UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS
UNIDADE ACADÊMICA DE DIREITO
CURSO DE CIÊNCIAS JURÍDICAS E SOCIAIS

ARIADNÉE ABREU DE FRANÇA

LEGÍTIMA DEFESA DIGITAL: UMA NOVA PERSPECTIVA DO DIREITO MODERNO

SOUSA - PB
2010

ARIADNÉE ABREU DE FRANÇA

LEGÍTIMA DEFESA DIGITAL: UMA NOVA PERSPECTIVA DO DIREITO MODERNO

Monografia apresentada ao Curso de Ciências Jurídicas e Sociais do CCJS da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharela em Ciências Jurídicas e Sociais.

Orientador: Professor Dr. Iranilton Trajano da Silva

SOUSA - PB
2010

ARIADNÉE ABREU DE FRANÇA

LEGÍTIMA DEFESA DIGITAL: uma nova perspectiva do direito moderno

Data de Aprovação:____/_____/_____

Banca Examinadora

Orientador. Prof. Esp. Iranilton Trajano da Silva

Examinador interno: Prof. Msc. Márcio Flávio Lins Souto

Examinador interno: Prof. Esp. Leonardo Figueiredo de Oliveira

SOUSA – PB
2010

À minha família que com a graça de Deus forma o suporte da minha vida; especialmente, ao meu irmão Vinícius que por estar envolvido na área digital trouxe grandes reflexões sobre o tema e a minha mãe profª Lúcia Abreu pela sua visão humanista, pelo senso crítico e de justiça. Ao meu avô Luiz de França (in memorian) por acreditar no meu talento sempre. "DEDICO"

AGRADECIMENTOS

Ao meu professor orientador Prof. Esp. Iranilton Trajano da Silva pela paciência, dedicação e confiança neste projeto.

A meus familiares pela presença em todos os momentos.

A Diana Athenas, amiga de todas as horas.

"As pessoas sempre temem as mudanças. Temeram a eletricidade quando foi inventada, não foi? Temeram o carvão, temeram as máquinas a gás... Sempre haverá a ignorância, e a ignorância leva ao medo. Mas com o tempo, as pessoas acabarão aceitando seus mestres de silício." (Bill Gates).

RESUMO

Este trabalho de conclusão de curso enfoca o instituto da legítima defesa no âmbito virtual/digital. Objetiva fomentar o debate a partir da análise do tema através do referencial teórico que apresenta subsídios para um possível estabelecimento da legítima defesa digital. Procurando atender aos pressupostos didáticos, o estudo com base no método empírico indutivo, realiza *a priori* uma análise fenomenológica da realidade histórica e cultural do Direito, *a parte objecti*, e, em seguida volve atenção à estimativa da experiência jurídica tal como se encontra refletida no contexto social atual. Vivemos na contemporaneidade, a denominada III Revolução Industrial, também reputada como Revolução Tecnológica. Neste sentido, o Direito como instrumento regulador e produto cultural deverá amoldar-se as novas tendências para não se tornar obsoleto, fazendo-se mister uma reflexão iminente sobre o tema. A legítima defesa digital é uma excludente plenamente aplicável nos casos que envolvem crimes virtuais (cibercrimes), já que se trata da mesma legítima defesa *stricto sensu* que vêm definida no Código Penal Brasileiro, o qual se difere desta ultima apenas em relação ao meio (virtual/digital).

Palavras Chave: Legítima defesa digital. Crimes virtuais (Cibercrimes). Revolução tecnológica e Direito.

ABSTRACT

This work of course conclusion focuses on the institution of self-defense under virtual / digital. Aims to stimulate debate from the analysis of the topic by through theoretical reference that provides subsidies into the possible establishment of a digital self-defense. Seeking to meet the educational assumptions, the study based on empirical inductive method, achieves *a priori* a phenomenological analysis of historical and cultural reality of law, *a parte objecti*, and then,- volve attention to the estimate of legal experience as it is reflected in current social context. We live in contemporary times, the so-called III Industrial Revolution, also reputed to Technological Revolution. In this sense, the law as a regulatory tool and cultural product should be the new trends for not becoming obsolete, making it is essential to a reflection on the imminent issue. The digital self-defense is an fully applicable exclusionary in cases involving cyber crime (cybercrime), since it is the same defense that are strictly defined in the Brazilian Penal Code, which differs from the latter only in relation to the environment (virtual / digital).

Keywords: Self-defense, digital virtual Crime (Cybercrime), Technological revolution and Law.

LEGÍTIMA DEFESA DIGITAL: uma nova perspectiva do direito moderno

1 INTRODUÇÃO

O avanço tecnológico trouxe para a civilização benefício considerável. Surgem conseqüentemente novas terminologias. A tecnologia digital estabelece noções inovadoras sobre os conceitos de tempo, espaço e contato, transcendendo definições que se encontravam estáticas a um campo ilimitado de possibilidades reais de abordagem. Mas também, ampliou com a chegada das novas mídias (*internet, celular, notebooks)* as possibilidades de ação delituosa.

Devido à incidência cada vez mais freqüente de crimes digitais *(cibercrimes),* surge a preocupação no âmbito político, jurídico e social de combater de forma segura e legal as ações praticadas no âmbito virtual que refletem conseqüências nocivas no mundo real ou presencial.

Assim, considerando que a ciência jurídica nasce da realidade vivida pelas pessoas, torna-se necessário acompanhar as modificações ocorridas na sociedade. O Direito como construção cultural deve estar atento a tais transformações buscando adequar-se a elas, ou seja, o direito é elaborado pelo homem para atender as necessidades deste. O ser humano vive em constante mutação, de modo que, assim como ele, o direito também se transmuta.

Deste modo nasce a necessidade reflexiva de combater tais delitos através da adequação e aprimoramento das leis existentes, assim como da criação de novas leis quando esta atividade resultar de imperativo para atender casos específicos, criando assim, um campo próprio do direito: o Direito Digital.

A problemática fundamental reside no fato de que os crimes digitais *(cibercrimes)* devem ser reprimidos, no entanto, a legislação penal apenas indica o que não é possível fazer, deixando um leque de possibilidades que por não estarem codificadas, são legalmente permitidas.

Os Cibercriminosos justificam os seus delitos apoiados nas falsas idéias de que a internet é um ambiente livre, atuando sob a guarida do possível anonimato; e concomitantemente a impunidade persiste apoiada nas lacunas da legislação e na ausência de leis específicas.

Nesse momento, entra a importância do aplicador do direito, que deverá afastar os aparentes conflitos normativos, como também os possíveis desvirtuamentos legislativos, utilizando o melhor método hermenêutico na

subsunção da norma ao caso concreto para a busca da verdadeira justiça e da tão cultuada segurança jurídica; entretanto, para que haja maior segurança jurídica e menos prejuízos a sociedade far-se-á necessária a produção de medidas iminentes, tornando a solução condizente com a velocidade das relações sócio-tecnológicas. Mas será que a legitima defesa digital realmente pode ser aplicada? Como evitar os possíveis excessos no uso da legítima defesa digital?

A partir da pesquisa bibliográfica, o presente trabalho aprofunda esta temática por meio do método empírico indutivo conforme, a contribuição de autores como PINHEIRO (2009); GRECO(2008); CINTRA, GRINOVER E DINAMARCO (2008); CRUZ(2006); SILVA (2003) dentre outros.

Neste sentido apresenta abordagem sobre Sociedade e Tutela Jurídica; Era Digital; Direito Digital e Legitima Defesa Digital no seu desenvolvimento objetivando contribuir para a discussão da problemática e para o fomento de novos parâmetros jurídicos frente à questão.

2 SOCIEDADE E TUTELA JURÍDICA

É no âmbito da ciência do direito e da sociologia que se situa a *Epistemologia Jurídica*, traçando os limites essenciais da juridicidade, colocando em evidência a "sociedade" do *jus*. Nesse diapasão, nunca um brocardo jurídico amoldou-se tão bem à ciência do direito, quanto o que define o entendimento predominante de que não há sociedade sem direito (*ubi societas ibi jus*) e o de que do mesmo modo, não existe direito sem sociedade (*ubi jus ibi societas*). A própria dinâmica social exige que haja um sistema ordenador que tenha como função harmonizar as relações sociais intersubjetivas, compondo os conflitos que se verificam entre os seus membros; sendo o direito compreendido em seu aspecto sociológico, como um instrumento de controle social.

Na precisa lição de Cintra, Grinover e Dinamarco (2008, p.25):

> Por isso pelo aspecto sociológico o direito geralmente é apresentado como uma das formas – sem dúvida a mais importante e a mais eficaz dos tempos modernos – do chamado *controle social*, entendido como o conjunto de instrumentos de que a sociedade dispõe na sua tendência à imposição dos modelos culturais, dos ideais coletivos e dos valores que persegue, para a superação das antinomias, das tensões e dos conflitos que lhe são próprios.

A função que o direito exerce sobre a sociedade, ordenando-a de forma a organizá-la, demonstra que a tutela jurídica sempre foi e sempre será o melhor caminho para a pacificação dos conflitos sociais. Isso não quer dizer que o Direito evite e elimine os conflitos entre as pessoas, pois o mesmo, apenas trabalha para que as insatisfações se dirimam. Nesse contexto, insere-se a temática do direito à tutela jurisdicional do Estado, já que a Justiça é um bem acessível a todos, como meio de atender aos anseios dos cidadãos e interesses da sociedade caracterizando um verdadeiro direito fundamental.

O direito existe como instituto regulador da cooperação entre os indivíduos, porém, embora este seja capaz de atribuir-lhes bens, não é suficiente para evitar ou eliminar os conflitos de interesses que poderão surgir, havendo como conseqüência à insatisfação social, independentemente da pessoa ter direito ou não ao bem pretendido.

Acompanhando a evolução histórica da função jurisdicional observa-se que nas fases mais remotas e primitivas não havia um Estado suficientemente forte e

soberano para garantir o cumprimento do direito, e muito menos leis. Aquele que desejasse satisfazer a sua pretensão, o fazia de sua forma, como maneira de "vingança privada", ao qual se denomina como autotutela ou autodefesa.

Caracterizada pelo exercício das próprias razões por ter caráter nitidamente precário, aleatório e por não garantir a justiça, mas sim à vitória do mais forte, a autotutela é definida como crime, seja quando praticada pelo particular (*"exercício arbitrário das próprias razões"*, art. 345 do CPB), seja pelo próprio Estado (*"exercício arbitrário* ou *abuso de poder"*, art. 350 do CPB).

A autocomposição também foi outra maneira de resolver os conflitos nos sistemas primitivos, sendo tão antiga quanto à autotutela. Nesta forma, segundo CINTRA, GRINOVER E DINAMARCO (2008, p. 27) "os conflitos se resolviam por desistência (renúncia a pretensão), submissão (renúncia a resistência oferecida a pretensão) ou transação (concessões recíprocas)".

A autocomposição de certa maneira, sobrevive até hoje com relação aos interesses disponíveis, no entanto, todas essas soluções têm em comum a circunstância de serem parciais, no sentido de que dependem da vontade e da atividade de uma ou de ambas as partes envolvidas.

Com o passar do tempo os indivíduos acabaram constatando que o sistema parcial de solução de conflitos era falho. Atentos a necessidade de uma solução amigável e imparcial, recorreram a Arbitragem. Os árbitros eram pessoas de confiança mútua das partes. Geralmente se tratavam de sacerdotes ou anciões que decidiam conforme os costumes e padrões da sociedade.

Limitando-se a declarar a existência ou não de um direito, o cumprimento da decisão fixada através da autocomposição ou da arbitragem, naqueles tempos iniciais, continuava dependendo da imposição de solução violenta e parcial (autotutela), de modo que a ingerência do Estado ainda era repudiada.

A transição da justiça privada para a justiça pública foi se perfazendo aos poucos. O Estado passou a nomear os árbitros conseguindo que a arbitragem se tornasse obrigatória, e não mais facultativa. O Estado, deste modo, segundo SALOMÃO[1], se fortaleceu e passou a impor suas decisões e solucionar os conflitos exercendo o *jus punitionis*.

---

[1]SALOMÃO, Lídia. **Porque a sociedade não sobrevive sem a tutela jurídica?** Disponível em: <http://www.jurisway.org.br/v2/dhall.asp?id_dh=177 > acesso em: 19 de out.2010 às 21:08 horas.

Sendo assim, é através da jurisdição que o juiz age em substituição as partes, que não podem fazer justiça pelas próprias mãos, devendo estas provocar o exercício da função jurisdicional que deverá ser desenvolvida através do processo.

2.1 A Função estatal pacificadora

É através da Jurisdição que o Estado Moderno exerce o seu poder para a solução de conflitos inter-individuais. A Jurisdição caracteriza-se pela capacidade que o Estado tem, de decidir imperativamente e de impor decisões, assumindo características específicas com a finalidade pacificadora. O Estado a exerce distinguido-a das demais funções estatais (Executivo e Legislativo). Na realidade, o Estado visa no exercício da jurisdição os escopos político, social e jurídico. No entanto, o escopo social realizado através da pacificação é o objetivo magno da jurisdição.

Nesse sentido, atualmente prevalecem às idéias de *Estado Social*, em que ao Estado se reconhece a função precípua de promover a plena realização dos valores humanos. Afirma-se que o objetivo-síntese do Estado contemporâneo é o bem-comum e, quando se passa ao estudo da jurisdição, é lícito dizer que a projeção particularizada do bem comum nessa área é a pacificação com justiça, sendo o processo o meio efetivo para a realização desta função pacificadora.

Como bem exposto por Cintra, Grinover e Dinamarco (2008, p.31):

> É para a consecução dos objetivos da jurisdição e particularmente com aquele relacionado com a pacificação da justiça, que o Estado institui o sistema processual, ditando normas a respeito (direito processual), criando órgãos jurisdicionais, fazendo despesas com isso e exercendo através dele o seu poder.

No entanto, o processo é necessariamente formal, porque as formas constituem o modo pelo qual as partes têm a garantia de legalidade e imparcialidade no exercício da jurisdição, o que na realidade demanda muito tempo e provoca grandes gastos tanto para os civis quanto para o próprio Estado.

Assim sendo, surge a necessidade de garantir meios alternativos para a solução dos conflitos aos cidadãos. A primeira característica dessas vertentes alternativas é a ruptura com o formalismo processual que se apresenta a partir da

desformalização, quando se quer solucionar litígios rapidamente e de maneira eficaz, constituindo um fator de *celeridade* e de *delegalização*, caracterizada por amplas margens de liberdade nas soluções não-jurisdicionais (juízos de equidade e não juízos de direito, como no processo jurisdicional). A *gratuidade* também constitui característica alternativa marcante devido à preocupação social de levar a justiça a todos.

Com essas características presentes em maior ou menor intensidade conforme os direitos sejam disponíveis ou indisponíveis, paulatinamente são incrementados os meios alternativos de pacificação social, representados essencialmente pela conciliação, mediação e arbitramento. E, embora, a práxis judiciária demonstre ser insuficiente para atender os anseios dos cidadãos e pacificar a sociedade, ainda assim, a atividade jurisdicional prevalece como meio indispensável na solução de conflitos.

2.2 Controle jurisdicional indispensável

O Estado Democrático de Direito carrega como um de seus princípios fundamentais o da inafastabilidade da jurisdição, portanto, todos os conflitos de interesses que não sejam resolvidos espontaneamente (por acordo ou por vedação legal) deverão ser dirimidos pelo poder judiciário, conforme disposição constitucional: Art.5, XXXV: A lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito. (BRASIL, Constituição Federal Brasileira de 1988).

No entanto, com relação aos crimes digitais existe não só uma celeuma jurídica, como também divergentes entendimentos entre os especialistas em tecnologia da informação e a sociedade civil no que concerne a possibilidade de defesa das vítimas de ataques criminosos em ambientes virtuais.

Haja vista, que ao passo que crescem a quantidade de lesados que ingressam nos Tribunais Brasileiros buscando a punição dos criminosos virtuais e a diligente busca para afastar a sensação de vulnerabilidade nos meios eletrônicos, também surge teorias que explicam a defesa digital sem a interferência direta do órgão jurisdicional estatal, ou seja, a tendência atual resume-se na troca da burocratização e da falta de celeridade dos tribunais, por uma solução legalmente palpável no que concerne a adaptação e prática de institutos já consagrados pelo Direito a estes casos em comento.

Assim, a fim de demonstrar a aplicação das três teses mais discutidas dentre os posicionamentos defendidos pelos especialistas como BLUM, JIMENE, ATHENIENSE e PINHEIRO (2009); se faz mister supor que um Banco (Ex: Banco do Brasil) teve seus sistemas eletrônicos invadidos ilicitamente, tendo seus dados sigilosos "furtados" (Ex.: senhas de clientes e demais dados bancários) por um *cracker*. Ao constatar-se vítima de referido crime, o Banco aciona o departamento de Tecnologia da Informação – TI, que localiza o criminoso digital através dos indícios deixados e invade seus sistemas a fim de trazer de volta os dados que pertenciam à rede bancária.

Sob a análise do senso comum, a conduta acima descrita seria tão somente a prática da justiça, de forma que a vítima ao invadir o sistema do *cracker* para recuperar os seus dados, independentemente de autorização judicial para tanto, estaria utilizando de justiça própria para satisfazer a sua pretensão Portanto, *a priori*, o problema seria solucionado com base na primeira tese: a autotutela.

