FACER FACULDADES - UNIDADE RUBIATABA
CURSO DE DIREITO

CYBERCRIMES NO ORDENAMENTO JURÍDICO BRASILEIRO

Orientadora: Profa. Esp. Leidiane de Morais e Silva
Orientando: Cássio de Faria Cunha

Rubiataba - GO

2014

FACER FACULDADES - UNIDADE RUBIATABA
CURSO DE DIREITO

GO Faculdade de Ciências e Letras de Rubiataba
BIBLIOTECA
FACER
Biblioteca@facer.edu.br

CÁSSIO DE FARIA CUNHA

CYBERCRIMES NO ORDENAMENTO JURÍDICO BRASILEIRO

Monografia apresentada à FACER Faculdades Unidade Rubiataba, como requisito para obtenção do grau de Bacharel em Direito sob a orientação da professora Especialista Leidiane de Morais e Silva.

5-0514715
Tombo nº: 20463
Classif:
Ex: 1
Origem d
Data 25-05-15

De acordo:

_____
Professor (a) Orientador (a).

Rubiataba – GO

2014

FOLHA DE APROVAÇÃO

CÁSSIO DE FARIA CUNHA

CYBERCRIMES NO ORDENAMENTO JURÍDICO BRASILEIRO

COMISSÃO JULGADORA
MONOGRAFIA PARA A OBTENÇÃO DO BACHARELADO DE DIREITO
PELA FACER FACULDADES UNIDADE RUBIATABA

RESULTADO_____

Orientador_____

Profa. Esp. Leidiane de Morais e Silva

1° Examinador_____

Prof. Dra. Geruza Silva de Oliveira

2° Examinador_____

Prof. Esp. Edilson da Silva

Rubiataba, 2014

Este trabalho acadêmico é dedicado:

A Deus, por ter me dado saúde e força para superar as dificuldades.

Aos meus pais, a minha irmã, ao meu sobrinho e aos meus avós maternos, pelo amor, incentivo e apoio incondicional.

A todos os meus amigos e aos irmãos que Deus me presenteou durante essa jornada: José Alan, Ana Paula, Cleuverton, Larissa e Débora.

Aos mestres, diretores e funcionários da FACER, em especial a professora Leidiane de Morais e Silva , que me mostrou os primeiros passos a seguir para a conclusão deste trabalho monográfico.

In memoriam:

Aos meus avós paternos, por serem exemplos de superação e fé.

"Confia os teus cuidados ao Senhor, e Ele te sustentará: jamais permitirá que o justo seja abalado."

Salmo 55:22

"Você nunca sabe que resultados virão da sua ação. Mas se você não você não fizer nada, não existirão resultados".

Mahatma Gandhi.

SUMÁRIO

1 INTRODUÇÃO 12
2 O MUNDO VIRTUAL E O DIREITO PENAL 15
2.1 A INTERNET E SUA ORIGEM 15
2.2 RELAÇÃO ENTRE O DIREITO E A INTERNET 17
2.2.1 CONCEITO E FUNÇÕES DA PENA 20
2.2.1.1 FUNÇÕES REPRESSIVAS 21
2.2.1.2 FUNÇÕES PREVENTIVAS 22
2.2.2 TEORIA PREVENTIVA ESPECIAL 23
2.2.3 TEORIA MISTA OU UNIFICADORA 24
3. PRINCÍPIOS NORTEADORES DO DIREITO PENAL BRASILEIRO 27
3.1. PRINCÍPIO DA RETROATIVIDADE DA LEI 27
3.2 PRINCÍPIO DA FRAGMENTARIEDADE 28
3.3 PRINCÍPIO DA INTERVENÇÃO MÍNIMA 29
3.4 PRINCÍPIO DA OFENSIVIDADE 30
3.5 PRINCÍPIO DA INSIGNIFICÂNCIA 31
3.6 PRINCÍPIO DA CULPABILIDADE 31
3.7 PRINCÍPIO DA HUMANIDADE 32
3.8 PRINCÍPIO DA PROPORCIONALIDADE DA PENA 33
3.9 PRINCÍPIO DA PRESUNÇÃO DE INOCÊNCIA 34
3.10 PRINCÍPIO DO "NE BIS IN IDEM" 35
3.11 PRINCÍPIO DA LEGALIDADE OU DA RESERVA LEGAL 35
4. CRIMES CIBERNÉTICOS E PUNIBILIDADE: CONCEITO E NOÇÕES GERAIS 37
4.1 TRATAMENTO NA LEGISLAÇÃO ESTRANGEIRA 45
4.2 CRIMES PRÓPRIOS E IMPRÓPRIOS CIBERNÉTICOS TIPIFICADOS NO BRASIL 46
4.3 PROJETOS DE LEI EM TRAMITAÇÃO NO BRASIL 49
4.4 A (IM)PUNIBILIDADE DOS CRIMES CIBERNÉTICOS NO BRASIL 51
5. OS CRIMES VIRTUAIS E A ANÁLISE DA PROVA 54
5.1 CRIMES VIRTUAIS EM ESPÉCIE 54

5.2 A NECESSIDADE DE PROFISSIONAIS ATUALIZADOS, DE EQUIPAMENTOS ADEQUADOS E A POSSIBILIDADE DE IDENTIFICAÇÃO DO AGENTE CRIMINOSO....56
5.3 MANEIRAS DE IDENTIFICAR MÁQUINAS CRIMINOSAS E A RESPONSABILIDADE DO PROVEDOR....57
5.4 MEIOS DE PROVA/TÉCNICAS NOS CRIMES VIRTUAIS....60
CONCLUSÃO....65
REFERÊNCIAS....67

LISTA DE ABREVIATURAS/SÍMBOLOS

§- Parágrafo
Art. - Artigo
nº.- Número
p.- Página
pp.- Páginas

RESUMO

O presente trabalho pretende ilustrar as peculiaridades dos crimes praticados através da Informática e as dificuldades existentes na persecução criminal. Através de um método histórico e indutivo, procurou-se demonstrar que o avanço tecnológico propiciou um campo vasto para a atuação dos agentes denominados "hackers", sujeitos que possuem profundo conhecimento de informática. De início, abordará a evolução histórica do computador e da Internet e as classificações doutrinárias referentes ao tema. O trabalho busca discutir as questões processuais que dificultam a responsabilização dos autores dos crimes virtuais, questões essas referentes à "autoria", "maioridade penal", "produção de prova" e "competência em razão do lugar". Trata, ainda, dos crimes informáticos próprios e impróprios que representam relativa importância no âmbito da Internet. Há discussão a respeito da falta de legislação específica e a consequente existência de inúmeras condutas atípicas. Sobre este aspecto, será demonstrada a existência de argumentos comumente utilizados pela defesa para o fim de isentar o acusado de responsabilidade. A título de comparação, foi abordada a legislação de outros países, concernente ao tema da informática e da Internet. Por fim, concluiu-se pela extrema necessidade em se obter novas leis específicas e equipamentos técnicos adequados para a investigação. Entretanto, embora o Brasil não possua legislação e estrutura técnica suficiente para a ideal responsabilização dos agentes, tudo indica que as Autoridades Policiais e Judiciárias estão com atuando com seriedade, fazendo o possível para superar as dificuldades existentes.

Palavras-chave: História da Internet. Internet. Crimes de informática. Crimes de Internet. Cybercrimes. Direito Penal da Informática.

ABSTRACT

This paper aims to illustrate the peculiarities of the crimes committed through the Information Technology and the difficulties in criminal prosecution. Through a historical and inductive method, aimed to show that technological advancement has provided a vast field for the activities of agents called "hackers", subjects who have deep knowledge of computers. At first, addressed the historical evolution of computers and the Internet and the doctrinal ratings on the topic. The study aimed to discuss procedural issues that hinder the responsibility of the authors of cybercrime, these issues related to "authorship", "criminal responsibility", "production of evidence" and "competence by reason of place." This was also the proper and improper cybercrime represent relative importance within the Internet. There was discussion about the lack of specific legislation and the consequent existence of numerous atypical behaviors. In this respect, it was shown that arguments commonly used by the defense to the order to exempt the defendant from liability. By comparison, addressed the legislation of other countries, concerning the subject of computers and the Internet. Finally, it was concluded by the extreme necessity to get new specific laws and technical equipment suitable for research. However, although Brazil has no legislation and sufficient technical structure for optimal accountability of agents, it appears that the Police Authorities and Judicial are working with seriously, making it possible to overcome the difficulties.

Keywords: History of the Internet. Internet. Computer crimes. Internet crimes. Cybercrimes. Criminal Informatics Law.

1. INTRODUÇÃO

A análise da prova nos crimes cometidos através dos meios virtuais é de suma importância nos dias atuais, tendo em vista a crescente ascensão do uso dos computadores nas atividades cotidianas, e, ainda, a Internet, que é amplamente utilizada para estreitar as distâncias entre os diversos sujeitos de direito, interferindo nos bens da vida tutelados pelo ordenamento jurídico, em especial aqueles que, uma vez violados, figuram a ocorrência de um tipo penal, conhecido como conduta típica.

Entre os numerosos clientes da rede que se utilizam dessa facilidade para aferir lucros, concretizando negócios, para lazer pessoal ou em grupos, estão aqueles que veem ali uma oportunidade de praticar ilícitos penais, haja vista a facilidade com que podem realizar suas atividades virtuais delitivas, tanto pela velocidade, como pela dificuldade em identificar o agente causador dos danos.

Embora muitos se utilizem desses meios de maneira adequada, aumenta o número de casos onde os agentes, aproveitando-se deste anonimato e a impunidade, cometem ilícitos contra as outras pessoas que também utilizam a rede.[1]

Muitas vezes, o que atrai os criminosos no setor digital, é o fato de estarem amparados pela falta de legislação adequada sobre o tema, mas a esmagadora maioria é atraída pela ausência de meios adequados de prova, que identifiquem os autores do delito, uma vez que o sistema ainda não se adequou a nova realidade digital, e por vezes não tem equipamentos, nem peritos capacitados, que os levem aos criminosos.

Não apenas através do uso da internet, mas também pelos diversos meios virtuais criados pela ascendência do uso das tecnologias atuais, que modernizam aparelhos e transformam a realidade com que os conflitos acontecem, em número e possibilidades. As lides passam a ter uma roupagem diferente daquelas imaginadas pelo legislador antigo, que não podia prever os "cybers" criminosos.

O uso do desenvolvimento acelerado da tecnologia não é mais apenas uma tendência para os próximos anos, mas já é uma realidade gritante, e que, por isso, necessita de cuidados especiais dos juristas pátrios. Os avanços são utilizados não apenas para o cometimento de crimes, como ora exposto, mas também para o desenvolvimento de outras áreas do convívio

---

[1] BEPPLER, Daniela. **Internet e informatização: implicações no universo jurídico.** Florianópolis: Fundação Boiteux, 2000.

social, como medicina, lecionar, enfim, para todos os meios nos quais os seres humanos se relacionam.

Essa tendência evolutiva se inicia muito antes do desenvolvimento ou surgimento da internet, mas desde antes do feudalismo a humanidade vem se transformando, passando por revoluções específicas em cada época histórica, de maneira que as linhas de produção se modernizaram bem como o relacionamento homem-máquina se popularizou.[2]

No presente trabalho, enfatiza-se o setor virtual, que mais evolui, de maneira a estreitar os laços entre os indivíduos sujeitos de direito. Cada vez mais, pessoas que antes jamais teriam chances de interagirem no universo jurídico, ficam mais próximas, e aumentam as demandas nos juízos por todo o país.

Uma vez verificada essa parcela dentre o total de demandas, faz-se necessário que os operadores do direito se atualizem e saibam, processualmente, além do direto material, como lidar com essa realidade, para que o interesse das vítimas possa ser protegido e, ainda, garantido.

Os sujeitos que atuam criminosamente, chamados crackers ou hackers, aproveitando-se de seus conhecimentos na área de informática, roubam informações, destroem arquivos, realizam condutas descritas em tipos penais específicos do Código Penal, além de causarem graves prejuízos para as vítimas.

Na presente pesquisa, para o estudo dos meios de prova nos crimes virtuais, será utilizado o método dedutivo, lógico com aplicação da técnica análoga, onde se discutirá as questões relacionadas à prova nos "Cybercrimes", e os avanços que deverão ocorrer para que de identifique os autores dos delitos. Em relação aos recursos a serem utilizados, serão utilizados como fontes os livros jurídicos, jurisprudência e legislação pertinente ao tema, bem como a utilização da internet.

Questões polêmicas como identificar o sujeito que comete o delito, tarefa bem mais complexa que identificar a máquina utilizada pelo agente ativo, nos faz refletir que para uma condenação certa e segura, necessário se faz um estudo que possibilite ao magistrado conhecer o real causador dos danos. As provas que serão realizadas na instrução criminal possibilitarem tornar os indícios de autoria em autoria concreta, bem como facilitar a comprovação da materialidade.

Definir maneiras eficazes de prova nos crimes virtuais e soluções para que possam ser obtidas pelos órgãos jurisdicionais, possibilita a aplicação das normas penais já existentes no

---

[2] BEPPLER, Daniela. **Internet e informatização: implicações no universo jurídico.** Florianópolis: Fundação Boiteux, 2000.

ordenamento, porque, ainda que se tenha provado a materialidade do delito, por não poder identificar com certeza o agente, os criminosos continuam impunes.

Desta forma, uma vez esclarecidas dúvidas acerca do procedimento, o Estado poderá exercer seu poder coator e punir os reais agentes criminosos virtuais, que não mais continuaram impunes pelos atos que cometerem a outrem.

Com a análise do tema, será possível discutir quais são essas provas, de que forma, no processo penal, poderão ser obtidas, as necessidades do sistema em se reciclar, e de se adequar à nova era. Assim, uma vez garantida a coercitividade estatal contra os ilícitos virtuais, espera-se que os crimes na rede diminuam.

2. O Mundo Virtual e o Direito Penal

2.1 A internet e sua origem

Segundo o ensinamento de Gabriel Cesar, "o termo internet é uma abreviação de Inter Networking, significando uma interligação de redes locais".[3] "Tem sua origem no sistema de telecomunicações desenvolvido pelo Departamento de Defesa dos Estados Unidos, no ano de 1969[4]", cuja finalidade era impedir a interrupção das comunicações militares e governamentais americanas no caso de um possível ataque nuclear por parte da União Soviética.

Foram desenvolvidas diversas pequenas redes locais, chamadas LAN, em vários pontos estratégicos do país, as quais se interligavam através de redes de telecomunicação, denominadas WAN.

Desta forma, esta rede de computadores que, mais tarde foi chamada de ARPAnet (Advanced Research Projects Agency Network: agência avançada de desenvolvimento de projetos para trabalhos em rede) foi criada com a finalidade exclusivamente militar. Como preceitua CESAR:[5]

> Sua demonstração pública ocorreu no ano de 1972, na Conferência Internacional de Comunicação entre Computadores, realizada em Washington, no mesmo ano em que foi inventado o correio eletrônico. Com o seu crescimento, a ARPAnet passou a ser utilizada para todos os tipos de comunicação, acadêmicos ou militares, o que permitiu sua divisão em ARPAnet (para uso acadêmico) e MIinet (para uso militar).

Em razão da dependência de todas as redes em relação à ARPAnet, esta se transformou em uma espécie de redes das redes, passando a ser conhecida como ARPA-Interne e, mais tarde, apenas por internet.

