UNIVERSIDADE FEDERAL DO PIAUÍ – UFPI
CAMPUS SENADOR HELVIDEO NUNES DE BARROS - CSHNB
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

CRIMES CIBERNÉTICOS: UM ESTUDO BIBLIOGRÁFICO ABORDANDO A LEGISLAÇÃO PENAL BRASILEIRA

Francisca Gisele Soares Alves

PICOS
2016

FRANCISCA GISELE SOARES ALVES

CRIMES CIBERNÉTICOS: UM ESTUDO BOBLIOGRÁFICO ABORDANDO A LEGISLAÇÃO PENAL BRASILEIRA

Monografia submetida ao Curso de Bacharelado de Sistemas de Informação como requisito parcial para obtenção de grau de Bacharel em Sistemas de Informação.

Orientadora: Profª. Patricia Medyna Lauritzen de Lucena Drumond

PICOS
2016

FICHA CATALOGRÁFICA
Serviço de Processamento Técnico da Universidade Federal do Piauí
Biblioteca José Albano de Macêdo

A474c Alves, Francisca Gisele Soares.
Crimes cibernéticos: um estudo bibliográfico abordando a legislação penal brasileira / Francisca Gisele Soares Alves. – 2016.
CD-ROM: il.; 4 ¾ pol. (38 f.)

Monografia (Bacharelado em Sistemas de Informação) – Universidade Federal do Piauí, Picos, 2016.
Orientador(A): Profª. Ma. Patrícia Medyna Lauritzen de Lucena Drumond

1. Crimes Cibernéticos. 2. Crimes Cibernéticos-Legislação Brasileira. 3. Internet. I. Título.

CDD 004.019

CRIMES CIBERNÉTICOS: UM ESTUDO BIBLIOGRÁFICO ABORDANDO A LEGISLAÇÃO PENAL BRASILEIRA

FRANCISCA GISELE SOARES ALVES

Monografia aprovada como exigência parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Data de Aprovação

Picos – PI, 23 de fevereiro de 2016

Profª. Ma. Patrícia Medyna Lauritzen de Lucena Drumond
Orientadora

Profª. Ma. Patricia Vieira da Silva Barros
Membro

Prof. Esp. Ismael de Holanda Leal
Membro

Dedico este trabalho primeiramente a Deus, por ser essencial em minha vida, pela força e coragem durante toda essa caminhada, aos meus pais Lúcia e Assis, e aos meus irmãos Géssica e Geovane que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa de minha vida.

AGRADECIMENTOS

A minha querida e amável orientadora, professora Patricia Medyna Lauritzen de Lucena Drummond, pela orientação competente e por estar sempre disponível em todos os momentos. Por ser uma excelente professora e profissional, na qual me espelho. Agradecer também pelo apoio, incentivo, simpatia, pela paciência e presteza no auxílio às atividades e discussões sobre o andamento e normatização desta Monografia de Conclusão de Curso.

Agradeço a todos os funcionários da Universidade Federal do Piauí, mas não poderia deixar de mencionar a Professora Patricia Vieira da Silva Barros, que atenciosamente atendeu aos meus telefonemas e e-mails, mostrando-se disponível em todos os momentos.

A todos os professores do curso Bacharelado em Sistemas de Informação pelo carinho, dedicação e entusiasmo demonstrado ao longo do curso.

Aos meus colegas de classe pela espontaneidade e alegria na troca de informações e com certeza futuros excelentes profissionais.

Aos meus pais, Lúcia e Assis, pela determinação e luta na minha formação e dos meus irmãos, fazendo amparar os ensinamentos de meus avós. E aos meus irmãos, Géssica e Geovane, que por mais difícil que fossem as circunstâncias, sempre tiveram paciência e confiança.

E finalmente, a Deus, por guiar e iluminar meus passos, além da força concebida durante todos os momentos difíceis que vivenciei ao longo da minha vida, por proporcionar estes agradecimentos a todos que tornaram minha vida mais afetuosa, além de ter me dado uma família maravilhosa e amigos sinceros.

*“*A verdadeira motivação vem de realização, desenvolvimento pessoal, satisfação no trabalho e reconhecimento.”

(Frederick Herzberg)

RESUMO

O presente trabalho propõe um estudo bibliográfico sobre os Crimes Cibernéticos, abordando a Legislação Penal Brasileira e as leis que são aplicadas para esses crimes. Para isso, destaca-se a importância de alguns crimes cibernéticos, que já se encontram tipificados no ordenamento jurídico brasileiro, e alguns crimes que ainda não possuem uma legislação específica e que precisam urgentemente ser tipificados.

Palavras-chave: Crimes Cibernéticos; Leis; Legislação Civil e Penal.

ABSTRACT

This paper proposes a bibliographic study on Cybercrime, addressing the Brazilian Criminal Law and the laws that apply to these crimes. For this, it highlights the importance of some Cybercrimes, which are already typified the Brazilian legal system, and some crimes that do not have specific legislation and that urgently need to be typed.

Keywords: Cybercrime ; laws ; Civil and Criminal Law.

LISTA DE ABREVIATURAS E SIGLAS

SIGLA	SIGNIFICADO
Av.	Avenida
Art.	Artigo
CEP	Código de Endereçamento Postal
CONIN	Plano Nacional de Informática e Automação
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CF	Constituição Federal
CP	Código Penal
ECA	Estatuto da Criança e do Adolescente
ICP-Brasil	Infraestrutura de Chaves Públicas
IP	Internet Protocol
OCDE	Organisation de Coopération ET de Développemente Economiques

SUMÁRIO

1 INTRODUÇÃO

A explosão da globalização através do meio cibernético tem causado um aumento na prática dos crimes virtuais ou crimes cibernéticos. As distâncias tornaram-se mais curtas, e as relações entre as pessoas passaram a ser feitas na maior parte das vezes através da utilização de equipamentos eletrônicos conectados à *Internet*. Com isso, diversas culturas passaram a se encontrar na rede mundial de computadores e novas relações sociais passaram a surgir nesta Era Digital.