Contudo, sob o aspecto legal, considerando-se a possibilidade de responsabilização, a questão não é tão simples assim, ademais a autotutela só é permitida em raríssimas exceções devidamente expressas na legislação brasileira, como por exemplo, o art. 1.210, § 1º do Código Civil (BRASIL, Lei nº 10.406, de 10 de janeiro de 2002), que trata da manutenção ou restituição da posse turbada pela própria força do proprietário. Desta feita, estaria vedada a autotutela evitando assim, o exercício arbitrário das próprias razões, já que tal atitude, quando não prevista legalmente, consubstancia-se num crime contra a administração da justiça, como assim dispõe os artigos 345 e 346 do Código Penal Brasileiro:

> Art. 345 - Fazer justiça pelas próprias mãos, para satisfazer pretensão, embora legítima, salvo quando a lei o permite: Pena - detenção, de quinze dias a um mês, ou multa, além da pena correspondente à violência. [...]
> Art. 346 - Tirar, suprimir, destruir ou danificar coisa própria, que se acha em poder de terceiro por determinação judicial ou convenção: Pena - detenção, de seis meses a dois anos, e multa.[2]

Na segunda tese apresentada pelos especialistas, a defesa se caracteriza pela inexigibilidade de conduta diversa, que consiste na possibilidade de permitir que a vítima, nas circunstâncias em que ocorreu o fato, tivesse comportamento diferente

[2]ANGHER, Anne Joyce (Organização). **Vade Mecum Acadêmico de Direito – Coleção de Leis Rideel**. 9. Ed. São Paulo: Rideel, 2009. Pag. 371

que o permitido pela norma, agindo em desacordo com a lei. No entanto, no contexto de um Estado Democrático de Direito, as atitudes devem estar vinculadas a lei, evitando de tal modo a insegurança jurídica. Assim, esta não seria a solução mais favorável para o caso em tela, como lembra Blum e Jimene:

> Entretanto essa esteira de raciocínio é fundamentada no conceito de causa supralegal de exclusão de culpabilidade, ou seja, não há previsão em lei, mas pode ser aceita com base nos entendimentos dos doutrinadores, porém é um dos temas mais tensos dentro da dogmática penal. [3]

Por fim, apresenta-se a hipótese da legítima defesa digital como tese jurídica que justificaria o procedimento de invasão do Banco ao computador do *cracker*. Neste caso, a questão se encontra em âmbito digital e embora a sociedade disponha de todo ordenamento jurídico que devidamente acionado poderia impedir a utilização de tais dados; esta intervenção dificilmente seria realizada em tempo hábil para evitar maiores danos devido à carência do aparato judicial e de profissionais tecnicamente preparados para o atendimento de tais crimes.

Sendo assim, a teoria da legítima defesa digital parece ser a mais pertinente no que concerne a possibilidade de defesa em ambiente digital, sendo indispensável o controle exercido pela jurisdição, tendo em vista que a legítima defesa possibilita que haja apuração de provas e demais informações para que seja realizada a queixa ou a denuncia ao órgão jurisdicional, além de evitar maiores danos devido à procrastinação da atuação estatal, já que em alta velocidade as informações são contrabandeadas, podendo o manuseio indevido destas, causar graves danos não só a pessoa física ou jurídica, vítimas do golpe, como em última análise, a sociedade como um todo.

---

[3]BLUM, Renato Opice; JIMENE, Camilla do Vale. **A nova polêmica da era digital: vítimas ou criminosos nos meios eletrônicos?Jus Navigandi**, Teresina, ano 10, n. 1126, 1 ago. 2006. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=8730>. Acesso em: 29 set. 2010 às 20:00h.

3 ERA DIGITAL: EVOLUÇÃO HISTÓRICA DA INFORMATICA

Ao longo da história das civilizações verifica-se uma constante preocupação das mesmas em manter os registros sobre suas vidas, seja em paredes de cavernas ou em entalhes de madeira, dentre outros objetos. Uma das dificuldades da era primitiva residia no fator comunicação, porém, o que era antes realizado por gestos ou desenhos passou a ser expresso por sinais gráficos que deram origem a escrita. Entretanto, a dificuldade mais extremada residia na formulação de cálculos matemáticos e foi justamente esta que impulsionou todo o avanço tecnológico, na área da informática.

A história do desenvolvimento da informática se iniciou, realmente, a partir do conceito de armazenamento de informações, caminhando lado a lado com o desejo humano de realizar tarefas repetitivas e complexas. O ábaco foi o primeiro objeto destinado a este fim, sendo criado à pelo menos 3.500 a.c no Egito e permanecendo até o século XVII, pois apesar de ser um dispositivo manual, até então nenhum outro instrumento de cálculo o havia superado.

Em 1642, o matemático francês Blaise Pascal criou a Pascalina, primeira maquina automática de calcular. Logo em seguida registra-se alguns avanços isolados, dentre eles a criação de um tear automatizado e programado por uma série de cartões perfurados desenvolvidos em 1804 por Joseph Marie Jacquard; a máquina analítica projetada por Charles Babbage; o tabulador desenvolvido pelo americano Herman Hollerith para processar os dados do censo de 1890 nos Estados Unidos e o analisador diferencial aperfeiçoado pelo estudante norte-americano Claude Shannon, através da lógica binária, o que viria ser a base para a teoria da informação.

Mas, BARBUTO, OLIVEIRA E MONTEIRO (2002, p. 18) afirmam que "o impulso no desenvolvimento tecnológico aconteceu durante a Segunda Guerra Mundial (1939 -1945), acelerando o processo de criação de computadores para garantir o interesse bélico dos países envolvidos, com a criação dos computadores Z_3 pela Alemanha nazista e do *Colossus* pela Inglaterra".

Apesar do impulso forçado na fabricação de computadores e na área de processamento de dados com o objetivo de decifrar as mensagens codificadas pelas nações inimigas e calcular a trajetória dos mísseis, até então, o computador

pertencia à esfera de utilização exclusiva para pesquisa científica e não havia problemas decorrentes do seu uso ilícito, como assevera Silva (2003, p. 19):

> Durante toda a busca tecnológica de um equipamento que facilitasse os cálculos matemáticos, não houve notícia de que o homem tivesse agido de forma a lesionar ou pôr em perigo de lesão qualquer bem jurídico na utilização desses equipamentos em evolução. Vale dizer, que as máquinas construídas não foram utilizadas como meios para qualquer prática delitiva, mesmo porque eram de uso exclusivo de pesquisadores que tinham como meta única o aperfeiçoamento dos equipamentos e a obtenção de resultados rápidos e confiáveis que viessem a facilitar o trabalho dos pensadores.

Sendo assim, os problemas decorrentes do uso ilícito do equipamento eletrônico só vieram surgir a partir do momento em que este passou a ser manuseado por civis, saindo da esfera da pesquisa científica e do arsenal bélico para abranger também o cotidiano das populações.

Atualmente é difícil imaginar a separação entre o *peopleware,* o *hardware* e o *software,* pois estes três elementos formam a trindade tecnológica contemporânea, de modo que no sistema cibernético nenhuma atividade poderá se concretizar sem que haja a participação do homem, da máquina e do programa.

Em qualquer lugar do mundo é possível o acesso a tecnologia digital, seja através da TV interativa; do rádio, através do nosso computador pessoal; do celular para verificar o correio eletrônico e etc. Os equipamentos eletrônicos nos mantém conectados não só com as pessoas e situações mais próximas, como também com aquilo que acontece no mundo. A tecnologia passou a assumir papel essencial na vida moderna.

Para PIMENTEL (2000, p. 21) o computador "é uma máquina eletrônica composta de elementos físicos e lógicos, capaz de efetuar, em linguagem natural, uma notável multiplicidade de tarefas unindo os pressupostos da velocidade aos da precisão operacional". Os computadores de primeira geração eram baseados em tecnologias de válvulas eletrônicas. Esta geração vai de 1942/1951 até 1959. Segundo BARBUTO, OLIVEIRA e MONTEIRO (2002, p. 41) estes computadores "comparados com os atuais, eram modelos extremamente caros, grandes e complicados, com uma irrisória capacidade de processamento". Foram lançados nesta época o Mark I (1943), o ENIAC (1945), o EDVAC (1949), o UNIVAC I (1951) e o IBM 650 (1954).

Na precisa lição de SILVA (2003, p.18) "no final dos anos 50, a segunda geração de computadores apresenta os transistores em substituição às válvulas", sendo esta tecnologia usada de 1959 até 1965, já que neste período, o computador que até então era de uso científico-militar passa também a ser utilizado por civis. Consumia menos energia, era mais rápido e mais confiável. Os computadores da segunda geração calculavam em microssegundos, tendo como seu representante clássico o IBM 1401 e seu sucessor o IBM 7094, já totalmente transistorizado. Segundo SILVA[4], em um de seus artigos na internet este afirma que "entre os modelos 1401 e 7094, a IBM vendeu mais de 10.000 computadores".

Em meados da década de 60 surge a terceira geração, que perdurou de 1965 até 1980 e tem como característica a substituição dos transistores pela tecnologia de circuitos integrados. Os circuitos integrados nada mais eram do que um conjunto de transistores, resistores, diodos e de outros componentes eletrônicos miniaturizados e montados num único chip. Na medida em que, constatou-se uma considerável redução nos custos da fabricação do computador, as empresas de médio porte, os centros de pesquisa e as universidades menores puderam ter acesso ao equipamento. É neste período que surgem os microcomputadores.

A quarta geração acontece a partir de 1980, indo até 1990, e é caracterizada pela maior capacidade de armazenamento, rapidez e precisão no desenvolvimento do processamento de dados. Nesta década ocorreu o advento dos microprocessadores e dos microcomputadores, a partir do desenvolvimento da tecnologia de circuitos integrados em escalas superiores de integração. O uso dessa tecnologia foi responsável por cunhar o conceito de "*PC*", ou "*Personal Computer*" (Computador Pessoal) massificando o uso destas máquinas.

A quinta geração de computadores apresenta como marco inicial o ano de 1990 perdurando até os dias atuais. A principal característica desta geração são os avanços em termos de *hardware, software* e telecomunicações baseando-se, conforme KANAAN (1998, p.31) na "simplificação e miniaturização do computador, além de possibilitar a obtenção de recursos ilimitados". Basicamente esta geração

---

[4]SILVA, Marcelo Pereira. **Arquitetura de computadores.** Disponível em: < http://webcache.googleusercontent.com/search?q=cache:GsZqiviY3AJ:www.pcbrain.eti.br/cep/1ano/arquitetura/ARQUITETURA_DE_COMPUTADORES.doc+Entre+os+modelos+1401+e+7094,+a+IBM+vendeu+mais+de+10.000+computadores.&cd=26&hl=pt-BR&ct=clnk&gl=br> Acesso em: 19 de out de 2010 as 23:45 horas.

refere-se aos computadores modernos e a evolução cada vez mais rápida da informática. Percebe-se, pois, que com o avanço científico, o poder de cálculo avança de maneira que não se encontra paralelo na história humana, barateando os custos e tornando acessíveis os computadores às pessoas de baixa renda.

3.1 Internet – O fruto da revolução social, econômica e jurídica da contemporaneidade.

É notável o quanto os computadores evoluíram nos últimos anos, tanto interna quanto externamente, e em ultima análise como a informática se desenvolveu estando sua evolução atrelada à forma de melhorar a capacidade de uso e de armazenagem de dados. Não é difícil denotar que o fruto mais precioso advindo da evolução computacional é a internet.

Segundo BARBUTO, OLIVEIRA e MONTEIRO (2002, p. 31) "a internet nasceu na década de 1970, como resultado de um projeto do Ministério da Defesa norte-americana, que pretendia desenvolver uma rede de computadores que conseguisse resistir a um ataque atômico da União Soviética. Em 1985, essa rede chamada Arpanet, já interligava centenas de universidades e centros de pesquisa dos Estados Unidos, além de alguns no exterior, tendo sido, então, transformada no que é a Internet de hoje e ganhando o mundo exponencialmente".

A *Advanced Research Projects Agency* (Arpa) do departamento de Defesa Americana patrocinou a experiência de conectar computadores em todo o país, não só para manter a comunicação diante de um ataque inimigo como para melhorar a capacidade de uso e armazenagem de dados em outra esfera que não fosse a militar. Paralelamente, a pesquisa científica adaptou a rede de cunho militar as necessidades gerais da sociedade utilizando inicialmente como laboratório quatro universidades: Universidade da Califórnia em Los Angeles; Universidade de Santa Bárbara; Universidade de Utah e Instituto de Pesquisa de Stanford.

Os pesquisadores desenvolveram uma rede de comunicações sem um comando central, onde todos os pontos se equivaliam utilizando apenas uma placa modem interligada ao sistema telefônico. Este padrão tornou-se a base para o princípio de neutralização da rede afirmando que a Internet não tem proprietário, sendo, pois, comum a toda a sociedade global.

Conforme Silva (2003, p. 32):

> Não há um único centro que governa ou mesmo gerencia a Internet. As redes constituintes pertencem a alguma organização, mas ela não é de ninguém. Quando se fala em decisões sobre a internet, sendo estas apenas em padrões tecnológicos, elas são de responsabilidade de órgãos como a Internet Numbers Authority, a Internet Engineering Task Force e a Isoc, que é uma organização de membros voluntários conhecida como Internet Society, tendo como membro qualquer pessoa ou organização que apresentar interesse em aderir a ela.

Esse caráter de neutralidade, contudo, acarreta um sério problema de segurança. Por não haver um controle sobre o tráfego global prolifera-se a atividade criminosa na rede. Os "piratas da rede" acreditam que a Internet é um ambiente totalmente livre e se apóiam nesta falácia para cometer os seus crimes. A pretensa impunidade que lhes dá guarida também é questionada do ponto de vista técnico na medida em que o protocolo IP dos computadores indica quem é o usuário e em que localidade o mesmo tem acessado, além dos provedores de acesso que também guardam as informações relativas aos seus usuários.

No entanto, o princípio da neutralidade da rede atualmente vem sendo questionado não só devido a sua, *in thesis,* periculosidade, mas principalmente devido à lucratividade que pode ser gerada por intermédio do abrandamento ou até mesmo da superação deste princípio nas relações jurídicas que envolvam a Internet. A própria tendência histórica dos meios de comunicação mostra-nos que em princípio estes meios eram gratuitos e livres para apropriação, passando a assumir natureza onerosa, permitindo-se a concessão de uso e até mesmo a privatização.

De fato, a neutralidade da rede contribui para que seja ampliada a sua característica fundamental: a Universalidade. O avanço tecnológico na comunicação sempre perseguiu o objetivo de estabelecer uma "aldeia global", o que é totalmente possível na era das redes devido à ampliação do poder do indivíduo, que se vê capacitado desde cedo, por meio da tecnologia a estar em qualquer lugar, a qualquer tempo. Um exemplo disso são as crianças e adolescentes que podem jogar *RPGs online (Role-playing game)* de maneira interativa com outros jovens "RPGistas" de cidades, estados e até países diferentes do seu.

Analisando o aspecto sociológico da Internet, observa-se sua importância enquanto meio de integração social, trazendo inovações significativas nas formas de relacionamento entre as pessoas. Através da Internet o elo entre os indivíduos

passa a ser mais dinâmico e acessível mesmo em face da amplitude mundial. Neste contexto, apresentam-se as comunidades *online* de amigos ou comunidades virtuais, *blogs, fotologs, orkut, facebook, twitter,* dentre outros. Porém, ao passo em que se constata o progresso na comunicação mundial, também se visualiza a crescente onda de criminalidade que se prolifera no ambiente virtual, como afirma Pinheiro (2009, p. 255);

> É comum os usuários terem a falsa impressão de que somos completamente livres quando estamos *online*, e que a nossa conduta neste ambiente não é alcançada pela lei, ou seja, acham que o virtual não pode se tornar real. Pensam ainda que estão totalmente anônimos. Assim, falsidade ideológica, calúnia, difamação injúria, racismo, ameaça, violação de direito autoral, divulgação de segredo, violação de segredo profissional, tráfico de drogas, apologia ao crime ou criminoso e formação de quadrilha ou bando são apenas alguns exemplos de crimes livremente praticados nos *websites*.

Quanto ao aspecto econômico, a Internet abre-se como um mundo de possibilidades empresariais, onde a publicidade tem seu papel primordial. A abordagem direta da publicidade, ou seja, a divulgação do produto, serviço ou marca sem intervalos ou rodeios, faz com que a Internet seja um meio de comunicação bastante rentável para os empresários. O *e-business*, acrônimo do inglês *Electronic Business* (negócio eletrônico), é o termo que se utiliza para identificar os negócios efetuados por meios eletrônicos, geralmente na Internet, sendo muitas vezes associado ao termo comércio eletrônico.

Como conseqüência dessa difusão publicitária em massa, o comércio é ampliado e a transação comercial ganha nova nomenclatura dependendo do veículo de comunicação em que é transacionada, ou seja, de um computador (*e-commerce),* de um celular ou dispositivo de comunicação móvel (*m-commerce*), ou do aparelho de televisão (*t-commerce*). No entanto, PINHEIRO (2009, p. 69) preleciona que as transações de comércio eletrônico não diferem das relações econômicas que ocorrem no mundo real, de modo que os consumidores também estão resguardados pelo Código de Defesa do Consumidor – CDC (Lei nº 8.078/90), exceto quando não se tratar de relação com consumidor final, mas sim, de relação comercial entre empresas, mas conhecida como B2B (*Business- to-Business*).

Por derradeiro, apesar dos especialistas em Tecnologia da Informação como em Ciências Jurídicas afirmarem que a rede mundial de computadores está sujeita

as normas de Direito, seja este internacional ou nacional, os leigos e os criminosos ainda insistem em negar este aspecto jurídico da rede. Vivemos num Estado Democrático de Direito e por estarmos sujeitos a ordem jurisdicional em nossas relações intersubjetivas, temos que a Internet não se exclui desta regra, justamente por ser um campo fértil onde brotam tais relações, inobstante os *cibercrimonosos* se apõem na falsa idéia de impunidade existente na rede e na carência legislativa para difundir a idéia da "terra de ninguém". Porém, a situação não é tão simples assim.