Dessa forma, pode-se definir a internet como uma "espécie de associação mundial de computadores," todos interligados por meio de um conjunto de regras padronizadas,

---

[3] Disponível em: http://pt.shvoong.com/books/239170-conceito-crime: acesso em: 13/04/2014

[4] Idem.

[5] INELLAS, Gabriel César Zaccaria. Crimes da Internet. 1ª Edição. Editora Juarez de Oliveira, 2004, p.01.

denominada de protocolo, que especifica o formato, a sincronização e a verificação de erros em comunicação de dados.[6]

Convém destacar, ainda que superficialmente, como funciona a internet. CÉSAR preceitua que:[7]

> O usuário se conecta a internet por meio de uma linha telefônica discada, chamada dial-up, ou através de conexões de alta velocidade: ADSL (sistema de transmissão de dados através de linhas telefônicas tradicionais), fibra óptica, TV a cabo, satélite. Na primeira, a linha telefônica deve estar ligada a um modem, que por sua vez está conectado ao computador e a um provedor de acesso para onde o usuário vai ligar e solicitar o seu acesso a internet.

De posse de uma assinatura (seja ela paga ou não) com o provedor, haverá disponibilização de um único endereço para usuário. Através dos computadores do provedor, o usuário também terá um espaço para armazenar/guardar as suas informações e mensagens eletrônicas.

A internet não este em um lugar específico ou determinado, muito menos possui um servidor central. Mas podemos dizer que é como uma teia de aranha que tem diversas direções a ir. Nessa linha de pensamento, afirmou Érica Lourenço de Lima Ferreira: "é uma autêntica teia de aranha que permite múltiplas direções (navegações/websurfing) de um lado a outro do planeta".[8]

Esta interconexão de redes se dá através de dois componentes: o software (programa necessário para o funcionamento da máquina) e o hardware (componente físico, como o gabinete, o teclado, o mouse, o monitor). Segundo CESAR[9]

> Um dos elementos mais importantes para que haja essa comunicação entre um computador e outro é o já mencionado protocolo, denominado Transmission Control Protocol/Internet Protocol (TCP/IP), que nada mais é do que a língua comum entre os computadores que integram a internet. O protocolo TCP é o responsável por manipular uma quantidade grande de dados e garantir que as informações transmitidas entre dois computadores da rede não contenham erros.

---

[6] Ministério Público Federal e Comitê Gestor da Internet no Brasil. Crimes Cibernéticos-Manual Prático de Investigação. 2006, p.03

[7] INELLAS, Gabriel César Zaccaria. Crimes da Internet. 1ª Edição. Editora Juarez de Oliveira, 2004, p.03.

[8] FERREIRA, Érica Lourenço de Lima. INTERNET-Macrocriminal idade e Jurisdição Internacional . Curitiba. Juruá Editora, 2007, p.82.

[9] FAGUNDES, Eduardo Mayer. Como funciona a internet? Disponível em <http: //www.efagundes.com/artigos/Como%20funciona%20a%20INTERNET.htm>. Acesso em 14/05/2014.

Destaca-se ainda que na internet existem duas categorias básicas de computadores, segundo a sua função: clientes e servidores. O cliente é o computador que acessa os serviços disponíveis pelo servidor. O servidor é o computador que utiliza programas para providenciar acesso à rede.

A doutrina especifica os serviços da Net em seis categorias, cujo conhecimento é necessário para pensar em tipificar condutas jurídicas. São elas: serviços de transferência de arquivos, correio eletrônico (e-mail); listas automatizadas e distribuição de notícias (News/site); serviços de informação interativa (www); serviços de diretórios que possibilitam encontrar os endereços eletrônicos (homepage), serviços interativos multiusuários que permitem a interação entre grupos (chat); serviços de indexação que facilitam a busca de informações (como o google, por exemplo).

2.2 Relação entre Direito e Internet

A informática, em sentido amplo, contendo a internet seu principal instrumento, fez surgir novos campos de estudos na área jurídica. Como já mencionado, a internet surgiu e evoluiu no meio social de modo muito rápido, exigindo do direito soluções as quais não estavam preparados para lidar.

O direito se viu limitado na sua mais precípua função: regular condutas e solucionar conflitos. Através dos ensinamentos de CÉSAR entende-se[10]

> Em 1980, o Conselho da Comunidade Europeia reconheceu oficialmente o Direito da Informática, como sendo uma reunião de todos os aspectos jurídicos da informática. Na verdade, tanto serve ao conhecimento de outras áreas como também acaba por influenciá-las.

Para alguns doutrinadores, o Direito da Informática é um novo ramo do direito, conceituado como um conjunto de normas e princípios aplicáveis aos fatos decorrentes da informática."Nascido justamente dessa necessidade social em face dos fatos informáticos. No entanto, não há unanimidade no reconhecimento da autonomia deste ramo".[11]

---

[10] Idem.
[11] Idem.

Diante das interferências da internet na vida social, modificando comportamentos e criando ao mesmo tempo novas situações, a sensação é que a necessidade social parece estar desprovida de tutela jurídica.

Não se pode esquecer que a influência da informática e mais especificamente da internet não se resume apenas em uma inovação técnica, mas é um fator que acelera outros fatores, modificando o comportamento de uma sociedade inteira. Segundo CÉSAR está claro e evidente:[12]

> [...] a sua influência na área jurídica, provocando questionamentos sobre a proteção de direitos fundamentais, como liberdade de informação, liberdade de atividade intelectual ou privacidade, no âmbito do direito constitucional. O aumento das transações comerciais e prestações de serviço, também proporcionadas pela internet, modificam uma realidade já consolidada no âmbito do direito comercial, tributário e consumidor, por exemplo.

Não se pode olvidar a mais preocupante influência deste sistema dentro do direito: a prática de condutas ilícitas. O direito penal não pode estar alheio a estas transformações:[13]

> Além de estar atento às adaptações do seu sistema jurídico tradicional, deve também se abrir ao estudo desta nova criminalidade, mostrando-se apto a oferecer respostas à sociedade no seu combate, antes mesmo da persecução penal, tipificando novas condutas, que até o presente momento, apesar das violações a bens juridicamente relevantes, ainda não estão descritas em lei.

Em suma, o crescimento sem limites da informática está, cada vez mais, obrigando o direito a uma adaptação forçada no âmbito legislativo, sobretudo, para que este cumpra sua precípua função: regular as relações humanas, ainda que viabilizadas através de máquinas, com o fito de garantir a paz social.

Com base na doutrina, fica claro entender que o Fato Social é a base para entendermos o que é Direito. O Direito tem como sua as necessidades fundamentais das Sociedades Humanas, que são ajustados por ele como condição essencial a sua própria sobrevivência.

Assim pode-se afirmar que é no Direito que se encontra a segurança de tudo que está ligado a vida humana pelas normas e fundamentos que vem a compor a ordem jurídica. "O

---

[12] Idem.
[13] Idem.

fato social que se mostra contrário a norma de Direito forja o ilícito jurídico, cuja forma mais séria é o ilícito penal, que atenta contra os bens mais importantes da vida social."[14]

Assim sendo, o Estado estabelece sanções para punir a prática desses fatos, vindo ainda na tentativa de tornar invioláveis os bens que protege. Juntamente com essa sanção o Estado também fixa outras medidas com o intuito de reprimir ou prevenir o acontecimento de fatos lesivos dos bens jurídicos do cidadão. "A mais severa das sanções é a pena, estabelecida para o caso de inobservância de um imperativo. Dentre as medidas de repressão ou prevenção encontramos as medidas de segurança."[15]

O Estado estabelece normas jurídicas com o intuito de vir a combater o Crime. Dando-se a esse conjunto de normas jurídicas o nome de Direito Penal.

A forma do Direito Penal para exercer sua função é aplicando a Pena, para assim satisfazer uma exigência da Justiça, punindo o autor da conduta típica penalmente e submetendo-o a um mal que está ligado a gravidade ao dano por ele causado. Assim podemos conceituar o Direito Penal como[16]

> [...] o ramo do Direito público que se encarrega de selecionar condutas atentatórias aos mais importantes bens jurídicos – juntamente aqueles considerados essenciais para a vida em sociedade , sancionando-se com uma pena criminal ou medida de segurança. Tem por função primordial servir como modelo orientador de condutas adequadas , promovendo o normal funcionamento da vida em sociedade.

O Direito Penal visa expressar e estabelecer normas que serão expostas a sociedade que terão o dever de cumprir os ordenamentos de acordo com a lei e no caso do não cumprimento da mesma ocorrerá punições devidas para cada ato em si praticado.

Comenta-se que o Direito é uma ciência que se enquadra no âmbito normativo e cultural. Como nos ensina MIRABETE:[17]

> [...] é uma ciência cultural porque indaga o dever ser; traduzindo-se em regras de conduta que devem ser observadas por todos no respeito aos mais relevantes interesses sociais. Diferencia-se assim das ciências naturais, em que o objeto de estudo é o ser, o objeto em si mesmo."4 "[...] é também uma ciência normativa, pois seu objeto é o estudo da lei, da norma, do Direito Positivo, como dado fundamental

[14] JESUS, Damásio E.de. Direito Penal.Volume 1: Parte Geral . 30.ed. São Paulo: Saraiva 2009. p.03.
[15] Idem.
[16] ESTEFAM. André. Direito Penal ,1: Parte Geral . 4.ed. rev, e atual . São Paulo: Saraiva 2008. p.01.
[17] MIRABETE, Julio Fabrine. Manual de Direito Penal , vol . 1parte geral , 24ed, ver . E atual. Até 31 de dezembro de 2009. reimpr . São Paulo. Atlas, 2007.p.04.

> e indiscutível em sua observância obrigatória. Não se preocupa, por tanto com a verificação da gênese do crime, dos fatos que levam a criminalidade ou dos aspectos sociais que podem determinar a prática do ilícito, preocupação próprias das ciências causais explicativas, como a criminologia, a sociologia criminal etc.

Pode-se afirmar que o Direito Penal é considerado como valorativo, finalista e sancionador. Assim, pode-se afirmar que a Norma Penal é valorativa porque vem a tutelar os valores mais elevados da sociedade, sendo expostos em uma escala hierárquica e valorando assim os fatos diante a gravidade dos mesmos, ou seja, quanto mais grave o crime mais severa será sua punição para o autor. MIRABETE afirma que:[18]

> [...] tem ainda a lei Penal caráter finalista, por quanto visa a proteção de bens e interesses jurídicos merecedores da tutela mais eficiente que só podem ser eficazmente protegidos pela ameaça legal de aplicação de sanções de poder intimidativo maior, como a pena. Essa prevenção é a maior finalidade de lei Penal.

Para melhor entendimento, o Direito Penal como sendo uma ciência jurídica possui um caráter dogmático, já que tem como base o Direito Positivo, exigindo, assim, o cumprimento de todas suas normas pela sua obrigatoriedade.

2.2.1 Conceito e funções da Pena

Entende-se que a pena é uma resposta dada pelo Estado ao autor de uma infração penal, seja o crime ou contravenção.[19]

> A pena é a resposta dada pelo Estado ao autor de uma infração penal (crime ou contravenção). Tem ela o objetivo de aplicar um castigo pelo descumprimento da lei penal e evitar a prática, pela mesma ou por outras pessoas, de novos delitos, além de buscar reeducar o delinquente para a vida em sociedade. São espécies de pena: penas privativas de liberdade, penas restritivas de direitos e multa.

---

[18] Idem.

[19] Disponível em: http://www.resultadoconcursos.net/direito-penal-1-conceitos-emresumo-para-estudar/: Acesso em 14/05/2014.

A pena é uma resposta estatal que é aplicada ao autor de um ato considerado como injusto penal, consistente na privação ou restrição de Diretos. No que se refere a crimes praticados pelo mundo virtual, essa resposta estatal não acontece.

Em se tratando das teorias mais conhecidas, temos a teoria relativa, também meramente conhecida como prevencionista, e ainda, a teoria absolutista.[20]

> "[...] em oposição as absolutistas, as teorias relativas, também conhecidas como prevencionistas, são marcadamente teorias finalistas, por verem a pena não como um fim em si mesmo, mais como um meio a serviço de um fim em si mesmo, mais como um meio a serviço de um fim."

Salienta-se que antes de efetivar a punição de um autor do delito, procura-se estabelecer normas de conteúdo proibitivo e cominação de sanções para se evitar a prática do ilícito. Não logrando êxito essa função preventiva, a sanção que outrora foi cominada abstratamente, agora será concreta, tornando a prevenção genérica em prevenção específica.

2.2.1.1 Funções Repressivas

De acordo com os estudos feitos por Paulo Queiroz, as teorias preventivas da pena são aquelas teorias que atribuem à pena a capacidade e a missão de evitar que no futuro se cometam delitos. "Podem subdividir-se em teoria preventiva especial e teoria preventiva geral".[21]

Vale salientar, que segundo sua essência, a pena se traduz num mal para quem a sofre. Mas, como instrumento político-criminal destinado a atuar no mundo, não pode a pena bastar-se com essa característica, em si mesma destituída de sentido social-positivo. Para se justificar, a pena tem de usar desse mal para alcançar a finalidade precípua de toda a política criminal, precisamente, a prevenção ou a profilaxia criminal.

A Teoria Repressiva considera que a pena se esgota na ideia de pura retribuição, tem como fim a reação punitiva, ou seja, responde ao mal constitutivo do delito com outro mal que se impõe ao autor do delito.

---

[20] Idem.
[21] Idem.

Esta teoria somente pretende que o ato injusto cometido pelo sujeito culpável deste, seja retribuído através do mal que constitui a pena. Ensina HASSEMER e CONDE[22]

> [...] que existe uma variante subjetiva da Teoria Retributiva que considera que a pena deve ser também para o autor do delito uma forma de „expiación", ou seja, uma espécie de penitência que o condenado deve cumprir para purgar (expiar) seu ato injusto e sua culpabilidade pelo mesmo.

A Teoria Repressiva considera que a exigência de pena deriva da ideia de justiça. Enfim, a pena Repressiva esgota a sua função ao causar um mal ao delinquente como compensação ou expiação do mal por ele cometido, recebendo o devido castigo.[23]

> "Nesta medida é uma doutrina puramente social-negativa que acaba por se revelar estranha e inimiga de qualquer tentativa de socialização do delinquente e de restauração da paz jurídica da comunidade afetada pelo crime".

Em suma, a pena possui a função de atuar preventivamente, evitando que o indivíduo venha a cometer algum delito, demonstrando-se assim a pretensão de controle e domínio do fenômeno da criminalidade.

2.2.1.2 Funções Preventivas

A teoria preventiva geral está direcionada à generalidade dos cidadãos, esperando que a ameaça de uma pena, e sua imposição e execução, por um lado, sirva para intimidar aos delinquentes potenciais (concepção estrita o negativa da prevenção geral), e, por outro lado, sirva para robustecer a consciência jurídica dos cidadãos e sua confiança e fé no Direito (concepção ampla ou positiva da prevenção geral). QUEIROZ nos diz:[24]

> [...] releva notar que a ideia de justificar a pena positivamente, embora só recentemente tenha merecido maior destaque, parece remontar a DURKHEIM.. Com efeito, dizia Queiroz que a pena não serve, ou só serve de maneira muito

[22] HASSEMER, Winfried y MUÑOZ CONDE, Francisco. Introdución a la Criminologie, pág. 226.
[23] Disponível em: http://www.uj.com.br/publicacoes/doutrinas/2146: Acesso em 14/05/2014.
[24] Idem.

