

**Organização Sete de Setembro de Cultura e Ensino – LTDA  
Faculdade Sete de Setembro – FASETE  
Curso de Bacharelado em Direito**



**ÉLTON LAERTE CAMPOS FERREIRA**

**A DIFICULDADE NA PERSECUÇÃO DOS CRIMES  
REALIZADOS ATRAVES DA INTERNET**

Paulo Afonso

2014

**ÉLTONLAERTE CAMPOS FERREIRA**

**A DIFICULDADE NA PERSECUÇÃO DOS CRIMES  
REALIZADOS ATRAVES DA INTERNET**

Monografia apresentada ao curso de Bacharelado em Direito, da Faculdade Sete de Setembro - FASETE, como requisito necessário à obtenção do grau de Bacharel em Direito.

Professor orientador: Msc. Pedro Camilo de Figueirêdo Neto

Paulo Afonso

2014

**ÉLTON LAERTE CAMPOS FERREIRA**

**A DIFICULDADE NA PERSECUÇÃO DOS CRIMES  
REALIZADOS ATRAVES DA INTERNET**

Monografia submetida à Faculdade Sete de  
Setembro – FASETE, como requisito parcial  
à obtenção de grau em Bacharel em Direito.

Aprovada por:

Prof. \_\_\_\_\_ Orientador.

Prof. \_\_\_\_\_

Prof. \_\_\_\_\_

PAULO AFONSO  
2014

## **AGRADECIMENTOS**

Grato a Deus pelo dom da vida, pelo seu amor infinito, sem ele nada sou. Agradeço aos meus pais, Goretti e Rogério, meus maiores exemplos em tudo na vida e a minha irmãzinha que tanto amo Daisy. Obrigado por cada incentivo e orientação, pelas orações em meu favor, pela preocupação para que estivesse sempre andando pelo caminho correto.

Aos meus colegas de classe, Jediael Perreira, Naylla Eunice, Rosman Albuquerque, Wagner Lima, Gilton Ferraz, Marcela Perreira, Bruna Santos, Maryha Brandão e Midiã Monteiro, por todo companheirismos e amizade que criamos ao longo desses anos e que vou levar para toda a vida. Aos meus tios e tias, vozinha, vozinho, e aos meus primos que sempre estiveram presentes.

Ao professor Pedro Camilo que com muita paciência e atenção dedicou do seu valioso tempo para me orientar em cada passo desse trabalho.

Obrigado a todos que, mesmo não estando citados aqui, tanto contribuíram para a conclusão desta etapa em minha vida.

Ainda que eu andasse pelo vale da  
sombra da morte, não temeria mal  
algum, porque Tu estás comigo; a tua  
vara e o teu cajado me consolam.

(Salmo 23)

FERREIRA, Élton Laerte Campos. **A Dificuldade na Persecução dos Crimes Realizados Através da Internet**. 2014. 44 pg. Monografia (Bacharelado em Direito) Faculdade Sete de Setembro – FASETE, Paulo Afonso-BA.

## RESUMO

O presente trabalho traz consigo todo o desenvolvimento histórico e conceitos relacionados ao Direito e Informática. E a inconformidade a respeito da dificuldade persecução do Direito Penal, nos crimes praticados na internet, e apresenta uma análise sobre parte do texto da lei nº 12.737, em que apresenta uma serie de lacunas, referentes a sua aplicabilidade e eficácia, uma vez que suas penas são brandas e dão a possibilidade de dupla interpretação em um caso prático. Para a realização do estudo, a pesquisa utilizada foi à bibliográfica, onde foram exploradas, além da literatura doutrinária e legislações específicas, artigos publicados em sites jurídicos, entre outras obras congêneres, no qual se constatou que o legislador deveria ser mais objetivo com o texto da referida norma concernentes ao Delitos Informáticos.

**Palavras chave:** Delitos informáticos, Persecução Penal, Direito Informático, Eficácia e Aplicabilidade.

FERREIRA, Élton Laerte Campos. **A Dificuldade na Persecução dos Crimes Realizados Através da Internet**. 2014. 44 pg. Monografia (Bacharelado em Direito) Faculdade Sete de Setembro – FASETE, Paulo Afonso-BA.

## **ABSTRACT**

This paper brings all the historical development and concepts related to Law and Informatics. And the disagreement about the difficulty prosecution of criminal law, the crimes committed on the Internet, and present an analysis on part of the text of Law N° 12,737, which presents a series of shortcomings regarding its applicability and effectiveness, since their feathers are soft and give the possibility of double reading in a practical case. For the study, the survey used was the literatures, which have been exploited beyond doctrinal literature and specific laws, articles published in legal sites, among other similar works, in which it was found that the legislature should be more objective with the text said concerning the Computer Crimes standard.

**Keywords:** Computer Crimes, Criminal Prosecution, Computer Law, Effectiveness and Applicability.

## LISTA DE ABREVIATURAS E SIGLAS

CP = Código Penal

art. = artigo

p. = página

Dos = Disk Operating System

TI = Tecnologia da Informação

BR = Brasil

ARPANET = Advanced Research Projects Agency Network

NASA = National Aeronautics and Space Administration

WWW = World Wide Web

WEB = webpage

ASP = Application Solution Providers

TV = Televisão

TCP = TransmissionControlProtocol

IP = Internet Protocol

ISDN = Integrated Services for Digital Network

TSE = Tribunal Superior Eleitoral



# SUMÁRIO

<b>1.INTRODUÇÃO</b> .....	10
<b>2.DIREITO E INFORMÁTICA</b> .....	12
2.1 SURGIMENTO DA INTERNET .....	13
2.2. CONCEITO INFORMÁTICA E INTERNET.....	18
2.2.1. PROTOCOLO DE TRANSMISSÃO - TCP/IP .....	18
2.2.2 PROVEDOR DE ACESSO.....	21
2.2.3 CARACTERÍSTICAS.....	22
<b>3.OS DELITOS INFORMÁTICOS</b> .....	23
3.1 UM NOVO BEM JURÍDICO ?.....	26
3.2. DEFININDO O DELITO INFORMÁTICO .....	27
3.3 DELITOS INFORMÁTICOS IMPRÓPRIOS.....	30
3.4 DELITOS INFORMÁTICOS PRÓPRIOS.....	32
<b>4. LEI CAROLINA DIECKMANN (LEI Nº 12.737)</b> .....	34
4.1 CONCEITO .....	34
4.2 APLICABILIDADE .....	35
<b>5. CONSIDERAÇÕES FINAIS</b> .....	40
<b>REFERÊNCIAS</b> .....	42

## 1. INTRODUÇÃO

No transcorrer do presente trabalho buscar-se-á abordar questões concernentes à consecução do Direito Penal nos casos de cibercrimes, sendo feita uma minuciosa análise quanto à viabilidade e aplicabilidade nos casos práticos a partir da referida Lei Carolina Dieckmann (Lei nº 12.737), sendo que apesar desta referida lei apresentar várias falhas e brechas nas suas entrelinhas, ainda assim retrata um grande avanço no campo dos cibercrimes no ordenamento jurídico brasileiro.

A escolha do presente tema se deu pelo inconformismo e injustiça que hoje aterroriza a sociedade indefesa nesse novo campo do direito brasileiro uma vez que as brechas oriundas dessa lei são utilizadas para prática de crimes, visto que como instrumento utilizado é muito abrangente, virtual e de difícil elucidação (a internet) há certa complexidade para se investigar e punir os agentes delituosos, o que faz com que, na maioria das vezes, estes agentes fiquem impunes de tais crimes.

O objetivo geral da pesquisa consiste na análise da persecução penal dos crimes realizados na internet e conseqüentemente na difícil investigação e punição desses crimes, uma vez que a Lei Carolina Dieckmann (Lei nº 12.737), por trazer em seu bojo muitas lacunas propicia uma impunidade dos agentes delituosos, mesmo diante de provas obtidas lícitamente a serem utilizadas no processo penal brasileiro. Como objetivos específicos visaram-se demonstrar que a referida lei não consegue abarcar de forma eficaz os crimes a qual elenca ocasionando uma sensação de impunidade perante a sociedade brasileira, uma vez que o agente delituoso pode estar em qualquer parte do mundo e que apesar do avanço tecnológico, que será detalhadamente abordado no decorrer desse trabalho, ainda necessita-se avançar muito mais nesse campo, em que o tempo sobrepõe o tempo físico em que existimos.

Na metodologia, o método inicialmente utilizado fez-se necessário o uso dos métodos documental e indutivo. O método dialético foi o utilizado para abordar o discurso doutrinário, no que tange os pontos divergentes entre os citados autores. Quanto à metodologia procedimental, o método bibliográfico foi o principal para a exploração e o desenvolvimento da pesquisa.

O trabalho encontra-se dividido em cinco capítulos. No capítulo inicial será abordada a parte introdutória, referente ao que será abordado ao decorrer do presente trabalho.

No segundo capítulo será abordada toda parte histórica referente à internet e a informática, apresentando suas origens, finalidades e seu desenrolar até os dias atuais.

No terceiro capítulo consecutivo analisar-se-á o conceito de crime, fazendo menção aos crimes virtuais em si suas classificações e características.

Por seguinte, no quarto capítulo será feito um aprofundado estudo sobre a Lei Carolina Dieckmann (Lei nº 12.737/2012), desde sua origem, conceituação e características e também a sua aplicabilidade na prática. Por fim no último capítulo serão explanadas as considerações em relação às falhas e as possíveis medidas senatorias aos problemas da pesquisa.