Conforme Cruz (2006, p. 42):

> [...] Nem todas as condutas abusivas realizadas pelos meios informáticos são merecedoras de uma nova qualificação penal, na medida em que podem ser abrangidas pelos delitos tradicionais. Isso ocorre, por exemplo, quando a utilização do elemento informático não muda em nada a essência da conduta criminosa descrita na legislação. Mas essa adequação ou, melhor dizendo, interpretação da lei traz o risco de violar garantias penais e constitucionais, incorrendo em uma analogia proibida em Direito Penal – analogia contra o réu. Ademais, como dissemos isso também pode acarretar uma flagrante violação do princípio da legalidade, uma vez que estariam sendo criminalizadas condutas ainda não tipificadas na legislação.

O fato é que uma pesquisa bem recente com mais de 27 mil adultos em 26 países mostra que a grande maioria das pessoas acredita que o acesso à internet deve ser considerado um direito humano básico. Através deste estudo podemos atestar a necessidade de se ampliar o horizonte dos direitos fundamentais, dado o caráter dinâmico e mutante da ciência jurídica na mesma proporção da complexidade social e científica, como expõe Nátaly Dauer:

> De acordo com uma pesquisa conduzida pela empresa *GlobeScan* para a *BBC World Service*, no Reino Unido, 4 em cada 5 pessoas no mundo acham que a internet deveria ser um direito dos cidadãos. O estudo está relacionado à implementação da Lei de Economia Digital (*"Digital Economy Bill"*), do governo britânico [...] As maiores preocupações demonstradas pelos entrevistados foram o fácil acesso a conteúdo explícito e de violência (36% de respostas brasileiras) e perigos de fraude (35%). Os resultados mundiais também apontam medo em relação à privacidade dos usuários.[5]

Assim sendo, deve-se ressaltar o fim precípuo da Internet, qual seja, o desenvolvimento humano em suas relações intersubjetivas a nível mundial,

---

[5]DAUER, Nátaly. **Quatro em cinco pessoas acreditam que acesso à internet é um direito humano.** Disponível em: http://www.geek.com.br/blogs/832697706/posts/12441-quatro-em-cinco-pessoas-acreditam-que-acesso-a-internet-e-um-direito-humano. Acesso em: 09 de abril de 2010 às 13:15 horas.

possibilitando maior interação entre os indivíduos. E por ser considerada a invenção mais brilhante da era globalizada, por proporcionar desenvolvimento econômico, social, cultura e científico mundial merece especial atenção, já que os seus efeitos ganham destaque na atualidade cada vez mais, devendo inclusive, ser regulamentada por um direito próprio, ou seja, o Direito Digital.

3.2 Sistemas de Informação – A virtualização da informação

No decorrer da evolução histórica percebe-se que diversos bens foram considerados preciosos de acordo com a época vivenciada. Na sociedade feudal, o bem mais valioso era a terra, na sociedade industrial capitalista os bens mais preciosos eram as máquinas e o dinheiro, na atualidade constatamos que na sociedade digital o bem mais valioso é a informação.

Conforme Silva (2003, p. 27);

> A informação é importante para a atualidade, refletindo diretamente na capacidade das sociedades de se sobreporem às outras, estabelecendo uma hierarquia de poder: quanto maior o grau de informação e as melhorias nas condições tecnológicas para a sua obtenção, maior o poder desta sociedade em relação às outras que não gozam deste mesmo privilégio.

Nesse sentido, a informação passou a ser um elemento relevante na construção social, devido a sua capacidade em influenciar as ações humanas e não tão somente estas, como também as ações dos computadores, já que os mesmo só realizam as tarefas que lhes são atribuídas através das informações constates nos dados. A partir desta realidade, concluí-se que o dado é apenas uma informação que deverá ser considerada, processada, operada e transmitida por um sistema de computador ou programa de computador para a consecução de um determinado fim.

A palavra informação deriva do latim *informare,* que significa "dar forma". WIENER (1993, p.17) expõe que o termo informação assim designa:

> O conteúdo daquilo que permutamos com o mundo exterior ao ajustar-nos a ele, e que faz com que nosso ajustamento seja nele percebido. O processo de receber e de utilizar informações é o processo de nossos ajustes as contingências do meio ambiente e de nosso efetivo viver nesse ambiente.

O computador compõe-se de uma parte física que é o processador, memória, dispositivos de entrada, saída e armazenagem em disco. Este grupo de componentes chama-se *hardware* e é absolutamente dependente do *software que* por sua vez é composto por programas que permitem atender às necessidades dos usuários dando vida aos primeiros. (SILVA, 2003, p.32). No entanto, entende-se por sistema de Informação um conjunto de componentes inter-relacionados, trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir informação com a finalidade de facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório em empresas e outras organizações. (LAUDON, 1999, p.4).

Com o sistema informático a linguagem passou a ser artificial, a matemática e a eletrônica compõem um fenômeno de metalinguagem realizado pelas máquinas. A fusão entre a informação e automação proporcionou a virtualização da informação, possibilitando o tratamento racional e automático da linguagem através da transformação do que é materialmente palpável em objetos virtuais, promovendo a mutação do átomo em *Binary Digit – Bits* (Dígito Binário). O *Bit* é a menor unidade de informação que pode ser armazenada ou transmitida na computação ou na teoria da informação, apresentando apenas 2 (dois) valores para cada dígito, qual sejam 0 (zero) ou 1 (um), que deverão representar duas proposições antagônicas, por exemplo: verdadeiro ou falso, positivo ou negativo, aberto ou fechado, dentre outras infinidades de proposições. Embora os computadores tenham instruções (ou comandos) que possam testar e manipular *bits*, geralmente são idealizados para armazenar instruções em múltiplos de *bits*, chamados *bytes*.

Desta feita, toda e qualquer informação que for armazenada no computador deverá ser transcrita para essa linguagem, de modo que, se pegarmos a palavra JUSTIÇA (em letras maiúsculas) teríamos a seguinte representação: J=01000011; U=01001111; S=01001110; T=01010100; I=01010010; Ç=01000001 e A=01010100. Assim sendo, para cada letra na memória do computador temos a sequência de 8(oito) *bits,* que ao final formaram a palavra JUSTIÇA, ficando bem claro que se as letras estivessem minúsculas ter-se-ia outra representação traduzindo o fenômeno da digitalização da informação exposto por Silva (2003, p. 39);

> Digitalizar uma informação é traduzir sua mensagem em código, o que equivale dizer que o suporte armazenado não conterá texto legível pelo homem, mas códigos que, ao serem traduzidos e apresentados pelo equipamento eletrônico, exibirão, em tela, uma reserva potencial.

Diante disso, percebe-se que tudo o que é tido no mundo físico como uma "coisa" tangível e material, pode ser idealizado no mundo virtual, passando a ser uma "coisa" intangível e imaterial sem perder o seu valor agregado. Tomemos como exemplo a cifra constante na tela do caixa eletrônico que traduz uma realidade intangível para o cliente, no entanto, você sabe que ali está apenas a representação do valor numérico expresso em dinheiro, ou seja, é apenas a representação ideal das cédulas de dinheiro. Nesse sentido, o dinheiro que antes era apenas palpável passou a ser expresso também em *bits/bytes* e não tão somente em cédulas de papel, pois, naquela mensagem eletrônica está expresso o valor do crédito do cliente da agência bancária.

Assim sendo, o computador potencializa a informação individualizando-a para cada operador da máquina. Atualizando e virtualizando a mensagem de forma particular, transcende-se às barreiras físicas para possibilitar um maior alcance da experiência humana. A estrutura material das "coisas" se modifica para que estas componham o mundo virtual, o que de fato não as tornam irreais, necessitando tão somente da atualização para serem utilizadas no mundo físico.

4 DIREITO DIGITAL: ADEQUAÇÃO DO DIREITO À TECNOLOGIA DA ERA DAS REDES.

A sociedade digital provocou grandes reflexões sobre a dogmática jurídica contemporânea, já que passamos a viver sobre a influência de dois universos paralelos: o mundo virtual e o mundo real. As limitações agora são outras. O tempo e o espaço já não são fatores limitadores da conduta humana, mas ainda o são a ética, a moral e o direito, de modo que, este último não pode se tornar obsoleto em meio a tantas mudanças comportamentais. Neste contexto, surgem também novos institutos e elementos em todos os ramos do direito, seja ele civil, constitucional, financeiro, tributário ou comercial.

Entretanto, existem peculiaridades da internet e do computador que devem ser contempladas pelo Direito Digital, que não chega a ser um novo ramo do Direito propriamente dito, mas um conjunto de leis especializadas nesta temática. O Direito digital consiste na evolução do próprio direito, abrangendo os princípios fundamentais vigentes e estabelecendo novos princípios norteadores da atividade em ambiente virtual. Numa sociedade globalizada e convergente o Direito Digital surge como uma ciência que possui princípios e institutos próprios que deverão ser aplicados a lógica jurídica para possibilitar soluções necessárias ao meio virtual, preenchendo as lacunas legais existentes neste ambiente.

Neste sentido, Pinheiro (2009, p. 30) preleciona:

> O que propomos aqui, portanto, não é a criação de uma infinidade de leis próprias – como vimos, tal legislação seria limitada no tempo (vigência) e no espaço (territorialidade), dois conceitos que ganham outra dimensão em uma sociedade convergente. A proposta é que o Direito siga sua vocação de refletir as grandes mudanças culturais e comportamentais vividas pela sociedade. No Direito Digital prevalecem os princípios em relação às regras, pois o ritmo de evolução tecnológica será sempre mais veloz que o da atividade legislativa. Por isso, a disciplina jurídica tende à auto-regulamentação, pela qual o conjunto de regras é criado pelos próprios participantes diretos do assunto em questão, com soluções práticas que atendem ao dinamismo que as relações de Direito Digital exigem.

A internet é um meio de comunicação semelhante aos outros, embora seja um pouco mais abrangente. Do mesmo modo que inexiste um Direito da Televisão ou do rádio, inexiste um Direito da Internet. No entanto, existe um Direito para a televisão e para o rádio, assim como para a internet, sendo este último caracterizado

pela prevalência dos princípios sobre as normas devido à velocidade em que as relações em ambiente virtual se perfazem.

4.1 Crimes informáticos (*Cibercrimes*)

O sistema informático, como fruto da revolução tecnológica, vem provocando inúmeras indagações no campo jurídico, principalmente no que diz respeito ao Direito Penal, porém, haja vista que surgem divergências doutrinárias quanto à nomenclatura, o crime eletrônico é sinônimo de crime virtual, de crime digital, de delito informático e de crime informático.

São altos os índices de pedofilia, espionagem, fraude, estelionato, extorsão, entre outros crimes, o que nos leva a constatação de que a maioria dos crimes cometidos em ambiente virtual são condutas já tipificadas no mundo real, apresentando modalidades distintas dependendo do bem jurídico tutelado. A internet tem sido vista como um campo fértil para a proliferação da marginalidade digital devido à facilidade e principalmente a noção errônea de anonimato.

Conforme Pinheiro (2009, p. 226):

> A internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital se referem a territorialidade e a investigação probatória, bem como a necessidade de tipificação de algumas modalidades que, em razão de suas peculiaridades merecem ter um tipo penal próprio.

A especialização do tema é evidente quando se trata do aspecto criminológico em sistemas teóricos e operacionalmente complexos. De modo que, muitas vezes os usuários assumem a postura de vítimas potenciais devido a pouca formação intelectual ou falta de habilidade com a máquina. Tal fator gera certa apreensão social, econômica e política por evidenciar as vulnerabilidades e armadilhas encontradas no mundo virtual. A complexidade dos sistemas informatizados é apontada como um dos fatores que provocam a insegurança nos ambientes virtuais, porém, a insegurança não constitui um óbice para que as pessoas interajam neste ambiente.

Como afirma Martini (2008, p.152);

> Portanto, temos que aceitar que todo *framework* de nossos sistemas, que são baseados num modelo de segurança flexível, granular e dinâmico, irá terminar num usuário que está invariavelmente numa plataforma computacional insegura. Mas tal assertiva não deve ser vista como uma declaração pessimista. O uso da Internet no Brasil não vai esperar messianicamente por um modelo perfeito de tal plataforma. Em suma, o comércio eletrônico, por exemplo, não irá esperar por clientes com plataformas ótimas em segurança, ou usuários altamente treinados.

Seguindo as diretrizes traçadas pela existência de regras no próprio "jogo", teríamos um mecanismo de autoajuda virtual disposto diretamente na tela do computador e visível nos sites para navegação. Esta seria uma ótima alternativa para educar e conscientizar os usuários. Uma proposta bastante oportuna, para solucionar tais problemas, principalmente no que concernem as relações consumeiristas seria a publicação de "normas digitais", no formato *disclaimers,* ou seja, um aviso legal ou termo de responsabilidade encontrado comumente em mensagens eletrônicas e páginas da Web, que informam ao leitor de um determinado documento ou usuário de um determinado serviço quais serão as responsabilidades assumidas ou, normalmente, não assumidas pelo autor deste documento ou por quem oferece o serviço. (PINHEIRO, 2009)

Ressalte-se que, não devemos confundir os erros humanos e falhas técnicas eventuais com a atividade com fim delituoso, pois, é evidente o total despreparo da policia investigativa e da perícia para apurar estes crimes. Neste caso, a problemática maior seria a descrença da sociedade não só na apuração e punição destes *cibercrimes* como também nos delitos em geral, culminando na ausência de denúncias e consequente dificuldade em traçar um perfil real sobre criminosos, vítimas e crimes mais frequentes.

Hoje já é possível fazer um Boletim de Ocorrência *(BO)* pela internet. No Estado da Paraíba o Boletim de Ocorrência *(BO)* [6] disponibilizado pela Delegacia *Online* da Policia Civil pode ser utilizado para registrar furtos, extravio de documentos ou objetos e também para registrar o desaparecimento de pessoas, somente sendo registrados os casos em que não houve violência de qualquer natureza. No entanto, são poucas as equipes de profissionais preparados para a investigação dos casos de delinqüência informática, ou seja, daqueles crimes que

[6]Delegacia *Online* do Estado da Paraíba – Boletim de Ocorrência: http://beo.ssp.pb.gov.br/beo/

ocorrem em sistemas informáticos ou que utilizam o meio virtual para a consecução do intento criminoso.

Deste modo, segundo PINHEIRO (2009, p.230) "o Direito Digital traz a obrigação de atualização tecnológica não só para advogados e juízes, como para delegados, procuradores, investigadores, peritos e todos os demais participantes do processo. Tal mudança de postura é necessária para que possamos ter uma sociedade digital segura; caso contrário, coloca-se em risco o próprio ordenamento jurídico," já que assim como os civis e as empresas, os criminosos aderiram às facilidades e maravilhas do mundo digital e principalmente da Internet, concorrendo para a proliferação vertiginosa da marginalidade neste ambiente.

4.2 Delinquentes informáticos (*Cibercriminosos*)

No submundo da Internet encontra-se um tipo de crime cujo traço cultural se aproxima do vandalismo, onde os atores principais são intitulados como *hackers*, sendo até mesmo denominado por alguns doutrinadores como subcultura *ciberpunk.* Nesse diapasão, compreende-se que para desvendar este universo se faz necessário analisar e entender como funciona a mente dos que estão escondidos atrás das telas dos computadores para praticar condutas delituosas.

Vários especialistas em psicologia forense tentaram classificar estes criminosos virtuais, seja usando o critério do nível técnico empregado, da atividade desempenhada ou pela motivação, embora, esta classificação muitas vezes torne-se imprecisa devido à abrangência e magnitude destes delitos.

A princípio apresentam-se dois pólos de atuação. De um lado, os *hackers* e do outro os *crakers (hackers não éticos*). Embora o nome *hacker,* às vezes soe pejorativo, na realidade este termo traduz um elogio e é considerado um dos rótulos mais cobiçados pelos aficionados por computadores, por se referir a especialistas que invadem os sistemas informáticos com o objetivo de aprimorar seus conhecimentos, para melhor desenvolver seus próprios programas.

No entanto, os *crackers* são conhecidos como o lado negro da atividade *hacker*, pois, geralmente invade sistemas para atingir objetivos financeiros ou simplesmente danificar o equipamento da vítima e corromper as informações existentes, o que caracteriza uma atividade nitidamente predatória e maliciosa.

O elemento comum entre *hackers* e *crakers* reside no fato de que ambos invadem sistemas informáticos, ou seja, obtém acesso aos dados (informações informatizadas) de determinados computadores sem a autorização do proprietário ou usuário, o que pode dar ensejo à invasão de privacidade ou quebra ilegal de sigilo, de modo que esta invasão não autorizada é considerada criminosa na maioria dos países, inclusive no Brasil.

Conforme o seu *modus operandi*, os *hackers* podem ser classificados segundo a definição de CERQUEIRA, IRIART e MORENA (2001, p.182 e 183) como: 1) CRAKERS DE SERVIDORES – *hackers* que invadem computadores ligados em rede; 2) CRACKERS DE PROGRAMAS – *hackers* que quebram proteções de *software* cedido a título de demonstração para usá-lo por tempo indeterminado; 3) PHREAKERS – *hackers* especialistas em telefonia móvel ou fixa; 4) DESENVOLVEDORES DE VÍRUS, WORMS e TROJANS: programadores que criam pequenos *softwares* que causam algum dano ao usuário; 5) PIRATAS – Indivíduos que clonam programas, fraudando direitos autorais; e 6) DISTRIBUIDORES DE WAREZ – *webmasters* que disponibilizam em suas páginas *softwares* sem autorização dos detentores dos direitos autorais.