> secundária, para corrigir o culpado ou intimidar seus possíveis imitadores; desse duplo ponto de vista, sua eficácia é duvidoso e, em todo caso, medíocre.

Deste modo, por uma parte, a pena pode ser concebida como forma acolhida de intimidação das outras pessoas através do sofrimento que com ela se inflige ao delinquente e que, ao fim, as conduzirá a não cometerem fatos criminais (prevenção geral negativa ou de intimidação). Por outra parte, a pena pode ser:[25]

> "[...] concebida, como forma de que o Estado se serve para manter e reforçar a confiança da comunidade na validade e na força de vigência das suas normas de tutela de bens jurídicos e, assim, no ordenamento jurídico-penal; como instrumento por excelência destinado a revelar perante a comunidade a inquebrantabilidade da ordem jurídica, apesar de todas as violações que tenham tido lugar (prevenção geral positiva ou de integração)."

Vale salientar que o Estado carrega uma responsabilidade de conceder a Pena no intuito de assegurar a segurança e a confiança da sociedade em geral.

2.2.2 Teoria Preventiva Especial

A teoria preventiva especial está direcionada ao delinquente concreto castigado com uma pena. Tem por denominador comum a ideia de que a pena é um instrumento de atuação preventiva sobre a pessoa do delinquente, com o fim de evitar que, no futuro ele cometa novos crimes. Deste modo, deve-se falar de uma finalidade de prevenção da reincidência.

Essa teoria não busca retribuir o fato passado, senão justificar a pena com o fim de prevenir novos delitos do autor. Portanto, diferencia-se, basicamente, da prevenção geral, em virtude de que o fato não se dirige a coletividade. Ou seja, o fato se dirige a uma pessoa determinada que é o sujeito delinquente. Deste modo, a pretensão desta teoria é evitar que aquele que delinquiu volte a delinquir.

Nesta tendência, a prevenção especial pode subdividir-se em duas grandes possibilidades, cuja diferenciação está baseada nas distintas formas de atuar, segundo o tipo

[25] Disponível em: http://www.uj.com.br/publicacoes/doutrinas/2146: Acesso em 15/05/2014.

de delinquente. Deste modo, podem ser: prevenção positiva (ou ressocializadora) e prevenção negativa (ou inocuizadora).

> "A prevenção positiva persegue a ressocialização do delinquente, através, da sua correção. Ela advoga por uma pena dirigida ao tratamento do próprio delinquente, com o propósito de incidir em sua personalidade, com efeito de evitar sua reincidência". "A finalidade da pena-tratamento é a ressocialização. Por outro lado, a prevenção negativa, busca tanto a intimidação ou inocuização através da intimidação – do que ainda é intimidável –, como a inocuização mediante a privação da liberdade – dos que não são corrigíveis nem intimidáveis". "A prevenção especial negativa tem como fim neutralizar a possível nova ação delitiva, daquele que delinquiu em momento anterior, através de sua "inocuização" ou "intimidação"[26]

2.2.3 Teoria Mista ou Unificadora

As Teorias Mista ou Unificadora tentam agrupar em um conceito único os fins da pena. Essa corrente tenta recolher os aspectos mais destacados das teorias absolutas e relativas. Contudo, essa unidimensionalidade, em um ou outro sentido, mostra-se formalista e incapaz de abranger a complexidade dos fenômenos sociais que interessam ao Direito Penal, com consequências graves para a segurança e os direitos fundamentais do homem. Esse é um dos argumentos básicos que ressaltam a necessidade de adotar uma teoria que abranja a pluralidade funcional da pena.

De acordo com os estudos realizados por Paulo Queiroz, quanto à legislação penal brasileira, pode-se perceber que os legisladores expressam uma certa preferência pelo dogmatismo, mantendo-se filiados às teorias ecléticas ou mistas ou de união ou unitárias que unificam as ideias de retribuição ao mal do crime o mal da pena e prevenção, tanto geral (ameaça a todos para que não venham a delinquir), como especial (evitar que o criminoso volte a delinquir). Como nos ensina QUEIROZ,[27]

> [...] no entanto, o Código Penal, especialmente quando da cominação das penas, o que faz segundo critério não apenas de prevenção geral ou, ainda, quanto da aplicação da pena, busca ajustá-la à proporção e a gravidade do comportamento delituoso praticado, ao determinar por exemplo, no artigo 29, que o partícipe de crime responde na medida de sua culpabilidade.

---

[26] Idem.

[27] QUEIROZ, Paulo. Função da Pena: Legislação versus Deslegitimação do Sistema Penal. 3 ed. Ver. E atual. São Paulo. Editora Revista dos tribunais, 2008. P. 77.

O estabelecimento de critério punitivo reitor do sistema a imposição da pena justa e merecida, isto é, da pena proporcional à gravidade objetiva do fato e à culpabilidade do seu autor, o Código Penal visa não só à prevenção à prática de outros, como à repressão.

Como contemplou as vigas mestras de um modelo de Estado que se caracteriza por ser constitucional e democrático de Direito, não há dúvida que dos seus princípios, "regras e valores que são elas justiça, liberdade, segurança, dignidade da pessoa entre outros, pode-se inferir importantes limites à intervenção penal". [28]

Logo no momento da sentença, como se vê, a pena deve ser aplicada com o sentido retributivo e preventivo. "No momento da execução, firmou-se a orientação primordial da integração social (prevenção especial)". [29]

De qualquer modo, o sentido da pena em um determinado momento (da sentença) não se exclui quando ela passa para a fase seguinte (executiva). "A pena de prisão, na atualidade, está longe de cumprir sua missão ou finalidade ressocializadora do individuo para com a sociedade". [30] QUEIROZ diz:[31]

> "Aliás, não tem cumprido nem sequer a função inoculizadora (isolamento), visto que, com frequência, há fugas no nosso sistema. A pena de prisão no nosso país hoje é cumprida de maneira totalmente inconstitucional, desumana, cruel e torturante".

Os presídios não apresentam sequer condições mínimas para ressocializar alguém. "Ao contrário, dessocializam, produzindo efeitos devastadores na personalidade da pessoa. Presídios superlotados, vida subhumana etc". [32] Sanção é a pena, condenação, dada ao infrator de uma norma, após o processo legal onde o autor é julgado. "A sanção tem como objetivo a reeducação, ressocialização da pessoa ao mundo, ou seja, na própria sociedade e o seu castigo".

No ramo do Direito Penal tem-se como forma de punição a sanção penal, punição essa que serve para impor restrições ao Direito individual do indivíduo. Esse tipo de sanção pode ocorrer de duas formas, onde tem a sanção penal como punição ao infrator, sendo mera

---

[28] Idem.
[29] Idem.
[30] Idem.
[31] Idem.
[32] Idem.

resposta do ordenamento jurídico ou da sociedade à prática de um ato ilícito e ainda a sanção penal como medida educativa.

Também vale salientar, a vingança privada, uma forma de punição imposta pelo próprio ofendido ao autor do ilícito, que atualmente é expressamente proibida em nosso ordenamento jurídico, pois o jus puniendi pertence exclusivamente ao Estado-Juiz. "Na época em que a vingança era permitida, a comunidade realizava o ato vingativo como forma de evitar uma reação desproporcional ao delito."[33]

De acordo com QUEIROZ e CARNELUTTI, a sanção tem suas próprias características, que são:

> a) Legalidade: significa que a pena deve ser prevista em lei vigente a data do fato.
> b) Anterioridade: a lei já deve estar em vigor na época em que for praticada a infração penal.
> c) Personalidade: a pena não pode passar da pessoa do condenado. Assim, a pena de multa, ainda que considerada dívida de valor para fins de cobrança, não pode ser exigida dos herdeiros do falecido.
> d) Individualidade: a sua imposição e cumprimento deverão ser individualizados de acordo com a culpabilidade e o mérito do sentenciado
> e) Inderrogabilidade: salvo as exceções legais, a pena não pode deixar de ser aplicada sob nenhum fundamento. Assim, por exemplo, o juiz não pode extinguir a pena de multa levando em conta seu valor irrisório.
> f) Proporcionalidade: a pena deve ser proporcional ao crime praticado.
> g) Humanidade: não são admitidas as penas de morte, salvo em caso de guerra declarada, perpétuas (CP, art. 75), de trabalhos forçados, de banimento e cruéis (CF, art. 5º, XLVII).[34]

A sanção deve ser aplicada de acordo com a lei vigente, a pena varia de acordo com o tamanho do delito, ou seja, vai acontecer de forma proporcional. E com a explanação do mundo virtual, sua relação com o direito e o direito penal analisará no próximo capítulo os princípios relacionados com os Cybercrimes.

---

[33] Disponível em: http://www.resultadoconcursos.net/direito-penal-1-conceitos-emresumo-para-estudar/. Acesso em 16/05/2014.

[34] CARNELUTTI, Francesco. O Problema da Penal, rad. De Hi tomar Martins Oliveira. Belo Horizonte. Ed. Líder.2003.p.70.

3. PRINCÍPIOS NORTEADORES DO DIREITO PENAL BRASILEIRO

Será indispensável discutirmos sobre os princípios norteadores do direito penal brasileiro que estão ligados aos Cybercrimes. Princípios são:

> [...] as ordenações que se irradiam por todo o sistema, dando-lhe contorno e inspirando o legislador (citação da norma) e o juiz (aplicação da norma) a seguir-lhe os passos. Servem, ainda de fonte para interpretação e integração do sistema normativo.[36]

Ou seja, conceito é a base de qualquer estudo, pois é através dele que o doutrinador tem a fundamentação para o desenvolver . Os princípios são existentes não apenas no Direito Penal, mais em qualquer ramo do Direito.

O ramo do Direito Penal também é regido por alguns princípios específicos, que se apresentam como garantias ao cidadão diante do poder punitivo estatal.

3.1. Princípio da Retroatividade da Lei

O princípio da retroatividade da lei penal significa que esta não alcança os fatos praticados antes de sua vigência. No entanto, é importante mencionar que este princípio se refere apenas à lei mais grave, dizendo de outro modo, admitese a retroatividade de lei penal mais benigna, tendo em vista o benefício do réu. Guilherme de Souza Nucci diz que:

> [...] é natural que havendo anterioridade obrigatória à lei Penal incriminadora, não se pode permitir a retroatividade de leis especificamente as prejudiciais ao acusado.

---

[36] NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2tir . São Paulo. Editora Revista dos Tribunais.2007. p.75.

> Logo, quando novas leis entram em vigor, devem envolver somente fatos, sob a sua égide.[37]

Pode-se iluminá-la também, "como Princípio da Irretroatividade da Lei Penal, adotando como regra que a lei Penal não poderá retroagir, mas, como exceção, a retroatividade da lei benéfica ao réu ou condenado." [38]

3.2 Princípio da Fragmentariedade

O princípio da fragmentariedade está assentado na ideia de que nem todas as condutas que lesionam um bem jurídico são proibidas pelo direito penal. Este se limita a punir as ações mais graves praticadas contra os bens jurídicos mais importantes. Daí a fragmentariedade, pois seleciona qual bem jurídico será tutelado.

Segundo Nucci a fragmentariedade significa "que nem todas as lesões a bem jurídico protegidos devem ser tutelados e punidas pelo direito penal que, por sua vez, constitui somente parcela do ordenamento jurídico."[39]

As condutas cometidas pelos indivíduos, pois, são divididas de acordo com os níveis de lesão que causam aos bens jurídicos, sendo esta composta de diversos fragmentos. Os fragmentos tutelados são:

> [...] apenas a parte de um todo, razão pela qual o direito penal deve ser visto, no campo dos atos ilícitos, como fragmentário, ou seja, deve ocupar –se das condutas mais graves, lesivas à vida em sociedade, passíveis de causar distúrbios de monta a segurança pública e à liberdade individual.[40]

---

[37] NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2t i r . São Paulo. Editora Revista dos Tribunais.2007. p. 68.
[38] Idem.
[39] NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2t i r . São Paulo. Editora Revista dos Tribunais.2007. p. 71.
[40] Idem.

Questões diferenciadas devem ser resolvidas pelos demais ramos do Direito através de indenizações civis ou até mesmo punições administrativas. Pode-se ainda falar em fragmentariedade de 1° grau e de 3° grau.

> A primeira refere-se a forma consumada do delito, ou seja, quando o bem jurídico precisa ser protegido na sua integridade. A segunda Cingese à tentativa, pois protege-se o risco de perda ou de lesão, bem como a lesão parcial do bem jurídico.[41]

3.3 Princípio da Intervençãc Mínima

O princípio da intervenção mínima, conhecido como ultima ratio, significa que a tipificação de uma determinada conduta só será legítima se for estritamente necessária para a proteção de um bem jurídico. Somente diante de uma situação extrema, apresentando-se como indispensável para a manutenção da ordem, é que atua o direito penal, em razão de ser a forma mais agressiva do Estado interferir na conduta humana.

De acordo com Nucci, significa "que o Direito Penal não deve interferir em demasia na vida do indivíduo, retirando-lhe autonomia e liberdade."[42]

Pois a lei penal nunca deve ser considerada como uma primeira opção para o legislador para compor conflitos existentes em sociedade e diante do atual estado de desenvolvimento moral e ético da humanidade.

O Direito Penal é considerado como sendo a última cartada do sistema legislativo, quando se compreende que não se pode haver senão a citação da lei penal incriminadora, que vem a impor a sanção penal ao infrator. Como bem assinala Mercedes Garéa Aráma

> [...] o direito penal deve conseguir a tutela da paz social obtendo o respeito à lei e aos direitos dos demais, mais sem prejudicar a dignidade, o livre desenvolvimento da personalidade ou a igualdade e restringindo ao mínimo a liberdade.[43]

---

[41] Idem.

[42] NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2t i r . São Paulo. Editora Revista dos Tribunais.2007. p. 69.

[43] Fundamentos y aplicación de penas y medidas de seguridad em El Código Penal de 1995.p.36.

O Direito Penal deve ser visto como subsidiário aos demais ramos do Direito. "Fracassando outras formas de punição e de composição de conflitos, lança-se mão da lei Penal para coibir comportamentos desregrados, que possam lesionar bens jurídicos tutelados."[44]

3.4 Princípio da Ofensividade

Esse princípio também pode ser conhecido como princípio da lesividade e se trata de um princípio autônomo, que alegam que somente podem ser criados tipos penais incriminadores capazes de ofender um bem jurídico alheio, que esteja devidamente tutelado.

Não se pode aceitar a incriminação de uma conduta não lesiva ou que seja provocadora de uma lesão de um bem jurídico determinado. "O estado deve respeitar a esfera íntima do cidadão. Se o fizer, haveria respeito a intervenção mínima e, como consequência, ao princípio da ofensividade." [45]

Entende-se que não é todo bem jurídico protegido que merece a proteção do Direito Penal, para isso existem outros ramos do Direito, mas vale salientar que é possível encontrar situações que sejam ofensivas a determinados bens, mas que se enquadre de forma inofensiva na matéria penal. Nucci defende então que:

> [...] a ofensividade ou lesividade devem estar presentes no contexto do tipo penal incriminador, para validá-lo, sob pena de se esgotar o Direito Penal em situações inócuas e sem propósito, especialmente quando se contrasta a conduta praticada com o tipo de sanção para ela prevista como regra, ou seja, a pena privativa de liberdade.[46]

Por fim, a ofensividade é uma consequência do respeito a intervenção mínima.