## 2. DIREITO E INFORMÁTICA

Quando admitimos que a informática é uma fonte primária inclusive geradora de direitos e deveres -, passamos a uma segunda etapa, admitindo fontes secundárias e, assim, teremos um conceito mais abrangente quando adotamos o termo Direito Eletrônico. E é certo que a informática é espécie do gênero eletrônica.

Desta forma, entendemos por Direito Eletrônico o conjunto de normas e conceitos doutrinários destinados ao estudo e normatização de toda e qualquer relação em que a informática seja o fator primário, gerando direitos e deveres secundários. É, ainda, o estudo abrangente, com auxílio de todas as normas codificadas de direito, a regular as relações dos mais diversos meios de comunicação, dentre eles os próprios da informática. (FILHO, 2005, p. 15).

Existem vários conceitos para Direito informático, mas todos vêm atender uma única finalidade que é a considerada como a aplicação dessa tecnologia informática no Direito, que vem a ser um ramo dentro da Ciência do Direito que é Direito Informática.

Com o advento do surgimento da internet vieram não somente benefícios como também problemas em escala acelerada, com isso o homem teve de se adequar a realidade, mas como o Direito não consegue alcançar a sociedade na mesma velocidade esses problemas, muitas das vezes estes não são solucionados, sendo apenas algumas vezes remediados e praticamente em nenhum caso são sanados. Tais casos são de difícil resolução porque ainda não existe uma legislação específica e eficaz para solucionar esse tipo de crime. (MIRANDA, 2013, p. 04)

Devido ao crescimento vertiginoso da internet e foram surgindo, contudo novas condutas criminosas em que por vezes o Direito não consegue acompanhar. Hoje já existe uma legislação em relação aos crimes informáticos, contudo a mesma não consegue ter a devida eficácia<sup>1</sup> para sanar essas condutas.

Os crimes oriundos do advento da internet se modificam a cada dia e os agentes delituosos estão cada vez mais atualizados as várias formas e facetas criminosas. A grandiosa rede não possui um proprietário nem um local físico, mas tudo que é produzido nela reflete no mundo físico, dessa forma refletindo também em quem esta por traz do computador. Nesse momento é que o direito entra para salvaguarda os direitos não só de um usuário, mas de toda a sociedade. Visto que o ramo da informática é um campo ainda muito recente com infinitas possibilidades para o bem como para o mal o Direito sempre tenderá a estar presente nesse universo. (MIRANDA, 2013, p. 04)

As condutas criminosas na internet estão sempre em constante evolução, das mais variadas formas, tais condutas na internet são de difícil elucidação visto que esse local não existe no mundo físico dificultando a investigação, pois não é tarefa fácil saber o local de onde foi praticada a conduta. Contudo quando sempre existirá a ciência do Direito que sempre estudara essas condutas para salvaguardar os direitos de toda a sociedade.

## 2.1 SURGIMENTO DA INTERNET

A internet ou rede mundial de computadores surgiu em meados da guerra fria, pelos norte-americanos visando manter a comunicação em caso de ataques inimigos. Nos anos de 1970 e 1980 também foi utilizada como grande ferramenta para troca de mensagens entre professores e alunos de universidades dos Estados Unidos. (Patrícia P. Pinheiro, 2010, pág. 58).

De acordo com, Jaqueline Lima da Silva (2013) Podemos conceituar internet como um conjunto de computadores interligados em várias redes em comunicação com protocolos unificados, de forma que as pessoas que estão conectadas usufruam de serviços, informação e comunicação de alcance mundial influenciando alguns aspectos da vida dos seres humanos.

A mesma autora sustenta ainda que somente dez anos depois essa poderosa ferramenta começou a ser utilizada pela população com a implementação da sua interface gráfica com World Wide WEB que trouxe consigo páginas de navegação que facilitou a interação e a comunicação entre os usuários, fazendo surgir a rápida evolução da Internet por todo o mundo.

A partir daí foram sendo criados novos navegadores, cada vez mais modernos e tendentes a facilitar o meio de navegação entre os usuários, o que consideravelmente contribuíram para o crescimento em larga escala desse meio de comunicação. Além disso, foram desenvolvidos meios de interação entre usuário, como portais, com conteúdo para estudantes e também os exclusivamente de diversão, os famosos bate-papos, tornando-se a internet um grande meio de encontro entre usuários de todo o mundo. (Patrícia P. Pinheiro, 2010, pág. 58).

Pinheiro (2010, p. 61) acrescenta que os empresários também se interessaram muito por essa ferramenta, pois se utilizando da internet, eles fazem grande divulgação de seus produtos a baratos custos. Com isso, a internet se tornou uma verdadeira vitrine de loja online, em que o cliente para fazer compras ou consultar serviços não precisa sair da comodidade de sua casa.

Murilo Miranda (2013, p. 04) dispõe que:

Atualmente com a evolução tecnológica e precisamente com o surgimento da internet foram-se modificando o modo de as pessoas interagirem e de se comunicarem.

A Internet modificou a forma como as pessoas se comunicam de tal maneira que nenhuma invenção anterior teve o condão de alterar. O telégrafo, o telefone, o rádio e até mesmo o computador pessoal condensaram funcionalidades e prepararam a humanidade para o que estava por vir, uma era de inter-relacionamentos virtuais. Porém fundindo os propósitos e ferramentas de todos os meios de comunicação existentes, surgiu a rede mundial de computadores. Na simples e clara definição dada por Liliansa Minardi Paesini: "[...] a Internet é uma imensa rede que liga elevado número de computadores em todo planeta". (MIRANDA, 2013, p. 04).

É notório que a internet trouxe consigo uma gama infinita de possibilidades e uma demasiada proliferação de conhecimento, de modo que as barreiras antes existentes fossem quebradas e surgisse uma massiva troca de informações de forma rápida, simples, barata, independentemente de onde possam estar.

Segundo Demi Getschko, Diretor-Presidente do Núcleo de Informação e Coordenação do Comitê Gestor da Internet citado por Murilo Miranda (2013, p. 05) "O Brasil atingiu, em outubro de 2008, a marca de 1,5 milhão de domínios. br (sites aqui abrigados). Sinal de que o País não está apenas comprando computadores, mas também construindo a Internet que deseja". (MIRANDA, 2013, p. 05).

O supracitado autor elucida ainda esta questão abordando seguintes aspectos que tornaram possíveis essa grande expansão:

Primeiramente, a evolução tecnológica que começou com as primeiras pesquisas sobre trocas de pacotes de dados e a ARPANET – um esboço de rede integrada de computadores locais, de onde a pesquisa atual continua a expandir os horizontes da infraestrutura em várias dimensões como escala, desempenho e funcionalidade de mais alto nível;

b) O segundo ponto convergente orbita sobre os aspectos operacionais e gerenciais de uma infraestrutura operacional complexa e global;

- c) Deve-se também ressaltar o aspecto social que resultou numa larga comunidade de internautas trabalhando juntos para criar e evoluir com a tecnologia;
- d) E, por fim, o aspecto de comercialização que resulta numa transição extremamente efetiva da pesquisa numa infraestrutura de informação disponível e utilizável.

Quando, em 1957, a antiga União Soviética colocou em órbita o primeiro satélite espacial do mundo, o presidente norte-americano Dwight Eisenhower tratou de prontamente anunciar a criação de uma agência federal norte-americana, nos moldes da NASA, chamada AdvancedResearchProjectsAgency (Arpa), com a missão de pesquisar e desenvolver alta tecnologia para as Forças Armadas norte-americanas. Em meados da década de 1960 a Rand Corporation publicou um relatório sobre a segurança das redes de comunicação e sua vulnerabilidade em caso de um conflito nuclear. Dentre os pontos fracos apontados pelo relatório estavam a centralização excessiva de algumas redes e a forte dependência de centros de coordenação. Não havia nenhuma liberdade operacional em caso de uma interrupção de comunicação com os centros de controle.

Em 1969, a rede de comunicações militares que terminou sendo criada com esse projeto, foi denominada Arpanet (rede da agência de projetos avançados de pesquisa). O seu caráter descentralizado continua presente até hoje, na Internet. Em 1969, a rede de comunicações militares que terminou sendo criada com esse projeto, foi denominada Arpanet (rede da agência de projetos avançados de pesquisa). O seu caráter descentralizado continua presente até hoje, na Internet. (VLADMIR, 2007, p. 171 – 173).

Com isso, podemos perceber que a evolução da internet é de enorme complexidade, pois a mesma não depende de um único fator, ela se comunica com várias áreas, não tecnológicas, mas também percorrem as áreas organizacionais e comunitárias, não se impondo tão somente seus profundos conhecedores, uma vez que cada dia mais suas ferramentas são utilizadas por todos os seus usuários, sem restrições, tanto para realizações de transações econômicas como para o meio social que a envolva.

A internet trouxe como sua primeira ferramenta o e-mail, que até os dias atuais é um instrumento indispensável, tanto por sua rapidez como praticidade, para facilitar a comunicação entre pessoas em todas as partes do mundo.

Foi lançada em 1992 e conquistou os usuários por sua versatilidade, recebendo o nome de world wide web (larga teia mundial), ou simplesmente web, e popularmente conhecida pelas letras “WWW” (Spencer Sydown 2013, p. 31).