Em rigor somente as três primeiras categorias são de *hackers*, pois as demais não exigem conhecimento técnico avançado para agir, mas resolvemos constatá-las para que possamos ter uma classificação geral dos criminosos informáticos. Hoje sabemos que não é necessário ter um alto nível intelectual para cometer delitos virtuais, pois, muitos destes delitos são praticados por jovens curiosos que encontram estes procedimentos facilmente na rede, estimulando a iniciativa individual; de modo que, os autodidatas poderão seguir passo-a-passo os ensinamentos de *hackers* experientes na realização de qualquer tarefa com o computador, por exemplo, a de produzir um *vírus* ou *trojan (cavalo de tróia)*.

Não obstante, os *hackers* possuem sua própria hierarquia para distinguir os novatos da elite Intelectual e embora esta classificação não possua cunho científico, a mesma serve para demonstrar como eles próprios se definem em relação não só aos membros da comunidade digital, como também na sociedade em geral. O texto *The Conscience of a Hacker* produzido e publicado por um *hacker* conhecido como *The Mentor*, cujo conteúdo ganhou repercussão mundial como o *manifesto hacker,* é um exemplo clássico do "auto-retrato" de um *hacker* (Anexo: Texto 1, p. 52).

O estudo sobre criminosos virtuais ainda é incipiente, porém, os mesmos utilizam-se de excusas relacionadas à negação da ilicitude (o *hacker* interpreta sua conduta como proibida, no entanto, não a considera imoral ou danosa), ao apelo a instâncias superiores (a maioria dos *hackers* segue um código de ética de acordo com a classe a que pertence), a condenação e repúdio dos que condenam (os *hackers* julgam viver em uma sociedade hipócrita, em que as pessoas que os condenam cometem crimes mais gravosos que os deles), a negação da vitimização (por se tratarem de vítimas potencias, os *hacker* acreditam que as mesmas mereceram a invasão, por não tomarem as medidas de segurança necessárias para impedir o ato) e a exclusão da própria responsabilidade (muitos *hackers* sustentam que suas atitudes são incontroláveis, podendo ser consideradas como um vício) para justificarem os seus crimes.

Neste sentido, o manifesto *hacker* é bastante significativo e atual porque demonstra que o sistema de valores de um *hacker,* torna-se, pois totalmente diverso do sistema de valores sociais predominantes. Passam a respeitar códigos de ética próprios criados dentro da subcultura, onde o conhecimento é a moeda de maior valor (daí muitos deles desprezarem os que agem com fins econômicos). De modo que, a situação é bem complexa, de sorte que se faz necessário ultrapassar as especulações teóricas para enfrentar a realidade preparando-se na prática para desvendar estes crimes. (CERQUEIRA, IRIARTE, MORENA, 2001).

4.3 O problema na tipificação legal dos crimes digitais

O Direito Penal tem como escopo fundamental a proteção aos bens jurídicos considerados relevantes pela sociedade. Sendo assim, em nome da segurança jurídica e do bem estar social faz-se necessário a tipificação legal destas condutas nocivas, impondo-se as suas respectivas sanções. Em alguns crimes o bem jurídico é o patrimônio, em outros é a integridade física das pessoas ou a honra destas, enquanto que no crime informático a tutela jurídica recai sobre o sistema informático, ou seja, o bem jurídico é a informação informatizada. Assim, neste caso se faz necessária a intervenção do Direito Penal na Informática, partindo do pressuposto de que existe o crime informático.

Faz-se, *mister,* salientar que é importante distinguir os delitos onde o computador e a internet são apenas um *modus operandi* para a consecução do intento criminoso, daquele em que o computador e seu sistema informático são os alvos da operação criminosa. Por exemplo, no estelionato praticado por meio da internet, o bem jurídico protegido é o patrimônio, ou seja, a rede mundial de computadores foi apenas o modo de operação utilizada para este fim; no entanto, a sabotagem informática visa introduzir, alterar, apagar ou suprimir dados ou programas informáticos com o elemento subjetivo do agente direcionado a interferir no sistema informático, entravando ou perturbando o funcionamento deste sistema ou desta linha de comunicação à distância, caracterizando, portanto, a informação informatizada como bem jurídico que deverá ser protegido.

Percebe-se que a informática possibilita não somente a prática de novos crimes, como potencializa alguns outros tradicionais, no entanto, aqui, o enfoque se resume aos primeiros, quais sejam os crimes informáticos. A proteção a informação informatizada traz consigo inúmeros desafios e questionamentos para os estudiosos do direito. Um destes questionamentos refere-se ao conflito aparente entre direitos fundamentais descritos no art. 5º da nossa Carta Magna, de modo que, com relação a estes crimes é muito comum a existência de um choque de forças entre o direito a intimidade e o direito a informação:

> Art.5º da CF/88, X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...]
> XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional. (ANGHER, 2009,p.24).[7]

Neste contexto, *a priori*, a definição do bem jurídico tutelado e o conflito aparente de normas são apenas alguns dos problemas na tipificação legal dos crimes digitais. E apesar da analogia, da auto-regulamentação e da arbitragem serem incentivadas no que tange a resolução de conflitos que envolvam mídias digitais, ainda permanece a problemática da analogia *in malam partem*, que é proibida no campo criminalístico, como pertinentemente assevera Cruz (2006, p. 26);

---

[7]ANGHER, Anne Joyce (Organização). **Vade Mecum Acadêmico de Direito – Coleção de Leis Rideel** . 9. Ed. São Paulo: Rideel, 2009. Pag. 24.

> A partir do momento em que foi superado o tabu com o qual a delinqüência informática vinha sendo tratada desde suas primeiras manifestações, foi possível regular condutas que eram deixadas a margem do Direito penal em virtude da equivocada afirmação de violação do princípio da legalidade. Através de uma interpretação extensiva, é possível recorrer aos preceitos penais tradicionais para resolver questões acerca da adequação das condutas ilícitas que representam a criminalidade informática. Entretanto, para tal interpretação, não se podem utilizar operações axiológicas ou valorativas. Se assim o fosse, estaríamos diante de uma interpretação analógica proibida em Direito Penal.

Diante de um conflito aparente de normas deve-se analisar o caso concreto para assegurar-se sobre qual norma melhor se sobressai. No entanto, nos casos de crimes informáticos é imprescindível a necessidade da criação de legislação específica para evitar estes questionamentos que só servem para entravar a resolução dos delitos.

Na esfera jurídica internacional a Convenção sobre o *Cibercrime*, celebrada pelo Conselho da Europa em Budapeste, na Hungria, em 23 de novembro de 2001, teve papel bastante significativo ao incentivar a cooperação internacional na resolução dos crimes virtuais e ao recomendar procedimentos processuais penais específicos na resolução destes crimes, tendo como signatários 43 (quarenta e três) países europeus e ainda os Estados Unidos, Canadá e Japão, devendo cada um destes ratificar as disposições constantes da referida Convenção no seu ordenamento jurídico interno.

Embora, o Brasil ainda não seja signatário da Convenção sobre o Cibercrime cumpre registrar que o país pode ser considerado harmônico com suas deliberações, pois, com o Projeto do Senador Eduardo Azeredo (PSDB-MG) que conta com a assessoria do Dr. José Henrique Santos Portugal, atende às diretrizes estabelecidas a nível internacional. Ademais, existem na legislação brasileira normas que coadunam com os crimes tipificados na convenção, como podemos constatar através da tabela (ANEXO; p. 63) disponibilizada por TOMÁS[8] em um de seus artigos na internet, que sistematiza a legislação penal em cada Estado signatário e que traz a respectiva correspondência na legislação brasileira.

---

[8]TOMÁS, Eliane Maria Cordeiro. **CRIMES INFORMÁTICOS: Legislação brasileira e técnicas de forense computacional aplicadas à essa modalidade de crime.** Disponível em: <http://www.artigos.etc.br/crimes-informaticos-legislacao-brasileira-e-tecnicas-de-forense-computacional-aplicadas-a-essa-modalidade-de-crime.html > Acesso em: 10 de outubro de 2010 as 11:46 hs.

Não obstante, o Substitutivo de autoria do Senador Eduardo Azeredo é o mais importante dentre os vários Projetos de Leis em tramitação na busca de regular o uso de sistemas informáticos no Congresso Nacional. Sendo um Substitutivo de 3 (três) projetos que já tramitavam na casa: O PLC 89, de 2003, de autoria do Deputado Luiz Piauhylino, que altera o Código Penal, Decreto-Lei nº. 2.848, de 7 de dezembro de 1940 e a Lei de Interceptações Telefônicas, Lei nº. 9.296, de 24 de julho de 1996. O PLS 76, de 2000, de autoria do Senador Renan Calheiros, nos termos do Substitutivo, altera as duas leis, *a priori,* citadas e mais o Código Penal Militar, o Decreto-Lei nº. 1.001, de 21 de outubro de 1969, o Código do Processo Penal, Decreto-Lei nº. 3.689, de 3 de outubro de 1941, a Lei da Repressão Uniforme, a Lei nº. 10.446, de 8 de maio de 2002 e o Código do Consumidor, Lei nº. 8.078, de 11 de setembro de 1990. E por derradeiro o PLS 137, de 2000, de autoria do Senador Leomar Quintanilha, que determina o aumento das penas ao triplo para delitos cometidos com o uso de informática.

Por tratar-se do mais completo texto legislativo já produzido sobre crimes informáticos no país e por ser pioneiro no assunto, a pauta das condutas que passam a ser criminalizadas conta com 11(onze) tipificações: Roubo de senha; Falsificação de cartão de crédito; Falsificação de telefone celular ou meio de acesso a sistema informático; Calúnia e difamação; Difusão de Código Malicioso para causar dano a sistema informático; Acesso não autorizado a sistema informático; Obtenção não autorizada de informação e manutenção, transporte ou fornecimento indevido de informação obtida; Divulgação não autorizada de informações disponíveis em banco de dados; Furto Qualificado por uso de meio informático; Atentado contra a segurança de serviço de utilidade pública e os Ataques a redes de computadores.

O substitutivo inclui também sugestões apresentadas por especialistas em audiências públicas realizadas no Congresso Nacional para debater o tema e outras quatro emendas apresentadas durante a tramitação no Senado Federal. No total, o projeto recebeu 24 (vinte e quatro) emendas, entre elas a emenda número 3 (três) da Comissão de Constituição e Justiça – CCJ, de autoria do senador Valter Pereira (PMDB-MS), que determina que a Lei Afonso Arinos (que proíbe a discriminação racial no Brasil), passe também a abranger os crimes de discriminação de raça e de cor cometidos na internet.

A aprovação da proposta é um dos principais objetivos da Frente Parlamentar de Informática, que vê a medida como arma destinada a aumentar a segurança no uso de novas tecnologias no Brasil. Assim, se o Projeto de Lei for aprovado em caráter final, não mais persistirá a falta de tipos penais específicos para o enquadramento de algumas condutas delituosas (o que tem inibido, por exemplo, a repressão da difusão de vírus), bem como não haverá dúvidas sobre o cabimento da aplicação de tipos tradicionais como o furto e o estelionato.

Por este prisma, o Substitutivo também trazia a idéia de legítima defesa digital, devido ao seu caráter inovador ampliava o instituto da legítima defesa para que este pudesse abarcar as situações em que a integridade dos sistemas informáticos estivesse em perigo, principalmente no que concerne em possibilitar a estabilidade e segurança das organizações estatais, empresariais ou familiares.

No entanto, segundo FELLITI[9] o Projeto de Lei elaborado pelo senador Eduardo Azeredo (PSDB-MG) para combater crimes digitais teve um de seus conceitos mais polêmicos alterado no dia 30 de março de 2007, durante sessão na Comissão de Constituição e Justiça (CCJ) do Senado, acatando o pedido de emenda feita pelo senador Flexa Ribeiro (PSDB-PA) para que o conceito de "defesa digital" fosse retirado do Projeto de Lei, que congrega as leis da Câmara de nº 89, de 2003, e do Senado de nº 76 e 137, de 2000.

Sendo assim, agindo em consonância com as necessidades das delegacias, principalmente, as especializadas em crimes eletrônicos, e dos tribunais, o Substitutivo é visto como um importante arsenal normativo na luta contra a criminalidade informática, podendo todos os cidadãos acompanhar a sua tramitação através do *site* do Senado Federal[10], no portal sobre a atividade legislativa. Quanto ao conceito de defesa digital este foi retirado do Substitutivo sob a justificativa de que o mesmo permitiria que agentes técnicos ou profissionais habilitados usassem ferramentas e técnicas maliciosas para contra-atacar os ataques dos *crackers* em redes privadas, o que daria margem para a ação de justiceiros virtuais sem qualquer tipo de regulamentação.

---

[9]FELLITI, Guilherme. **Senador retira conceito de "defesa digital" de projeto de crimes virtuais.** Disponível em: < http://idgnow.uol.com.br/internet/2007/05/30/idgnoticia.2007-05-30.8128470176/ > Acesso em: 11 de outubro de 2010, as 12:14hs.

[10]SENADO FEDERAL – **Projetos e matérias legislativas**. Disponível em: < http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=43555 >

5 LEGÍTIMA DEFESA DIGITAL: NOVAS ABORDAGENS, NOVAS PERSPECTIVAS.

O instituto da legítima defesa não é algo novo. O próprio instinto humano encarrega-se de exteriorizá-lo quando necessário para defesa de sua integridade física e bem como dos seus interesses. Sendo algo inerente ao homem, vem sofrendo modificações, buscando adequar-se a evolução humana e as suas necessidades.

Dentro de uma nova perspectiva da sociedade digital, faz-se *mister* repensar e aprimorar alguns princípios jurídicos, muitos deles considerados basilares para a ciência do direito, bem como suscitar os valores inerentes a tais princípios, já que os mesmos motivaram a existência das leis que se encontram em vigor.

As novas situações jurídicas decorrentes da Era Digital convergem para uma nova possibilidade de hermenêutica jurídica. Partindo do pressuposto de que as novas situações merecem novas respostas, torna-se inteiramente natural pensar que uma infração ou conflito de direito cometido em ambiente virtual, tanto pode como deve ensejar um ato protetivo da vítima com relação aos seus interesses.

Com a proliferação do fenômeno da internet, passam a ser comuns situações ilícitas contra pessoas físicas e jurídicas em ambientes eletrônicos e informatizados (ataques, agressões, vandalismo, roubo de informações). Porém, enquanto os números de crimes virtuais crescem gradativamente percebe-se que as ações de legítima defesa digital também evoluem, de modo que, se estas ações não forem disciplinadas e praticadas de maneira responsável contribuirão para formar uma conjuntura de instabilidade e insegurança no meio eletrônico.

Os *cibercrimes* não afetam apenas os bens jurídicos individuais como também os coletivos (lesão a direitos difusos), à exemplo da liberdade informática e a segurança no tráfego de informação. Deste modo, a cibernética para a doutrina majoritária é englobada aos direitos de 3ª dimensão, embora que para alguns doutrinadores seja considerada como direito pertencente a 5ª dimensão de direitos e garantias fundamentais. A Terceira geração ou terceira dimensão de direitos e garantias fundamentais foram desenvolvidas no século XX, e estariam ligadas aos Direitos da Fraternidade, relacionando-se a um profundo humanismo e ao ideal de uma sociedade mais justa e solidária, ou seja, são os direitos difusos ou coletivos (ex.: direito a um meio ambiente equilibrado, uma saudável qualidade de vida,

progresso, e outros). Deste modo, tornar-se-á pertinente questionar sobre a legítima defesa em ambientes de sistemas informatizados, como, por exemplo, na internet, sendo de fundamental importância traçar os limites da atuação de defesa para que esta não seja considerada infração. Assim sendo, nos filamos à teoria da legítima defesa digital preceituada por PINHEIRO (2009, p. 240) que é a mesma definida no art. 25 do Código Penal Brasileiro, tendo os mesmos pressupostos (agressão injusta, atual ou iminente; meios necessários e a defesa de direito seu ou de outrem – *animus defendi*), porém, ocorrida em meio diverso, qual seja o meio virtual ou não presencial.

Partindo do princípio de que o crime é uma estrutura que pode ser tripartida em fato típico, antijurídico e culpável de acordo com a teoria analítica do crime, assim, a legítima defesa sendo causa de justificação, bem como, discriminante putativa, exclui a possibilidade de caracterização do ilícito, muito embora o fato possa ser considerado típico. Nesse diapasão, se existem situações ocorridas em ambiente virtual e, portanto não presencial, que podem ser compreendidas como crime amoldando-se ao sistema analítico, então estas situações denominadas como *cibercrimes* também podem abrigar-se sob a guarida das excludentes já que não se deve retroceder diante de um injusto.

Na realidade da sociedade digital, o conceito de legitima defesa em *stricto sensu* bem se aplica as situações lesivas ocorridas virtualmente, como aduz Pinheiro (2009, p. 242):

> A prerrogativa da autodefesa é uma causa de justificação que se baseia no princípio de que o Direito não precisa retroceder diante de um injusto e, ainda de que a defesa vale, pois, não só para o bem jurídico ameaçado, mas também, simultaneamente, para a afirmação da ordem jurídica. Sendo assim o art. 25 do Código Penal define: *"Entende-se em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual e iminente, a direito seu ou de outrem.*

Pretende-se declinar com o acima exposto, que utilizando do conceito legal desprendido do art. 25 do Código Penal Brasileiro, temos os pressupostos da legítima defesa em *stricto sensu* (agressão injusta, atual ou iminente; meios necessários e a defesa de direito seu ou de outrem – *animus defendi*), podendo ser compreendido também como elementos da legítima defesa digital, já que o único diferencial é que esta ocorre em meio diverso, qual seja o meio virtual ou não

presencial, sendo a teoria da legítima defesa digital perfeitamente compatível com a visão garantista do ordenamento jurídico brasileiro.