---

[44] NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2t i r . São Paulo. Editora Revista dos Tribunais.2007. p. 75.
[45] NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2t i r . São Paulo. Editora Revista dos Tribunais.2007. p. 74.
[46] NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2t i r . São Paulo. Editora Revista dos Tribunais.2007. p. 75.

3.5 Princípio da Insignificância

Esse princípio descansa no princípio maior que é inconcebível um tipo de delito sem ofensa. Esse mesmo pressupõe o princípio da "utilidade penal", onde só é idôneo punir quando a conduta for efetivamente lesiva a terceiros.

Sendo assim, consideram-se atípicas as ações ou omissões que, dada a sua irrelevância, ofendem um bem jurídico que é protegido, só podendo punir as condutas que são consideradas como lesivas. Em outras palavras, Luis Flávio afirma que "o princípio da insignificância é o instrumento para a exclusão da imputação objetiva de resultados", ou seja, é um critério para determinação do injusto penal."[47] Nesse mesmo sentido, leciona Bittencourt que:

> [...] a tipicidade penal exige uma ofensa de alguma gravidade aos bens jurídicos protegidos, pois nem sempre qualquer ofensa à esses bens ou interesses é suficiente para configurar o injusto típico. Segundo esse princípio (...) é imperativa uma efetiva proporcionalidade entre a gravidade da conduta que se pretende punir e a drasticidade da intervenção.[48]

Sendo assim, malgrado algumas condutas enquadrem-se a determinado tipo penal, sob o ponto de vista formal, estas podem não apresentar relevância material, uma vez que, em verdade, não chegam a ofender nenhum bem jurídico.

3.6 Princípio da Culpabilidade

O princípio da culpabilidade, em apertada síntese, significa que não há crime sem culpabilidade. Deve ser vista não como um fenômeno individual, mas, sobretudo, social.

---

[47] GOMES, Luis Flávio. **Princípio da Ofensividade no Direito Penal** . Vol . 6, São Paulo: Revista dos Tribunais, 2002.

[48] BITENCOURT, Cezar Rober to. **Tratado de Di rei to Penal** . Vol . 1. 8ª ed. São Paulo: Saraiva, 2003.

Nada mais é do que uma relação de forças sociais existentes em determinado momento, as quais irão determinar os limites do que é ou não culpável. Segundo Nucci significa:

> [...] que ninguém será penalmente punido, se não houver agido com dolo ou culpa, dando mostras de que a responsabilização não será objetiva, mais subjetiva. Trata-se de conquista do Direito Penal moderno, voltado a ideia de que a liberdade é a regra, sendo exceção a prisão ou a restrição de Direitos.[49]

Além disso o próprio código penal vem estabelecer que somente é considerado como crime quando existir presente o dolo ou a culpa.

> Art. 18 - Diz-se o crime:
> Crime doloso
> I - doloso, quando o agente quis o resultado ou assumiu o risco de produzi-lo;
> Crime culposo
> II - culposo, quando o agente deu causa ao resulta por imprudência, negligência ou imperícia.
> Parágrafo único - Salvo os casos expressos em lei, pode ser punido por fato previsto como crime, senão quando o pratica dolosamente.[50]

A punição só acontece se o infrator tiver agido com dolo ou culpa , no que sem entende e dar-se o nome no Direito Penal de Crime Doloso e Crime Culposo.

3.7 Princípio da Humanidade

O princípio da humanidade sustenta que ao poder punitivo estatal é vedada a aplicação de sanções que atinjam a dignidade humana ou que violem a integridade física ou psíquica dos sentenciados, como penas cruéis, tortura, entre outras. Pretende-se que este princípio seja interpretado tendo em vista a reeducação e reinserção social do infrator.

---

[49] NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2t i r . São Paulo. Editora Revista dos Tribunais.2007. p. 71.

[50] VADE MECUN. Obra coletiva de autor ia da Editora Saraiva com a colaboração de Antonio Luiz de Toledo Pinto. Maria Cristina Vaz dos Santos. 10 ed.atual .e ampl . São Paulo. Saraiva. 2010.p.542.

Ora, é sabido que não basta que seja aplicada uma pena, pelo cometimento de um ilícito. O infrator mantém ainda a sua dignidade como ser humano, devendo essa ser respeitada. A sua violação afronta o princípio que está sendo comentado. Neste sentido, Nucci nos ensina que:

> [...] que o Direito Penal deve pautar-se pela benevolência, garantindo o bem-estar da coletividade, incluindo-se os dos condenados. Estes não devem ser excluídos da sociedade, porque infringiram a norma penal, tratados como se não fossem seres humanos, animais ou coisa.[51]

A constituição Federal assim determina:

> Art. 5º XLIV - constitui crime inafiançável e imprescritível a ação de grupos armados, civis ou militares, contra a ordem constitucional e o Estado Democrático.[52]

Na realidade existe uma relação imprecisa, pois as penas cruéis se encaixam no gênero das demais penas (pena de morte, prisão perpétua, banimento e trabalho forçado "logo, na alínea e, onde se lê cruéis, deve-se incluir as penas corporais, que implicam em castigos físicos." [53]

3.8 Princípio da Proporcionalidade da Pena

A pena deve variar de acordo com a gravidade do ato infracional cometido "não tendo cabimento o exagero, nem tampouco a extrema liberalidade na confirmação das penas nos tipos penais incriminadores"[54]

---

[51] NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2t i r . São Paulo. Editora Revista dos Tribunais.2007. p. 69.
[52] VADE MECUN. Obra coletiva de autor ia da Editora Saraiva com a colaboração de Antonio Luiz de Toledo Pinto. Maria Cristina Vaz dos Santos. 10 ed.atual .e ampl . São Paulo. Saraiva. 2010.p.542.
[53] NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2t i r . São Paulo. Editora Revista dos Tribunais.2007. p. 69.
[54] NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2t i r . São Paulo. Editora Revista dos Tribunais.2007. p. 72.

A constituição ao estabelecer as modalidades de penas que a lei ordinária deve adotar, vem a consagrar de forma explícita a proporcionalidade corolativa natural da aplicação da justiça, que é dar a cada um o que é seu por merecimento. Artigo 5° da constituição federal

> XLV - nenhuma pena passará da pessoa do condenado, podendo a obrigação de reparar o dano e a decretação do perdimento de bens ser, nos termos da lei, estendidas aos sucessores e contra eles executadas, até o limite do valor do patrimônio transferido;[55]

O infrator será punido de acordo com a gravidade do seu ato, de forma haver um nexo de proporcionalidade entre o ato lesivo, o dano causado ao bem jurídico e a reprimenda do Estado.

3.9 Princípio da Presunção de Inocência

Esse princípio está bem direcionado no que se determina que antes da sentença condenatória transitar em julgado não pode o acusado sofrer efeitos da execução de pena. É a chamada "pena antecipada".

No art. 5º, inciso LVII, da Constituição Federal, dispõe que "ninguém será considerado culpado até o trânsito em julgado da sentença penal condenatória".[56]

Consagrando-se um dos princípios basilares do Estado de Direito como garantia processual penal, visando à tutela da liberdade pessoal. Com efeito, o sistema normativo constitucional, através de seus preceitos, exerce notória influência sobre os demais ramos do Direito. Esta influência destaca-se no âmbito processual penal que trata do conflito existente entre o jus puniendi do Estado, que é o seu titular absoluto, e o jus libertatis do cidadão, bem intangível, não podendo ser considerado objeto da lide, reputado o maior de todos os bens jurídicos afetos à pessoa humana.

---

[55] VADE MECUN. Obra coletiva de autor ia da Editora Saraiva com a colaboração de Antonio Luiz de Toledo Pinto.Maria Cristina Vaz dos Santos. 10 ed.atual .e ampl . São Paulo. Saraiva. 2010.p.07.
[56] Idem.

> Efetivamente, o plano social prevê punição para aqueles indivíduos que desenvolve comportamento de normas de condutas socialmente predispostas a manter o imprescindível equilíbrio entre os membros da comunidade. Foi assim que o Estado criou mecanismos regulamentares da atuação estatal que propiciam na esfera criminal, a detectação da existência do ilícito penal, com a respectiva criação de limites à liberdade individual, com a aplicação de sanção que implicara no cerceamento do direito de locomoção. Agindo, como guardião do interesse coletivo e do indivíduo, já que o Direito existe, para dar ao homem garantias, sendo este a fonte e objetivo daquele.[57]

A materialização do direito-dever estatal de punir, todavia, deve ser compatibilizado com os preceitos fundamentais que tutelam o direito de liberdade, vez que de suma relevância para a coletividade, constituindo-se em garantia para cada cidadão, o respeito aos preceitos oriundos do texto constitucional e que mantém pertinência com o processo penal.

3.10 Princípio do "ne bis in idem"

Nesse princípio ninguém pode ser condenado mais de uma vez por causa da prática do mesmo ato com base em leis penais gerais.

3.11 Princípio da Legalidade ou da Reserva Legal

O princípio da legalidade é um dos princípios mais importantes do ordenamento jurídico Pátrio, é um dos sustentáculos do Estado de Direito, e vem consagrado no inciso II do artigo 5º da Constituição Federal, in verbis:" (...) ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei (...)".

No início do século XIX, consagrou tal princípio na fórmula "nullum crimen, nulla poena sine lege". A elaboração das normas penais é função exclusiva da lei, nenhum fato pode ser considerado crime se não houver expressa previsão legal, definindo-o e cominando-

[57]Disponível em: http://jus.uol.com.br/revista/texto/162/o-principio-da-presuncaode-inocencia-e-sua-repercussao- infraconstitucional . acesso em: 19/06/2014.

lhe sanção. Pode-se afirmar que é através da legalidade que o direito penal encontra a sua legitimidade. Nucci nos ensina que:

> [...] trata-se do fixador do conteúdo das normas penais incriminadoras, ou seja, os tipos penais mormentes os incriminados, somente podem ser criados através de lei em sentido estrito, emanada do Poder Legislativo, respeitando o procedimento previsto da constituição.[58]

Encontra-se previsto, expressamente na Constituição Federal e no Código Penal no artigo 5°, inciso XXXIX, da Constituição Federal, que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;"[59]

No código Penal no seu artigo 1° encontramos , Art. 1° - "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal."[60]

Porém, os ditames desse princípio não podem limitar a aplicação da reprimenda estatal, diante da violação de um bem jurídico protegido por lei. Nessa situação, temos as condutas lesivas praticadas no mundo virtual que não estão tipificadas no ordenamento jurídico pátrio, de modo que, por força do principio da legalidade estrita, há quem entenda que seriam atípicas.

---

[58] CCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral . Parte Especial . 3.ed. rev.atual .e ampla2tir . São Paulo. Editora Revista dos Tribunais.2007. p.67.

[59] VADE MECUN. Obra coletiva de autoria da Editora Saraiva com a colaboração de Antonio Luiz de Toledo Pinto.Maria Cristina Vaz dos Santos. 10 ed.atual .e ampl . São Paulo. Saraiva. 2010.p.09.

[60] VADE MECUN. Obra coletiva de autoria da Editora Saraiva com a colaboração de Antonio Luiz de Toledo Pinto.Maria Cristina Vaz dos Santos. 10 ed.atual .e ampl . São Paulo. Saraiva. 2010.p.542.

4. Crimes Cibernéticos e Punibilidade: conceito e noções gerais

A evolução da internet, ao passo que incentiva a busca de novos conhecimentos, a expansão da cultura, o avanço das informações e negócios comerciais, também propiciou o surgimento dos chamados criminosos digitais.

A proliferação destes crimes ocorre numa velocidade considerável, tendo em vista o grande número de usuários em todo o mundo. Faz-se necessário analisar as peculiaridades do sistema informático para procurar oferecer uma resposta adequada a esta pergunta.[61]

Sobretudo, sob a perspectiva do princípio da legalidade, pelo qual não se podem punir condutas que não estão devidamente descritas em lei. Para uma melhor análise do tema, tentar-se-á apresentar uma sistematização acerca de dois fundamentos: os atos ilícitos praticados por meio do sistema informático e aqueles praticados contra este mesmo sistema.

É por esta razão que se deve ter cautela em adaptar as leis já existentes aos delitos praticados através da internet, bem como não se pode esquecer que há situações que ensejam tutela específica, com a criação de novas leis. Convém destacar que o objetivo não é apontar todas as condutas ilícitas praticadas contra o sistema informático, mas destacar algumas, que se mostram cada vez mais comuns no "mundo virtual" e que trazem grandes consequências para o "mundo real". Silva nos ensina que:

> A primeira dificuldade teórica que se observa do presente tema é a própria denominação "crime informático". Não há um consenso sobre esta, ora se utiliza o sistema informático como elemento indissociável da conduta praticada pelo agente, ora este papel é assumido pelo computador, ora se citam ambos como elementos integrantes do conceito.[62]

Segundo esclarece Silva:

---

[61] SILVA, Rita de Cássia Lopes. Direito Penal e Sistema Informático. Editora Revista dos Tribunais. São Paulo, 2003, p. 57.

[62] Idem.

> Diante disso, a nominação crime informático parece ser mais adequada por se tratar de expressão que se refere não só ao equipamento eletrônico em si, mas também a toda tecnologia que possa ser por ele utilizada. Abrange ainda condutas que possam estar ligadas à informação e à sua transmissão isolada ou em conjunto.[63]

Numa definição clássica e genérica, pode-se conceituar o crime informático como sendo um fato típico, antijurídico e culpável, cometido contra ou através do uso do sistema informático. De posse dessa conceituação, pode-se classificá-lo

> [...] em crime informático impróprio e crime informático próprio. Os primeiros não seriam crimes informáticos, seriam crimes comuns nos quais o computador é usado como instrumento para a sua execução. Exemplos de crimes informáticos impróprios podem ser a calúnia (art. 138 do Código Penal), difamação (art. 139 do Código Penal), injúria (art. 140 do Código Penal), todos podendo ser cometidos, por exemplo, com o envio de um e-mail, correio eletrônico através do qual os usuários trocam mensagens.[64]

Os crimes informáticos próprios são aqueles praticados contra o sistema de informática. Neste sentido, leciona a professora Ivette Senise Ferreira:

> Muitas das condutas já tipificadas nas leis penais podem ser realizadas com a utilização da informática, para mais facilmente atingir o resultado pretendido pelo agente, com a ofensa de bens jurídicos de diversas categorias, de acordo com a prevalência daqueles aos quais se dirige a tutela da lei. Não se trata, propriamente, de crimes de informática, mas de crimes (comuns ou especiais), tipificados para proteger determinados bens jurídicos, em que o sistema de informática é, apenas, o meio ou o instrumento utilizado para a sua realização.[65]

---

[63] SILVA, Rita de Cássia Lopes. Direito Penal e Sistema Informático. Editora Revista dos Tribunais. São Paulo, 2003, p. 58.

[64] SILVA, Rita de Cássia Lopes. Direito Penal e Sistema Informático. Editora Revista dos Tribunais. São Paulo, 2003, p. 59.

[65] FERREIRA, Ivette Senise. Direito e Internet -Aspectos jurídicos relevantes. Edipro-Edições Profissionais Ltda, São Paulo, 2000, p. 220.

