CENTRO UNIVERSITÁRIO LUTERANO DE PALMAS
COMUNIDADE EVANGÉLICA LUTERANA "SÃO PAULO"
Credenciado pelo Decreto de 06/07/2000 - D.O.U. nº 130 de 07/07/2000

Luís Godinho Júnior

LEI N.º 12.737/12 – CRIMES ELETRÔNICOS: uma análise da efetividade da norma na prevenção dos delitos

Palmas – TO
2013

CENTRO UNIVERSITÁRIO LUTERANO DE PALMAS
COMUNIDADE EVANGÉLICA LUTERANA "SÃO PAULO"
Credenciado pelo Decreto de 06/07/2000 - D.O.U. nº 130 de 07/07/2000

Luís Godinho Júnior

LEI N.º 12.737/12 – CRIMES ELETRÔNICOS: uma análise da efetividade da norma na prevenção dos delitos

Projeto de Pesquisa apresentado como requisito parcial da disciplina de Trabalho de Curso em Direito II (TCD II), do Curso de Direito do Centro Universitário Luterano de Palmas – CEULP/ULBRA.

Orientador: Prof. Gustavo Paschoal Teixeira de Castro

Palmas – TO
2013

Luís Godinho Júnior

LEI N.º 12.737/12 – CRIMES ELETRÔNICOS: uma análise da efetividade da norma na prevenção dos delitos

Projeto de Pesquisa apresentado como requisito parcial da disciplina de Trabalho de Curso em Direito II (TCD II), do Curso de Direito do Centro Universitário Luterano de Palmas – CEULP/ULBRA.

Orientador: Prof. Gustavo Paschoal Teixeira de Castro

Aprovado em:_____/_____/_____

BANCA EXAMINADORA

_____
Prof. Gustavo Paschoal Teixeira de Castro
Centro Universitário Luterano de Palmas

_____
Prof. Thiago Perez Rodrigues da Silva
Centro Universitário Luterano de Palmas

_____
Prof. Sinvaldo Conceição Neves
Centro Universitário Luterano de Palmas

Palmas – TO
2013

RESUMO

Qualquer profissional, em especial da área jurídica, deve está atento as modificações que atingem a sociedade principalmente as que fazem surgir novos hábitos. A Internet tem proporcionado uma revolução e devemos entender que não se trata de uma realidade fria, exclusivamente tecnológica, longe do mundo cotidiano. Nos últimos 20 anos as pessoas tem passado cada vez mais tempo conectadas na Internet, e por consequência os crimes cometidos no ambiente virtual também cresceram tais como: violação de email, pirataria de software, pichação de Home Page, vandalismo em redes virtuais, danos provocados por vírus. Partindo do pressuposto que o Direito deve acompanhar a evolução da sociedade, e como estudante de Direito devemos nos projetar a frente destes anseios por inovações, propondo, discutindo regulamentos e normas a minimizar conflitos dos indivíduos que utilizam destes inventos.

Palavras-chave: cibercrime – invasão a dispositivos informáticos – ciberespaço.

Dedico este trabalho:

a Deus por me iluminar não só neste trabalho, mas na vida;
aos meus pais (Luis e Aparecida);
a minha Esposa (Jacqueline);
ao meu filho (Gabriel) e ao Professor Gustavo que além de me orientar, me empresou um livro que me ajudou muito neste trabalho;
e a todos que direta ou indiretamente me incentivaram a concluir esta obra, que parecia não sair do lugar. Agora sim terminei!

SUMÁRIO

INTRODUÇÃO

O ser humano é bastante laborioso na busca por sua evolução e atualmente somos protagonistas na chamada revolução da informação, onde o bem de valor é o conhecimento. Em decorrência das inovações e descobertas que a grande rede (Internet) possibilita fez tornar a sociedade mais conectada e cujas condutas se tornam cada vez mais virtuais.

Segundo recomendações e boas práticas para o uso seguro da Internet para toda a família disponibilizada em 2011 pela OAB-SP em forma de cartilha afirma que: infelizmente, para cada nova descobertas existem vantagens e desvantagens, e neste caso, a desvantagem trazida por esta poderosa ferramenta de comunicação foi a facilidade de se cometer alguns delitos, incrementando a pratica de crimes comuns e com a facilidade de realiza-los a distancia, tais como: (furto, estelionato, ameaça, extorsão, pornografia infantil etc.) de forma que os delitos virtuais tiveram aumento na mesma proporção dos avanços tecnológicos.