5.1 Agressão injusta: Incidentes de Segurança

Um dos fatores que legitimam a situação de defesa é a caracterização de uma agressão injusta, ou seja, um ato humano que lese direito/bem seu ou de outrem e que não esteja amparado pelo ordenamento jurídico, sendo necessário um ato efetivo e não tão somente uma provocação para possibilitar ao agredido defender-se legitimamente de acordo com os limites legais. No campo digital, esta agressão injusta se consubstancia na maioria das vezes em um incidente de segurança, ou seja, numa ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo tratado pela política de segurança sobre um sistema informático.

Segundo Dias (2001, p. 44);

> A sociedade industrial foi substituída "por uma sociedade exasperadamente tecnológica, massificada e global, onde a ação humana, em grande parte anônima, revela-se suscetível de produzir riscos também globais ou, tendendo a isso, suscetíveis de serem produzidos em tempo e lugar completamente distintos de onde provém a ação que os originou.

Ante tal cenário, não surpreende o anacronismo vivido pelo direito penal. Fundamentado nos princípios liberais do iluminismo e de cunho marcadamente antropocêntrico, o direito penal foi elaborado para tutelar bens jurídicos tradicionais como a vida, a integridade física, a saúde e o patrimônio, enquanto que, no atual universo pós-moderno, as ações humanas, potencializadas pelo desenvolvimento da razão técnico-instrumental, alcançam novas dimensões, em relação de espaço-tempo peculiares, em que os riscos globalizam-se e geram danos muitas vezes diferidos, atingindo novos bens jurídicos, sendo estes bens não necessariamente tangíveis, o que na opinião de Greco (2007, p. 341) não obsta a legítima defesa:

> Tem-se entendido que o instituto da legítima defesa tem aplicação na proteção de qualquer bem juridicamente tutelado pela lei. Assim, pode-se, tranquilamente, desde que presente seus requisitos, alegar a legítima defesa no amparo daquelas condutas que defendam seus bens, materiais ou não.

É cediço que, quanto a esta regra de que todos os bens são suscetíveis de defesa pelo ofendido, deve-se trazer a colação a peculiaridade existente no caso dos bens comunitários, em que tais bens constituem exceção a regra, a menos que para sua defesa o ofendido não tenha tempo suficiente ou não possa procurar o necessário amparo das autoridades constituídas para tanto.

Conforme a afirmação do notório jurista espanhol Cerezo (2001, p. 209);

> Os bens jurídicos supra-individuais cujo portador é a sociedade (por exemplo, a fé pública, a saúde pública, a segurança do tráfego) ou o Estado como órgão do poder soberano (a segurança exterior e interior do Estado, a ordem pública, o reto funcionamento da Administração Pública, da Administração da Justiça e etc.); não são, por isso, suscetíveis de legítima defesa. Somente quando o Estado atuar como pessoa jurídica serão seus bens jurídicos (a propriedade, por exemplo) suscetíveis de legítima defesa.

Nesse diapasão, a *internet* é considerada um bem comunitário, sendo uma rede totalmente aberta e civil, portanto, poderíamos descartar a aplicação da legítima defesa neste ambiente se seguíssemos o posicionamento do professor José Cerezo Mir. No entanto, como ficaria a questão das redes privadas ou *intranets*? As *intranets* por serem redes coorporativas se enquadram perfeitamente ao instituto da legitima defesa, se configurando como constante alvo da atividade criminosa dos *crakers*, tendo em vista que muitos destes são contratados por empresas ou até mesmo entidades governamentais rivais para promover incidentes de segurança.

Não obstante, mesmo respeitando a lição do nobre professor e jurista espanhol, o nosso posicionamento coaduna com a possibilidade da utilização da legítima defesa digital na *internet*, pois, embora, a rede mundial de computadores seja aberta e, portanto, considerada um bem comunitário, é notório que nela há esferas privadas, pois, as instituições que regulam o seu funcionamento concedem permissões ou promovem concessões de uso, bem como é inegável que os usuários da rede devem ter a sua privacidade e integridade moral-psicológica resguardada em face das agressões, ataques e vandalismos frequentes na rede, de certo que estes incidentes não podem ficar impunes.

5.2 Respostas aos Incidentes de segurança: Meios moderadamente necessários para evitar incidentes.

A legítima defesa digital consiste na utilização pelo agente, contra incidentes de segurança, de uma resposta moderada e necessária, na defesa da integridade e resguardo de informações dispostas em um sistema informatizado seu ou de outrem. Para a incidência da causa excludente de ilicitude em comento, deve o ofendido agir com moderação para repelir a injusta agressão.

A moderação no uso da legítima defesa rege-se pelo princípio de proporcionalidade entre a defesa empreendida e o ataque sofrido, além da razoabilidade na escolha do meio utilizado pelo ofendido para defender-se e fazer cessar esta injusta agressão, como Greco (2007, p. 348) aduz:

> Os princípios reitores, destinados à aferição da necessidade dos meios empregados pelo agente, são o da proporcionalidade e o da razoabilidade. A reação deve ser proporcional ao ataque, bem como deve ser razoável. Caso contrário, devemos destacar a necessidade do meio utilizado e, como conseqüência lógica, afastar a exclusão da ilicitude.

A agressão injusta nos delitos informáticos assume o conceito de incidente de segurança, devendo haver proporcionalidade entre o incidente de segurança sofrido e o meio utilizado para cessá-lo, para não incorrermos na hipótese de excesso de legítima defesa punível.

Para Mirabete (1994, p.177) "a legítima defesa, porém, é uma reação humana e não se pode medi-la com um transferidor, milimetricamente, quanto à proporcionalidade de defesa ao ataque sofrido pelo sujeito". No caso dos crimes informáticos esta aferição é bastante complexa, pois, existe uma linha bastante tênue que separa a moderação do seu excesso. Nesse sentido, as grandes empresas e corporações, principalmente os bancos, já se utilizam da política de governança empresarial em que se contrata uma equipe multidisciplinar, denominada de grupo de gerenciamento de risco para coibir as atividades criminosas realizadas pelos meios computacionais.

Os grupos de gerenciamento de risco geralmente são compostos por analistas de sistemas, cientistas da informação, administradores, economistas e advogados, formando então, um grupo de profissionais especialistas em tecnologia

da informação – TI e segurança da informação – SI como uma verdadeira "liga da justiça" dos delitos virtuais.

De fato, a legítima defesa digital por analogia pode ser entendida como legítima defesa em *stricto senso*, porém, deve ser mais bem regulamentada para não gerar arbitrariedades e consequentemente dar ensejo ao tão temido caos jurídico-virtual. È necessário, pois, a criação de um grupo responsável para coibir os incidentes de segurança, de modo que, não aprovemos as ações de "justiceiros virtuais"[11], ou seja, combatemos, também, como forma de prevenção, os leigos que pretendem fazer justiça sob a excusa da legítima defesa digital, mas que, no entanto, se igualam aos criminosos digitais por utilizarem-se das mesmas praticas ilícitas de maneira irresponsável e arbitrária.

A legítima defesa digital é uma realidade. Já existem empresas e corporações que se utilizam deste instituto. E com razão, pois, a legítima defesa é uma ação inerente ao homem e por ser de tal modo inevitável, deve ser regulamentada, sendo, pois, caracterizada como um direito do cidadão, devendo o mesmo agir neste sentido, como bem nos lembra Pinheiro (2009, p. 242);

> Assim, verificamos que a defesa da vitima ou a ação de outro que venha a responder ao ataque, não será passível de punição se sua atitude se enquadrar em legítima defesa. Para internet deve-se definir claramente o que significa o "emprego moderado dos meios necessários". Neste sentido aplica-se o brocardo jurídico que afirma "*nemo expectare tenetur donec percutietur*", que significa que ninguém (para defender-se) está obrigado a esperar até que seja atingido por um golpe.

É bem verdade que, a prática e a legislação computacional forense caminham a passos tétricos, no entanto, deve-se reconhecer que se faz *mister* a regulamentação a nível corporativo e empresarial da defesa digital. A legislação será ampliada aos poucos para que se possa atingir a sociedade em sua totalidade, pois, a comunidade em geral ainda não está preparada para a utilização deste instituto, de modo que, deve deixá-lo sob o cuidado de profissionais competentes, sendo iminente a regulamentação desta atividade.

[11]SaferNet Brasil, **Seção: Prevenção.** Disponível em: <http://www.safernet.org.br/site/prevencao/cartilha/safer-dicas/justiceiros>. Acesso em: 05 fev. 2010 às 17: 19 horas.

5.3 Atualidade e iminência da agressão: A relativização do conceito de tempo e espaço na Era Digital.

Na era digital mudanças são cada vez mais freqüentes, ocorrendo tão velozmente que as esferas político-econômico-jurídicas custam a acompanhá-las. Adequamos ao sistema tridimensional (fato, valor e norma) criado por Realle (1999), o elemento temporal, formando um sistema quadrimensional (fato, valor, norma e tempo) para facilitar a abordagem do direito no mundo tecnológico, criando assim, uma especialização do direito: o Direito Digital.

Neste sentido, Pinheiro (2009, p. 37) aduz:

> A aplicação, portanto da fórmula tridimensional do direito adicionada do elemento Tempo resulta do Direito Digital. Esse quarto elemento é determinante para estabelecer as obrigações e limites de responsabilidades entre as partes, quer seja no aspecto dos contratos, serviços, direitos autorais, quer seja na proteção da própria credibilidade jurídica quanto a sua capacidade em dar solução a conflitos.

Do mesmo entendimento comunga o Dr. Renato da Silveira Martini, Diretor-Presidente do Instituto Nacional de Tecnologia da Informação (Casa Civil), órgão federal que executa as políticas de certificação digital no Brasil, ao asseverar que:

> Deve-se sair do labirinto clássico da Filosofia do direito, deve-se encontrar a entrada e a saída: nós nos referimos a mera e simples escolha entre as dimensões (fatos-normas-valores). Se a desmaterialização é um fato, um "estado das coisas" (Sachverhalt), com seus sistemas técnicos e informatizados, encontra-se, também ao seu lado, as regras jurídicas. (MARTINI, 2008, p. 08).

Portanto, os termos "atualidade" e "iminência" passam a ser entendidos sob uma nova dinâmica hermenêutica, pois, [...] atual é a agressão que está acontecendo; e iminente é aquela que esta prestes a acontecer. [...] Tais conceitos não resolvem, em determinadas situações, casos de ordem prática que podem ocorrer no dia-a-dia daqueles que militam perante a Justiça Criminal (GRECO, 2007, p. 350); de modo que, é necessária uma atualização destes conceitos à realidade vivenciada na Era Digital.

O próprio jurista Miguel Reale (1999, p. 699, 700) preleciona que;

> A integração dos três elementos na experiência jurídica (o axiológico, o fático e o técnico-formal) revela-nos a precariedade de qualquer compreensão do Direito isoladamente como *fato, valor* ou como *norma*, e, de maneira especial, o equívoco de uma compreensão do Direito como pura forma, suscetível de albergar, com total indiferença, as infinitas e conflitantes possibilidades dos interesses humanos.

Deste modo, o Direito não é uma fórmula matemática, devendo a respeitável tricotomia, cuja compreensão do Direito tem em vista a sua vinculação social e aos valores, ser encarada sob mais um aspecto, qual seja o temporal. Os pontos de vista sociológico, lógico e filosófico e temporal, possibilitam entender o Direito na sua totalidade como atualização freqüente do sentido de Justiça e dos valores, determinando, com possível rigor, o significado do Direito à luz da experiência social e histórica do homem.

Composição de valores socialmente vividos, o direito é dever ser, mínimo ético, ou uma espécie de moral objetiva, portanto, deve se adequar a realidade vivida, qual seja a Era Digital e "a sociedade de risco". Na Era digital os incidentes de segurança ocorrem com freqüência e num curto período de tempo, o que demonstra a relativização destes dois conceitos (tempo e espaço), visto que o espaço passa a ser imaginário, intangível, virtual e o tempo passa a correr de forma mais vertiginosa que os ponteiros do relógio, características estas que emergem da "sociedade de risco". Os perigos na "sociedade de risco" mostram-se abstratos e incalculáveis, sendo primordial que o direito penal e as instituições jurídicas se adéqüem a esta realidade, pois, na maioria das ocasiões será impossível socorre-se de imediato da proteção estatal, ademais o estilo de processo judicial não é compatível com a celeridade exigida para a resolução de *cibercrimes*. No entanto, como nem sempre o Estado estará presente para exercer a sua função pacificadora, foi resguardado pela lei ao cidadão o direito à legítima defesa.

Grecco (2007, p. 340) preleciona:

> Contudo, tal permissão não é ilimitada, pois que encontra suas regras na própria lei penal. Para que se possa falar em legítima defesa, que não pode jamais ser confundida com vingança privada é preciso que o agente se veja diante de uma situação de total impossibilidade de recorrer ao Estado, responsável constitucionalmente pela nossa segurança pública, e, só assim, uma vez presentes os requisitos legais de ordem objetiva e subjetiva, agir em sua defesa ou na defesa de terceiros.

Assim sendo, a legítima defesa digital surge como uma importante aliada, juntamente com o arsenal legislativo pátrio, para auxiliar as delegacias, principalmente as especializadas em crimes informáticos, e os tribunais, na resolução destes delitos, podendo neutralizar ou dirimir os incidentes de segurança, além de possibilitar a colheita de provas no sentido de punir os *Cibercriminosos.*

5.4 Defesa do direito próprio ou de terceiro: A importância social da resposta em uma sociedade de risco.

A preocupação maior da sociedade, não só no Brasil, mas como também em todo o mundo é a de combater os crescentes níveis de criminalidade cometida com o auxílio dos meios informáticos, pois, no campo dos meios de comunicação de massa, esses malefícios se refletem de diversas formas. Em relação ao uso abusivo da informática, encontramos situações como o acesso não autorizado a dados informatizados. Trata-se de uma conduta que pode trazer graves conseqüências às relações sociais, pois, em geral, serve de meio para a realização de outras atividades ilícitas de maior gravidade. (CRUZ, 2006,p.11).

Nesse sentido, a expressão "legítima defesa" cobra interpretação extensiva, não estando restrita à integridade física do ofendido ou ao seu patrimônio, abrangendo, também, a honra, no caso do emprego de calúnias, injurias ou difamações em ambientes virtuais, ou ainda, no caso do tráfico de dados. A resposta as contingências virtuais devem se mostrar eficientes para garantir a proteção a reputação ou patrimônio nos meios eletrônicos, o que se consubstancia na devida salvaguarda de ativos intangíveis.

A sociedade passa por evoluções e revoluções, onde os patamares costumeiros e tecnológicos são alterados. Os marcos históricos sempre deixam uma nova impressão no contexto social, por promoverem uma alteração no plano histórico, social, industrial e mercadológico. O Direito Penal não pode ignorar essas sensíveis mutações sociais, sob pena de tornar-se obsoleto perdendo sua função precípua de tutela aos bens jurídicos penais. Para tal, os conceitos penais devem passar por uma atualização para se adequarem a sociedade de risco.

Nesta perspectiva, corroboramos com a idéia de legítima defesa digital, por estarmos atentos ao fato de que a defesa digital já vem sendo utilizada como política de segurança em agências bancárias, pois, alguns executivos deste ramo, apoiados

em pareceres jurídicos, começam a reagir e a contra-atacar os *hackers* antes mesmo de terem em mãos uma autorização judicial.

Conforme ATHENIENSE (2010) [12] "a legítima defesa na internet é polêmica e tabu entre os bancos e os próprios advogados, mas é apoiada até mesmo por policiais que acreditam que este pode ser um bom dispositivo não só para evitar que furtos a contas correntes se concretizem, como também para evitar que o hacker – e seu rastro – desapareçam".

No entanto, a Federação Brasileira dos Bancos (Febraban), não admite que esta seja uma prática corriqueira nas agências bancárias, afirmando que nenhum banco usa do contra-ataque aos hackers como forma de proteção. Mas entre os especialistas PINHEIRO e ATHENIENSE é corrente a aceitação e a utilização da defesa digital, salientando que muitas vezes o alvo principal não são os bancos, mas sim os seus clientes quando o ataque é feito por *e-mails* com *links* ou anexos que chegam as caixas postais com algum código malicioso. Também é comum o roubo de senhas através de *keyloggers,* quando o usuário realiza alguma operação no *internet banking* em um computador que tenha este artifício malicioso.

O fato é que estes incidentes de segurança não ocorrem apenas em bancos, mas também em empresas e corporações. Qualquer usuário de computador seja de *intranet* ou *internet,* está suscetível de ser vítima de um ataque informático. No entanto, é possível observar que na esfera empresarial não é tão simples revelar publicamente que seus sistemas são vulneráveis a um ataque, porque, tal afirmação implicaria em perca de clientela, ou seja, inibiriam os "consumidores virtuais" ou usuários destas lojas, bancos, livrarias e redes sociais em ambiente virtual.

Deste modo, estas empresas, corporações e bancos contratam grupos de gerenciamento de risco para trabalharem em seu nome inibindo os ataques em seus sistemas informáticos. Neste caso, o direito/bem protegido por este grupo pertence a terceiro, ora contratante dos seus serviços, pois, é preciso utilizar deste artifício porque não há tempo para esperar uma autorização judicial, que leva em média 48 (quarenta e oito) horas, para interceptar o *cracker* e se possível recapturar os dados.