É importante destacar que, nos casos de ausência de previsão legal, o termo crime informático próprio, torna-se inadequado, tendo em vista a ausência de um nos seus elementos essenciais na conceituação de crime, qual seja, a tipicidade. Com base dos ensinamentos de Rita de Cássia ainda:

> [...] classificam-se os crimes informáticos destacando-se três tipos de ações: aquelas em que o sistema informático é objeto material, aquelas que se utilizam deste como mais um meio para atingir outros bens jurídicos e aquele que também se utilizam como meio, mas este seria o único modo. São os chamado crimes puros, impuros ou comuns, respectivamente.[66]

Os puros se referem aos novos delitos surgidos com o uso da internet, sendo o sistema informático meio e fim. Os impuros são aqueles que não dependem dela, esta é apenas meio para a prática de determinado delito já definido na legislação penal. E por fim, os comuns, que também utilizam o sistema informático como meio para prática de crimes já tipificados. Difere do impuro, por este se referir a ações contra bens tutelados, mas armazenado em suporte virtual, enquanto que nos comuns, o sistema informático é um meio a mais. Na atuação ilícita por meio do sistema informático, o que se constata é a possibilidade de afetação aos mais variados bens jurídicos. Segundo Rita de Cássia Lopes da Silva,

> Pode o agente agir contra o sistema informático, caracterizando uma ação danosa contra o hardware ou contra o software, ou ainda, agir sobre o objeto material informação armazenada, provocando, de consequência, a intranquilidade social.[67]

No que se refere à ação contra a informação armazenada se busca qual o bem jurídico afetado pela ação nociva. Uma ação cometida através do sistema informático que venha injuriar alguém tem como objeto a honra subjetiva. No entanto, é possível praticar uma ação que viola um determinado bem que componha os elementos do próprio sistema de

---

[66] FERREIRA, Ivette Senise. Direito e Internet -Aspectos jurídicos relevantes. Edipro-Edições Profissionais Ltda, São Paulo, 2000, p. 221.
[67] SILVA, Rita de Cássia Lopes. *Op. Cit.* p.64.

informática. Em outras palavras, o computador, enquanto bem físico, material, pode ser objeto do crime de furto, de dano, por exemplo, mas há casos em que uma conduta afeta os componentes imateriais, como o software, objeto do processamento do sistema informático, neste caso, urge a necessidade de uma legislação específica para tutelá-lo.

Importa destacar que a informação pode constituir um bem muito valioso, vez que pode ser objeto de armazenamento ou transmissão por meio do sistema informático. Como afirmou Maria Helena Junqueira Reis, a informação é um bem em si mesmo, pode valer milhões de dólares, ou pode ser vital para a segurança dos Estados ou de certos organismos[68]. Podendo ser uma obra literária ou um saldo bancário, ambos grafados em bits. Mais uma vez, convém destacar a lição de Rita de Cássia Lopes da Silva:

> [...] conclui-se que, nos delitos praticados com o uso do informático, de regra, tem como bem jurídico tutelado a informação. No entanto, esta informação traduzir-se em patrimônio, se ação for ofensa ao patrimônio, em honra, se ofenderem a honra; e assim, numa cadeia lógica e coerente, proteger-se-á o bem jurídico tutelado pela norma e que efetivamente corresponde à lesão provocada pela conduta praticada.[69]

Entretanto, não é possível chegar a tal especificidade. A informação pode ser vista como objeto imaterial, dados registrados sob forma de impulsos magnéticos, como também bem material, podendo ser manipulada como objeto, sendo guardada ou subtraída. Enfim, definir se é material ou imaterial é discutir sobre a possibilidade de ser objeto material do delito de furto, por exemplo, ou se exige uma matéria a ser regulada especificamente.

O conteúdo da informação apresenta-se de modo diferente em cada caso e por tal motivo deve ser protegida de acordo com sua individualidade. Dinheiro depositado em um banco e grafado por meio de bits (virtualizado) faz parte do patrimônio material e, portanto, é bem material. Se refere-se à uma obra literária, virtualizada, é imaterial. Assim, a necessidade de se criar normas penais está diretamente ligada ao conteúdo do bem jurídico a ser protegido.

Como é sabido, o direito penal não intervém em todas as ações lesivas, mas naquelas mais relevantes, as quais não podem ser solucionadas de outra forma, tendo em vista o

---

[68] REIS, Mar ia Helena de Junqueira. Computer Crimes: A criminal idade na era dos computadores. Del Rey, Belo Horizonte, 1996, p.37

[69] SILVA, Rita de Cássia Lopes. *Op.ci t*. p.66.

princípio da fragmentariedade, como corolário do princípio da intervenção mínima. Convém trazer à discussão o posicionamento da professora Ivette Senise Ferreira:

> A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidade de lesões dos bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar e, qualitativamente, aperfeiçoar os seus métodos de execução.[70]

No caso dos crimes informáticos próprios, a ação típica se realizará contra um sistema de informática ou pela utilização do processamento automático de dados ou a sua transmissão. Segundo Ivette Senise Ferreira convém:

> [...] mencionar, ainda que sucintamente, algumas técnicas que são utilizadas pelos criminosos informáticos. Destacam-se o Scanner, programa que detecta falhas de segurança de um computador, permitindo a obtenção de informações e de dados, para que aquela máquina seja invadida. O Cracking, cuja técnica consiste em destruir um sistema de segurança, descobrindo a chave de acesso, é muito utilizado para descobrir números de cartões de crédito ou desativar a proteção de senhas. Outra forma, mais conhecida, é o vírus, software que visa à destruição ou alteração de dados da máquina infestada, bem como sua proliferação, infectando outros computadores.[71]

O Cavalo de Tróia, ou Trojan Horse, consiste em incluir um evento a um programa para obter do computador compartimentos imprevistos. E por fim, o Sniffer que é um procedimento que permite a captura de informações ao longo da rede. Verifica-se que há uma grande lacuna no ordenamento jurídico brasileiro no que se refere à legislação específica a respeito de crimes virtuais ou informáticos. Conforme salientou Érica Lourenço de Lima Ferreira:

---

[70] FERREIRA, Ivette Senise. *Op.cit*. p. 207.
[71] Idem.

> [...] este vácuo que ainda persiste decorre não apenas da novidade desta tecnologia, bem como, da rapidez com que ela evolui, possui vida própria realizando uma metamorfose quase que constante, todo dia aparecem novidades tecnológicas, e a principal pergunta que paira no ar é: como o Direito vem se adequando e respondendo às novas exigências da vida contemporânea, sobretudo quanto à regulamentação dos atos gerados com a internet? (...) quem irá puni-lo e com base em que arcabouço normativo.[72]

A obediência ao princípio da legalidade é premissa inafastável para o combate a esta criminalidade. Pois, como se sabe, somente se pode falar em cometimento de um crime se a conduta realizada estiver previamente descrita em lei.

Destaque-se que há quem se posicione contra esta tendência de optar pelo aumento da tipificação destas condutas lesivas do sistema informático, sob o argumento de que seria deixada de lado a adoção de medidas de prevenção ou a previsão legal de ilícitos administrativos. É o que afirma Luciana Boiteux:

> Há necessidade de se adotarem medidas de prevenção a este tipo de criminalidade, por meio de utilização de métodos não-penais com o objetivo de prevenir a prática de crimes, ao invés de optar-se pela mera previsão legal de tipos especiais, diante do reconhecimento de que o direito penal não serve à finalidade de impedir a prática de delitos.[73]

Assim, para esta autora, haveria uma atuação preventiva antes da prática do delito, através da aplicação de sanções administrativas e medidas educativas, com o intuito de inibir e desestimular a prática de condutas reprováveis por parte dos potenciais infratores.

Para aqueles que defendem tal posicionamento, não há como se falar nesse tipo de delito sem antes falar em medida de segurança tecnológica. Argumenta-se sobre a necessidade de se combinarem medidas técnicas de segurança voluntárias, a serem adotadas pelos usuários, juntamente com medidas compulsórias exigidas das empresas de tecnologia para proteção dos usuários. Neste sentido, aduz ainda Luciana Boiteux: "a implementação de

---

[72] FERREIRA, Érica Lourenço de Lima. *Op.cit*. p.20.

[73] BOITEUX, Luciana. Crimes Informáticos: reflexões sobre política criminal inseridas no contexto internacional atual . Revista Brasileira de Ciências Criminais, v.47.Coordenador : Theodomiro Dias Netto. Edi tora: Revista dos Tribunais . Categoria: Direito Penal , 2004, p. 158.

medidas preventivas seria mais eficaz para deter os crimes informáticos dos que leis penais incriminadoras".[74]

Tais medidas preventivas estariam relacionadas ao incentivo à pesquisa em segurança informática, exigência de padrões de segurança e controle pelas empresas, e na necessidade de aumentar a responsabilidade administrativa das empresas fabricantes de sistemas e dos provedores de acesso a internet. O controle administrativo, com imposição de multas e até mesmo a pena de fechamento seria, para os defensores da óptica preventiva, mais eficaz do que a responsabilidade penal, proposta por muitos, aos provedores de acesso, por exemplo.

Ademais, salientam que devem ser aumentados os esforços, do ponto de vista educacional, para se estabelecerem valores éticos na comunidade dos usuários de computadores. Em que pese este respeitável posicionamento, é dever do direito penal a proteção de bens jurídicos tradicionalmente reconhecidos e lesionados com o uso da tecnologia da informática, bem como a proteção de outros valores jurídicos recentes havidos com o advento e proliferação dos computadores[75] e isto se dá através da tipificação penal. Sustenta Paulo Marco Ferreira Lima:

> A consequência direta de não fazê-lo será a ausência de figuras concretas que possam ser aplicadas nessa matéria, o que pode levar à ausência de punição aos autores desses fatos ou a obrigar os tribunais a aplicar preceitos que não se ajustem de forma perfeita à natureza dos fatos cometidos.[76]

A sociedade não pode submeter-se à falta de interpretação das leis já existentes ou ficar à mercê do direito costumeiro e da analogia para definir a sua aplicação.[77] Assim, é válido destacar que é necessário ter cautela, pois o anseio pela reprimenda de crimes informáticos não pode sobrecarregar o ordenamento jurídico penal de inúmeras imputações. É preciso elaborar normas efetivas que atendam à proteção dos bens jurídicos ofendidos pelos infratores informáticos.[78]

---

[74] BOITEUX, Luciana. *Op.cit*. p. 162.
[75] LIMA, Paulo Marco Ferreira. Crimes de Computador e Segurança Computacional .Campinas/SP. Editora Millennium, 2006, p. 15.
[76] LIMA, Paulo Marco Ferreira. Op. cit. , p. 18.
[77] DAOUN, Alexandre Jean. Os novos crimes de informática . Jus Navigandi, Teresina, ano 4, n. 37, dez. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1827>. Acesso em: 04/10/2014.
[78] FERREIRA, Ivette Senise. *Op.cit*. p. 207

> Diante da latente necessidade de uma ampliação de figuras repressivas relativas a esses novos riscos, é importante analisar e identificar qual seria o bem jurídico a ser protegido nesta área, tendo em vista que o direito penal somente deve agir para preservar os bens mais relevantes (princípio da fragmentariedade) dentro dos limites do princípio da intervenção mínima (última ratio).[79]

A multiplicidade de condutas de ataque cibernético está entre a ilicitude e a falta de tipificação, o que também dificulta a identificação do bem jurídico. No que se refere aos delitos já tipificados no Código Penal e na legislação extravagante, não há dificuldades para operar o sistema penal. A diferença consiste nas formas de persecução penal pelos órgãos oficiais, principalmente no tocante à investigação criminal.

O problema reside na solução para as condutas lesivas ou potencialmente lesivas que possam ser praticadas contra o sistema informático e que não encontrem adequação típica no rol de delitos existentes no Código Penal e nas legislações extravagantes. Por exemplo, a conduta de introduzir, por transferência de arquivos, um vírus de computador, que acaba por provocar travamento dos programas instalados no aparelho atingido, poderia até pensar na tipificação do delito de dano, previsto no art. 163 do Código Penal, mas indaga-se: um programa de computador pode ser considerado coisa? Do mesmo modo, se houver a cópia deste, sem a devida autorização, pode ser considerada coisa móvel e ser objeto do crime de furto? Ademais, quando se recorda que a cópia do programa não retira a coisa da esfera de disponibilidade da vítima e não há diminuição no patrimônio do sujeito passivo, pois permanece em seu banco de dados os arquivos "furtados" ou copiados clandestinamente.

Outros exemplos de crimes informáticos próprios, apontados pela doutrina, merecem ser citados. Saliente-se que este trabalho não tem a pretensão de esgotar o tema, mas tem o intuito de relacionar as figuras existentes, muitas ainda não tipificadas na legislação penal brasileira. São elas: Segundo o Doutrinador Paulo Marco Ferreira

> a) Cibergrilagem- atividade na qual o delinquente se apropria de domínios virtuais registrado em nome alheio;
> b) Desvio de DNS-Domain Name System- atividade de alterar o endereço eletrônico de um site de forma a desviar quem queira o acesso para outro local diverso da rede;

[79] DAOUN, Alexandre Jean. Os novos crimes de informática . Jus Navigandi, Teresina, ano 4, n. 37, dez. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1827>. Acesso em: 04/10/2014.

> c) Uso ilegítimo de sistemas informáticos alheios e computadores alheios- também chamado de furto de tempo, consistindo na utilização sem autorização dos computadores, sistemas e programas alheios;
> d) Intrusão informática- trata-se do acesso não autorizado, com a utilização específica de passwords (senha usada para identificação do utilizador, em conjunto com o login) e a entrada em um sistema informático sem autorização do proprietário. O bem jurídico a ser protegido é a privacidade que pode ser atingida com a mera invasão;
> e) Sabotagem informática- atentado contra a funcionalidade de um sistema informático dirigido a danificar ou destruir sistemas eletrônicos, suas instalações, seus dados, informações, programas ou ainda a interrupção, ainda que parcial, de seu funcionamento.[80]

Verificar-se-á, mais adiante, que o ordenamento jurídico brasileiro está muito aquém no combate a esta nova criminalidade e, por tal motivo, mostram-se necessárias certas providências em termos legislativos, para que não corramos o risco de sermos atropelados pela tecnologia, uma vez que esta não espera o Direito.[81]

No próximo tópico será destacado como alguns ordenamentos estrangeiros vêm lidando com esta nova forma de criminalidade.

4.1 Tratamento na Legislação Estrangeira

À luz do tema proposto, pode-se destacar que alguns países estão punindo os delinquentes informáticos através da promulgação de diversas leis. É o que se pode extrair das lições de Paulo Marco Ferreira Lima[82], abaixo relacionadas.

A opção da Alemanha na luta contra a criminalidade informática foi a de introduzir um número relativamente alto de novos tipos penais. Adotou-se a Segunda Lei contra a Criminalidade Econômica, de 15.05.86, onde se contemplam os delitos de espionagem de dados, extorsão informática e sabotagem informática.

O ordenamento francês, com o advento da Lei n. 88/19, de 05.01.88, tipificou as condutas de acesso fraudulento a um sistema de elaboração de dados. Por este dispositivo são

---

[80] LIMA, Paulo Marco Ferreira. *Op. Cit*.p. 59-61.

[81] MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via Internet .Jus Navigandi, Teresina, ano 4, n. 37, dez. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/teto.asp?id=1828>. Acesso em: 07/10/2014.