Este momento chamado de "sociedade da informação", mais do que antes, traz a necessidade de esclarecimento à sociedade a cerca dos crimes cometidos no ambiente cibernético. A inexistência de uma legislação específica que trate de todos os crimes cometidos em ambiente virtual e a questão dos crimes praticados em diferentes territórios facilita a ação de criminosos, que em muitas vezes, podem ser pessoas conhecidas.

No Brasil ainda não existe uma legislação específica que trate de todos os crimes cibernéticos, mas somente leis esparsas, que tentam solucionar alguns desses crimes que, na maioria das vezes, tem aplicação somente no território brasileiro, não contando com o apoio internacional, caso fuja da jurisdição e territorialidade.

O presente trabalho constitui uma pesquisa bibliográfica realizada na área do Direito e da Informática, visto que trata dos crimes que são praticados na *Internet*, ou seja, os denominados *Cibercrimes*.

Foram utilizadas ferramentas diversas (bibliografias, apostilas, artigos, *web sites*, livros) para aprofundamento e concepção do conteúdo necessário para atingir o objetivo ora proposto. O trabalho se baseia nos crimes cibernéticos e nas Leis que já são tipificadas e aplicadas para tais crimes, em seguida analisadas para a sua melhor utilização de acordo com as metas propostas para o desenvolvimento do projeto.

O trabalho procura dar uma visão global e abrangente do tema, ilustrando alguns crimes que são praticados na *Internet*, deixando clara a pena aplicada, para aqueles que já possuem uma legislação específica.

1.1 OBJETIVO

A pesquisa desenvolvida tem como objetivo principal um estudo entre alguns tipos de crimes virtuais, abordando a Legislação Penal Brasileira, mostrando a tipicidade desses crimes e a pena aplicada para os mesmos.

1.2 ORGANIZAÇÃO DO TRABALHO

O presente trabalho está dividido em 6 (seis) capítulos. No capitulo 2 será mostrado um resumo sobre o surgimento dos crimes cibernéticos. No capítulo 3 fez-se um levantamento da legislação nacional frente aos crimes virtuais, o que a atual legislação utiliza para reprimir as condutas dos criminosos, os Projetos de Lei existentes, e a análise de algumas legislações internacionais que tratam desse assunto. No capítulo 4, foi feita uma pesquisa dos principais doutrinadores referentes aos Crimes Cibernéticos, e, qual legislação que se aplica quando se realiza algum crime em ambiente virtual. No capítulo 5 foi feito um levantamento sobre as leis que já são tipificadas para esses crimes que são praticados por meio da *Internet*. No capítulo 6 foi feita uma breve conclusão sobre os crimes cibernéticos.

2 SURGIMENTO DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos tiveram origem nos anos 60, tornando-se um grande problema mundial, em vista dos avanços tecnológicos, das facilidades de se cometer tais crimes, juntamente com a dificuldade em definir a autoria do crime e além das Leis de alguns países serem ineficazes (FERREIRA, 2005).

Desde os tempos antigos até os dias atuais, o homem vem sempre buscando desenvolver novas máquinas e ferramentas que tornem as atividades diárias mais fáceis, e de certa forma, mais prazerosas**.** Para facilitar tais atividades surgiram os computadores. O computador é uma máquina que armazena os dados inseridos pelo homem e os transforma em informações úteis para tomada de decisão a partir de um sistema de informação bem definido. As tarefas que antes eram realizadas em espaços de tempo muito longos, passaram a ser realizadas quase que de forma instantânea.

O primeiro caso de prisão por crime cibernético veio acontecer no ano de 1988, quando o jovem estudante Robert Tappan Morris Junior foi condenado a cinco anos de prisão, depois de ter transmitido um *Worm*[1] que contaminou cerca de 6.000 computadores que usavam o sistema operacional *Unix*[2] (ROQUE, 2007).

Os crimes cibernéticos vêm crescendo a cada dia e ganhando enorme repercussão, principalmente os ligados à invasão de *sites* de grandes corporações e do Governo. Esses acontecimentos ocorreram após a prisão do australiano Julian Assange, cofundador do *site wikileaks*, acusado de divulgar documentos sigilosos do governo norte americano e, da prisão do fundador do *site* de gerenciamento de arquivos Megaupload, Kim Schmitz, acusado de pirataria *online* (ANONYMOUS BRASIL, 2003). Outro crime que vem tendo grande repercussão é a exposição da intimidade das celebridades na *Internet*.

2.1 CRIMES CIBERNÉTICOS E SUAS CATEGORIAS

São diversos os conceitos dados para os crimes cibernéticos, que também

---

[1] ***Worm:*** é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

[2] **Unix** - é um sistema operativo (ou sistema operacional) portátil (ou portável), multitarefa e multiutilizador (ou multiusuário).

podem ser conhecidos como cibercrimes, crimes virtuais, crime da informática, crimes informáticos.

> As várias possibilidades de ação criminosa na área de informática, assim entendida no seu sentido lato, abrangendo todas as tecnologias de informação, dos processamentos e transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais lhe fornecem um dominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores. (FERREIRA, 2005)

Para serem praticados os crimes cibernéticos nem sempre necessitam da utilização de computador, podendo sua prática ser através de tabletes, smartphones e outros equipamentos eletrônicos, conectados a *Internet.*

A cada dia vem crescendo mais o número de pessoas que fazem uso da *Internet*, com diversas finalidades, seja para negociações comerciais, buscar conhecimento, conhecer novas pessoas, manter relacionamentos, produzir atividades de marketing pessoal, buscar diversão e ainda, promover transtornos para outras pessoas, incluindo prejuízos financeiros nas vítimas.