---

[12] ATHENIENSE, Alexandre (organização). **Os Bancos partem para a legítima defesa diante dos ataques de hackers** < http://www.dnt.adv.br/noticias/direito-penal-informatico/os-bancos-partem-para-a-legitima-defesa-diante-dos-ataques-de-hackers/ > Acesso em 12 de outubro de 2010 as 13:17 **hs.**

No futuro, será possível encontrar usuários comuns agindo sob a guarida da legítima defesa digital com o propósito de defender direitos ou bens seus do ataque de *Cibercriminosos,* porém, nos limitamos a apoiar a utilização do instituto apenas por profissionais especializados, devido a evidente caracterização do *animus defendi* nestes últimos, tendo em vista todo o aparato técnico e intelectual que eles carregam.

A realidade é que num país que enfrenta altos índices de analfabetismo, este não é o único fator que impede a disseminação segura da idéia de legítima defesa digital, pois, constata-se que existem muitas pessoas intelectualizadas e competentes que ainda caem em ciladas virtuais. No entanto, é inegável a necessidade de conhecimento especializado para a resolução destes conflitos, para que o agente não incorra em excesso de legítima defesa, podendo ser punido por tal excesso como preleciona Greco (2007, p. 360):

> Toda conduta praticada em excesso é ilícita, devendo o agente responder pelos resultados dela advindos. Os resultados que dizem respeito as condutas praticadas nos limites permitidos pela legítima defesa não amparados por esta causa de justificação; os outros resultados que surgiram em virtude do excesso, por serem ilícitos, serão atribuídos ao agente, a que por eles terá que ser responsabilizado.

O ser humano é naturalmente falível em suas ações podendo correr em erro sobre os limites de uma causa de justificação, e nesse caso, como em qualquer modalidade de erro, deve-se aferir se era evitável ou não. Se inevitável, o agente, embora atuando em excesso, será considerado isento de cumprir a pena; se evitável o erro, embora o fato por ele praticado seja típico, ilícito e culpável, verá sua pena reduzida entre os limites de um sexto a um terço, nos termos da parte final do art. 21 do Código Penal Brasileiro.

Nesse diapasão, o Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil – CERT/BR[13] desenvolve projetos de análise sobre tendências de ataques, com o objetivo de melhor entender suas características no espaço da Internet Brasileira. O CERT/BR é um órgão mantido pelo Núcleo de Informação e Coordenação do Ponto BR – NIC.br. e do Comitê Gestor da Internet no Brasil, tendo a responsabilidade de atender a qualquer rede brasileira conectada à Internet.

---

[13] CERT/BR. Disponível em: < http://www.cert.br/ > Acesso em : 12 de outubro de 2010, as 18:57 hs.

Visando treinar profissionais e estabelecendo diretrizes gerais para aumentar a capacidade de detecção de incidentes e correlação de eventos, o CERT/BR tem como papel fundamental impedir a conseqüente caracterização de excesso na atividade de gerenciamento de risco. Por ser um centro de resposta a incidentes de segurança para a internet brasileira, o CERT/BR tem um *software* que dá suporte a atividade dos grupos de gerenciamento de riscos no Brasil disponibilizando em seu *site* publicações, cursos, palestras, projetos, *links* e estatísticas sobre o quadro de gerenciamento de segurança a nível brasileiro de internet como poderemos constatar nos anexos (pag. 64/71).

Segundo Greco (2008,p.23), "é importante salientar que na persecução criminal transcorre cotidianamente um duelo entre duas forças que colidem tensamente, de um lado se procura demonstrar a existência do fato delituoso e sua autoria (princípio instrumental punitivo), mas para isso conflitamos com a garantia dos direitos fundamentais (princípio instrumental garantista)". No entanto, a persecução criminal é necessária para que haja a coleta e a produção de provas que poderão demonstrar a existência do fato delituoso e sua autoria, sendo a legítima defesa digital uma aliada da persecução criminal neste sentido.

Sendo assim, devemos nos guiar pela legislação nas atividades de gerenciamento de riscos, pois, a resposta ao incidente dada pelo agente, embora inicialmente legítima, poderá transforma-se em uma agressão injusta, ou seja, em um incidente de segurança para o agressor inicial e assim configurar-se-iam em *legítima defesa sucessiva* no que diz respeito a este. Pois, quem viu repelida a agressão que inicialmente era injusta, pode alegar a excludente a seu favor, porque, o agredido passou a ser considerado agressor ao incorrer no excesso de defesa. Portanto, devemos ter bastante cautela ao utilizarmos da excludente de legítima defesa digital.

6 CONCLUSÃO

A sociedade é regida por princípios e estes devem ser observados com devida primazia sobre a legislação. De modo que, torna-se necessário formarmos cidadãos digitalmente conscientes de seus direitos e obrigações ao utilizarem as mídias digitais, dando-lhes subsídios jurídicos para que possam se defender legalmente destas ações nocivas realizadas contra os mesmos, principalmente no âmbito da internet, agindo de modo racional, adequado e seguro.

A legítima defesa digital foi concebida com o propósito de incentivo à criação de políticas de segurança da informação em ambientes informatizados, possibilitando a regulação e atuação de grupos de respostas a incidentes em instituições públicas ou privadas, como por exemplo, empresas, bancos e a própria Administração Pública consubstanciada nos seus órgãos, tendo em vista, evitar os crimes informáticos e combater a impunidade gerada por estes.

A regulamentação da legítima defesa digital inibiria a atividade dos "justiceiros virtuais" ou "heróis da internet", além de possibilitar uma atuação mais controlada e segura dos grupos de resposta a incidentes, pois, a atividade profissional desenvolvida por estes teria um escopo jurídico explícito na legislação pátria.

Neste caso, a maior preocupação reside em traçar os limites de atuação da pessoa jurídica, ou mesmo da pessoa física em suas estratégias de defesa eletrônica, já que as tendências convergem para que seja possível a legítima defesa no campo virtual, estando esta limitada ao uso restrito dos meios reputados eficazes e suficientes para repelir a agressão. Desta feita, o direito digital deverá definir claramente o que significa o emprego moderado dos meios necessários para não incorrer em ilícitos penais, tendo em vista que nem todo ato de defesa ou de autodefesa é legítimo, ou seja, autorizado pela ordem jurídica.

O Direito Digital ajusta o mundo jurídico à realidade virtual, propiciando uma adequação da norma aos fatores concretos que traduzem as necessidades sociais, com o fim de atender a demanda cada vez mais crescente de casos envolvendo a área digital. O substitutivo do Senador Eduardo Azeredo (PSDB – MG) propõem um grande avanço neste sentido, muito embora, um dos seus pontos mais polêmico, qual seja a legítima defesa digital, tenha sido vetado e retirado da proposta. Sendo assim, o instituto da legítima defesa digital traduz uma ordem de cooperação e de coexistência na comunhão de um fim social: o combate aos crimes virtuais. De modo

que, em nome do progresso social não demorará muito para que a sua regulamentação se torne uma realidade.

Assim, com o presente trabalho, pretendemos contribuir para desmitificar a idéia sobre legítima defesa digital, não pretendendo estabelecê-la como uma nova *panacéia* dos tempos modernos, mas, com o intuito de incutir nos leitores a reflexão sobre o tema, pois, parafraseando Fernando Pessoa: "*O universo não é uma idéia minha, mas é minha a idéia que tenho do universo".* De modo que, advogamos a proposta de alavancar o progresso no campo da forense computacional pela necessidade de punição de tais ilícitos pelas instituições legais.

REFERÊNCIAS BIBLIOGRÁFICAS:

ANGHER, Anne Joyce (Organização). **Vade Mecum Acadêmico de Direito – Coleção de Leis Rideel** . 9. Ed. São Paulo: Rideel, 2009.

ATHENIENSE, Alexandre (organização). **Os Bancos partem para a legítima defesa diante dos ataques de hackers.** Disponível em: < http://www.dnt.adv.br/noticias/direito-penal-informatico/os-bancos-partem-para-a-legitima-defesa-diante-dos-ataques-de-hackers/ > Acesso em 12 de outubro de 2010 as 13:17 hs.

BARBUTO, Claudio;OLIVEIRA, Jefferson Guedes de; MONTEIRO, Rodrigo Fernandes. **Tecnologia da informação para todos / projeto Bei Comunicação.** São Paulo: Bei Comunicação, 2002. (Coleção entenda e aprenda)

BARROS, Larissa; MIRANDA, Isabel. **O papel das redes sociais para a construção e o compartilhamento do conhecimento em Tecnologias Sociais.** Notícias da Rede, nº 132, Brasília, 28 de maio de 2010 - Edição especial de aniversário de 5 anos da Rede de Tecnologia social. (http://www.rts.org.br/artigos/artigos_-_2009/o-papel-das-redes-sociais-para-a-construcao-e-o-compartilhamento-do-conhecimento-em-tecnologias-sociais)

BLUM, Renato Opice; JIMENE, Camilla do Vale. **A nova polêmica da era digital: vítimas ou criminosos nos meios eletrônicos?Jus Navigandi**, Teresina, ano 10, n. 1126, 1 ago. 2006. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=8730>. Acesso em: 29 set. 2010 às 20:00h.

CEREZO MIR, José. ***Curso de derecho penal español*** *– Parte general. Madrid: Editorial Tecnos*, 2001. V. II e III.

CERQUEIRA, Tarcísio Queiroz; IRIARTE, Erick; MORENA, Márcio (organizadores). **Informática & Internet: aspectos legais internacionais.** Rio de Janeiro : Esplanada, 2001. 386p.; (Coleção ADCOAS).

CINTRA, Antonio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. **Teoria Geral do Processo**. 24. ed, São Paulo: Malheiros, 2008.

CRUZ, Danielle da Rocha; **Criminalidade Informática: a tipificação penal das condutas ilícitas realizadas com cartões de crédito.** Rio de Janeiro: Forense, 2006.

DAUER, Nátaly. **Quatro em cinco pessoas acreditam que acesso à internet é um direito humano.** Disponível em: http://www.geek.com.br/blogs/832697706/posts/12441-quatro-em-cinco-pessoas-acreditam-que-acesso-a-internet-e-um-direito-humano. Acesso em: 09 de abril de 2010 às 13:15 horas.

DIAS, Jorge de Figueiredo. **O direito penal entre a "sociedade industrial" e a "sociedade de risco":** Revista brasileira de ciências criminais: V.9, n.33. jan/mar. 2001.

GRECO, Rogério. **Curso de Direito Penal, parte geral. v. I**. 9. ed. Rio de Janeiro: Impetus, 2007.

_____. **Curso de Direito Penal, parte especial. v. IV**. 4. ed. Niterói, RJ: Impetus, 2008.

KANAAN,João Carlos. **Informática Global: Tudo o que você precisa saber sobre informática.** São Paulo: Pioneira, 1998.

LÉVY, Pierre. **Cibercultura**. São Paulo, Editora 34, 1999.

LINHARES, Marcelo Jardim. **Legítima Defesa**. 2. Ed. Rio de Janeiro, Forense, 1980.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de Informação com internet.** Trad. Dalton Conde de Alencar. 4. Ed. Rio de Janeiro. LTC; 1999.

MARTINI, Renato da Silveira. **Tecnologia e cidadania digital: ensaio sobre tecnologia, sociedade e segurança.** Rio de Janeiro: Brasport, 2008.

MENTOR. ***The Conscience of a Hacker*** Disponível em: < http:// http://www.phrack.org/issues.html?issue=7&id=3&mode=txtl > Acesso em: 11 de agosto de 2010 às 10:10 hs.

MIRABETE, Júlio Fabbrini. **Manual de direito penal – Parte geral.** v.1. 8 ed. São Paulo: Atlas, 1994.

MONTENEGRO FILHO, Misael. **Curso de direito processual civil, volume 1: Teoria geral do processo e processo de conhecimento.** 4 Ed. – 5 reimpr. – São Paulo: Atlas, 2008.

OLIVEIRA, Marcus Vinícius Amorim de. Direito fundamental à tutela jurisdicional do Estado . **Jus Navigandi**, Teresina, ano 3, n. 28, fev. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=258>. Acesso em: 06 jul. 2010.

PACHECO, Denilson Feitoza. **Direito processual penal: teoria, crítica e práxis.** 5. Ed. rev e atual. Com Emenda Constitucional da Reforma do Judiciário. Niterói, RJ: Impetus, 2008.

PINHEIRO, Patricia Peck; **Direito Digital** – 3. Ed. São Paulo : Saraiva; 2009.

PIMENTEL, Alexandre Freire. **O direito cibernético: um enfoque teórico e lógico-aplicativo.** Rio de Janeiro: Renovar; 2000.

REALE, Miguel. **Filosofia do direito**. 19. Ed, São Paulo-SP: Saraiva 1999.
SaferNet Brasil, **Seção: Prevenção.** Disponível em:<http://www.safernet.org.br/site/prevencao/cartilha/safer-dicas/justiceiros>. Acesso em: 05 fev. 2010 às 17: 19 horas.

SALOMÃO, Lídia. **Porque a sociedade não sobrevive sem a tutela jurídica?**Disponível em: <http://www.jurisway.org.br/v2/dhall.asp?id_dh=177 > acesso em: 19 de out.2010 às 21:08 horas.

SILVA, Marcelo Pereira. **Arquitetura de computadores.** Disponível em: < http://webcache.googleusercontent.com/search?q=cache:GsZqiviY3AJ:www.pcbrain.eti.br/cep/1ano/arquitetura/ARQUITETURA_DE_COMPUTADORES.doc+Entre+os+modelos+1401+e+7094,+a+IBM+vendeu+mais+de+10.000+computadores.&cd=26&hl=pt-BR&ct=clnk&gl=br> Acesso em: 19 de out de 2010 as 23:45 horas.

SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. São Paulo:

Revista dos Tribunais – RT, 2003. (Ciência do direito penal contemporânea; v.4)
TOMÁS, Eliane Maria Cordeiro. **CRIMES INFORMÁTICOS: Legislação brasileira e técnicas de forense computacional aplicadas à essa modalidade de crime.** Disponível em: < http://www.artigos.etc.br/crimes-informaticos-legislacao-brasileira-e-tecnicas-de-forense-computacional-aplicadas-a-essa-modalidade-de-crime.html > Acesso em: 10 de out de 2010 as 11:46 hs.

VADE MECUM RT – ANEXO. **Resumos – Das 10 principais matérias jurídicas para provas e concursos.** São Paulo: Editora Revista dos Tribunais, 2007.
VELOSO, Fernando de Castro. **Informática: conceitos básicos.** 2. ed. Rio de Janeiro: Campus, 1997.

WIENER, Nobert. **Cibernética e sociedade: o uso humano de seres humanos.** Tradução José Paulo Paes. 2 ed. São Paulo: Cultrix.

ANEXOS

GLOSÁRIO:

- **Trojan (Cavalo de Tróia):** Programa, normalmente recebido com um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de janela, jogos e etc.), que executa não só as funções para o qual foram aparentemente projetados, ma também outras funções normalmente maliciosas e sem o conhecimento do usuário

- **Chat (*Internet Relay Chat*):** Conversa em tempo real através do computador.

- **Código malicioso:** Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em computador. Ex: vírus, cavalos de tróia, *rootkits* e etc.

- **Criptografia:** Método de codificação de dados que permite o acesso apenas de pessoas autorizadas, possuidoras de chave de acesso. Ciência e arte de escrever mensagens cifradas ou em código. É parte de um capo de estudo que trata de comunicações secretas. É utilizada, entre outras finalidades, para autenticar a identidade de usuários, autenticar as transações bancárias; proteger a integridade de transferências eletrônicas de fundos e proteger o sigilo de comunicações pessoais e comerciais.

- **Ciberespaço:** É o conjunto das redes de computadores e serviços existentes na internet. É uma espécie de planeta virtual, onde as pessoas se relacionam virtualmente, por meios eletrônicos. Termo inventado por William Gibson no seu romance *Neuromancer* e idealizado em analogia com o espaço sideral explorado pelos astronautas.

- **DOS** (*DoS -- Denial of Service):* notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

- ***E-commerce* (comércio eletrônico):** É qualquer forma de transação comercial em que as partes interagem eletronicamente. Conjunto de técnicas e tecnologias computacionais utilizadas para facilitar e executar transações comerciais de bens e serviços através da internet.

- ***E–Business:*** Palavra que identifica transações e comércios através da Internet que estão baseados em algum sistema de *e-commerce*. Qualquer tipo de negócio efetuado por meio da rede mundial de computadores.

- ***Endereço IP:*** É o endereço real de uma máquina na internet. Consiste em uma série de números separados por pontos. Cada máquina conectada a rede tem um endereço IP.

- ***Firewall:*** Em português: muro corta-fogo. É o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra. Este conceito é comumente associado a redes TCP/IP.

- **Fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro" ou obter vantagem.

- **Incidente de Segurança:** É qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo tratado pela política de segurança.

- **Informação:** É um ativo composto por um conjunto de dados ou elementos, que como qualquer outro ativo importante para os negócios, tem valor para a organização e, consequentemente, necessita ser adequadamente protegido.

- **Internet:** Rede mundial de computadores e outros dispositivos interligados que possibilitam acesso à informação nele disponibilizada.

- **Intranet:** São redes corporativas que se utilizam de tecnologia e infra-estrutura de dados da *internet*. São utilizadas na comunicação interna da própria empresa e/ou na comunicação com outras empresas.

- **Invasão:** ataque bem sucedido que resulte em acesso, manipulação ou destruição não autorizada de informação a um computador ou rede.

- IP – ***Internet Protocol***: Protocolo responsável pelo percurso de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP desenvolvida e usada na *internet*.