Por sua vez a internet trouxe a WEB que é ambiente gráfico onde se é possível interagir por aplicativos e até mesmo baratear despesas até mesmo do próprio governo como preleciona Murilo Miranda (2013, p. 03):

A WEB é outra grande funcionalidade da Internet. Ela modificou a forma como os clientes são atendidos, o marketing, a educação, o aprendizado e etc. A Internet é o meio que proporciona a WEB, que nada mais é do que ambiente multimídia daquela. A telefonia pela Internet já está, á grandes passos, extinguindo o telefone convencional, que demanda enormes custos com centrais de telefonia, torres de transmissão e cabos, além de baratear consideravelmente as ligações telefônicas. E não irá parar por aí. As próximas vítimas serão a televisão e o cinema, que migrarão para a Internet com o advento da transmissão em tempo real.

O referido autor supracitado acrescenta que atendimento online com visualização online, transmissão de vídeo em alta qualidade, tradução de conteúdo para outros idiomas, prontuário eletrônico de pacientes com acesso descentralizado pela Internet, ênfase na educação à distância em nível de treinamento de cargos ou tutoriais de classes, pesquisas e eleições interativas, são exemplos de serviços que estarão disponíveis na Internet em poucos anos. Agora existem os ASP- ApplicationSolutionProviders, que são empresas especializadas no desenvolvimento de aplicações para a Internet. O número de possíveis aplicações na Internet é absolutamente infinito. Veja o sucesso no Brasil da entrega do Imposto de Renda pela Internet, tanto em termos de comodidade para a população como em termos de redução de custos para, no caso, o Governo.

Segundo Patrícia Peck Pinheiro (2010, Página 47), nos anos 70, Alvin Tofler já destacava a necessidade de uma evolução na sociedade por ele denominada como sociedade da evolução, onde existiriam duas formas de tempo, um analógico e outro digital, em que o primeiro seguiria um tempo físico, vinte quatro horas por dia ou sete dias por semana. Já o digital seguiria um tempo virtual, tempo esse que sobrepõe os limites existentes das horas e dos dias, nesse tempo exigiria dessa “sociedade de informação” que executasse várias ações simultaneamente umas às outras exigindo assim que cada vez mais todos seus adeptos realizem mais obrigações, absorvam mais informações, ultrapassando assim a barreira de fusos



horários e das distâncias físicas. Essas tarefas devem ser executadas num tempo que o autor denominava-o de tempo paralelo, que era o mesmo que o tempo digital. Tofler ainda sustenta que a velocidade da tomada de decisão dentro de uma organização seria o instrumento de sua própria sobrevivência. Hoje, vivemos esta realidade. A agilidade imposta às empresas da economia digital exige um pensamento jurídico capaz de ultrapassar a barreira do tempo exigido pelas repartições públicas, pelos órgãos de registro, pelo poder Judiciário. Se a fórmula jurídica estiver errada, mesmo que possa corrigi-la, o custo do tempo pode ser fatal. (Pinheiro, 2010, pág. 47)

Diante disso ressaltamos que hoje somos praticamente obrigados a exercer funções cada vez mais rápidas e complexas. Vivenciamos a mencionada “sociedade da evolução” que exige cada vez mais de seus adeptos um maior dinamismo e praticidade em sua atuação.

A humanidade está constantemente se reinventando, hoje a rapidez em que as informações navegam de um lugar para o outro é espantosa, assim como também o meio pelo qual elas são enviadas. A sociedade da informação a qual Tofler faz menção surgiu em meados do século XX com o avanço dos meios de comunicação. Essa época ficou conhecida como da comunicação em massa, hoje tal denominação não tem mais respaldo, pois uma nova sociedade surgiu tendo como principal foco a diversidade. (PATRICIA, 2010, pág. 47).

Ainda de acordo com Patrícia Pinheiro (2010,pág,48), Tofler dividiu a evolução da humanidade em três partes:Tendo início quando a nossa espécie (humana), começou a evoluir do nomadismo para a cultivo das terras, período em que a terra passou a dar status de poder a propriedade de terra e esta se tornou o meio de se adquirir poder. A segunda etapa teve seu apogeu na Revolução Industrial, em que a mixagem de propriedade, trabalho e capital derivava em riqueza. Mas o seu auge se deu com a segunda guerra mundial, com advento do modelo de produção em grande escala trazidas pelas nações envolvidas. Por fim a terceira e última fase se deu num curto período de tempo entre o fim do século XIX e o início do século XX, a fase da informação que se deu com o surgimento dos meios de comunicações como o telefone, cinema, rádio e TV.

A grande marca dessa terceira fase se deu devido aos meios de comunicação progressivos de informações, ao modelo de produção em larga escala, do

envolvimento de grande número das massas populares e o poder centralizado e devido de padronização imposto pela era industrial.

## 2.2 CONCEITO DE INFORMÁTICA E INTERNET

A Informática é o emprego do tratamento automático das informações. Isto posto, é de se entender que é necessária uma linguagem uniforme para que o uso, a transformação e a transmissão de informações sejam amplos e difundidos de maneira global. (SYDOW, 2013, p. 29).

É a Ciência que estuda o tratamento de informações por meio de computadores. Tecnologia essa que permite a disseminação da informação pelo mundo através dos computadores.

A internet é uma rede classificada como WAN ( Rede de Dimensão Global) e conecta diversas outras redes em todo o mundo, através de estruturas robustas chamadas de backbone. ( MORAES, 2011).

A Internet (com I maiúsculo) é um imenso sistema de redes gateways e de computadores permanentemente interligados entre si a nível mundial e que funcionam como emissores e receptores de informação, utilizando para isso um conjunto de protocolos de comunicação denominados TCP/IP. A Internet permite interligar sistemas informáticos de todo o mundo, possibilitando a comunicação e a troca de informação de uma forma fácil e rápida. Os meios para efetuar essas ligações são diversos, e incluem rádio, linhas telefônicas, linhas digitais, satélite, ISDN, fibra-óptica, etc. (NUNES, 2007).

A Internet é composta por várias redes de computadores existentes por todo o mundo, que se comunicam entre si, recebendo e enviando informações umas com as outras.

### 2.2.1 PROTOCOLO DE TRANSMISSÃO – TCP/IP

De acordo com Elaine Martins. Um protocolo é um conjunto de regras que governam como computadores conversam a cada outro. TCP/IP é um protocolo extensamente usado e muito popular. Com TCP/IP, sistemas de computador diferentes podem trocar dados de maneira confiável em uma rede interconectada. As configurações desses protocolos tem como função controlar como a informação é passada de uma rede a outra, e como manipular. (MARTINS, 2012).

Mesmo que dois computadores estejam ligados a uma mesma rede, eles não vão conseguir se comunicar sem o uso de um "idioma" comum. E na internet essa é a função do TCP/IP, um conjunto de protocolos criado para ser um recurso da ARPANET. Dessa forma, os computadores conseguem enviar e receber informações – que vão desde um e-mail até uma página que se carrega no navegador. (RAMUSSEN, 2013).

O modelo utilizado pelo TCP/IP é o de cliente/servidor, no qual um computador envia solicitações, como carregar uma página da web, a um outro computador. O TCP (Protocolo de Controle de Transmissão) é o responsável por quebrar uma mensagem em partes menores, enviando-as pela internet. O computador que recebe esses pacotes de informação utiliza outra ferramenta do TCP para reunir estes dados na mensagem original.

Para que esses pacotes cheguem ao destino certo, utiliza-se o IP (Protocolo de Interconexão), que fornece o endereço certo para a entrega das informações. Nesse processo, os fragmentos da mensagem original podem até tomar rotas diferentes, mas chegarão ao mesmo destino para que a informação esteja completa.

Para (Vladimir, 2007, p. 170 – 171), A Internet é, portanto, um conjunto de várias redes interconectadas em todo o mundo para o intercâmbio de dados, graças à adoção de um padrão comum de troca de dados: os denominados protocolos de comunicação TCP e IP. Eles permitem que sistemas informáticos situados em qualquer lugar do mundo e equipados com qualquer sistema operacional (como DOS, Windows, Linux etc.) viabilizem o acesso dos usuários aos vários serviços oferecidos no âmbito da Internet, tais como o e-mail (correio eletrônico), a World Wide Web, as salas de “bate-papo” (chats) etc.

E o famigerado termo protocolo? Protocolo é a designação dada aos formatos de mensagens e suas regras entre dois computadores para que possa haver a troca de mensagens, ou seja, o protocolo permite a comunicação entre dois computadores. (PIMENTEL, 2010, p. 13).

O TCP/IP é um conjunto de protocolos de comunicação entre computadores em rede (também chamado de pilha de protocolos TCP/IP). Seu nome vem de dois protocolos: o TCP (TransmissionControlProtocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Interconexão). (MIRANDA, 2013, p. 06).

O mesmo autor sustenta que o conjunto de protocolos pode ser visto como um modelo de camadas, onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada

superior. As camadas mais altas estão logicamente mais perto do usuário (chamada camada de aplicação) e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração.