A classificação dos delitos informáticos como: Manipulações (podem afetar o *input (*entrada), o *output* (saída) ou mesmo o processamento de dados); Espionagem (subtração de informações arquivadas abarcando-se, ainda, o furto ou emprego indevido de *software)*; Sabotagem (destruição total ou parcial de programas) e Furto de tempo (utilização indevida de instalações de computadores por empregados desleais ou estranhos) (TIEDEMANN, 1980).

Um conceito mais amplo na classificação foi feita por um doutrinador estrangeiro, o 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 (ROVIRA DEL CANTO, 2003).

As condutas dos crimes virtuais dividem-se da seguinte maneira: condutas perpetradas contra um sistema informático e condutas perpetradas contra outros bens jurídicos (GRECO FILHO, 2000).

> Focalizando-se a *Internet,* há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticada 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, como, 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.

Outra classificação dar-se da seguinte forma (ARAS, 2001):

> a) uma primeira categoria, 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 e pontos em comum a considerar. Algumas posições atribuem os meios eletrônicos como objeto protegido (bem jurídico) e meios eletrônicos como meio/instrumento de se lesionar outros bens. Esta classificação torna-se umas das mais oportunas, tendo em vista que abarca mais opções acerca das práticas.

É uma tarefa muito difícil analisar as condutas dos criminosos que se espalham pela *Internet*, devido à dificuldade de verificar onde o agente que praticou se encontra, visto que os crimes cibernéticos não encontram barreiras na *Internet* e se propagam livremente pela rede.

Os crimes cometidos no ambiente virtual já eram praticados antes, só que sem o intermédio da *Internet* e de equipamentos eletrônicos. Com o surgimento da *Internet* os criminosos só encontraram um novo modo de praticar esses crimes que já existiam e criaram novas modalidades de crimes. O que ocorre é que existem alguns crimes com algumas particularidades, fazendo com que seja necessária uma adequação quanto ao seu tipo penal. Os crimes virtuais e outros crimes existentes que passaram a ser executados por meio da *Internet* são apresentados nas seções seguintes.

2.1.1 Fraudes Virtuais

As fraudes virtuais estão ficando cada vez mais frequente na vida das pessoas. Entre as principais tentativas de golpe estão à emissão de cartões de crédito, financiamento de eletrônicos, compras de celulares com documentos falsos ou roubados, abertura de contas, compras de automóveis e abertura de empresas.

O roubo de identidade foi um dos maiores problemas enfrentados pelos internautas brasileiros em 2013, segundo a Serasa *Experian* (CERT.BR, 2015).

2.1.2 Estelionato

São diversas as condutas estelionatárias por meio da *Internet*, a questão é tipificá-las como Estelionato. O legislador previu, como meio executório, a fraude com o objetivo de obter o consentimento da vítima, iludindo a mesma para que voluntariamente entregue o bem. Assim o agente leva a vítima ao erro, enganando a mesma e mantendo-a em erro.

Um dos exemplos mais comuns das condutas estelionatárias praticadas por meio da *Internet* consiste na conduta de um agente encaminhar *e-mails* com conteúdo falso a um usuário, induzindo o mesmo a clicar em *links* que estão disponíveis no corpo do *e-mail*, direcionando-o, na maioria das vezes, para um *site* falso onde o mesmo repassa informações pessoais ao agente que formulou a página falsa.

As condutas podem variar conforme o uso que o agente faz dos meios eletrônicos neles disponíveis, com fim de atingir um objetivo. O estelionato tem sido um dos crimes mais populares tanto na *internet* como fora dela. O Código Penal 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.

2.1.3 Invasão de Privacidade

Com o enorme avanço dos acessos na rede mundial de computadores, cada dia mais as pessoas passaram a disponibilizar um número quase que ilimitado de informações na rede, desde informações que são lançadas em cadastros em *sites* de *e-commerce*[3]**,** até as informações de preenchimento de *perfis* nas redes sociais.

---

[3] ***E-commerce:*** é uma modalidade de comércio que realiza suas transações financeiras por meio de dispositivos e plataformas eletrônicas, como computadores e celulares.

O uso da rede mundial de computadores pelas pessoas tem uma variedade de finalidades, entre elas, o acesso a informações diversas, compra de produtos, enfim, para um número ilimitado de situações no qual a *internet* possibilita realizar inúmeras questões. O que ocorre, é que as informações que estão disponibilizadas ou não na *internet*, podem trazer uma penalidade para as pessoas físicas ou jurídicas, que as utilizam sem a autorização, ou seja, o direito a privacidade constitui um limite natural ao direito à informação (RAMOS, 2008).

Na verdade o que se procura é proteger o cidadão com relação aos seus dados que estão disponibilizados na rede, sejam aqueles disponíveis em órgãos públicos, sejam em órgãos privados, mesmo porque os dados pessoais do cidadão não podem ser tratados como mercadoria, tendo em vista que devem considerar seus aspectos subjetivos. Sendo assim o Estado deve garantir os direitos da pessoa, proteger sua identidade, e os cidadãos devem exigir das empresas que armazenam seus dados que as mesmas se preocupem com a segurança dos mesmos, e os utilizem apenas para aquele fim específico.

2.1.4 Crimes contra Honra

Os crimes contra a honra são muito comuns na *Internet* e tem como vista um alto número 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 a 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 irão definir a sua aceitação ou não para conviver em determinado grupo social.

O Código Penal estabelece 3 crimes contra a Honra: a difamação, a calúnia e a injúria. A difamação que se encontra definido no art. 139: “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.

A prática do crime de difamação por meio da *internet* tem várias formas, seja por meio da perpetuação de *e-mails* enviados a diversas pessoas, imputando a esta, algum fato que ofenda a sua honra objetiva, ou através das redes sociais publicando as mesmas ofensas. No crime de difamação a pessoa jurídica não pode ser sujeito

passivo, tendo em vista que no Art. 139 do código penal a norma é dirigida à pessoa humana, mas, quando o crime for praticado por meio da imprensa, pode-se aplicar a Lei de nº 5.250/67- Lei de Imprensa (PECK, 2002).