- ***Keylogger***: Significa registrador do teclado em inglês. É um programa de computador do tipo *spyware* cuja finalidade é registrar tudo o que a vítima digita, a fim de capturar suas senhas, números de cartão de crédito e afins. Muitos casos de *phishing*, assim como outros tipos de fraudes virtuais, se baseiam no uso de algum tipo de *keylogger*, instalado no computador sem o conhecimento da vítima, que captura dados sensíveis e os envia a um *cracker* que depois os utiliza para fraudes. Existem *softwares* apropriados para se defender deste tipo de ameaça. É sempre oportuno que um computador conectado à internet seja protegido através de um *software "AntiSpyware"* de um "*Firewall*" e de um "AntiVirus". O *Keylogger* também é um programa muito utilizado por empresas para monitorar o que seus funcionários fazem em suas maquinas, porém em muitos casos as pessoas utilizam o programa de forma mal-intencionada.

- ***Links:*** Elo ou ligação. Conexão entre um elemento de hipertexto, com uma palavra, expressão, símbolo ou imagem, e outro elemento do documento, outro documento de hipertexto, um arquivo ou *script*. O usuário ativa o vínculo dando um clique sobre o elemento vinculado, que é geralmente sublinhado ou apresentado em cor diferente do restante do documento para indicar que o elemento está vinculado.

- ***M-commerce:*** É o *e-commerce* realizado em plataforma móvel como telefones celulares, PDAs e etc.

- ***Modem:*** Modulador DEModulador: Conversor de sinais analógicos (linha telefônica) em sinais digitais (microcomputador) e vice-versa. É usado para ligações entre computadores por meio da linha teleffônica. Ao adicionar-se uma placa FAX/MODEM, ampliam-se os recursos de microcomputador.

- ***Phishing:*** É uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir usuários ao fornecimento de dados pessoais e

financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na *internet*. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além de mensagens que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

- ***Role-playing game* – RPG**: é um "jogo de interpretação de personagens", ou seja, um tipo de jogo em que os jogadores assumem os papéis de personagens e criam narrativas colaborativamente. O progresso do jogo de RPG se dá de acordo com um sistema de regras predeterminado, dentro das quais os jogadores podem improvisar livremente. As escolhas dos jogadores determinam a direção que o jogo irá tomar.

- ***Scan***: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

- ***Scams* (com "m"):** são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

- ***Site:*** Local na *internet* identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações multimídia.

- **Sistema de Proteção:** Módulo de sistema operacional que controla o acesso aos recursos por parte de programas e usuários, possibilitando a criação de controles e dá suporte à sua execução, autentica operação, mantém registro de operações feitas para auditoria e análise.

- ***Software:*** Programas de computador; instruções que o computador é capaz de entender e executar.

- ***T-banking:*** É a oferta de serviços de Bancos por intermédio da Televisão Interativa.

- ***T –commerce:*** É o comércio eletrônico por meio da Televisão interativa.

- ***URL:*** É um identificador na *internet* que mostra qual o tipo de servidor deve ser acessado, o equipamento em que a informação reside e sua localização nesse equipamento, como por exemplo: <http://oolimpoenlouqueceu.blogspot.com/

- ***Vírus:*** Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa tornar-se ativo e dar continuidade ao processo de infecção.

- **Vulnerabilidade:** Falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

- ***Worm:*** Programa capaz de se propagar automaticamente por meio de redes, enviando cópias de si mesmo de computador para computador. Diferente do *vírus*, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá mediante a exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

- ***Wireless:*** Sem fio

- ***WWW:*** Sistema de acesso a informações da *internet* por meio de hipertextos com capacidade de ler e transmitir várias tecnologias e tipos de documentos, identificados todos os conteúdos por um só endereço URL.

- ***Web - incidentes***: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

TEXTO 1: THE CONSCIENCE OF A HACKER – MANIFESTO HACKER

The Conscience of a Hacker

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?I am a hacker, enter my world...Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..." Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here...Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found. "This is it... this is where I belong..." I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic

bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike."(++++The Mentor++; Written on January 8, 1986)[14]

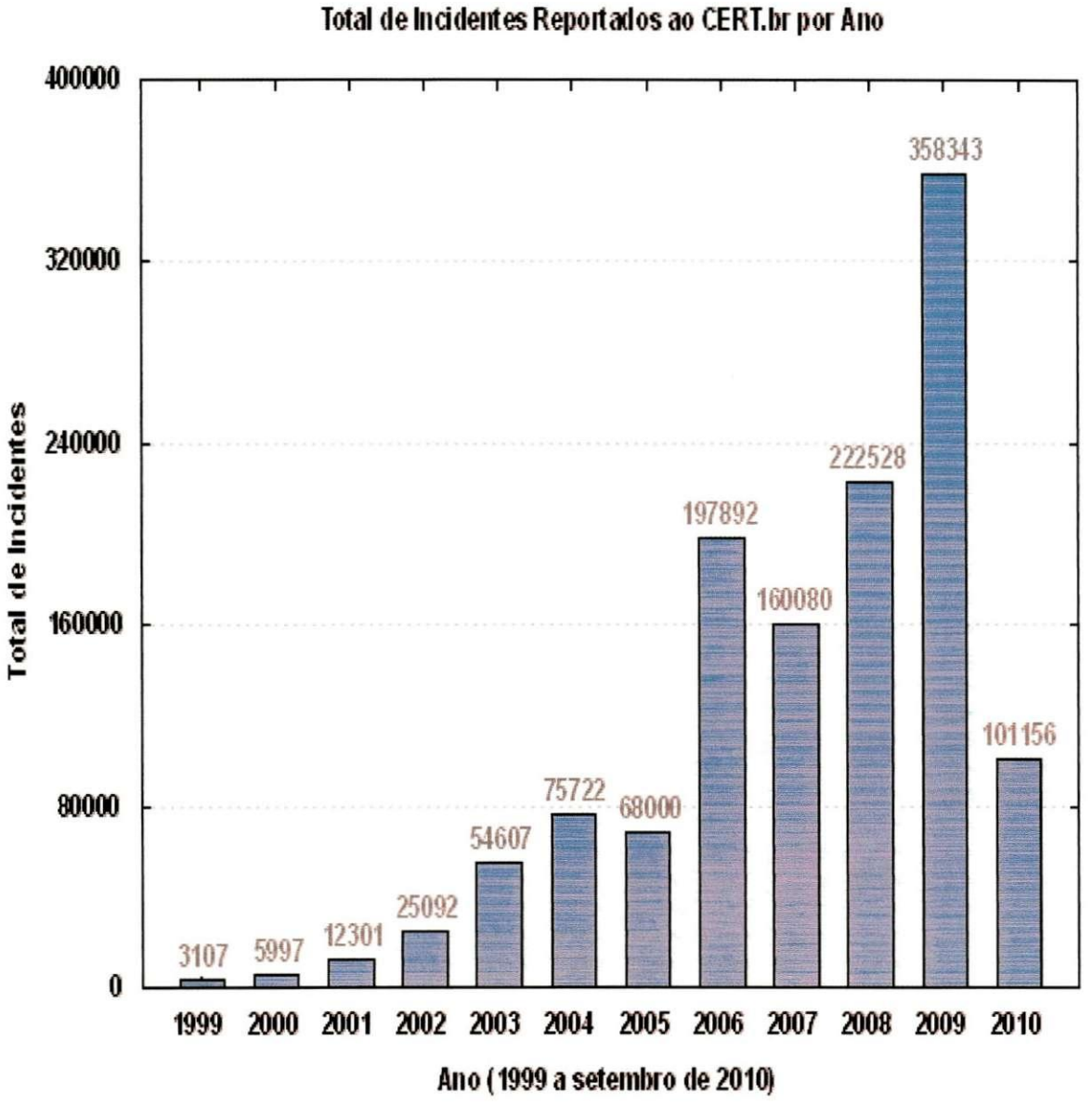
---

[14]*Consciência de um Hacker*: "Mais um foi pego hoje, está em todos os jornais. "Adolescente Preso em Escândalo de Crime Informático", " Hacker preso após invadir Banco"... " Malditos garotos". Eles são todos iguais". Mas você, com sua elegante psicologia e pensamento dos anos 50, alguma vez olhou no fundo dos olhos de um hacker? Você já imaginou o que o faz agir, quais forças o motivam, o que o tornou assim? Eu sou um hacker, entre em meu mundo. Meu mundo é aquele que começa na escola. Eu sou mais esperto que a maioria das outras crianças, esta besteira que nos ensinam me irritam. "Malditos fracassados". Eles são todos iguais. Eu estou na escola no colegial. Eu escutei os professores explicarem pela qüinquagésima vez como reduzir uma fração. Eu entendo isto. " Não, Sra. Smith, eu não demonstrei meus cálculos. Eu o fiz de cabeça". "Criança maldita". "Provavelmente colou. Eles são todos iguais ". Eu fiz uma descoberta hoje. Eu encontrei um computador. Espere um segundo, isto é legal. Faz o que eu mando. Se cometer um erro, é porque eu o obriguei a isso. Não porque não gosta de mim, ou se sinta ameaçado por mim, ou pensa que sou inteligente, ou não gosta de ensinar ou não devesse estar aqui. Criança maldita. Tudo que ele faz é jogar. Eles são todos iguais. E então aconteceu... uma porta abriu-se para um mundo...surfando rapidamente pela linha telefônica como heroína pelas veias de um viciado, uma pulsação eletrônica é enviada, um refúgio para a incompetência do dia-a-dia é procurado...Encontramos uma BBS. "É isto...este é o mundo ao qual pertenço..." Eu conheço todos aqui...até mesmo aqueles que nunca encontrei, com quem nunca conversei, e talvez jamais torne a escutá-los...Eu sei quem são...Crianças malditas. Interrompendo a linha telefônica novamente. Eles são todos iguais...Quer apostar o seu cu que somos todos iguais.... na escola fomos alimentados com comida de bebê quando estávamos famintos por bife ...os pedaços de carne que deixaram escapar já estavam mastigados e insípidos.. Nós fomos dominados por sádicos, ou ignorados pelos apáticos. Os poucos que tiveram algo a nos ensinar quando crianças encontraram em nós discípulos fieis, mas esses foram raros como gotas d'água no deserto. Agora este é o nosso mundo... o mundo do elétron e do computador, a beleza do baud. Nós fazemos uso de um serviço que já existe sem pagar por aquilo que poderia ser baratíssimo se não fosse explorado por especuladores insaciáveis, e vocês nos chamam de criminosos. Nos exploram...e nos chamam de criminosos. Nós buscamos conhecimento...e vocês nos chama de criminosos. Nós existimos sem cor de pele, sem nacionalidade, sem preconceito religioso...e você nos chama de criminosos. Vocês constroem bombas atômicas, vocês promovem guerras, vocês assassinam, enganam, e mentem para nós e tentam nos fazer crer que é para nosso próprio bem, e ainda assim os criminosos somos nós. Sim, eu sou um criminoso. Meu crime é a curiosidade. Meu crime é o de julgar as pessoas pelo que eles dizem e pensam, não pelo que aparentam ser. Meu crime é ser mais inteligente que vocês, algo que jamais irão me perdoará. Eu sou um hacker, e este é meu manifesto. Vocês podem parar este indivíduo, mas vocês não nos poderão parar todos nós...afinal de contas, nós somos todos iguais." (+++ O Mentor+++; escrito em 8 de janeiro de 1986)

TABELA 1: A legislação brasileira e a Convenção sobre o Cibercrime

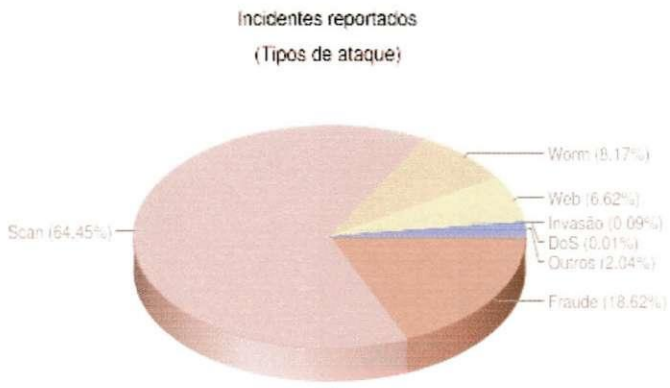
Recomendação da Convenção	Artigos das leis ou códigos
1 – do acesso ilegal ou não autorizado a sistemas informatizados	154-A e 155 4º,V do CP339-A e 240 6º,V do COM
2 – da interceptação ou interrupção de comunicações	art. 16 do Substitutivo
3 – da interferência não autorizada sobre os dados armazenados	154-D, 163-A e 171-A do CP339-D, 262-A e 281-A do COM
4 – da falsificação em sistemas informatizados	163-A, 171-A, 298 e 298-A do CP262-A e 281-A do COM
5 – da quebra da integridade das informações	154-B do CP339-B do COM
6 – das fraudes em sistemas informatizados com ou sem ganho econômico	163-A e 171-A do CP262-A e 281-A do COM
7 – da pornografia infantil ou pedofilia	241 da Lei 8.069, de 1990, Estatuto da Criança e do Adolescente (ECA), alterado pela Lei 10.764, de 2003;
8 – da quebra dos direitos de autor	Lei 9.609, de 1998, (a Lei do Software), da Lei 9.610 de 1998, (a Lei do Direito Autoral) e da Lei 10.695 de 2003, (a Lei Contra a Pirataria);
9 – das tentativas ou ajudas a condutas criminosas	154-A 1º do CP339-A do COM
10 – da responsabilidade de uma pessoa natural ou de uma organização	art. 21 do Substitutivo
11 – das penas de privação de liberdade e sanções econômicas	Penas de detenção, reclusão ou multa, com respectivos agravantes e majorantes das Leis citadas e dos artigos do substitutivo

GRÁFICO 1: VALORES DE INCIDENTES DE SEGURANÇA ACUMULADOS DO ANO DE 1999 AO ANO 2010[15]



[15]CERT/BR. Disponível em: < http://www.cert.br/stats/incidentes/ > Acesso em : 12 de outubro de 2010, as 18:57 hs.

GRÁFICO 2: TIPOS DE ATAQUES (Incidentes reportados ao CERT/BR no período de julho a setembro de2010) [16]



Obs.: Vale lembrar que não se deve confundir scan com scam.

GRÁFICO 3: *SCANS* REPORTADOS POR PORTA (Percentual *CERT*.br -- Julho a Setembro de 2010)[17]

[16]CERT/BR. Disponível em: < http://www.cert.br/stats/incidentes/2010-jul-sep/tipos-ataque.html > Acesso em : 12 de outubro de 2010, as 18:57 hs.

[17]CERT/BR. Disponível em: < http://www.cert.br/stats/incidentes/2010-jul-sep/scan-portas.html > Acesso em : 12 de outubro de 2010, as 18:57 hs.

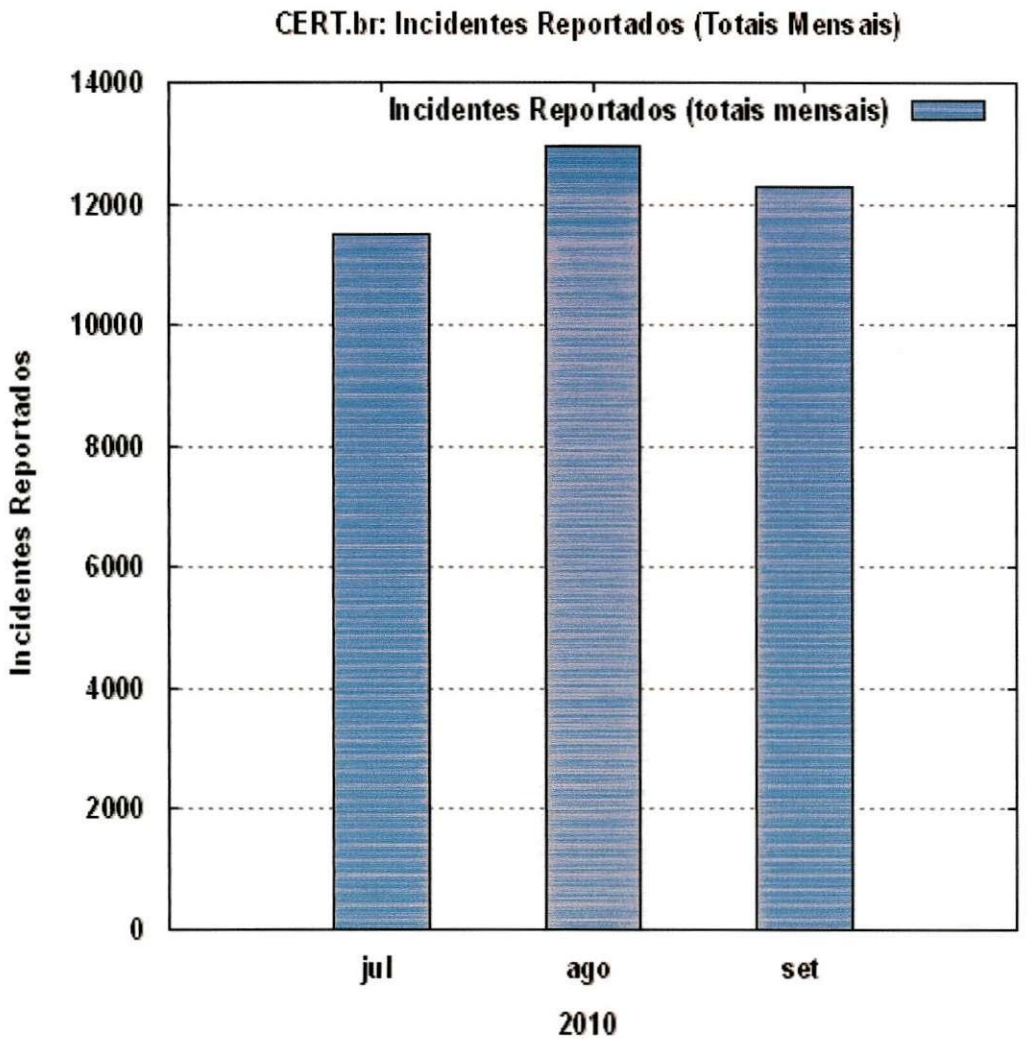
GRÁFICO 4: TENTATIVAS DE FRAUDES (Percentual CERT.br -- Julho a Setembro de 2010)[18]

Legenda:

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

[18]CERT/BR. Disponível em: < http://www.cert.br/stats/incidentes/2010-jul-sep/fraude.html> Acesso em: 12 de outubro de 2010, as 18:59 hs.