TCP/IP é o protocolo basilar do recebimento e envio de dados é ele quem dita a rota a que os dados irão seguir para chegar ao computador para o qual foi enviado. Esse procedimento ocorre tanto na Internet como na Intranet, que é uma rede de computadores privada que assenta sobre a suíte de protocolos da Internet, porém, de uso exclusivo de um determinado local, como, por exemplo, a rede de uma empresa, que só pode ser acessada por seus usuários ou colaboradores internos, tanto internamente como externamente ao local físico da empresa. São através dos Protocolos que os computadores se comunicam (MIRANDA, 2013, p. 02).

Este protocolo IP, permite a comunicação entre os computadores, utilizando-se de duas formas: na primeira, o Protocolo divide a informação a ser compartilhada em pequenos pacotes que chegam ao computador de destino ordenadamente. Na segunda, o Protocolo manipula o mecanismo de endereçamento dos computadores, permitindo que cada máquina procure, identifique e comunique com a outra. (MIRANDA, 2013, p. 02).

Nota-se que o meio pelo qual os dados são endereçados e enviados de um computador a outro é através de protocolos pela internet e o protocolo responsável é o TCP/IP, e é por meio dele que o usuário deixa sua marca, pois para o envio ou recebimento é necessário o local físico do destinatário, ou seja, o local onde deve ser enviado ou recebido os dados e é por meio desse mecanismo que se pode identificar o indivíduo que por ventura venha a cometer crimes através da Internet. Seria uma espécie de impressão digital do computador, pois cada computador possui um único (Murilo Miranda, 2013, p. 03).

Com tudo o Protocolo TCP/IP, é o meio pelo qual as informações serão gerenciadas e enviadas em outras palavras é o meio pelo qual elas conversão é por intermédio desse protocolo que sistemas de computadores mesmo sendo diferentes uns dos outros podem se comunicar perfeitamente, com a troca de dados de forma segura, e ele ainda controlando como vai ser a passagem das informações de uma rede a outra.

## 2.2.2. PROVEDOR DE ACESSO

De acordo com Márcia Chacon, podem-se considerar os provedores de acesso à internet, como sendo as instituições se conectam a internet, disponibilizando o acesso a terceiros. Quando a pessoa se conecta a internet o provedor de acesso atribui um endereço conhecido como IP-Internet Protocol, criando com isso um arquivo que identifica a pessoa que está ligada àquela porta.

O provedor de acesso nada mais é do que uma determinada empresa que presta serviços de conexão de Internet que traz consigo outros serviços relacionados à Internet, como por exemplo: e-mail, hosting de páginas web e blogs, dentre outros serviços que detém ou também utilizam consigo a mesma tecnologia.

Hoje o que podemos dizer é que as empresas responsáveis pelos serviços de provedores não são apenas menos aglutinadores do mundo virtual, mas sim são peças de fundamental relevância no âmbito jurídico, pois são eles que fornecem o meio pelo qual o usuário irá ter acesso a rede de Internet pública ou nas privadas. Isso significa que muitas das soluções jurídicas para a proteção de valores sociais e das relações interpessoais na rede tem seu início nos provedores e podem ser mais bem controladas por meio deles.

Inicialmente vamos entender as características jurídicas da dupla atuação dos provedores de acesso. São duas as posições jurídicas. A primeira atua como operadores de telecomunicações responsáveis pela transmissão de mensagens e conteúdos por meio da rede. A segunda, de editores responsáveis pela hospedagem, publicação e até produção de conteúdo na Internet. Cada uma dessas situações determina níveis de responsabilidade distintos.

As características dos serviços contratados dos provedores são custo, competência técnica, confiabilidade no plano de segurança, de usuários, o que significa que é uma modalidade de empresa relacionada com a área de telecomunicações, mas com características próprias e peculiares ao veículo de comunicação Internet, que é não só meio, como mídia. (PINHEIRO, 2010, p. 103)

### 2.2.3 CARACTERÍSTICAS

Direito Informático é uma disciplina jurídica autônoma. Sua existência, e por não dizer necessidade, se justifica na medida em que as relações e conflitos jurídicos fruto do uso das novas tecnologias demandam tratamento jurídico. O Direito não pode negar-se a admitir a existência desta nova etapa na evolução humana, a chamada era da informação, da qual resultam inúmeros problemas que carecem de solução. (PEREIRA, 2001).

O Direito Informático é, pois, resultado da relação entre a ciência do Direito e a ciência das novas tecnologias (informática e telemática). Não há como negar que o Direito, como ciência, funciona melhor com o uso da informática e da telemática. Estas, por sua vez, necessitam de normas e regras as quais possibilitem sua correta e adequada utilização, é dizer, cabe ao Direito regular as relações sócio-jurídicas surgidas da influência da informática e da telemática na vida dos indivíduos de uma forma geral. (PERREIRA, 2005).

O Direito Informático surgiu com a necessidade de um novo ramo do Direito, que abarca-se uma nova criminalidade que surgiu com o avanços tecnológicos na área da informática. Então o direito veio para tutelar esses novos conflitos e aplicar as melhores soluções e coerentes aos casos concretos.

### 3. OS DELITOS INFORMÁTICOS

Para dar início ao estudo do presente capítulo sobre os delitos informáticos é mister que de início explique o que são os delitos informáticos, suas características e como também suas particularidades como também de que forma são classificados esses delitos informáticos e por fim quais os bem jurídicos envolvidos.

O significado da nomenclatura crimes informáticos aqui utilizado não é acolhida de forma geral pelos doutrinadores, assim existindo várias outras nomenclaturas utilizadas para o mesmo tipo de estudo as quais preleciona Spencer TothSydow: crimes da era da informação, crimes mediante computadores, crimes cibernéticos, cibercrimes, crimes de computador, crimes eletrônicos, crimes tecnológicos, crimes digitais, crimes high-tech, tecnocrimes, netcrimes, crimes virtuais, crimes da tecnologia da informação e e-crimes. (SYDOW, p. 55).

É a informática é um meio que estuda o tratamento das informações com o uso de computadores e vários outros dispositivos existentes hoje de tratamento de dados.

Desta forma por causa da sociedade pós-industrial foi desenvolvendo um forte impulso para a cultura da informação e comunicação, e a cada dia se expande mais os estudos em relação Tecnologia da Informação (TI). E o conjunto de atividades que regressa como o serviço de maior crescimento tem a denominação de informática.

Com a revolução industrial girando em volta de uma sociedade em que seus recursos são finitos, retirados da própria natureza em sua grande totalidade e modificados pelo ser humano. Na sociedade que hoje se encontra a informática, cujo é dada a conotação de sociedade pós-industrial ou também como a sociedade informática, sociedade do conhecimento, sociedade tecnizada ou sociedade em rede, ela encontra sua existência embasada (assegurada) e também organizada em volta da informação. O que aconteceu é que enquanto todos os recursos da revolução são finitos, a informação nunca esgota está sempre em constante expansão.

E com base em tal conclusão, podemos concluir que na sociedade contemporânea e futura a informação agrega valores como o econômico, gerando como consequência para os mesmos que adetem e sabem utilizá-las em forma de comercialização.

Spencer Toth (2013, p.57) dispõe: Conforme evoluímos, mais e mais deixamos que a tecnologia informática tome espaço em nossas vidas. O ferramental capaz de criar e armazenar documentos leva-nos a um momento em que fichas médicas, informações bancárias, planilhas de custos, projetos, fotos, filmes, livros, enfim, uma gama imensa de informações transforma-se em bits e fica disponível para consulta e utilização.

A cada dia que se passa a informática adentra mais no cotidiano das pessoas. Ela vem trazendo consigo uma imensa capacidade de armazenamento de informações que facilitam a vida com o acesso rápido desde a informações sobre a conta bancária a um simples e-mail e tudo é transformado em bits e tais informações podem ser consultadas de forma rápida e sempre que necessário se faça.

Spencer Toth (2013, p.57) Preleciona Até sem saber, os caminhos feitos dentro da rede, as aquisições feitas com cartão de crédito ou pelo celular, as conversas que ocorrem com outros usuários e até mesmo senhas e dados pessoais vagam pela rede, num ambiente em que cada informação importa.

Um ambiente cheio de comodidade para os usuários, desde a possibilidade de compras, vendas, acesso ao sistema bancário pessoal e conversas pessoais. Circulam em um ambiente seguro onde pessoas armazenam informações. Nesse ambiente em que toda informação tem um relevante valor econômico e pessoal.

Segredos industriais criados e armazenados como arquivos eletrônicos podem valer milhões, assim como uma próxima edição de um livro, e tais patrimônios não podem sequer ser acessados sem o auxílio da informática. (SYDOW, 2013, p.57).

Hoje a informática vem assumindo o papel de um imenso “cofre”, onde é armazenado todas as informações de caráter valioso, visto que existem informações de empresas de inimensurado valor econômico, como obras de empresas armazenadas nesse cofre que ainda nem se quer foram lançadas ao mundo para serem apreciadas pela sociedade o que o trona ainda amais valioso, toda essa informação é equivalente a fortunas em dinheiro, e para acessar toda esse cofre se faz necessário a utilização da informática.(minhas P)

Spencer Toth (2013, p. 57) o crime informático deve ser avaliado sob diferentes perspectivas por conta de suas peculiaridades.



As normas comumente utilizadas para definir condutas e regras para a sociedade levaram em conta a idéia de estado como uma instituição composta cumulativamente por população, território e governo, todos presentes e tangíveis. As regras penais e outras estavam alicerçadas no conceito de ambiente físico, onde crimes do mundo real ocorriam e que tem como pilstras (i) proximidade, (ii) a escala, (iii) o constrangimento físico e (iv) padrões.

