. 2014. Disponível em: http://g1.globo.com/fantastico/noticia/2014/04/virus-infectam-cerca-de-400-milhoes-de-computadores-no-mundo.html Acesso em 20 out. 2015.

FEITOZA, Luiz Guilherme de Matos. **Crimes Cibernéticos: O Estelionato Virtual**. Brasília, 2012. Disponível em: <http://repositorio.ucb.br/jspui/bitstream/10869/2819/1/Luis%20Guilherme%20de%20Matos%20Feitoza.pdf> Acesso em 10 out. 2015.

JÚNIOR, Eudes Quintino de Oliveira. **A Nova Lei Carolina Dieckmann**. JusBrasil. São José do Rio Preto, 2012. Disponível em: http://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann Acesso em 05 dez. 2015.

JÚNIOR, Sergio José Barbosa. **Crime Informáticos**. Recife, jun. 2014. Disponível em: <http://jus.com.br/artigos/29634/crimes-informaticos> Acesso em 09 out. 2015.

LIMA, Antônio Henrique Maia. **Crimes de Internet: da competência e da dificuldade de obtenção de provas por meio eletrônico**. Âmbito Jurídico. Rio Grande, ago. 2014. Disponível em:<http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=14253&revista_caderno=3> Acesso em 05 dez. 2015.

NETO, Mário Furlaneto; **GUIMARÃES**, José Augusto Chaves. **Crimes na Internet: elementos para um reflexão sobre a ética informacional**. Brasília, jan./mar. 2003. Disponível em: <http://daleth.cjf.jus.br/revista/numero20/artigo9.pdf> Acesso em 5 dez. 2015.

PAIVA, Raphael Rosa Nunes Vieira. **Crimes Virtuais**. Brasília, 2012. Disponível em: <http://www.conteudojuridico.com.br/pdf/cj037145.pdf> Acesso em 07 set. de 2015.

PINHEIRO, Emeline Piva. **Crimes Virtuais: Uma análise da criminalidade informática e da resposta estatal**. Rio Grande do Sul, jun. 2006. Disponível em:

<http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2006_1/emeline.pdf> Acesso em 07 set. 2015.

REGIS, André Tavares. **Crimes contra a honra na internet: Dificuldade na apuração dos fatos**. João Pessoa, 2011. Disponível em: <http://www.fespfaculdades.com.br/painel/uploads/arquivos/TCC%20ANDRE%20TAVARES%20REGIS.pdf> Acesso em 10 out. 2015.

SENNA, Tel. **Crimes virtuais: uma análise jurídica no Brasil**. Jus Navigandi. Paripiranga, set. 2004. Disponível em: <http://jus.com.br/artigos/32331/crimes-virtuais-uma-analise-juridica-no-brasil> Acesso em 07 set. 2015.

SILVEIRA, Artur Barbosa. **Os crimes cibernéticos e a Lei nº 12.737/2012**. Brasília, 22 jan. de 2015. Disponível em: <http://www.conteudojuridico.com.br/artigo,os-crimes-ciberneticos-e-a-lei-no-127372012,52253.html> Acesso em 02 nov. 2015.

SOUZA, Jason Levy Reis; MENESES, Tamires Gregório; SOIZA, Victor Siad dos Santos; CABRAL, Victória Benvenuto da Silva. **Crimes Virtuais, Punições Reais**. Salvador, 2012. Disponível em: <http://pt.slideshare.net/VictorSaid/artigo-crimes-virtuais-punies-reais> Acesso em 10 out. 2015.