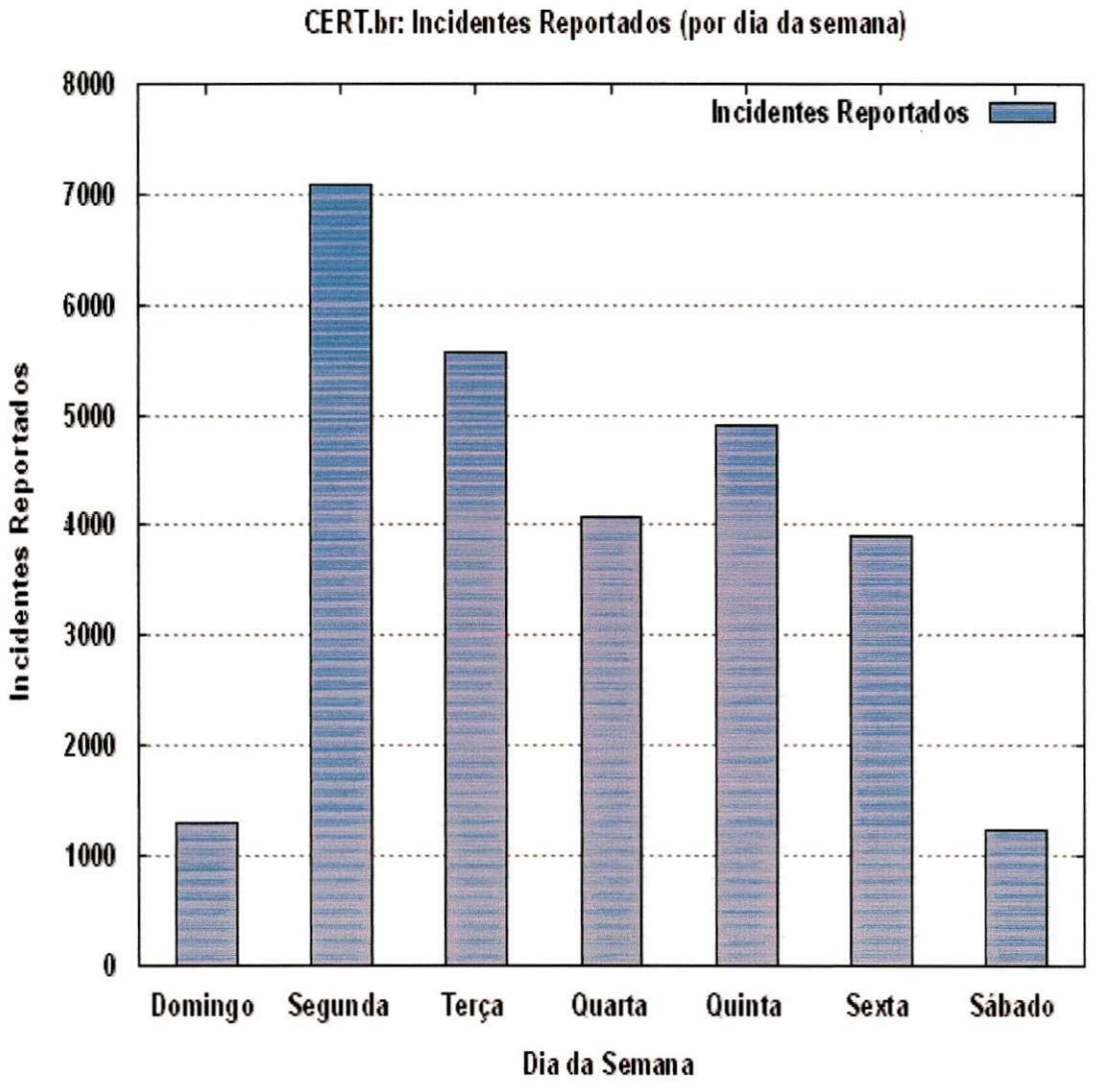
GRÁFICO 5: PERCENTUAL MESAL (Incidentes Reportados ao CERT.br -- Julho a Setembro de 2010)[19]



Obs: Este gráfico não inclui os dados referentes a worms.

[19]CERT/BR. Disponível em: < http://www.cert.br/stats/incidentes/2010-jul-sep/ataques-mensal.html >Acesso em: 12 de outubro de 2010, as 18:59 hs.

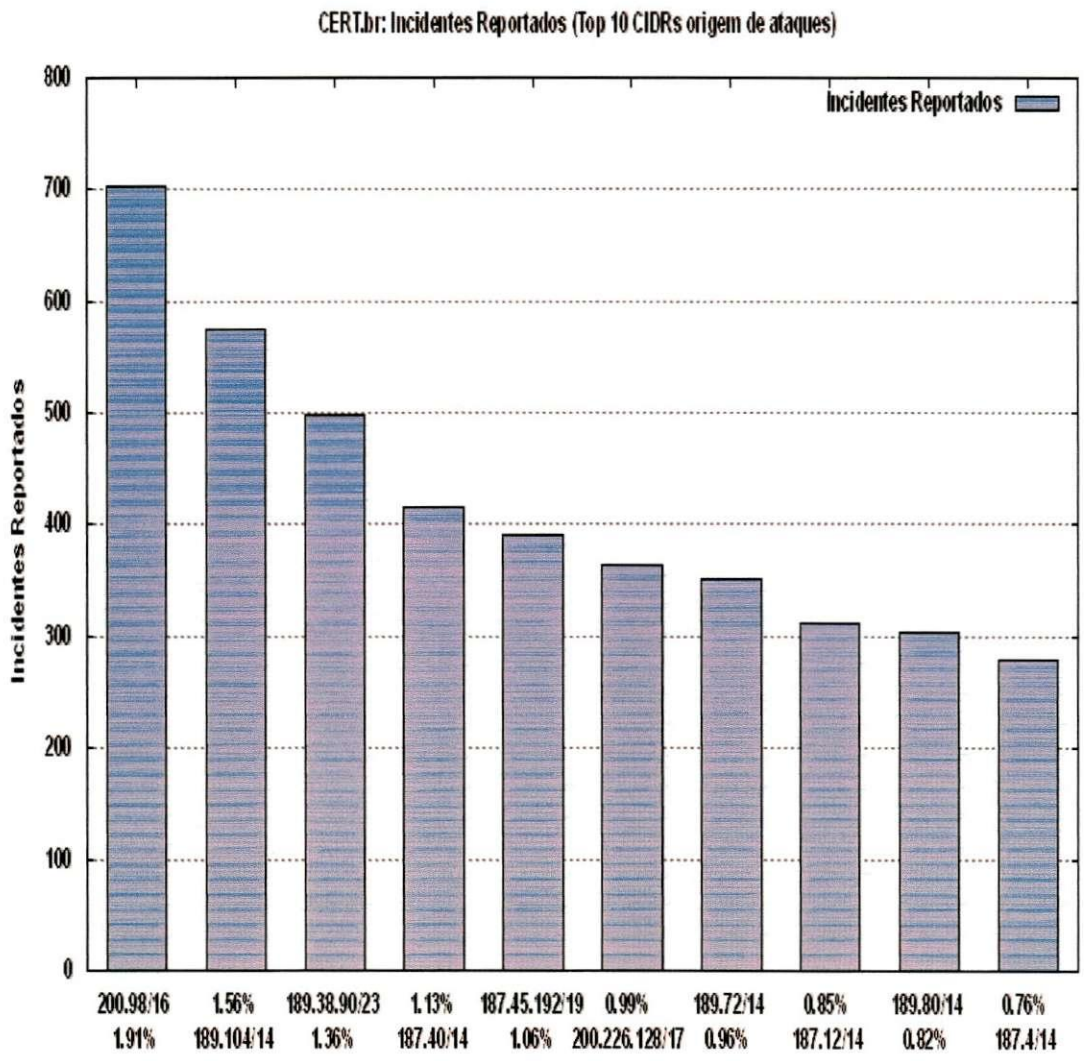
GRAFICO 6: NÚMERO DE INCIEDENTES POR DIAS DA SEMANA (Incidentes Reportados ao CERT.br -- Abril a Junho de 2010)[20]



Este gráfico não inclui os dados referentes a worms.

[20]CERT/BR. Disponível em: < http://www.cert.br/stats/incidentes/2010-jul-sep/weekdays-incidentes.html >Acesso em: 12 de outubro de 2010, as 18:59 hs.

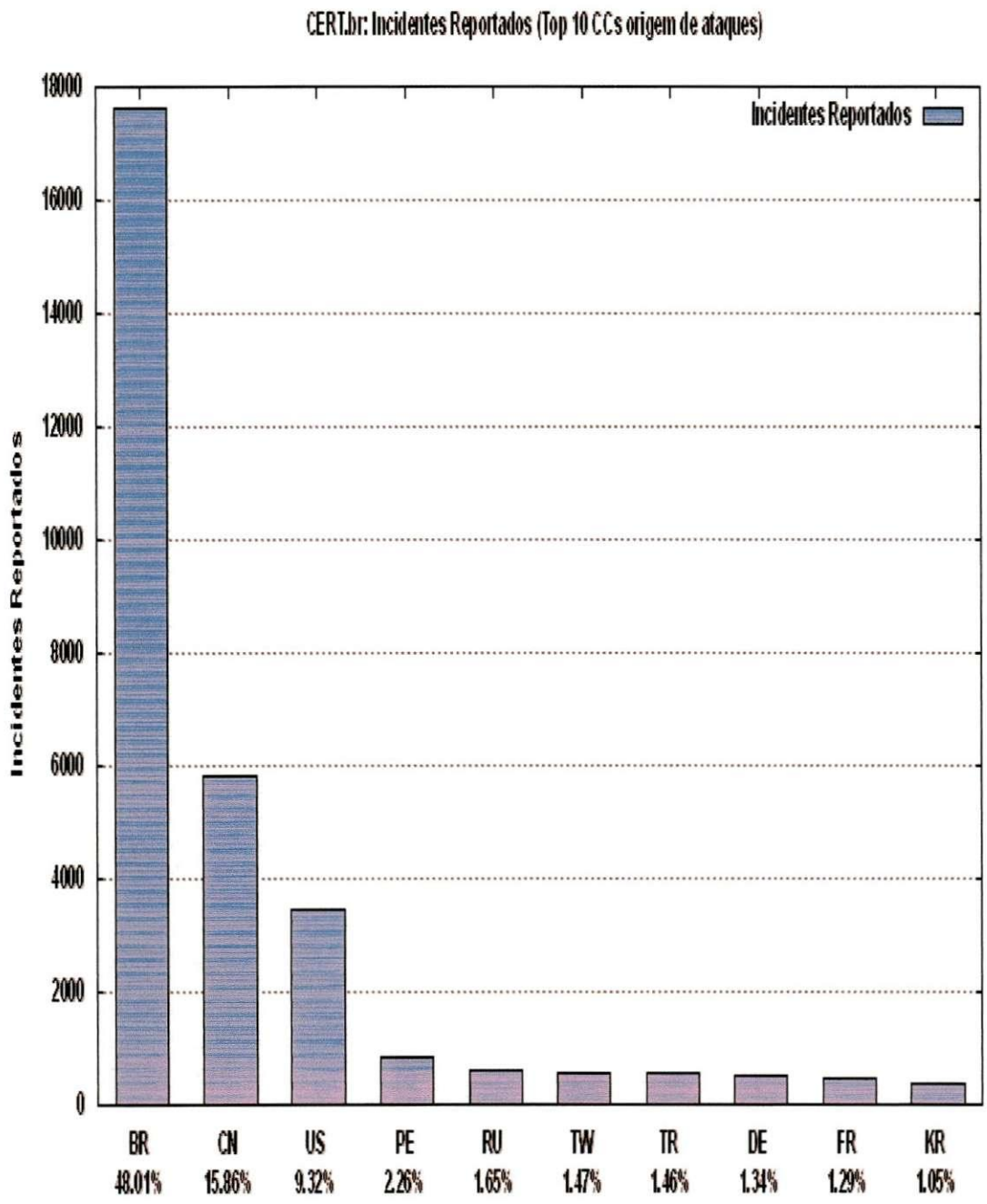
GRÁFICO 7: ORIGEM DOS ATAQUES – CIDR (Incidentes Reportados ao CERT.br -- Julho a Setembro de 2010)[21]



Obs: Este gráfico não inclui os dados referentes a worms.

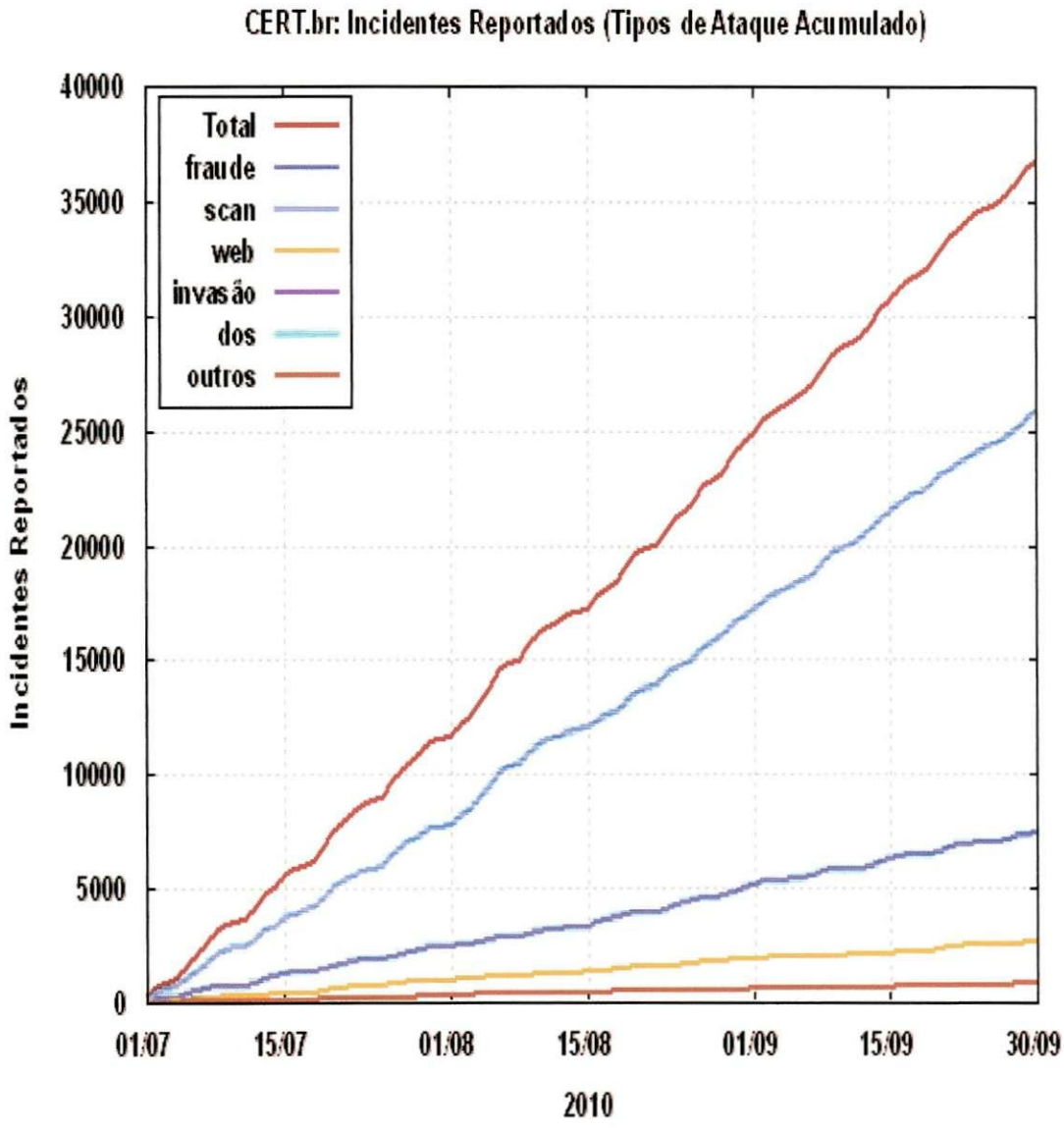
[21]CERT/BR. Disponível em: < http://www.cert.br/stats/incidentes/2010-jul-sep/top-atacantes.html >Acesso em: 12 de outubro de 2010, as 18:59 hs.

GRÁFICO 8: ORIGEM DOS ATAQUES – *Country Code* (Incidentes Reportados ao CERT.br -- Julho a Setembro de 2010)[22]



[22]CERT/BR. Disponível em: < http://www.cert.br/stats/incidentes/2010-jul-sep/top-atacantescc.html >Acesso em: 12 de outubro de 2010, as 18:59 hs.

GRÁFICO 9: TIPOS DE ATAQUE ACUMULADOS (Incidentes Reportados ao CERT.br -- Julho a Setembro de 2010)[23]



[23]CERT/BR. Disponível em: < http://www.cert.br/stats/incidentes/2010-jul-sep/tipos-ataque-acumulado.html>Acesso em: 12 de outubro de 2010, as 18:59 hs.