As normas jurídicas que existem em nosso ordenamento foram feitas para regulamentarem as condutas em sociedade.

Essas normas foram criadas tendo como fundamento o Estado como uma instituição formada pela população, território e governo, dessa forma percebe-se que esses fundamentos estão presentes em um plano em que são palpáveis e presentes. Dessa forma as normas da legislação penal e as demais foram criadas para regular condutas existentes no plano físico, ou seja no mundo real, onde eram cometidos esses delitos e tem como alicerce essas normas a proximidade, a escala, o constrangimento físico e padrões, a regular essas normas do direito penal.

Spencer Toth (2013, p. 58) De acordo com o Direito Penal do mundo físico, o ofensor e a vítima estão comumente próximos quando o fato típico ocorre, sendo. Pois, impossível o cometimento de, por exemplo, um estupro sem contato, portanto entre pessoas distantes.

A criminalidade em tal situação é entre seus singulares, e aquele que comete o fato ou minimamente o tenta, sem atingir o exaurimento) necessariamente deverá dispende algum tempo na preparação de um crime como. Por exemplo, um roubo a bancos.

Há necessidade de planejamento, análise, ponderação, visita ao local, e durante tal processo pode o delinquente ser visto e notar-se maneira suspeita em seu comportamento. Há, na criminalidade real, alto risco porquanto se exige movimento físico e contato.

Com isso, é de se dizer que a criminalidade do mundo real é mais simples de se combater, uma vez que o agente criminoso está limitado no espaço e comete apenas um crime (ou uma cadeia de crimes) por vez. Cometido o fato, o crime real tem local precisado e a polícia passa a agir in loco, focada no ambiente em que houve o fato jurídico, naquele segmento social.

O Código penal vigente existe para regular as atividades que acontecem no plano físico e todo ato típico ocorre quando as vítimas e o ofensor estão próximos um

do outro. Sendo impossível a possibilidade de o agente delituoso cometer um possível crime sem contar este com sua presença física. Dessa maneira para o cometimento dos crimes no plano físico, terá o agente delituoso que se expor para que exista a possibilidade de que o ato criminoso possa se realizar ou tentar, portanto a exposição do agente se faz necessária no plano físico pois sua preparação exige esse requisito, deixando assim o vulnerável o agente pois o mesmo terá, que estar em um local e planejar uma série de detalhes que o fará estar em posição desprivilegiada no mundo físico sendo assim fácil de combater, visto que esse agente estará em um lugar certo no plano físico e só conseguem praticar tais atos criminosos um por vez ou em sequência. Dessa forma todo ato criminoso se torna de fácil investigação em torno do local do crime podendo ser investigado pela polícia tendo local certo e ponto de início em que foi cometido o crime.

Spencer Toth (2013, p.58): Art.6º logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:

I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais;II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;VI – proceder a reconhecimento de pessoas e coisas e a acareações;

Hoje podemos ver a ineficácia de tal legislação que não acompanhou o avanço desses determinados delitos em que o local em que foi praticado o delito não existe no mundo real, tal delito possui nuances que o Código Penal não consegue abarcar em seu texto não existe mais o objeto a ser apreendido como prova para ser um meio para a investigação de tal delito. O criminoso com essa nova ferramenta ataca várias vítimas ao mesmo tempo, sem que se quer a vítima perceba que está sendo atacada pois em geral esses delitos acontecem de forma sorrateira.

### 3.1 UM NOVO BEM JURÍDICO?

Spencer Toth (2013, p. 76) A idéia de bem jurídico está ligada a valores que devem ser protegidos pelo Direito Penal, especialmente pelo fato de que o estado democrático de Direito deve garantir a seus cidadãos o desenvolvimento pacífico e a

coexistência de semelhantes em igualdade de condições necessárias, verdadeiramente como mantedor da ordem social.

O pensamento de determinado bem jurídico está vinculado a determinados valores, que estão salvaguardados por nosso Código Penal, pois o modelo de Estado em que vivemos nos garante a existência de uma sociedade igualitária para todos e todas as condições que se façam necessárias para a existência e as demais necessidades de toda a sociedade.

Foi após a grande revolução com o surgimento da grandiosa rede mundial de computadores que começaram a surgir novas práticas delitiva. Crimes esses que se incorporaram de forma rápida ao ponto que o Direito não conseguiu acompanhar tamanha evolução tecnológica. Essas práticas delitivas se camuflam entre a rede mundial de computadores, sendo ainda hoje difícil encontrar o responsável pelo ato criminoso e mais ainda puni-lo, pois ainda não existeno Brasil uma legislação eficaz para abarcar tais crimes, nem tão pouco profissionais suficientes e preparados para atender essa nova demanda como diria o grande político, estudioso e economistaUlpiano: "onde está a sociedade, ali está o direito", dessa forma o direto vem para salvaguarda o interesse da sociedade nesse ambiente repleto de lacunas e perigos para toda a sociedade.(MIRANDA, 2013, p. 03).

### 3.2DEFININDO OS DELITOS INFORMATICOS

Para darmos início ao presente estudo sobre os delitos informáticos e mister que se delimite o que seriam esses tipos de delitos, como também demonstrar suas características e particularidades e apresentar as formas de classificar tais delitos.

Os doutrinadores usam diversas nomenclaturas para nomear o mesmo tipo de estudo.

O Código Penal atual não destaca uma definição para o conceito de crime, como podia ser visto nas leis antigas, o crime evoluiu com o passar dos séculos. Como bem lembra o Prof. Heleno Fragoso: "a elaboração do conceito de crime compete à doutrina" (MIRABETE, 2009, p. 80).

Os mesmos autores relatam que o próprio Código Penal vigente, com suas alterações oriundas da Lei nº7.209/84 que reformulou toda a Parte Geral do Código

de 1940, não define o que é "crime". O Código Criminal do Império de 1830 determinava o conceito de crime em seu artigo 2º, parágrafo 1º: Julgar-se-á crime ou delito toda ação ou omissão contrária às leis penais. Já o Código Penal Republicano de 1890 assim elucidava em seu artigo 7º: "Crime é a violação imputável e culposa da lei penal."

O que existe hoje é uma divisão do conceito de crime em três partes diferentes. Pela Doutrina a conceituação de crime é dividido em: conceito formal, material e analítico.

Sob o aspecto formal crime é tido como "o fato humano contrário à lei (Carmignani); qualquer ação legalmente punível; toda ação ou omissão proibida pela lei sob ameaça de pena; ea conduta (ação ou omissão) contrária ao Direito, a que a lei atribui uma pena". (Mirabete, Fabrini, 2009, p. 81).

A definição do conceito material de crime indaga a forma externa do crime, dessa forma tende-se a um estudo mais amplo, pois a partir daí verifica-se o porquê do legislador tenha concebido a esse fato uma punição e de outros não. Esse conceito abrange várias áreas não apenas jurídicas como também as áreas da sociologia, filosofia, psicologia.

Diante disso, afirma Noronha apud Mirabete, Fabrini (2009, p. 82) que "a melhor orientação para obtenção de um conceito material do crime é aquela que tem em vista o bem protegido pela lei penal. Tem o estado a finalidade de salvaguardar a paz interna, a segurança e estabilidade coletiva diante dos conflitos inevitáveis entre os interesses dos indivíduos e entre os destes e os do poder constituído, mantendo a ordem, a harmonia e o equilíbrio social".

Nota-se que nessa conceituação material de crime são valorados os bens e interesses tanto individuais como coletivos sendo esses bens protegidos através da lei penal com a aplicação das devidas penas.

O conceito analítico de crime é dividido em duas teorias: a bipartida e a tripartida.

Na tripartida, o crime é caracterizado como um ato ilícito e antijurídico e a culpabilidade é apenas o meio pelo qual o agente desse crime irá ser punido com as devidas penas ao caso concreto. Já o conceito tripartido do crime é um fato praticado pelo agente típico, antijurídico e culpável. (Mirabete, Fabrini, 2009, pág. 83)

A legislação brasileira necessita urgentemente de uma reforma no sentido de se adequar a essas novas tendências mundiais de crimes, para não mais depender de analogias jurídicas realizadas pelos magistrados realizadas para a adequação delituosa do criminoso “virtual” e os usuários precisam se informar e se inteirar mais sobre esses novos crimes, sua metodologia para então aprender a como se defender dessa nova face criminosa e tão ou mais perigosa que as utilizadas no plano físico. (Oliveira, Silva, 2013, p. 04)

Luiz Oliveira e Marília Silva (2013, p. 05) dispõem que:

Os crimes virtuais utilizam a mesma metodologia de crimes utilizados em crimes já conhecidos. A técnica empregada que difere um pouco dos delitos presentes em nosso ordenamento jurídico penal, mas o fim que se pretende é o mesmo da conduta já tipificada. A intenção do criminoso pode ser de ludibriar uma pessoa para obter uma vantagem financeira ou pessoal, enganar suas vítimas ou mesmo furta informações particulares com o intuito de utilizá-las em proveito próprio.