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 um ambiente virtual, por exemplo, ocorre quando alguém espalhar um ato ofensivo a uma pessoa pelas redes sociais, e os usuários presentes fizerem a leitura do fato ofensivo.

Já a Calúnia está descrita no Art.138 do CP, o qual versa: “Caluniar alguém, imputando-lhe falsamente fato definido como crime”. Neste o agente atribui a 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 vitima, conforme estabelece o tipo penal que está o Art. 140 do CP: ”Injuriar alguém, ofendendo lhe a dignidade ou o decoro”.

2.1.5 Espionagem Eletrônica

Diante do enorme crescimento no uso da tecnologia por pessoas, e o uso dependente de *softwares* diversos pelas empresas, a cada dia as pessoas permanecem mais tempos conectados a rede de computadores. Cada vez mais se percebe a necessidade de um hábito de segurança das informações, seja por prevenção, seja por monitoramento.

São diversos os tipos de espionagem eletrônica, dentre as várias que existem podemos destacar, por ser uma das mais comuns, a chamada de SIGINT (*Signals intelligence*), a qual teve sua origem na interceptação, decodificação, tradução e analise de mensagens através de um terceiro, além do emissor e do destinatário (GERMAN, 2008). No passado imaginava-se que a espionagem eletrônica seria praticada apenas por empresas, as quais iriam tentar burlar o sistema de segurança das concorrentes com o fim de apropriar-se de informações privilegiadas. Ao contrário do que se imaginava, pessoas dentro da empresa são as

envolvidas e permitem acesso ao ambiente, agindo para coletar e apagar informações das quais o espião tem interesse.

Não existe um tipo penal especifico que venha a especificar o crime de espionagem eletrônica, sendo que a conduta está definida no Código Penal nos Arts. 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 que as empresas devem fazer é investir em segurança no seu ambiente laboral, fazer uso de diferentes ações e equipamentos para monitoramento de tudo que venha a acontecer na empresa, tendo em vista que as ameaças internas são mais difíceis de serem apanhadas, uma vez que o agente que exerce a conduta é normalmente um usuário legítimo e exerce a espionagem, apagando os registros, não deixando assim qualquer rastro que possa ser apanhado.

Diante do conjunto de condutas da espionagem eletrônica é necessário um controle mais eficaz para que tenha reduzido sua capacidade de exercer sua conduta de espionagem, aumentando a probabilidade de pegar o infrator, seja por meio de um número maior de evidências como *Logs*[4], por exemplo, ou pelo uso da Perícia Digital[5].

2.1.6 Crimes contra a Propriedade Intelectual

Pode-se entender que o direito da propriedade intelectual é um conjunto de prerrogativas, conferidas por Leis, ao individuo que criou determinada obra intelectual, para que o mesmo tenha benefícios resultantes da exploração de sua criação.

---

[4] **Logs:** é uma expressão utilizada para descrever o processo de registro de eventos relevantes em um sistema computacional.

[5] **Pericia Digital:** carreira que mescla a formação jurídica com a tecnologia da informação e que cresce na esfera pública e privada à medida que conflitos, fraudes, furtos e agressões passam a ser cometidas por intermédio de dispositivos informáticos e telemáticos, de um computador de mesa a um dispositivo móvel celular.

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.

No âmbito informático há uma ausência de fiscalização, ausência de territorialidade, o que propícia uma rapidez na circulação de informações, permitindo que cópias de materiais disponibilizados sejam feitas de maneira desordenada, onde muitas das vezes o criador é desrespeitado, tendo em vista que não tem qualquer respeito com os direitos do autor que está tendo sua obra replicada.

2.1.7 *Software*

Diante dos *softwares*, temos os *softwares* livres que são aqueles em que os usuários podem redistribuir cópias, efetuar modificações, ou seja, o usuário é livre para fazer o que bem entender do mesmo.

Temos outro tipo de *software*, que são os *softwares* não livres, nesse tipo de *software*, o usuário não terá acesso ao código fonte, e não pode copiá-lo, ou esta distribuindo o mesmo, para que possa fazer essa distribuição, deverá haver uma contraprestação.

Dentre os crimes de violação do direito autoral, um dos mais comuns é a pirataria de *software*, que consiste basicamente em cópias não autorizadas de *softwares*, seja por meio de usuários finais, seja por empresas que adquirem algumas licenças e efetuam cópias adicionais para comercialização.

2.1.8 Dano

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 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 Código Penal, e o problema atual consiste na aplicação do citado artigo à conduta do agente quando efetua o dano informático, sendo que o mesmo não pode ser entendido como algo tangível,

material, não dizendo respeito ao dano a computadores e equipamentos de informática, pois o art. 163 abarca os danos causados a estes, mas fala-se sobre os danos causados aos dados disponíveis em CD-ROM, *pen drives*, *hard disks (HD)*, quando não há deterioração dos dados neles contidos.

Não se pode simplesmente atribuir como material algo que é imaterial. O que ocorre é que hoje se alguém praticar algum dano a dados informáticos de um terceiro, mesmo que de forma dolosa, não estará sujeito as penas do código penal, somente será responsabilizado no que dispõe a legislação civil.

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.

2.1.9 Pornografia Infantil

O crime de pornografia infantil é o crime mais comum no Brasil, somente no ano de 2013, 993 páginas foram denunciadas às autoridades por conter material envolvendo pornografia infantil. O número representa um aumento de 3,83% em comparação ao ano 2012 (TERRA, 2012).

O mercado da pornografia infantil vem movimentando no mundo mais de R$ 4 bilhões por ano, e segundo dados da Interpol o Brasil é o 4º colocado no *ranking* dos países que exploram esse mercado. È muito importante comentarmos o art.234 do Código Penal, 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 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.