[82] LIMA, Paulo Marco Ferreira. *Op.ci t*. pgs. 80, 86, 87, 92/93.

sancionados tanto o acesso ao sistema como ao que se mantenha nele, aumentando a pena correspondente em caso desse acesso resultar a supressão ou modificação dos dados contidos no sistema ou resultar a alteração do seu funcionamento.

A Itália introduziu através do Decreto Legislativo nº 518/92, a figura da mencionada sabotagem informática, e entre outras, a fraude informática, que pune a conduta de quem altera dados em sistema alheio para obter vantagem ilícita.

Na Inglaterra, pode-se destacar a Lei do Terrorismo nº 2.000, que classifica como ciberterroristas as pessoas que põem vidas em risco através da manipulação de sistemas de computadores públicos. A ideia é aumentar a definição de terroristas, colando ao lado dos grupos como IRA[83] e Hezbollhah[84], os crackers.

Em Portugal, a Lei nº 109, de 17.08.91, trata dos crimes informáticos, criando seis novas condutas: a falsidade informática (que penaliza a introdução, modificação ou supressão de dados ou de programas informáticos, com o intuito de falsear a obtenção de dados eletrônicos); o acesso ilegítimo (responsabiliza criminalmente a intrusão a sistemas informáticos), a interceptação ilegítima (que penaliza a interceptação ilegítima de comunicações informáticas, em qualquer ambiente computacional).

Nos Estados Unidos, pode-se destacar a Lei nº 18- U.S.C/1030. Há disposição legal referente à proteção dos computadores de órgãos públicos governamentais, punindo a fraude mediante acesso a um sistema eletrônico de interesse federal para a obtenção de vantagem econômica ilícita. São punidos também a produção, uso ou tráfico de dispositivos de acesso falsificados; o uso ou obtenção, sem autorização, de dispositivos de acesso.

Como se observa, há, pelos países supracitados, uma preocupação em oferecer uma resposta aceitável, através da tipificação penal, para a solução quanto às condutas lesivas ou potencialmente lesivas que possam ser praticadas contra o sistema informático e que anteriormente não encontravam adequação típica no rol dos delitos existentes.

4.2 Crimes Próprios e Impróprios Cibernéticos Tipificados no Brasil

Importa destacar que os crimes praticados através de um sistema informático ou da internet, mais especificamente, já se encontram tipificados no Código Penal pátrio, como nas

[83] LIMA, Paulo Marco Ferreira. Op.ci t .p.67.
[84] LIMA, Paulo Marco Ferreira. Op.ci t .p.68.

legislações extravagantes. A diferença se encontra no meio através da qual a conduta foi realizada.

Dentre os delitos informáticos impróprios, pode-se destacar o homicídio. Este pode ser praticado por meio do computador e deverá ser punido nos mesmos moldes do art. 121 do Código Penal. Seria o caso em que um cracker invade a rede de computadores de um hospital e muda as prescrições médicas relativas a um determinado paciente, substituindo os remédios ou alterando as dosagens, com o animus necandi.

De igual modo, aplica-se o tipo do art. 155, §4º, inciso II, do Código Penal (furto qualificado pela destreza) ao usuário que viola o sistema de senhas e de segurança digital de um banco comercial, penetra na rede de computadores da instituição financeira e desvia para a sua conta uma determinada quantia em dinheiro.

Destacam-se ainda as condutas descritas na Lei nº 7.716/89 (racismo), no art. 138 (calúnia), no art. 147 (ameaça), no art. 171 (estelionato), no art. 286 (a incitação ao crime), todos do Código Penal vigente, entre tantas outras.

Sendo o equipamento eletrônico objeto material, não há problemas em solucionar os delitos à luz do direito penal comum. O hardware (equipamento físico, como o teclado, o mouse, o monitor, o gabinete) pode ser objeto de crime de furto, de dano, de apropriação indébita.

Importante destacar que os delitos de forma livre, que podem ser praticados através da internet, podem ter ou não a previsão deste meio na norma penal. Há delitos comuns que já eram tipificados, como no caso do delito de divulgação de pornografia infantil, previsto no art. 241 da Lei nº 8.069/90 (Estatuto da Criança e do Adolescente), que não previa a prática através da internet.

Ocorre que o relativo anonimato, propiciado por esta, favoreceu e tem favorecido, cada vez mais, a produção e distribuição de fotos e vídeos contendo crianças e adolescentes em cena de sexo explícito. Por esta razão, houve uma modificação legislativa, através da Lei Federal nº 10.764/03, para incluir os termos "rede mundial" e "internet". A redação anterior previa:

> Art. 241. Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.
> Pena: reclusão de 01 (um) a 04 (quatro) anos. [85]

[85] ARAS, Vladimir . Crimes de informática. Uma nova criminal idade. Jus Navigandi , Teresina, ano 5, n. 51, out . 2001. Disponível em: <http: / / jus2.uol .com.br /doutrina/ texto.asp?id=2250>. Acesso em: 08/10/2014.

A modificação da Lei nº 10.764/03, acrescentando os termos "rede mundial" e internet, não teve o condão de caracterizar tal delito como sendo um crime informático próprio, não houve a criação de um novo delito. Veja-se a nova redação:

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou
> cenas de sexo explícito envolvendo criança ou adolescente:
> Pena - reclusão de 2 (dois) a 6 (seis) anos, e multa.
> § 1o Incorre na mesma pena quem:
> I - agencia, autoriza, facilita ou, de qualquer modo, intermedia a participação de criança ou adolescente em produção referida neste artigo;
> II - assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do caput deste artigo;
> III - assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do caput deste artigo.
> § 2o A pena é de reclusão de 3 (três) a 8 (oito) anos:
> I - se o agente comete o crime prevalecendo-se do exercício de cargo ou função;
> II - se o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial.[86]

No mesmo sentido, destaque-se a conduta descrita no art. 153 do Código Penal, cuja redação foi modificada pela Lei nº 9.983/03:

> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
> Pena - detenção, de um a seis meses, ou multa.
> § 1° Somente se procede mediante representação
> § 1o-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:
> Pena - detenção, de 1 (um) a 4 (quatro) anos, e multa.
> § 2o Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada. [87]

Quanto aos delitos informáticos próprios, pode-se mencionar o art. 313 A e 313 B, incluídos no Código Penal pela Lei nº 9.983/03, cujas redações merecem ser transcritas:

---

[86] Idem.
[87] Idem.

> Inserção de dados falsos em sistema de informações Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
> Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa.
> Modificação ou alteração não autorizada de sistema de informações Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa.
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.[88]

A questão se torna complexa também quando a ação delitiva recai sobre o software (programa de computador), que nada mais é o que uma forma de expressão intelectual do seu criador, podendo ser protegido à luz dos direitos autorais. Cite-se a Lei nº 7.646/87, que regulamenta a proteção à propriedade intelectual sobre programas de computadores, bem como a Lei 9.609/98.

No entanto, é pertinente salientar que tais tipificações esparsas não resolvem o problema da criminalidade na internet, do ponto de vista do direito objetivo, mas revelam a preocupação do legislador infraconstitucional de proteger os bens informáticos e de assegurar, na esfera penal, a proteção a dados de interesse da Administração Pública e do Estado democrático, bem como à privacidade "telemática" (comunicação à distância de um conjunto de serviços informáticos fornecidos através de uma rede de telecomunicações) do indivíduo.[89]

4.3 Projetos de Lei em Tramitação no Brasil

Observando a realidade brasileira, percebe-se a existência de diversos projetos de lei em tramitação no sentido de propor modificações em tipos penais já existentes, onde 2 (dois)

---

[88] Idem.

[89] ARAS, Vladimir . Crimes de informática. Uma nova criminal idade. Jus Navigandi , Teresina, ano 5, n. 51, out . 2001. Disponível em: <http: / / jus2.uol .com.br /doutrina/ texto.asp?id=2250>. Acesso em: 08/10/2014.

desses projetos vem se destacando mais no nosso ordenamento, esses projetos vêm com a finalidade de acrescentar novas condutas delitivas, até o presente momento, ainda não tipificadas, demonstrando a preocupação em se reprimirem determinadas condutas danosas contra os dados e sistemas informáticos.

No nosso ordenamento nenhuma legislação penal específica. Mas circula os Projeto de Lei 84/99, da Câmara dos Deputados, Dispõe sobre os crimes cometidos na área de informática, suas penalidades e outras providências. Deputado Federal Luiz Piuahylino. Lei 9.609, de 19/02/98 - Lei sobre Propriedade Intelectual de Programa de Computador. Também dispõe a Lei 9.610, de 19/02/98 - Lei de Direitos Autorais, Lei 9.800, de 26/05/99 – Sistema de Transmissão de Dados e Imagens via fax ou similar, o próprio Código Penal e o Estatuto da Criança e do Adolescente.

Um dos mais importantes projetos de lei nesta área, em tramitação, é o de nº 84/99, que segue em anexo, do Deputado Luiz Piauhylino, apresentado em 24 de fevereiro de 1999, já aprovado pela Comissão de Constituição e Justiça e de Redação (CCJR) da Câmara dos Deputados.

Em suas disposições gerais, o referido Projeto de Lei busca inicialmente conferir proteção à coleta, ao processamento e à distribuição comercial de dados informatizados, exigindo autorização prévia do titular para a sua manipulação ou comercialização pelo detentor. Estabelece os direitos de conhecimento da informação e de retificação dessa informação, o direito de explicação quanto ao seu conteúdo ou natureza, bem como o de busca de informação privada, instituindo-se a proibição de distribuição ou difusão de informação sensível e impondo-se a necessidade de autorização judicial para acesso de terceiros a tais dados.

No tocante ao rol de novos tipos penais, procura inserir no ordenamento brasileiro os crimes de dano a dado ou programa de computador; acesso indevido ou não autorizado; alteração de senha ou acesso a computador, programa ou dados; violação de segredo industrial, comercial ou pessoal em computador; criação ou inserção de vírus de computador; oferta de pornografia em rede sem aviso de conteúdo; e publicação de pedofilia, cominando-se penas privativas de liberdade que variam entre um e quatro anos.

Outro que merece destaque é o Projeto nº 76/2000, também em anexo, do ex-senador Renan Calheiros, tido hoje como um dos mais específicos na determinação das práticas que serão considerados crimes. Pela proposta, é crime a alteração ou transferência de contas representativas de valores, a difusão de material injurioso, o uso da informática para ativar explosivos, alteração de registros de operações tributárias e a sonegação de tributos

decorrentes de operações virtuais, dentre outras. Também pretende o mencionado Projeto incriminar a divulgação de mensagens contrárias aos bons costumes, a interferência em programas relacionados a armamentos, a indução a atos de subversão e a veiculação de mensagens ameaçadoras à soberania nacional.

Como se observa, embora haja a proposta da tipificação penal de algumas condutas ainda não descritas pela lei, como a inserção de vírus, por exemplo, muitos dos projetos acima citados apenas almejam a previsão da internet como sendo uma circunstância agravante, tendo em vista a sua potencialidade lesiva.

4.4 A (im) punibilidade dos crimes cibernéticos no Brasil

Para facilitar o entendimento sobre o assunto abordado, pode-se entender que para a prática desse tipo de crime cibernético é necessário a existência de um computador devidamente conectado a internet, onde receberá comandos de um individuo, esteja este utilizando de forma direta esta máquina, ou por meio de outra a ela conectada, possibilitando o acesso remoto. Caracteriza-se, portanto, a internet como o meio utilizado para a execução e consumação das condutas ilícitas praticadas na rede mundial de computadores.

A prática dessas condutas são marcadas pelo anonimato que a rede mundial de computadores proporciona além da suposta impunibilidade que se apresenta com a falta de legislação pertinente ao assunto, explicando-se assim porque tal modalidade de delito aumenta consideravelmente no mundo contemporâneo, de forma a obrigar a população em geral e as autoridades a buscar mecanismos de prevenção contra os criminosos.

Com o avanço da sociedade brasileira o número de computadores aumentou em grande percentual, e com esse crescimento a privacidade no mundo virtual se tornou cada vez mais preocupante para o mundo externo, pois com mais usuários, alguns sem a noção de que a internet possui várias armadilhas, a prática de condutas que causam danos a bens jurídicos vem sendo constantemente vislumbrada. Segundo Gama:

> Antes da invenção dos computadores a proteção legal das pessoas, com respeito ao conteúdo das informações pessoais, estava limitada. Com o surgimento da informática, novas tecnologias ampliaram as possibilidades de acesso a informações,

> causando novas ameaças à privacidade. Isto provocou muitos sistemas jurídicos estrangeiros a ordenar novos regulamentos civis e penais direcionados a proteção da privacidade.[90]

Já no Brasil, nós não nos disponibilizamos de nenhuma legislação específica para tratar desses crimes cometidos pela internet, assim sendo deve-se nos basear apenas na utilização da analogia in bonam partem, ou seja é possível, apenas compararmos a conduta praticada na internet pelo autor do fato com os crimes tipificados em nossa legislação penal, quando houver uma verdadeira lesão a um bem jurídico, e tivermos uma conduta semelhante em nossa legislação penal, para que possa ser estabelecida a responsabilização penal.

Sabe-se que seria de suma importância a criação de um Código específico, para nortear a punição das condutas criminosas praticadas no mundo cibernético.

Analisando os entraves para a punibilidade dessas condutas, vislumbramos que um dos grandes problemas relativos aos característicos "cyber crimes" é o fato de ser difícil identificar o causador do dano praticado. Com base no estudo dos princípios, mais direcionado ao princípio da legalidade, pode-se notar que diversos delitos praticados no mundo virtual ainda não são cabíveis de punição.

Vale salientar que isso ocorre porque o nosso ordenamento jurídico do Brasil traz como garantia o fato de que ninguém pode ser condenado por um delito que não esteja previamente tipificado, ou seja, que do ponto de vista legal, não é considerado crime.

Contudo, diante da ausência de legislação específica sobre o assunto, a questão dos crimes virtuais torna-se um grave problema para a sociedade, uma vez que as omissões existentes na lei sobre o tema encorajam cada vez mais criminosos a continuarem praticando delitos virtualmente.

Os crimes praticados na internet vêm a causar lesões aos bens jurídicos, exigindo a reprimenda do estado. Por esse fato, necessária se faz a aplicação da analogia para que os autores desses fatos não fiquem impunes diante da sociedade.

No espaço virtual, os defeitos e os atos ilícitos dos internautas se produzem com a mesma facilidade que no espaço real. Todavia, o Direito ao pretender tutelar o bem jurídico do cidadão precisa, necessariamente acompanhar esta evolução, a fim de possibilitar tal garantia.

---

[90] GAMA SILVA, Remy, Cr imes da informát ica, Edi tora: CopyMarket .com, 2000.

A necessidade de uma legislação própria para esses tipos de crimes, aumenta cada vez mais a nação brasileira, e já se percebe a mobilização de alguns representantes do Congresso Nacional para a tipificação dessas condutas. Tramitam no Congresso Legislativo cerca de 14 (quatorze), projetos de lei relacionados com os crimes cibernéticos, onde apenas 2 (dois) estão se destacando, sendo visível a falta de interesse político no desenvolvimento dessa matéria.