Ultimamente uma modalidade de crime que vem se tornando muito comum na internet é o envio de e-mail simulando ser de algum órgão estatal conhecido, como é o caso da Receita Federal, TSE (Tribunal Superior Eleitoral), Polícia Federal e Serasa. A metodologia empregada é enganar o proprietário do e-mail, com uma mensagem dizendo que existe alguma pendência com o órgão e que este deve clicar em algum link para solucionar tal situação ou até mesmo para saber mais detalhes sobre o fato. Ao clicar em tal link, o usuário é redirecionado para uma página em que o intuito é instalar um programa conhecido como sanguessuga no computador da vítima, e a partir desse momento, o criminoso começa a receber dados sigilosos.

Outra modalidade bem comum emprega a mesma metodologia de envio de e-mail à vítima, mas ao invés do remetente da mensagem ser um órgão oficial do governo, os criminosos utilizam nomes de Instituições Financeiras. Esta modalidade de envio de e-mail é bem mais específica, pois a vítima deve possuir laço com a instituição financeira utilizada, e ao clicar no link contido no e-mail, o usuário é direcionado a uma falsa página do banco, onde este deve digitar seus dados bancários para uma suposta atualização bancária, e após digitar esses dados o remetente da mensagem recebe todos esses dados e com isso pode efetuar diversas transações bancárias lesando a vítima.

Existem crimes que o intuito do delito é de demonstrar a fragilidade de sistemas, como é o caso das recentes invasões às páginas de órgãos oficiais. Nesta modalidade o criminoso é motivado por uma questão de desafiar a segurança de sites do governo. Existe uma infinidade de crimes virtuais, muitos ainda nem possuem um modo de operação conhecido, outros ainda nem foram descobertos. As polícias científicas necessitam urgentemente se aperfeiçoar para tentar primeiramente descobrir quem são esses indivíduos que agem no anonimato na internet, de onde são realizadas tais operações e principalmente como puni-los.

### 3.3 DELITOS INFORMÁTICOS IMPRÓPRIOS

Os crimes virtuais com a denominação de impróprios se utilizam do computador como instrumento para realização das condutas tidas como ilícitas que atingem todo o bem jurídico já tutelado, crimes, que já tipificados que são realizados agora com a utilização do computador e da rede, utilizando o sistema de informática seus derivados como mais um meio para realização de crimes. Se diferencia quanto a não essencialidade do computador para concretização do ato ilícito que pode se dá de outras maneiras e não precisamente pela informática para chegar ao fim a que se é desejado, como no caso de crimes como o de pedofilia. (Carneiro, 2012, p. 186)

A problemática em torno da formulação de uma definição precisa de “crime informático” deve-se em parte ao fato de que os dados e sistemas informáticos tanto podem constituir o objeto material de determinada conduta, bem como o instrumento utilizado para cometê-la. A noção de “crime informático” pode envolver, portanto, várias espécies de condutas humanas.

As condutas definidas como “crime informático” pelas leis internas dos Estados contemporâneos geralmente representam uma lista variada de atividades, incluindo a prática de atos envolvendo pornografia infantil, corrupção de menores<sup>29</sup>, fraude, estelionato, violações de direitos autorais, extorsão on-line, invasão não autorizada de sistemas informáticos ou hacking, divulgação não autorizada de dados informáticos, propagação de vírus de computador etc.

Muitas dessas condutas podem representar delitos tradicionais, cometidos através da utilização de um sistema informático. Isso pode significar simplesmente a utilização das novas tecnologias informáticas para viabilizar

a prática de condutas já tradicionalmente sancionadas pelo Direito Penal. Portanto, ao ser utilizado como mero instrumento, o sistema informático pode constituir apenas um novo *modus operandi* para a prática de condutas já tradicionalmente tipificadas pelo Direito Penal dos Estados, como, por exemplo, o homicídio de um paciente provocado pela adulteração intencional da dosagem de medicamentos prescrita no prontuário eletrônico do sistema informático de uma unidade de terapia intensiva de um hospital, ou mesmo a alteração de dados ou a manipulação de sistemas que controlem o pouso e a decolagem de aviões, o tráfego aéreo, as rotas de trens e de metrô, os semáforos, podendo provocar, portanto, colisões e mortes. Note-se que o resultado pretendido pelo agente – o homicídio – poderia ser alcançado sem a necessária utilização de um sistema informático. (Vladimir,2007, p.18-21.)

O mesmo autor acima citado trata os crimes eletrônicos impuros ou impróprios como “aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática”.

Spencer Toth (2013, pag.87) dispõe que são delitos informáticos impróprios:delitos informáticos impróprios são delitos comuns, portanto condutas típicas, antijurídicas e culpáveis, que são perpetradas utilizando-se de mecanismos informáticos como ferramental, sendo que outros meios poderiam ter sido igualmente eleitos para a prática.

Seguindo entendimento semelhante, Maria José Crepaldi Ganancio LIBERATI. Crimes informáticos impuros ou impróprios: aqueles em que o sistema computacional funciona como ferramenta para a prática de condutas lesivas ao bem jurídico já protegido, não relacionado com a informática, produzindo resultado naturalístico que ofendem o mundo real.

Os delitos informáticos impróprios são aquelas condutas praticadas pelo agente delituoso, já classificado como típicas, culpáveis e antijurídicas. Para essas condutas serem cometidas a utilização da informática nada más é que um meio pelo qual esse agente que pratica o delito escolheu para a realização do delito , sendo que o mesmo poderia ter executado o delito por outro meio, sem sé fazer necessário a utilização da informática para concretizar o delito.

### 3.4 DELITOS INFORMÁTICOS PRÓPRIOS

Os crimes virtuais são classificados em duas espécies. Os chamados crimes próprios são aqueles em que o sujeito se utiliza necessariamente do computador, do sistema informático do sujeito passivo em que o computador é usado, através da utilização de objetos e meios para prosseguir com a execução ato criminoso. Nessa aba de crimes está não só a invasão de dados não autorizados mais toda a interferência em dados informatizados como, por exemplo, invasão de dados armazenados em computador seja com a intenção de modificar, alterar, inserir dados falsos, ou de forma, que atinjam diretamente o software ou hardware do computador e só podem ser concretizados pelo computador ou contra ele e seus periféricos.

Marco Túlio Viana (2003, pag. 13-26) trata as condutas como próprias como: “aquelas em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).

Spencer Toth (2013, pag.87) pré leciona tais condutas próprias como: Por sua vez, delitos informáticos próprios são as condutas típicas antijurídicas e culpáveis que visam atingir um sistema informático ou seus dados, precisamente violando sua confidencialidade, sua integridade ou sua aplicabilidade.

Seguindo entendimento semelhante, Maria José Crepaldi Ganancio LIBERATI. Crimes informáticos puros ou próprios: aqueles praticados por meio de um computador onde o resultado da conduta se opera em meio eletrônico, sendo a informática o bem jurídico protegido.

Os delitos informáticos próprios são também praticas típicas, antijurídicas e culpáveis. Esses delitos têm como intuito ataques a um sistema informático ou suas informações quebrando todas e quaisquer barreiras de proteção de um sistema para se chegar as informações contidas em determinado sistema informático. Para o cometimento desse delito informático próprio se faz necessário a utilização da informática, sem que a não utilização da mesma não se conseguiria chegar a praticar tal conduta.



“Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado”. (CARNEIRO, p. 185).

Há ainda aqueles casos em que o sistema informático em si, bem como os dados nele armazenados, processados ou transmitidos constituem o objeto material da conduta. Várias são as condutas que podem ser praticadas diretamente contra sistemas informáticos ou contra os dados armazenados, processados ou transmitidos por sistemas informáticos, como por exemplo, o acesso não autorizado a sistema informático e aos dados nele armazenados, a sua reprodução, divulgação ou transmissão a terceiros, o seu apagamento, alteração ou eliminação definitiva, a sua coleta ou interceptação não autorizadas, a interferência no correto funcionamento de um sistema informático etc. Nestes casos, verifique-se que as condutas só tornaram-se possíveis graças ao advento da tecnologia informática. Não se tratam de condutas tradicionais, mas representam ainda verdadeiras novidades para o Direito Penal e para o ordenamento jurídico de grande parte dos Estados contemporâneos. Pode-se dizer, então, que representam um fenômeno completamente diferente das demais condutas delituosas tradicionalmente sancionadas. (VLADIMIR, 2007, p.21)

## 4. LEI CAROLINA DIECKMANN (LEI Nº 12.737)

Spencer. 2013, p. 279) Este normativo aproveitou-se da circunstância histórica de ter havido vazamento de fotos de uma atriz, a partir de uma manutenção técnica de seu computador, em que foram encontradas fotos íntimas dela. Por meio da obtenção ilegítima de tal mídia, houve um delito de extorsão, ocorrido graças ao acesso indevido de delinquentes aos dados pessoais da vítima.

A referida lei foi aprovada graças a influência da mídia sobre o legislador após a obtenção não permitida de fotos íntimas da atriz Carolina Dieckmann, e o cometimento do delito de extorsão por parte do técnico em informática, tal fato acabou tomando grande repercussão e clamor da sociedade para que tal delito fosse contemplado por lei.

### 4.1. CONCEITO

Um grande passo para a nossa legislação foi a criação da referida Lei Carolina Dieckmann (lei nº12.737/1012), passando a punir os crimes tanto os crimes realizados por meio da internet como aqueles que se utilizem de algum dispositivo eletrônico para poderem ser concretizados, deixando claro que para a efetivação da conduta criminosa o deli quente terá de efetivamente invadir dispositivo que estiver protegido ao contraio não será tido como crime e também aquele que apenas invadir um sistema para demonstrar suas falhas com o intuito de aprimoramento do mesmo não estará cometido crime. (JOSÉ MILAGRE, 2011, p. 05).