A pornografia infantil é um fenômeno mundial e histórico caracterizada pela

exploração sexual comercial, principalmente por parte de indivíduos pedófilos, que tem a criança como principal objeto de mercadoria. O interesse de adultos por crianças remonta à antiguidade e tratava-se de comportamento comum que não afetava o moralismo da sociedade.

A Lei nº 8.069 de 1990 contempla o Estatuto da Criança e do Adolescente – ECA que surge com o intuito de proporcionar maior segurança e efetividade aos direitos fundamentais da criança e do adolescente devido à implantação de políticas capazes de promover uma proteção integral e especializada do indivíduo que, porventura venha a cometer as tipificações penais dispostas nos artigos 225 a 258 da referida lei. De fato, a lei possibilita a construção de um microssistema jurídico provedor de um desenvolvimento significativo no nosso ordenamento jurídico brasileiro (FEVEREIRO, 2009).

O Estatuto da Criança e do Adolescente, Lei 8.069/1990, estabelece algumas penalidades para o Pedófilo e aquele que divulga ou comercializa imagens, vídeos envolvendo crianças em cena de sexo, ou seja, Pornografia Infantil.

3 LEGISLAÇÃO A CERCA DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos possuem uma legislação nacional e internacional para seu julgamento. Será descrito a legislação com relação a esses crimes.

3.1 LEGISLAÇÃO NACIONAL EM RELAÇÃO AOS CRIMES CIBERNETICOS

Com o surgimento das novas aplicações tecnológicas, surgiram usuários que utilizam tais inovações, mais especificamente a *Internet*, para praticar atos ilícitos, seja criando novas modalidades de crimes, seja criando novas formas de praticar crimes que já estão tipificados na legislação penal brasileira, passando-se, com isso, a exigir soluções que o Direito não estava preparado para resolver.

Infere-se que o Brasil não apresenta uma legislação específica referente a essas modalidades de crimes, ressaltando a necessidade urgente de regulamentação definitiva dos novos tipos penais, com o intuito de evidenciar tais praticas delitivas que permaneciam impunes e continuavam causando atos lesivos a sociedade.

Dentre essas mudanças que ocorreram devido ao crescimento desenfreado de novas tecnologias, percebe-se o surgimento de novos métodos de interação entre os indivíduos. Novas formas de se relacionar, entretanto, criam também novos problemas, tendo em vista o surgimento de situações que ainda não possuem previsão legal especial (ROSA, 2007).

Embora o Poder Judiciário venha punindo os infratores com base nos tipos penais já existentes (passíveis, portanto, de imediata aplicação), vê-se a necessidade de se criar uma legislação especifica o mais breve possível, pois a tentativa de adaptar tais crimes em leis antigas e ultrapassadas, nem sempre é possível, mostrando-se ineficaz em muitos casos, acabando por gerar impunidade.

No Brasil, não há uma cultura de Informática Jurídica e de Direito de Informática disseminada na sociedade. Embora por meio dos projetos de lei, existam no país algumas inciativas, no sentido de regulamentar os novos tipos de condutas delitivas, muitas se encontram ainda tramitando no Congresso Nacional, sem que medidas efetivas tenham sido colocadas em prática.

O Ordenamento Jurídico Brasileiro não acompanhou, portando, as mudanças tecnológicas ocorridas na sociedade, em contraste com a expansão cada vez maior do número de usuários que utilizam o computador e consequentemente a *Internet*.

A legislação nacional em relação aos crimes cibernéticos sancionou a Lei nº 12.737/2012, que tipifica como crime uma série de condutas no ambiente virtual. A lei sancionada garante que se invadirem dispositivos como computador, smartphones e tabletes de outra pessoa para obter informações sem autorização passa a ser crime com pena de detenção de três meses a um ano, além de multa. Nesse caso, a pena ainda pode ser agravada se a informação roubada causar algum prejuízo econômico.

Existem atualmente Projetos de Lei em andamento que tratam do tema de delitos tecnológicos (CRESPO 2011). Dentre os projetos de maior relevância destaca-se o Projeto de Lei nº 84/99 que trata de uma maneira ampla e sistematizada dos crimes cometidos por meio da internet, 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.

O ambiente virtual se mostra muito propício para os mais variados tipos de crimes, apesar da falta de uma legislação especifica, é relativamente protegido juridicamente, pois no Ordenamento Jurídico Brasileiro já se encontra algumas normas que tratam da matéria, tais como a Lei nº 9.829/08, que combate a pornografia infantil na internet; a Lei de nº 9.609/98, que trata da proteção da propriedade intelectual do programa de computador; a Lei de nº 9.983/00, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da administração pública; a Lei de nº 9.296/96 disciplinou a interceptação de comunicação telemática ou informática; e a Lei de nº 12.034/09, que delimita os direitos e deveres dentro da rede mundial (*Internet*), durante as campanhas eleitorais.

3.2 LEGISLAÇÃO INTERNACIONAL EM RELAÇÃO AOS CRIMES CIBERNETICOS

A convenção da Budapeste foi aprovada no ano de 2001, a mesma trata dos

crimes praticados através do uso dos meios tecnológicos, sendo considerada como uma referência legislativa mundial a respeito dos crimes de internet. Essa Convenção, não dita às regras, mas sim orienta sobre o tema, deixando a cargo de cada País, criar sua legislação específica sobre a matéria.

A Convenção prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional e reconhece a necessidade de uma cooperação entre os Estados e a indústria privada.

Será feita uma análise da legislação de alguns países em relação à criminalidade informática (CRESPO 2011). Dentre esses países estão:

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.

Espanha – No Código Penal espanhol, em seu Art. 197, há incriminação daquele que se apodera, sem autorização, de papéis, cartas, mensagens de correio eletrônico ou qualquer outro documento, com o intuito de descobrir segredo ou violar a intimidade de outro. Já o Art. 256 do Código Penal espanhol incrimina a utilização não autorizada de terminal de telecomunicação, e o Art. 248, incrimina a fraude informática e o estelionato tendo como meio o uso de tecnologia.