> Dois destes projetos vem ganhando a atenção nacional. Um pertencente ao Deputado Luiz Piauhylin e outro do Senador Renan Calheiros. Ambos são vistos com ressalvas, mas entretanto, adverte o próprio senador, dizendo que "a tipificação desse tipo de delito pelas legislações de todos os países é medida urgente e que não pode esperar mais.[91]

Sendo um problema que atinge não somente a nação brasileira, uma vez que não há barreiras físicas ou virtuais para que os agentes de condutas lesivas a bens jurídicos, refletindo também em outras nações, a Organização dos Estados Americanos (OEA), vem pressionando, de forma diplomática, o Congresso Nacional para que proceda na aprovação desses projetos.

[91]Disponívelem:www.google.com.br/#hl=ptBR&q=no+brasil+como+se+puni+os+crimes+virtuais&oq=no+brasil+como+se+puni+os+crimes+virtuais&aq=f&aqi=&aql=&gs_sm=e&gs_upl=2855l20556l0l47l42l2l27l29l0l705l833l0.1.61&bav=on.2,or.r_gc.r_pw.&fp=dd888af28f656a1&biw=1366&bih=677. Acesso em: 09/10/2014.

5. OS CRIMES VIRTUAIS E A ANÁLISE DA PROVA

5.1 Crimes virtuais em espécie

Os crimes feitos pela internet são feitos de várias formas. Temos abaixo alguns deles que são tratados pela lei igualmente como crimes cometidos pessoalmente. Elenca, Fabrízio Rosa, alguns crimes virtuais comuns, sendo eles:[92]

> 1. Fraude/ Falsidade informática;
> 2. Danos afetando dados ou programas informáticos/danificação de informações e/ou programas de computadores;
> 3. pichação;
> 4. sabotagem informática;
> 5. acesso indevido/ilegal/não autorizado;
> 6. utilização não autorizada de um sistema informático;
> 7. interceptação não-autorizada;
> 8. pirataria/reprodução não autorizada de um programa informático protegido;
> 9. utilização não autorizada de um programa informático protegido;
> 10. espionagem informática/fuga de dados;
> 11. spam;
> 12. furto de informações;
> 13. divulgação de informações sem autorização de autoridade competente ou de pessoa interessada, quando necessária; (2002, p. 15/16).

A estes delitos, somam-se aqueles que dispostos em lei penal como de cometimento real, ou seja, pessoalmente, mas que podem ser cometidos, também, através de meios virtuais, como estelionato, crimes contra a honra, apropriação indébita, furto, pedofilia, entre outros.

Os criminosos atuam das mais diversas formas. Eles utilizam sites para proliferarem ideais racistas, invadem contas bancárias, praticam pedofilia e interceptam comunicações eletrônicas, piratarias que ferem o direito autoral, por exemplo, sem que para isso precisem utilizar qualquer ferramenta palpável, como armas, mas apenas sofisticados programas tecnológicos que possibilitam que o agente esteja até mesmo em outro território, a quilômetros de distância da vítima alvo da sua empreitada criminosa. A doutrina de Liliana Paesani exemplifica a ação desses agentes:[93]

[92] ROSA, Fabrízio. **Crimes de informática.** Campinas: Bookseller, 2002.

[93] PAESANI, Liliana Minardi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2003.

> Com referência aos crimes praticados na Internet, a Policia Federal fez ampla investigação de hackers brasileiros (piratas da Internet) que estão tentando romper as barreiras de segurança e entrar nos arquivos dos computadores da Agência Espacial Norte-Americana (Nasa). Recentemente, foram constatadas tentativas de invasão da página da Polícia Federal na Internet, e os hackers conseguiram alterar algumas páginas de acesso público da instituição. (2003, p. 44).

O correio eletrônico também é amplamente utilizado pelos criminosos virtuais, que atuam enviando mensagens às vítimas de maneira a causar-lhes diversos prejuízos, como, por exemplo, aplicando golpes para enviar vírus, descobrir senhas bancárias, enviar programas piratas, dentre outros ilícitos penais.

Um dos mais comuns é a pornografia infantil através da rede, que historicamente é difundida pelo mundo através dos mais diversos meios, não seria diferente com a internet, onde os pedófilos atuam, tentando esconder-se no anonimato. É crescente o número de casos configurando esse ilícito penal, onde fotos e filmes expõem imagens de crianças nuas, entre outras obscenas, que causam repúdio mundial, principalmente de pais que se preocupam com os filhos, como com o conteúdo que eles podem acessar na net.

Outra ação popular dos criminosos virtuais consiste na pirataria, responsável pela maior parte dos programas vendidos atualmente. As cópias são produzidas em grande quantidade e comercializadas ou, ainda, distribuídas gratuitamente, tendo em vista o baixo custo da produção, além de disponibilidade dessas produções em sites para downloads pelos usuários, visando programas de computador, músicas, filmes, entre outros, ferindo assim o direito autoral e causando um enorme prejuízo aos reais proprietários.

Esses delitos são cometidos pelos agentes que são atraídos não apenas pela dimensão de alcance da rede, mas pelo anonimato que diversas vezes lhes é oferecido, bem como pela imperfeição dos programas utilizados pelos usuários, que são invadidos pelos criminosos.

Entre os métodos utilizados pelo "hacker" estão a chave-mestra, "sniffers", vírus, cavalo de tróia e "satan". Estes programas os ajudam a invadir máquinas, destruir sistemas, roubar informações, alterar dados importantes, vigiar rotinas, enfim, causar os mais diversos danos às suas vítimas.

Um vírus, por exemplo, pode contaminar uma máquina, proliferar-se, e atacar toda uma rede de computadores, nos casos em que os programas de antivírus não forem capazes de identificá-los. Nestes casos, se destruída ou "enganada" a segurança da máquina, o invasor pode atacar diversos bens jurídicos, como a intimidade, e também desviar valores de contas bancárias, destruir programas, ameaçar pessoas, etc.

5.2 A necessidade de profissionais atualizados, de equipamentos adequados e a possibilidade de identificação do agente criminoso.

Além da constante atualização dos peritos criminais, necessária também a atualização dos operadores do direito, para que possam atuar de forma mais segura. Implantar eventos relacionais ao tema em faculdades de Direito torna-se fundamental na busca de profissionais competentes. Os meios acadêmicos, o próprio Poder Judiciário, e também as entidades de classe devem ser alvo desta capacitação técnica.

Não se olvidando da capacitação jurídica, demasiadamente importante, os operadores do direito devem se adequar à nova realidade mundial, que busca diminuir fronteiras e a celeridade. O conhecimento acerca do ordenamento legal tem que ser associado ao conhecimento sobre as ferramentas virtuais, possibilitando o surgimento de profissionais capazes de solucionar conflitos atuais, que em sua maioria envolvem questões tecnológicas.

Além disso, o uso dessas tecnologias, associado à competência profissional, pode gerar a prestação de um serviço muito mais eficiente, além de tornar menos morosa a prestação jurisdicional. Ainda que estejam tecnologicamente atualizados, os operadores devem sempre se lembrar que:

> Os operadores jurídicos deverão utilizar o bom senso para dirimir questões jurídicas relacionadas à Internet, procurando sempre relacionar a parte técnica com o ordenamento jurídico em exercício. São as análises simples e lógicas que possibilitarão um eficaz entendimento das questões cotidianas de nossos tribunais, sendo, principalmente, os bancos acadêmicos os futuros responsáveis pela

> construção deste, já que é neles que existe uma verdadeira interdisciplinaridade, essencial para a resolução dessas novas questões." (CORRÊA, 2000, p. 107).[94]

Os chamados hackers ou crackers são os sujeitos ativos dos crimes praticados através dos meios virtuais. Eles invadem sistemas, roubam informações, destroem banco de dados, causando os mais diversos prejuízos. São agentes inteligentes, com um vasto conhecimento acerca de computadores, que utilizam diversas técnicas para atingir os bens das vítimas, pessoas físicas e jurídicas.

Alguns, no entanto, trabalham justamente para as vítimas em potencial, auxiliando na medida em que buscam invadir seus sistemas, a fim de para averiguar as falhas e determinar maneiras de suprir as lacunas por onde os invasores poderão atuar, aumentando a segurança das informações.

Os delitos virtuais ocorrem todos os dias, e são comuns, haja vista que quase todos os usuários estão desprotegidos contra a ação dos criminosos, necessitando implantar em suas máquinas as devidas proteções, que também não significam proteção total.

Desta forma, uma vez que os hackers atuam quase que sem ser percebidos, e sem deixar muitos vestígios, os peritos precisam estar constantemente se atualizando, tendo em vista, também, que os avanços tecnológicos na área da informática são velozes e numerosos. Para aumentar a segurança dos meios virtuais, as grandes empresas de navegação deveriam unir-se para desenvolver técnicas eficazes que possibilitassem a identificar o usuário agente criminoso.

5.3 Maneiras de identificar máquinas criminosas e a responsabilidade do provedor.

Assim como nós possuímos o R.G., os computadores possuem o I.P., capaz de identificar a máquina que está acessando a rede. São números fornecidos pelo provedor de

[94] CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet.** São Paulo: Saraiva, 2000.

acesso que possibilitam determinar o local da máquina e, dessa forma, comprovar se partiu dela os comandos da ação criminosa.

Nos casos em que o computador se conecta a uma rede particular, ao invés da rede mundial de internet, ainda será possível identificá-la através do endereço de IP. Contudo, nestas situações ele será fornecido pelo administrador da rede, mas terá a mesma eficácia probatória.

Na maioria das vezes, sempre que a máquina se conecta à rede, receberá um endereço de IP diferente, mas algumas conexões, como um Speedy especial, que depois de fornecido um número de IP este não muda mais, mesmo que o computador desconecte-se e volta a navegar mais tarde. A doutrinadora Carla Castro, em seu estudo, explica que:[95]

> Trataremos, inicialmente, da responsabilidade criminal, advertindo que a responsabilidade não é da pessoa jurídica e sim de seus representantes legais. Surge a questão: pode o provedor ser incriminado por atos dos usuários? Por exemplo, se o agente insere em uma homepage fotos de crianças em cenas pornográficas, pode o provedor ser responsabilizado?.

Assim, quanto à responsabilidade do provedor de acesso a internet, verifica-se que as pessoas de seus representantes legais é que serão responsabilizadas, ao invés da pessoa jurídica propriamente dita. Somente se poderá imaginar a responsabilidade da pessoa jurídica, ao invés de seus representantes, quando recair sobre a relação de consumo entre ele e o cliente, ainda que se trate de provedor gratuito, tendo em vista que ele recebe através de outros meios, que ainda assim o tornam oneroso.

Contudo, referida responsabilidade possui alguns limites, conforme será demonstrado, uma vez que não se trata de responsabilidade total dos atos praticados pelo usuário da rede.

O provedor de acesso não poderá ser responsabilizado pelas informações ou imagens que o usuário lança na internet, uma que são numerosos o número de clientes, bem como a quantidade de informações que são transmitidas, impossibilitando uma fiscalização mais adequada.

[95] CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais.** Rio de Janeiro: Lumen Juris, 2003.

Outro aspecto interessante é acerca da inexistência de uma norma penal que aponte a obrigatoriedade desta pessoa jurídica policiar o conteúdo presente nas comunicações, ou publicações. Logo, sem lei anterior que defina o delito, não poderá ser sancionado o provedor.

Se pensarmos na questão dos e-mails, correspondências trocadas virtualmente, abrangidas pela lei que protege a inviolabilidade das correspondências. Referida norma impede que nossas correspondências sejam abertas indiscriminadamente, protegendo assim nossa intimidade. Caso os provedores pudessem realizar uma análise sobre o conteúdo dos e-mails, estariam infringindo a norma mandamental prevista na Constituição Federal.

Ressalva-se, ainda, que é preciso proteger a liberdade de expressão. O maior meio de expressão e comunicação atual é a internet e caso os provedores de acesso restringissem as matérias que poderiam ser veiculadas pela internet estaríamos diante de uma gigantesca censura ilegal. Assim prevê a doutrina de Gustavo Corrêa:[96]

> Ou seja, além de inexistir lei acerca da responsabilidade dos provedores, existe norma constitucional que lhes proíbe o exame dos dados de seus servidores. Também, é impossível a fiscalização de todas as informações que entram e saem de um provedor, pois, além de servir seus usuários, também serve de "pista" para a Internet. Assim, um infindável número de informações, como e-mails, homepages, listas de discussões, chats, é atualizado instantaneamente por meio de procedimentos eletrônicos automáticos, sobre os quais o provedor não tem nenhum controle. Como responsabilizar alguém por aquilo a que não deu causa?. (2000, p. 100).

Nos casos em que o agente criminoso, para cometer o ilícito penal, utilize do e-mail anônimo, poderá o magistrado determinar que o prestador de serviço de correio eletrônico, como a "Hotmail", identifique o remetente, ou seja, indique o endereço daquele que escreveu a mensagem, como o usuário, podendo, ainda, tomar outras medidas ordenadas pelo Juízo criminal, de maneira que o agente seja detido, por exemplo. Da mesma forma, o autor do site será o responsável exclusivo pelas matérias que publicar na internet, sendo o provedor apenas o prestador de serviço de hospedagem, que não responderá pelos ilícitos cometidos.

[96] CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet.** São Paulo: Saraiva, 2000.

Os provedores devem adotar uma conduta de esclarecer aos usuários as responsabilidades que terão em razão das matérias que publicarem na rede, bem como pelos atos que desenvolveram, uma vez que os ilícitos cometidos, ainda que de maneira virtual, serão punidos pelo Estado, em razão de seu ordenamento jurídico.

5.4 Meios de prova/técnicas nos crimes virtuais.

Dentre os vários meios de prova, a prova pericial é de suma importância no caso dos crimes virtuais, uma vez que pode tornar certa a materialidade delitiva, bem como a autoria do crime. Perícia, portanto, trata-se do meio de prova no qual é examinada a máquina ou o meio onde o crime foi praticado, através de um profissional específico, chamado perito, possuidor do conhecimento das técnicas necessárias para a identificação necessária.

A utilização desses profissionais se deve ao fato de que o magistrado não tem o dever de deter o conhecimento nas diversas áreas do saber, distintas da área jurídica. No caso da informática e de sua perícia, o juiz deve nomear um perito, ou mesmo a autoridade policial, com o qual se determinará a ocorrência do crime ou mesmo a autoria dele, enquanto as partes poderão apenas requerê-las.

No processo penal, verifica-se dois momentos em que a prova pericial poderá ser requerida pelas partes, quais sejam a denúncia para o pólo ativo, ministério público ou ofendido, via de regra, enquanto ao pólo passivo, o réu, na defesa prévia, e, ainda, no momento do pedido de diligências para ambas as partes.

A razão pela qual apenas as autoridades judiciárias podem nomear os peritos que vão atuar nos autos, deve-se pela confiança que recai sobre o profissional, restando às partes apenas formular quesitos ou outros questionamentos necessários ao esclarecimento da prova e ao descobrimento da verdade, ou nomear assistente técnico. O laudo pericial nos crimes virtuais tem que informar o juiz, de forma detalhada, todos os aspectos do corpo de delito, em via de regra o equipamento utilizado para cometer o crime, como, por exemplo, os arquivos constantes no micro, ou mesmo o histórico de navegação da internet, dentre outros que o perito julgar necessário ou importante para a causa. Acerca do tema, Carla Castro dispõe que:[97]

[97] CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. Rio de Janeiro: Lumen Juris, 2003.