Sancionada no fim do ano passado, nesta semana entrou em vigor a lei 12.737/12, a primeira a acrescentar ao Código Penal dispositivos que tipificam determinados delitos informáticos (ou, mais precisamente, cibercrimes). No entanto, o legislador não se preocupou apenas com a invasão a computadores para fins de obtenção de informações pessoais. A norma também equiparou a clonagem de cartões à falsificação de documento particular, além de tratar dos casos de interrupção de serviços de comunicação. (MONTEIRO, 2013)

Um grande avanço no Direito brasileiro, a criação da referida lei, uma vez que não existia norma que se tipifica esses delitos informáticos. Contudo a lei em comento apresenta falhas em partes do seu texto a tornando de oprimindo sua a aplicabilidade e eficácia.

## 4.2. APLICABILIDADE

A lei Carolina Dieckmann, foi um grande avanço na legislação brasileira no tocante aos cibercrimes, contudo a mesma enfrenta dificuldades no tocante a sua aplicabilidade na pratica pois a mesma trouxe brechas no tocante a sua aplicabilidade como também sua pena é branda, é ainda no Brasil a consecução desses crimes ainda é tarefa muito complicada de difícil solução. (Vieira, 2013, p. 03).

Também é importante que apresentemos liminarmente nossa preocupação acerca de um novo movimento legislativo precipitado, simbólico, e pressionado por fatores midiáticos, capazes de fazer aprovar leis mal-acabadas e que não correspondem àquilo verdadeiramente necessitado pelo direito penal brasileiro. (SYDOW, p.269).

Hoje em dia com o vertiginoso poder de influência da mídia, o poder legislativo sofre grande pressão por parte da mídia como na criação e aprovação de leis mal acabadas. Como a referida Lei Nº 12.737/1012 acabam tendo mero valor emblemático não conseguindo atingir sua verdadeira finalidade e deixando o Código Penal ineficiente com relação a necessidade que a legislação em questão necessita.

Em nossa ótica, deve o princípio da intervenção penal mínima ser respeitado em elevado grau. A criação de novas legislações penais com aplicabilidade duvidosa termina por colocar o poder policial e judiciário em situação de ineficiência pragmática e o próprio Estado em posição de fragilidade, posto que não consiga aplicar a lei que criou e que permanece no ordenamento jurídico reafirmando tal fraqueza. (SPENCER, 2013, p. 269).

Deveras deve-se o poder legislativo tomar muito cuidado com a criação de tais normas, pois normas em que a aplicabilidade é falha acabam por deixar todo o sistema de investigação policial e também o da aplicabilidade do poder judiciário em situação delicada em relação a aplicabilidade de determinada norma, em um caso prático e acaba por colocar o Estado também em situação de fragilidade pois a lei criada não tem aplicabilidade e ainda assim continua no ordenamento jurídico causando um sentimento de impunidade e insegurança para a sociedade e deve sempre ser observado o princípio da intervenção penal mínima visto que o direito penal só deve entrar em ação quando os outros ramos do ordenamento jurídico não conseguirem salvaguardar os bens considerados de maior importância.

Na questão da informática, há ainda especial preocupação. Não é de hoje que se vêem reivindicações das polícias civil, militar e federal por equipamentos melhores e mais modernos. Armas, munição, coletes à prova de balas e carros equipados são antigas demandas. O mesmo se diga acerca do exército e dos frequentes debates de seu sucateamento. (SPENCER, 2013, p. 270).

Delitos informáticos demandam pessoal altamente especializado e equipamentos de última geração. Mais do que isso: necessária conexão de alta qualidade e apoio de países de todo o mundo para que as investigações não esbarrem em formalidades e entraves burocráticos.

Hoje a informática é uma relevante preocupação no país e o nosso sistema policial brasileiro está sucateado em relação aos equipamentos, salários e profissionais. Os crimes informáticos necessitam de profissionais altamente qualificados equipamentos avançados, e uma conexão de internet com alta velocidade e bem remunerada para que tais crimes possam ser elucidados e punidos, se faz necessários investimentos nessas áreas como também auxílio de todos os países do mundo para que toda fase de investigação dos crimes possa ser feita de forma rápida e com ajuda dos mesmos para a elucidação do delito informático isso se faz necessário para que o processo de investigação percorra todo caminho sem que esbarre nas burocracias dos países, pois o agente dos delitos informáticos pode estar em qualquer país. Por conta de tais questões o legislador tem de se atentar a tais nuances pois de nada adianta criar tal lei sem que haja a devida aplicabilidade e eficácia.

Spencer, (2013, p. 270) O delito informático não é brasileiro, nem o direito informático. Ele ocorre na virtualidade transoiberânica e a precisão do local em que as condutas ocorrem são difíceis e etárias.

Os crimes informáticos não são criação do Brasil, tão pouco o Direito Informático. Esses delitos são cometidos em um mundo virtual onde não existe soberania de um determinado país não existe local determinado da conduta criminosa o que torna difícil a localização do autor do delito. Os conceitos que aqui governam são a velocidade, virtualidade e a imaterialidade.

Spencer Sydow, 2013, p. 270) é delito de difícil contenção, de difícil previsão e de difícil visualização, em que normalmente o delinquente conhece todos os vestígios que deixa e sabe tratá-lo melhor do que os investigadores.

Pois via de regra quem pratica esses delitos são pessoas com grandes conhecimentos na área da informática e sabem quais medidas tomarem para apagar os rastros deixados ao praticarem os delitos o que torna a investigação de difícil elucidação.

A LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Art. 2º O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B: “Invasão de dispositivo informático. “Ação penal. Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.” Art. 3º Os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação: “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

A referida lei 12.737 de 30 de novembro de 2012 apelidada de lei Carolina Dieckmann, tem de ser repensada pelo legislativo pois a mesma na infeliz tentativa de salvaguardar os bens jurídicos uma vez que antes da criação da referida lei não tinha nada previsto na legislação brasileira no tocante aos delitos cometidos por meio da internet, o que existia era analogia aos crimes com algumas condutas já tipificadas pelo CP, mas essa analogia tinha penas brandas como a de detenção de até dois anos cumulada ou não com a multa.

De acordo com Marcos Paladini. (2014) Notório observar a garantia constitucional da anterioridade, pois a carta magna de 1988 em seu artigo 5º, inciso XXXIX prevê que não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Assim, o princípio da anterioridade bem como o princípio da legalidade traduz a garantia constitucional de que as condutas cuja previsão em abstrato não estejam amparadas pela lei não sejam puníveis. Logo, no Brasil, alguém só pode ser punido se anteriormente ao fato praticado exista lei que o defina como crime, ainda que este ato seja imoral, anti-social ou danoso não há possibilidade de se punir o autor.

Com base na referido artigo 5º, inciso XXXIX, não é caracterizado como crime aquela conduta que não tiver lei anterior que o defina, pois bem de acordo com o

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o 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.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

De acordo com § 1º do Art. 154-A, aqueles profissionais que fazem testes de segurança que invadem sistemas informáticos para testar a segurança e a melhorarem a mesma podem ser penalizados por tais condutas pois se alguma dos programas feitos por eles podem ser obtidos por um Script Kiddie ou Cracker, pois é a partir da pesquisa das vulnerabilidades que esses profissionais de conseguem compreender as falhas de segurança e sanar tais defeitos. MP

Outra falha está no em parte do texto do Art. 154-A, quando ele dispõe da seguinte forma: Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o 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. Só será enquadrado em tal lei aquele que Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança. Portanto o computador que não tiver algum tipo de Software de segurança instalado no computador como antivírus ou protegido por senha e seu computador for invadido, o agente que praticar tal ato o mesmo não estará cometendo nenhum delito.

O Art. 154-A, ainda apresenta mais uma falha em seu texto quando afirma que, quem mediante violação indevida de mecanismo de segurança e com o 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. Portanto quem somente entrar em um sistema que não tenha proteção para olhar o conteúdo existente ali não se enquadra agente praticante de delito. No mesmo Art. 154-A, em seu texto apresenta outra falha quando ele afirma que se faz necessário que quem for invadir para ser enquadrado na lei terá que, burlar o sistema de segurança e obtenha, adulterar ou destruir dados ou informações sem autoriza.

Desta forma não se enquadra como criminoso nesta lei quem entrar no sistema e não cometer nenhuma das condutas citadas.

A exposição da lei 12.737/2012 se faz necessária para que podemos compreender melhor o panorama do Direito Informático que estamos vivenciando hoje e Desta forma podemos compreender melhor o que cada falha por menor que seja em uma lei pode repercutir em um caso concreto. De acordo com explanado podemos também verificar que a falta de aplicabilidade da lei em questão causa uma sensação de impunidade e insegurança jurídica perante toda sociedade.

## 5. CONSIDERAÇÕES FINAIS

Hoje a sociedade da informação é uma nova etapa na evolução da humanidade que não tem mais volta e cabem ao Direito acompanhar essas mudanças e salvaguardar os Direitos da sociedade, nesse novo ramo que surgiu a partir criação da Informática, esta que cresce de forma vertiginosa e trazem consigo tantos benefícios para a sociedade como um todo.