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. O acesso fraudulento ao sistema de elaboração de dados, sendo considerados delitos tanto o acesso ao sistema, como nele manter-se ilegalmente. A sabotagem informática, punindo quem apaga ou falseia o funcionamento de sistema eletrônico. A destruição de dados punindo aquele que dolosamente introduz dados em sistema ou, suprime ou modifica dados. A falsificação de sistemas informatizados punindo quem falsifica documentos informatizados, com intenção de prejuízo a terceiros e o uso de documentos informatizados falsos, falsos retro mencionados.

Itália – O Código Penal italiano desde 1993 trata de alguma forma dos delitos relacionados com a informática, o Art. 615 – pune o acesso abusivo a sistema informático ou telemático. Já o 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. E o Art. 635 – pune aquele que causou destruição, deterioração ou inutilização a qualquer sistema informático.

Chile – o primeiro país da América 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° incrimina-se a interceptação indevida em sistema e no art. 3° pune aquele que altera, danifica ou destrua os dados contidos em determinados sistemas.

Argentina – Na Argentina o Art. 128 incrimina aquele que armazena mensagens que contenham pornografia de menores de 18 (dezoito) anos. Já o Art. 153 pune aquele que abra ou se aproprie sem autorização, de correspondência aberta ou fechada. Também incrimina o acesso não autorizado ao sistema informático, e 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 à manipulação e sabotagem informática, onde foi acrescentada 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 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. O Direito Penal norte-americano possui duas modalidades de incriminação: a tipificação estatutária (direito penal codificado) e os ilícitos decorrentes de decisões judiciais uma forma quase inexistente na atualidade.

Pode-se dizer que as primeiras manifestações informáticas ilegítimas aconteceram nos Estados Unidos quando Robert Tappan Morris, um estudante de pós-graduação, começou a trabalhar em um programa de computador, explorando os defeitos de segurança que havia descoberto na internet, a fim de demonstrar a inadequação das medidas de segurança nas redes de computadores, criando os *"Worms"* vírus capazes de se expandirem em outros computadores com o objetivo inicial de ocupar pouco do funcionamento das máquinas (já que a intenção do estudante era apenas demonstrar a insegurança das atuais redes

computacionais), porém, o “experimento” acabou tomando proporções maiores e os vírus começaram a se reproduzirem e infectarem as máquinas causando grande prejuízo as redes de computadores à época.

A partir de então, os Estados Unidos travaram um verdadeiro combate à criminalidade informática, tal combate se deu em dois patamares: o estadual e o federal. No âmbito federal encontrou-se a Lei de Proteção aos Sistemas Computacionais (*Federal Computer System Protection Act of 1981)* - que determinava como conduta delituosa o uso de computadores com o objetivo de praticar fraudes, furtos ou espécies de apropriação indébita. Em seguida, em 1982 surgiu a *Eletronic Funds Transfer Act* – lei que trata da regulamentação de transferências eletrônicas de fundos, incriminando as fraudes informáticas que não continham relações interpessoais (HATA, 2010).

A principal lei que traz à baila a responsabilização criminal de condutas ilícitas no âmbito informático é a *Computer Fraud and Act* – Lei de Fraude e Abuso Computacional – datada de 1986 que visa proteger a acessibilidade dos sistemas para a obtenção de segredos nacionais ou com o intuito de obter vantagens financeiras (HATA, 2010).

4 OBTENÇÃO DE PROVAS NO MEIO ELETRÔNICO

A existência da responsabilidade criminal e a sanção penal aplicada a uma determinada pessoa só pode ser anunciada, quando houver certeza da prática do ilícito penal e de sua autoria.

As provas têm como finalidade fornecer ao juiz conhecimento para solucionar o conflito sobre o fato criminoso e sua autoria, mas não apenas isso, todos os elementos objetivos e subjetivos, bem como todos os acontecimentos importantes que possam influenciar na responsabilidade penal e na fixação da pena ou de medida de segurança.

Que se entende por prova: provar é, antes de mais nada, estabelecer a existência da verdade; e as provas são meios pelos quais se procura estabelece-la. É demonstrar a veracidade do que se afirma, do que se alega. Entendem-se, também, por prova, de ordinário, os elementos produzidos pelas partes ou pelo próprio Juiz visando a estabelecer, dentro do processo, a existência de certos fatos (FILHO, 2000).

É visto que ainda há muita dificuldade para obtenção de provas e com isso, a investigação criminal relacionada a esses crimes virtuais se tornam bastante difícil. A obtenção de provas na maioria das vezes se torna escassa, pois os criminosos ao praticarem essas infrações no ambiente informático, muitas vezes não deixam rastros, e devido essa obscuridade da rede, o autor do crime fica à sombra no anonimato.

É importante também chamar atenção para as provas ilícitas que são decorrentes de investigações e realizadas sem autorização no ambiente cibernético, violando o artigo 5º da Constituição Federal (CF) e o artigo 157 do Código de Processo Penal (CPC). Assim, como ocorre nas investigações com quebra de sigilo telefônico, é necessário que tenha a autorização para apuração do crime praticado na rede virtual.

Alguns documentos eletrônicos como prova são admitidos pelo Direito como um documento de validade jurídica, porém muitos doutrinadores acreditam que não constituem uma prática totalmente confiável. Esses documentos sendo utilizados como prova ainda é um ponto bastante discutido no ordenamento jurídico brasileiro.

Portanto, discute-se se o documento eletrônico deve ser considerado como prova pericial ou documental. A teoria mais adotada é a que conceitua como prova pericial, pois carecem de pericia técnica.