> [...] para a realização da perícia, será preciso buscar e apreender o computador, na forma do artigo 240 do CPP. A busca poderá ser determinada de ofício pela autoridade ou mediante requerimento das patês (art. 242, CPP). O mandado de busca deverá conter o local da diligência, o nome do proprietário, o motivo, os fins da diligência e a assinatura da autoridade (art. 243, CPP). Realizada a busca e apreendido o material, este será encaminhado aos peritos. Nossa lei determina que sejam dois peritos oficiais; nos locais onde não houver, duas pessoas idôneas (art. 159, CPP). (2003, p. 114).

Outrossim, a questão da admissibilidade do e-mail como prova nos crimes virtuais é de relevante importância. Em que pese a posição de alguns estudiosos de que a Carta Magna veda a violação de correspondências, conforme dispõe o artigo 5º, inciso XII, do mesmo dispositivo legal, interpretando restritivamente o artigo e classificando o e-mail apenas como correspondência, há controvérsias. Nesse sentido Michele Mori:[98]

> [...] diante do entendimento de que é inconstitucional o parágrafo único da Lei, a inviolabilidade de dados é garantia constitucional e sua interceptação não é lícita, uma vez que a Lei não poderia ter contemplado as comunicações de telemática e de informática. Desta forma, reconhecendo o direito o sigilo de dados via computador se está protegendo a intimidade das pessoas." (2003, p. 81).

Ao disciplinar a interceptação de comunicações telefônicas, Lei nº 9.296/96, o legislador infraconstitucional entendeu por bem estender a eficácia da norma também aos meios de comunicação telemáticos e de informática. Desta forma, verifica-se que o e-mail é atingido pela referida lei, o que possibilita ao juízo ou autoridade policiaria "violar" o conteúdo dessas comunicações virtuais, uma vez observadas as regras legais.

Portanto, que esta ferramenta de comunicação pode ser utilizada como meio de prova, sendo, entretanto, necessária autorização judicial, o que possibilita ser utilizado na instrução criminal para provar tanto a materialidade como a autoria delitiva.

Contudo, via de regra, o magistrado ainda poderá interceptar uma conversa via internet se preenchido os requisitos legais da Lei, qual sejam, que o crime seja punido com pena de reclusão, e se este meio de prova for indispensável ao descobrimento da verdade, não restando outra alternativa probatória. Desta forma, restringe-se o campo de crimes que podem ser abrangidos por esse meio de prova.

Entretanto, a essa regra surgem algumas exceções. Nas ações que versam sobre mérito de natureza trabalhista, contratos ou código de defesa do consumidor, não poderão utilizar o e-mail como meio de prova lícita. Assim dispõe Carla Rodigures Castro:[97]

> Problema surge na área do Direito Privado, quando se analisam contratos; direito do consumidor e os direitos trabalhistas. Nestes casos não tem aplicação a Lei nº 9.296/96. (2003, p. 119).

Verifica-se ainda, segundo o princípio da proporcionalidade que o e-mail poderá ser utilizado como prova quando o bem jurídico a ser defendido se torna maior que aquele sobre o qual versa a matéria dos autos. Nos casos de defesa do direito a liberdade ou ampla defesa, por exemplo, alguns doutrinadores entendem que, ainda fora dos casos elencados na referida lei supraconstitucional, o e-mail poderia ser utilizado como prova lícita, haja vista a proporcionalidade entre os bens que se pretende tutelar.

Nos demais casos, em que se pretenda utilizar esse meio de prova, necessária se fazem a anuência dos interessados, para evitar a violação das garantias constitucionais de privacidade das correspondências. Com isso, a valoração da prova obtida através do e-mail deve ser justa, pois hoje se trata de prova segura, já que algumas ferramentas foram criadas, como a assinatura digital e a criptografia, por exemplo, que possibilitam identificar com segurança os envolvidos.

Nossa legislação assevera, em seu artigo 157, do Código de Processo Penal, que: O juiz formará sua convicção pela livre apreciação da prova. Logo, o juiz é quem valora a prova, contudo, especificando e fundamentando sua decisão. Deverá o magistrado abster-se de valores antigos e perceber que na atualidade os meios eletrônicos evoluíram a ponto de identificar, com certeza, fatos e pessoas, uma vez que também a produção de provas no direito pátrio é livre, desde que não seja por meio defesos em lei.

[97] CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. Rio de Janeiro: Lumen Juris, 2003.

Outro meio pelo qual se pode chegar à verdade dos fatos tratados na ação penal, refere-se ao computador. Referido objeto pode ser entendido como a arma do crime, logo, nele pode estar contida todas as informações com as quais o juiz condenará o acusado.

Verifica-se, neste caso, que a obtenção das provas contidas no micro deve acontecer de forma lícita, de maneira a não contaminar o conteúdo virtual ali estabelecido. Não pode ocorrer, por exemplo, a violação ao domicílio do agente para apreender o computador, nem mesmo violar a intimidade e a privacidade para invadir a máquina e obter as informações necessárias para incriminar o investigado.

Caso isso venha a ocorrer, as provas serão classificadas como ilícitas, uma vez que terão sido obtidas por meio ilícito, que acaba por contaminar, assim, as provas, é a chamada teoria dos frutos da árvore envenenada. Ressalva-se, por fim, que a prova testemunhal também poderá ser utilizada. Ocorre que, como o agente quase sempre age sozinho e buscando o anonimato, torna-se excessivamente difícil consegui-las, pois o meio virtual possibilita a atuação do agente quase que sem ser percebido na maioria dos casos. Mesmo assim, este é um meio de prova importante que deve ser lembrado, a fim de que mais um elemento possa constituir o conjunto probatório capaz de apontar o autor do delito, mesmo porque os agentes podem destruir as informações contidas nas máquinas utilizadas no delito, e este se tornar o único meio pelo qual o dono da ação penal poderá incriminá-lo, visando uma sentença meritória condenatória.

A autora Maria Reis esclarece a importância maior da prova pericial, uma vez que os delitos virtuais quase sempre deixam vestígios e que, por isso, devem ser provados com exame por força legal. Assevera que:[98]

> Sabemos que o exame de corpo de delito nada mais é do que a comprovação pericial dos elementos objetivos do tipo, no que diz respeito, principalmente ao evento produzido pela conduta delituosa. Será direto, obviamente quando procedido por inspeção pericial, e indireto quando a prova testemunhal suprir-lhe a falta. (1997, p. 47).

Outrossim, o objetivo de provar o delito no caso concreto determinará o meio de prova mais adequada a essa demonstração. Pois as provas são determinantes para encontrar o

[98] REIS, Maria Helena Junqueira. **Computer crimes:** a criminalidade na era dos computadores. Belo Horizonte : Del Rey, 1997.

criminoso, que muitas vezes usa identidade falsa. Mesmo com as provas, há casos em que a solução não é tão simples, mas sem elas seria impossível identificar o delito e o criminoso.

CONCLUSÃO

Diante de todo o exposto, não é forçoso concluir pela extrema importância do tema proposto, ainda mais se levado em conta a época em que vivemos, denominada de "Era da Informática". Nada obstante este grau de importância, restou evidenciado que os problemas relacionados à informática e à Internet não são tratados com o devido merecimento, notadamente aqui no Brasil.

É notória a falta de legislação a respeito do assunto, embora existam algumas raríssimas exceções. Aliás, em se tratando de Internet e informática, percebe-se a carência de discussões doutrinárias quanto às questões de cunho criminal.

Estes dois fatores conduzem a uma triste realidade no processo criminal, representada pela impunidade. Diante da falta de previsões legais, sobram teses defensivas, plenamente capazes de provocar uma absolvição.

Como se não bastasse, os problemas existem antes mesmo do início do processo. A começar pela identificação dos autores dos delitos virtuais, problema que certamente atribula as Autoridades encarregadas pela investigação. Isso é resultado da ausência de tecnologia adequada a disposição das Autoridades e do elevado nível de conhecimento técnico dos hackers. Aliada à dificuldade em se produzir prova, o problema da autoria é sem dúvida o grande obstáculo para a devida responsabilização dos agentes. É incrível que todos esses problemas existem num País onde se conta mais de 5.000 decisões judiciais sobre casos envolvendo a Internet.

Se isto serve de consolo, é oportuno dizer que existem 52 projetos de Lei tratando de assuntos relacionados à Internet, a exemplo do projeto de Lei n.º 84/99, de autoria do Deputado Luiz Piauhylino. Com base nesses números, é possível que num futuro próximo novas leis surjam, sanando de vez a carência na legislação brasileira.

Não poderia deixar de registrar a seriedade do Ministério Público no combate aos crimes virtuais. Não raras vezes é noticiada alguma atitude dos seus Membros na difícil missão de responsabilizar os sujeitos ativos dos crimes virtuais.

É evidente que não só o Ministério Público tem atuado na repressão dos crimes virtuais. Órgãos como a Polícia Federal, Interpol, Congresso Nacional e Empresas de Serviço Virtual têm contribuído consideravelmente nos casos envolvendo a Rede Mundial de Computadores.

Entretanto, mesmo diante dessas circunstâncias favoráveis, o Brasil encontra-se em situação muito aquém de outros países, como por exemplo, os Estados Unidos da América. Não representa uma justificativa o fator do subdesenvolvimento, eis que os números demonstram o elevado grau de desenvolvimento do Brasil em se tratando de informática e Internet. Pelo que parece, falta dedicação aos representantes dos Poderes Legislativo e Executivo, no sentido de criar alternativas para as autoridades encarregadas pela persecução criminal.

Muito embora isso aconteça, a sociedade espera ansiosamente por algumas mudanças, a fim de serem preservados os interesses e valores sociais predominantes. Neste mesmo sentido, espera-se que a repressão aos crimes virtuais tenha proporcional progressão com o constante e infinito avanço tecnológico.

REFERÊNCIAS

OBRAS:

VADE MECUN. Obra coletiva de autor ia da Editora Saraiva com a colaboração de Antonio Luiz de Toledo Pinto. Maria Cristina Vaz dos Santos. 10 ed.atual .e ampl . São Paulo. Saraiva. 2010.p.542.

BEPPLER, Daniela. Internet e informatização: implicações no universo jurídico.

BITENCOURT, Cezar Rober to. Tratado de Di rei to Penal . Vol . 1. 8ª ed. São Paulo: Saraiva, 2003.

BOITEUX, Luciana. Crimes Informáticos: reflexões sobre política criminal inseridas no contexto internacional atual . Revista Brasileira de Ciências Criminais, v.47.Coordenador : Theodomiro Dias Netto. Edi tora: Revista dos Tribunais . Categoria: Direito Penal , 2004, p. 158.

CARNELUTTI, Francesco. O Problema da Penal, rad. De Hi tomar Martins Oliveira. Belo Horizonte. Ed. Líder.2003.p.70.

CCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2tir . São Paulo. Editora Revista dos Tribunais.2007. p.67.

ESTEFAM. André. Direito Penal ,1: Parte Geral . 4.ed. rev, e atual . São Paulo: Saraiva 2008. p.01.

FERREIRA, Érica Lourenço de Lima. INTERNET-Macrocriminal idade e Jurisdição Internacional . Curitiba. Juruá Editora, 2007.

Fundamentos y aplicación de penas y medidas de seguridad em El Código Penal de 1995.p.36.

GAMA SILVA, Remy, Cr imes da informát ica, Edi tora: CopyMarket .com, 2000.

GOMES, Luis Flávio. Princípio da Ofensividade no Direito Penal . Vol . 6, São Paulo: Revista dos Tribunais, 2002.

HASSEMER, Winfried y MUÑOZ CONDE, Francisco. Introdución a la Criminologia, pág. 226.

INELLAS, Gabriel César Zaccaria. Crimes da Internet. 1ª Edição. Editora Juarez de Oliveira, 2004, p.01.

JESUS, Damásio E.de. Direito Penal.Volume 1: Parte Geral . 30.ed. São Paulo: Saraiva 2009. p.03.

LIMA, Paulo Marco Ferreira. Crimes de Computador e Segurança Computacional .Campinas/SP. Editora Millennium, 2006.

Ministério Público Federal e Comitê Gestor da Internet no Brasii. Crimes Cibernéticos-Manual Prático de Investigação. 2006, p.03

MIRABETE, Julio Fabrine. Manual de Direito Penal , vol . 1parte geral , 24ed, ver . E atual. Até 31 de dezembro de 2009. reimpr . São Paulo. Atlas, 2007.p.04.

NUCCI , Guilherme de Souza. Manual de Direito Penal : Parte Geral : Parte Especial . 3.ed. rev.atual .e ampla2tir . São Paulo. Editora Revista dos Tribunais.2007.

QUEIROZ, Paulo. Função da Pena: Legislação versus Deslegitimação do Sistema Penal. 3 ed. Ver. E atual. São Paulo. Editora Revista dos tribunais, 2008. P. 77.

REIS, Mar ia Helena de Junqueira. Computer Crimes: A criminal idade na era dos computadores. Del Rey, Belo Horizonte, 1996, p.37

SILVA, Rita de Cássia Lopes. Direito Penal e Sistema Informático. Editora Revista dos Tribunais. São Paulo, 2003.

ARTIGOS DE INTERNET:

ARAS, Vladimir . Crimes de informática. Uma nova criminal idade. Jus Navigandi , Teresina, ano 5, n. 51, out . 2001. Disponível em: <http: / / jus2.uol .com.br /doutrina/ texto.asp?id=2250>. Acesso em: 08/10/2014.

ARAS, Vladimir . Crimes de informática. Uma nova criminal idade. Jus Navigandi , Teresina, ano 5, n. 51, out . 2001. Disponível em: <http: / / jus2.uol .com.br /doutrina/ texto.asp?id=2250>. Acesso em: 08/10/2014.

DAOUN, Alexandre Jean. Os novos crimes de informática . Jus Navigandi, Teresina, ano 4, n. 37, dez. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1827>. Acesso em: 04/10/2014.

Disponível em: http://jus.uol.com.br/revista/texto/162/o-principio-da-presuncaodeinocencia-e-sua-repercussao- infraconstitucional . Acesso em: 19/06/2014.

Disponível em: http://pt.shvoong.com/books/239170-conceito-crime: acesso em: 13/04/2014

Disponível em: http://www.resultadoconcursos.net/direito-penal-1-conceitos-emresumo-para-estudar/: Acesso em 14/05/2014.

Disponível em: http://www.uj.com.br/publicacoes/doutrinas/2146: Acesso em 14/05/2014.

Disponívelem:www.google.com.br/#hl=ptBR&q=no+brasil+como+se+puni+os+crimes+virtuais&oq=no+brasil+como+se+puni+os+crimes+virtuais&aq=f&aqi=&aql=&gs_sm=e&gs_upl=28551205561014714212127129101705183310.1.61&bav=on.2,or.r_gc.r_pw.&fp=dd888af28f656a1&biw=1366&bih=677. Acesso em: 09/10/2014.

FAGUNDES, Eduardo Mayer. Como funciona a internet? Disponível em <http: //www.efagundes.com/artigos/Como%20funciona%20a%20INTERNET.htm>. Acesso em 14/05/2014.

MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via Internet .Jus Navigandi, Teresina, ano 4, n. 37, dez. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/teto.asp?id=1828>. Acesso em: 07/10/2014.

VADE MECUN. Obra coletiva de autoria da Editora Saraiva com a colaboração de Antonio Luiz de Toledo Pinto.Maria Cristina Vaz dos Santos. 10 ed.atual .e ampl . São Paulo. Saraiva. 2010.