Infelizmente é fato que com o advento dessas tecnologias vieram acompanhadas um a nova forma de cometimento de crime, que na maioria das vezes a vítima não sabe, mas está sendo atacada por esses delinquentes que atacam no silêncio de uma aparente segurança que o mundo virtual os proporciona o que por sua vez deixa ainda mais perigoso esse ambiente e as pessoas se exponham mais.

Hoje a comodidade e facilidade que a internet proporciona a todos de uma maneira geral é um dos atrativos para essa marginalidade, hoje todos tem acesso a dados bancários em instantes, compras com cartões de créditos sem sair de casa, e o delinquente sabe que pode tirar vantagem com o acesso a esses dados.

Infelizmente o sistema de investigação hoje do Brasil está necessitando de contingente altamente treinado e equipamentos que forneçam melhor qualidade e eficiência nas investigações que não são tarefa fácil pois o agente que pratica o delito pode estar em qualquer lugar do mundo não existe mais nesse tipo de crime um local para restringir como ponto de partida de uma investigação. Portanto para poder combater essa criminalidade que também via de regra é altamente qualificada no ramo da Informática se faz necessário não só uma polícia especializada nesses crimes mas também uma por parte do legislativo alteração na lei nº 12.737 de 2012, que por mais que tenha sido uma grande avanço na legislação que não avia até então antes da referida lei nenhuma norma que abarca-se esses delitos, contudo a mesma apresenta algumas lacunas no corpo do seu texto.

Portanto chega-se à conclusão de que a referida lei deveria ser colocada de forma mais objetiva pelo legislador pois o Direito penal é bem fechado deveria ser mais objetivo e especificar com clareza e fazer além disso uma dosimetria melhor da pena. Com essas medidas a lei se tornaria mais eficaz pois não daria margem a uma dupla interpretação ao passo que uma pena maior traria a sensação de



segurança pois o indivíduo hoje que pratica tais crimes sabe que difícil mente ira preso pois esses delinquentes em sua grande maioria são pessoas instruídas que sabem as atitudes as quais devem ser tomadas para apagar qualquer vestígio que possa incriminá-los, as penas não passam de sensação de que a lei está ali.

## REFERÊNCIAS

Bruna Rasmussen. **O que é o protocolo TCP/IP?** Disponível em:<<http://canaltech.com.br/o-que-e-o-que-e/O-que-e-o-protocolo-TCP/IP/>>. Acessado em: 25 de Abril. 2014.

CHACON, Marcia JosieneMonteir; LIMA, Magna Regina de Souza.**COMUNICAÇÃO, TELECOMUNICAÇÃO E PROVEDORES DE ACESSO A INTERNET: UMA TRILOGIA INOVADORA E SEUS ASPECTOS TRIBUTÁRIOS.** Disponível em:<[http://www.esuda.com.br/coord/cont/artigos/Artigo%20Tributacao%20na%20Internet\\_Enecon\\_Revisado.pdf](http://www.esuda.com.br/coord/cont/artigos/Artigo%20Tributacao%20na%20Internet_Enecon_Revisado.pdf)>. Acessado em: 09 de Maio. 2014.

Calebe dos Santos Pimentel, **CRIMES VIRTUAIS: A NECESSIDADE DE UMA LEI ESPECÍFICA.** Disponível em:<<http://twingo.ucb.br/jspui/bitstream/10869/2297/1/Calebe%20dos%20Santos%20Pimentel.pdf>>. Acessado em: 10 de Maio. 2010.

CARNEIRO, Adenele Garcia. **Crimes Virtuais: elementos para uma reflexão sobre o problema da tipificação.** Disponível em:<[http://ambitojuridico.com.br/site/?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=11529](http://ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529)>. Acessado em: 02 de Novembro. 2013.

Elaine Martins.**O que é TCP/IP?**Disponível em:<<http://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-.htm>>. Acessado em: 08 de Maio. 2014.

Jaziel Lourenço da Silva Filho. O Código e as Leis do Ciberespaço. Disponível em:<<http://idireitofbv.wikidot.com/lei>>. Acessado em: 08 de Maio.

Júlio Moraes. **Conceito de Internet e intranet e principais navegadores.** Disponível em:<<http://www.juliomoraes.com/pt/2008/08/conceito-de-internet-e-intranet-e-principais-navegadores/>>. Acessado em 01 de Maio. 2014.

João Carlos Caribé. Brasil.**Projeto de lei de crimes cibernéticos restringe direitos fundamentais e liberdade na internet.** Disponível em:<<http://meganao.wordpress.com/2011/11/08/brasil-projeto-de-lei-de-crimes-ciberneticos-restringe-direitos-fundamentais-e-liberdade-na-internet/>>. Acessado em: 01 de Maio. 2014.

Jose Carlos de Araújo Filho, **Direito Eletrônico ou Direito da Informática?**Disponível em:<[http://www.ip.pbh.gov.br/ANO7\\_N2\\_PDF/IP7N2\\_almeida.pdf](http://www.ip.pbh.gov.br/ANO7_N2_PDF/IP7N2_almeida.pdf)>. Acessado em: 10 de Maio. 2005.

Jaqueline Lima da Silva, **Privacidade na Internet: Uma abordagem sobre o Facebook:** 2013

Lóren Pinto Ferreira. OS “CRIMES DE INFORMÁTICA” NO DIREITO PENAL BRASILEIRO. Disponível em:<[http://www.oab.org.br/editora/revista/revista\\_08/anexos](http://www.oab.org.br/editora/revista/revista_08/anexos)>

/crimes\_de\_informatica.pdf>. Acessado em: 08 de Maio.

LEI CAROLINA DIECKMANN. Lei nº 12.737, de novembro de 2012.<[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm)>. Acessado em 10 de Maio. 2014.

Marcelo Cardoso Pereira. **Direito Informático.** Disponível em:<<http://www.buscalegis.ufsc.br/revistas/files/anexos/5537-5529-1-PB.htm>>. Acessado em: 01 de Maio. 2014.

**Marcelo Rodrigues da Silva.** Comentários à eminente lei de cibercrimes. (PARTE 1). Disponível em:<<http://atualidadesdodireito.com.br/marcelorodrigues/2012/11/08/comentarios-a-iminente-lei-de-cibercrimes/>>. Acessado em: 01 de Maio. 2014.

MARÍLIA MONTEIRO. **Sobre a nova lei de cibercrimes.** Disponível em:<<http://observatoriodainternet.br/sobre-a-nova-lei-de-cibercrimes>>. Acessado em: 09 de Maio. 2014.

**MARÍLIA MONTEIRO.** Sobre a nova lei decibercrimes. Disponível em:<<http://observatoriodainternet.br/sobre-a-nova-lei-decibercrimes>>. Acessado em: 01 de Maio. 2014.

Marcelo Cardoso Pereira. Breves considerações sobre Direito Informático e Informática Jurídica. Disponível em:<<http://jus.com.br/artigos/2255/breves-consideracoes-sobre-direito-informatico-e-informatica-juridica>>. Acessado em: 08 de Maio.

MARCOS. Paladini. **A "Lei Carolina Dieckmann" frente ao princípio da legalidade.** Disponível em:<<http://marcospaladini.jusbrasil.com.br/artigos/111965254/a-leicarolina-dieckmann-frente-ao-principio-da-legalidade>>. Acessado em: 03 de Março. 2014.

**MIRABETE, Julio Fabbrini; FABRINI Renato,** Manual de Direito Penal: **2009.**

MIRANDA Murilo. **Da Persecução Penal dos Crimes Virtuais.** Disponível em: <[http://www.jurisway.org.br/v2/dhall.asp?id\\_dh=9903](http://www.jurisway.org.br/v2/dhall.asp?id_dh=9903)>. Acesso em: 24 de Outubro. 2013.

OLIVEIRA, Luiz Gustavo Caratti de, SILVA Marília Gabriela. Autor. **Os crimes virtuais e a impunidade real.** Disponível em: <[http://www.ambitojuridico.com.br/site/index.php?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=9963](http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963)>. Acessado em: 03 de Novembro. 2013.

Paulo Floro. 22 Milhões de brasileiros foram vítimas de cibercrimes no último ano. Disponível em:<<http://blogs.ne10.uol.com.br/mundobit/2013/10/02/22-milhoes-de-brasileiros-foram-vitimas-de-cibercrimes-no-ultimo-ano/>>. A cessado em: 01 de Maio. 2014.

Paulo Nunes. **Ciências Informáticas e de Telecomunicações**. Disponível em:<<http://www.knoow.net/ciencinformtelec/informatica/internet.htm>>. Acessado em: 01 de Maio. 2014.

PINHEIRO. Patricia Peck; MORAES, Cristina Sleiman; **Tudo o Que Você Precisa Saber Sobre Direito Digit@l no Dia-a-Dia**.(pocket book): 2009.

**SYDOW**, Spencer Toth, **CRIMES INFORMÁTICOS E SUAS VÍTIMAS**: 2013.

VLADIMIR, Chaves Delgado;**Cooperação Internacional em Matéria Penal na Convenção sobre o Cibercrime: 2007**.

VIEIRA, Victor. **Lei Carolina Dieckmann enfrentará dificuldades na prática**. Disponível em:<<http://www.conjur.com.br/2013-abr-03/aplicacao-lei-carolina-dieckmann-enfrentara-dificuldades-tribunais>>. Acesso em: 05 de Novembro. 2013.