As provas que se encontram na rede possuem um grande risco de esgotamento, e sua coleta deve ser realizada com cuidado e atenção, para que elas não desapareçam, garantindo, dessa forma, a prisão dos autores e o devido processo legal. Essa criminalidade no ciberespaço deve ser combatida com o uso das mesmas armas, ou seja, utilizando as ferramentas oferecidas pelo próprio ambiente informático na prevenção, investigação, prova e repressão dos crimes virtuais.

Para isso é necessário unidades policiais especializados nesses crimes, assegurando a manutenção da integridade das provas ou vestígios, ao mesmo tempo em que possibilitaria a adequação dos órgãos policiais á velocidade desses crimes virtuais.

No ordenamento jurídico, não há qualquer empecilho para a utilização de provas eletrônicas, conforme versa o art. 225 do Código Civil: “as reproduções fotográficas, cinematográficas, os registros fotográficos, 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”.

Caso se verifique que o documento eletrônico não tenha sido assinado, ou certificado, pode-se realizar uma perícia no computador para que se verifique a autenticidade da documentação. O credenciamento serve como um selo de qualidade técnica, e não preponderante na apreciação de prova, sendo que o mesmo apreciará livremente as provas.

Atualmente as pessoas podem utilizar a assinatura eletrônica ou a certificação digital, sendo que a certificação é um tipo de tecnologia de criptografia a qual se usa uma ferramenta de codificação que é usada para o envio seguro de mensagens em redes eletrônicas. Já a assinatura eletrônica é uma chave privada, onde um código pessoal não poderá ser reproduzido, o qual se evita que o que estiver sendo transmitido seja lido somente por aquele receptor que possua a mesma chave e é reconhecida com a mesma validade da assinatura tradicional.

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

Quando um usuário navega pela *Internet*, lhe é atribuído um número de IP- *Internet Protocol* é esse número que propicia a identificação do usuário pela rede, ou a investigação de algum crime que tenha ocorrido. A questão é que esse número só é atribuído ao usuário no momento em que ele está conectado na rede, após esse período, quando o mesmo parar a conexão desligando o modem, o endereço de IP será atribuído a outro usuário, caso o mesmo não tenha optado por um endereço IP fixo.

No momento em que o IP é solicitado ao provedor de acesso à *Internet*, o provedor deve está ciente que esse deve vir acompanhado da data, hora da conexão, e ou fuso horário do sistema, sendo que esses dados são indispensáveis, tendo em vista que sem os mesmos fica impossível fazer a quebra do sigilo de dados.

Após a localização do provedor, deve ser feito um pedido ao juiz para a quebra de sigilo dos dados telemáticos, para que o provedor de acesso informe quem está vinculado ao endereço IP no momento em que ocorreu o crime, ou seja, seu endereço físico.

5 DESCRIÇÃO DE ALGUNS CRIMES PRATICADOS PELA INTERNET

No ordenamento jurídico, o Direito Penal define infrações que devem ser punidas rigorosamente pelo Estado, estando a maior parte prevista no Código Penal e nas Legislações Especiais que são punidas com privação de liberdade, restrição de direitos e multas.

Ainda não há em nosso ordenamento jurídico normas e leis claramente definidas na área de informática notadamente na tipificação de eventuais delitos cometidos através da *Internet*.

Estes tipos de crimes podem atingir todos os bens jurídicos, como patrimônio financeiro e material, pode atingir o cidadão com calúnias, injúrias e difamação, incitar crimes de racismo, pedofilia, e ainda provocar abalos no sistema financeiro como um todo, tanto envolvendo pessoas físicas, como pessoas jurídicas de direito público e privado.

Como estes fatos estão presentes no dia a dia de nossa sociedade com uma grande parcela de impunidade, são necessárias medidas urgentes para definir, a partir de denúncias, as competências das Polícias Judiciárias e da magistratura através do poder judiciário, enquanto não houver leis específicas tratando dos crimes cibernéticos.

É extremamente necessário e urgente, buscar a tipificação dos crimes de informática e condutas criminosas que são efetuadas através da *Internet*, sob o risco da própria sociedade como um todo entrar em uma área ainda por muitos desconhecidos, onde não há território delimitado e muito menos um ordenamento jurídico de controle social.

Estes crimes já vêm acontecendo desde o advento da *Internet* e sua massificação, assumindo proporções cada vez mais alarmantes e, por incrível que pareça ainda inimagináveis.

No caso de menores de idade, os pais serão responsabilizados ou aquele que tem a sua guarda, tutela ou curatela, pois se entende que os mesmos têm a obrigação da educação e exercer uma espécie de poder de vigilância sobre seus filhos menores. Quando os relativamente incapazes provocam danos a outrem, subjetivamente demonstra que faltou com seu dever de vigilância, sendo necessário provar que não foi negligente, sob o risco de responder pelos atos ilícitos.

Serão elencados alguns delitos cometidos com o uso de computador explicitando subjetivamente, e qual a melhor forma de buscar a tipificação em nosso ordenamento jurídico objetivamente, não restando ao infrator que esteja devidamente identificado, a responder pelos atos ilícitos. Foram relatadas 5 (cinco) situações subjetivas e como elas acontecem na grande maioria dos casos, e qual a melhor forma de tipificá-los pela autoridade policial:

Situação 1: Relata o uso de MSN ou qualquer meio de comunicação on-line via internet, criar e/ou participar de Blogs ou comunidades que qualquer usuário tenha acesso direto pelo computador, ou ainda direcionar Links (acessos) para páginas nacionais ou estrangeiras com sugestões de como a pessoa deve se matar ou sugerindo de como fazê-lo.

Crime: Induzimento, Instigação ou Auxílio ao suicídio (Art. 122 - CP)

Situação 2: É exposta para quem utiliza programas de computador sem autorização ou licença oficial de quem possui os direitos autorais ou de quem o represente, salvo programas denominados Beta para testes, desde que seja de conhecimento do proprietário do programa, ou seja, livremente liberado para o internauta.

Crime: Violar direitos de autor de programa de computador (Art. 12 – CP).

Situação 3: Crime em que são efetuados saques e transferências em Caixas Eletrônicos Bancários, com os dados do cliente sem sua permissão ou autorização.

Crime: Subtrair para si ou para outrem, coisa alheia móvel, devendo ser qualificado com o § 4º (Art. 155 - CP).

Situação 4: O usuário envia e-mail diretamente a uma pessoa, citando que vai pegá-la, ou que vai acertar as contas, ou colocar os pingos nos “is”, ou ainda, qualquer situação idêntica à ameaça.

Crime: Ameaçar alguém, por palavra escrita ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto ou grave (Art. 147 – CP).

Situação 5: Trata de quem promove via internet bingos, jogos de azar, cassinos on-line, sem autorização legal.

Crime: Estabelecer ou explorar jogos de azar em lugar público ou acessível ao público, mediante o pagamento de entrada ou sem ele (Art. 50 – CP).

6 CONCLUSÃO

A pesquisa desenvolvida demonstra a relação do Direito com a Legislação Penal Brasileira e considera também as novas modalidades de crimes que ocorrem entre os indivíduos em ambientes virtuais.

Portanto foi feito um levantamento de alguns crimes que ocorrem por meio da *Internet,* sendo que ficou bastante claro que a cada dia vem crescendo mais o número de usuários que fazem busca do ambiente virtual para propagar crimes de uma maneira desenfreada.

Portanto é demonstrada a importância da justiça em se adequar a nova realidade no que diz respeito aos crimes que são praticados com o uso de computador tendo por intermédio a *Internet*, como também a necessidade do poder público de aprovar os Projetos de Lei já existentes em pauta. É importante aplicar os mecanismos de maior rigor na apuração de ilícitos que venham a ocorrer em ambiente virtual, sendo que aos poucos a sociedade está se tornando cada vez mais digital.

REFERÊNCIAS

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: 15 nov. 2015.

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: 20 nov.2015.

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 dez. 2015.

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

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: 20 dez. 2015.

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: 23 nov. 2015.

DAOUN, Alexandre Jean; LIMA, Gisele Truzzi de. **Crimes Informáticos**: O Direito penal na Era da Informação. Disponível em: <http://www.truzzi.com.br/pdf/artigo-crimesinformativos-gisele-truzzi-alexandre-daoun.pdf>.Acesso em: 22 nov.2015

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: 22 set.2015

EDUCACIONAL. **Vida Inteligente o computador no dia-a-dia.** Disponível em: <http://www.educacional.com.br/vidainteligente/clickdigital02/e-commerce.asp>. Acesso em: 24 ago.2015

FEVEREIRO, Marco Aurélio. **Pornografia infantil cometida pela internet e os tipos penais previstos na Lei Federal nº 11.829/2008**. Disponível em: <http://www.viajus.com.br/viajus.php?pagina=artigos&id=4403> Acesso em: 15 nov. 2015.

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: 12 set.2015

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 nov. 2015.

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.

HATA, Fernanda Yumi Furukawa. **Direito Penal Internacional**. Revista SJRJ, Rio de Janeiro, V.17, n.29. p. 117-141, dez 2010. p.118.

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: 11.dez.2015

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 jan. 2016.

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

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

ROQUE, Sérgio Marques. **Criminalidade Informática – Crimes e Criminosos do Computador**. 1 ed. São Paulo: ADPESP Cultural, 2007

SILVA, Jacimar Oliveira da. **Tipificação de crimes efetuados pela internet**. Disponível em: <www.pc.ms.gov.br/controle/ShowFile.php?id=19374>. Acesso em: 12 jan.2016

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

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

GLOSSÁRIO

Blog: página na internet onde as pessoas escrevem sobre diversos assuntos de seu interesse.

Chat: espaço online que permite uma discussão em tempo real entre vários usuários de internet.

Crackear: Substituir o executável de um programa, por outro modificado.

Keyloggers: programas de computador cuja finalidade é capturar tudo o que é digitado.

Links: é o "endereço" de um documento (ou um recurso) na web.

Softwares: é uma sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas.

E-mails: é um serviço disponível na Internet que possibilita o envio e o recebimento de mensagens ("mails").

MSN: é a sigla de "Microsoft Service Network", que significa "Rede de Serviços da Microsoft". O portal MSN.com é diferente do programa de mensagens instantâneas.

Forward: Corrente de e-mail é o evento que ocorre quando um e-mail que é enviado para diversos conhecidos ao mesmo tempo e que são, eventualmente, repassadas adiante podendo se espalhar em ritmo exponencial a milhares ou até milhões de pessoas.

Firewall: é um software ou um hardware que verifica informações provenientes da Internet ou de uma rede, e as bloqueia ou permite que elas cheguem ao seu computador, dependendo das configurações do firewall.

TERMO DE AUTORIZAÇÃO PARA PUBLICAÇÃO DIGITAL NA BIBLIOTECA "JOSÉ ALBANO DE MACEDO"

Identificação do Tipo de Documento

( ) Tese

( ) Dissertação

(x) Monografia

( ) Artigo

Eu, **Francisca Gisele Soares Alves**, autorizo com base na Lei Federal nº 9.610 de 19 de Fevereiro de 1998 e na Lei nº 10.973 de 02 de dezembro de 2004, a biblioteca da Universidade Federal do Piauí a divulgar, gratuitamente, sem ressarcimento de direitos autorais, o texto integral da publicação **Crimes Cibernéticos: Um Estudo Bibliográfico Abordando a Legislação Penal Brasileira** de minha autoria, em formato PDF, para fins de leitura e/ou impressão, pela internet a título de divulgação da produção científica gerada pela Universidade.

Picos-PI 07 de Março de 2016.

Francisca Gisele Soares Alves

Assinatura