Qualquer profissional, em especial da área jurídica, deve está atento as modificações que atingem a sociedade principalmente as que fazem surgir novos hábitos. A Internet tem proporcionado uma revolução e devemos entender que não se trata de uma realidade fria, exclusivamente tecnológica, longe do mundo cotidiano. "Em breve análise pode-se dizer que a Internet é mais que um simples meio de comunicação eletrônica, não se trata apenas de uma rede de computadores, mas, também, de uma rede mundial de pessoas. Indivíduos conectados, que interagem e estabelecem relações jurídicas a cada clique." (PINHEIRO, 2007).

Nos últimos 20 anos as pessoas tem passado cada vez mais tempo conectadas na Internet, e por consequência os crimes cometidos no ambiente virtual também cresceram (CELLA, 2012). O crime praticado no meio virtual é denominado pelos doutrinadores, como: Patrícia Peck Pinheiro 2010 e Renato Opice Blum 2011, como sendo crimes digitais que é um subtipo de crimes eletrônicos (FILHO, 2005). Esses crimes podem ser divididos em próprios e impróprios, os próprios são aqueles que só podem ser praticados por meios dos recursos eletrônicos, tais como: violação de email, pirataria de software, pichação de Home Page, vandalismo em redes virtuais, danos provocados por vírus. Já os crimes ditos impróprios são aqueles que existiam independentemente dos recursos eletrônicos existirem, mas para potencializar os resultados da prática delituosa fazem o uso destes recursos, para cometer, por exemplo: estelionato, pedofilia, etc. (MORAIS, 2012).

A legislação vigente se aplica na maioria dos crimes eletrônicos, permitindo penalizar o autor do crime. É uma ilusão pensar que se está em "terra de ninguém" acreditando na

impunidade. As autoridades já elucidaram casos dos mais diversos crimes, neste meio em questão, resultando em condenações aos seus infratores.

Direito Eletrônico é um ramo, relativamente novo, autônomo da ciência jurídica com abrangência em diversos campos do direito, para não dizer todos, seu conteúdo científico aplicar-se-á na totalidade de matérias normativas. Relacionando com o Direito Constitucional, Direito Penal, Direitos Humanos, Propriedade Intelectual, Direito Civil, Direito Comercial, Direito Administrativo, Direito do Trabalho, Direito Tributário, Direito do Consumidor, Direito Eleitoral, Filosofia do Direito, Direito Ambiental, Direito Processual, Direito de Marcas e Patentes e a Ética na Advocacia. Neste sentido podemos dizer que Direito Eletrônico trata-se da inovação do próprio Direito (ZANATTA, 2010).

Partindo do pressuposto que o Direito deve acompanhar a evolução da sociedade (RICCI, 2011), e como estudante de Direito devemos nos projetar a frente destes anseios por inovações, propondo, discutindo regulamentos e normas a minimizar conflitos dos indivíduos que utilizam destes inventos.

Este trabalho tem por objeto central a analise da efetividade da Lei n.º 12.737/12 (popularmente conhecida como lei Carolina Dieckmann) na abrangência dos crimes eletrônicos.

O tema hora trabalhado demonstra sua relevância principalmente na prática, e refletirá cada vez mais de forma crucial no Direito, não só em relação a informática no âmbito jurídico, mais também em relação a novos institutos e situações que surgiram a partir desta inovação (Direito Eletrônico), como crimes no meio cibernético, os serviços eletrônicos disponíveis nos sítios do Supremo Tribunal Federal (e-STF), no Superior Tribunal de Justiça (e-STJ), serviços do governo eletrônico (e-gov), serviços da Receita Federal e-cpf, e-cnpj para que seja inseridos e validados nos contratos eletrônicos, Assinatura Digital que permite assinar por exemplo em processos eletrônicos, dentre outras inovações (MONTEIRO, 2010). Neste sentido, pode se afirmar que é notório a relevância teórica não só para os operadores do Direito, mas para a sociedade em geral.

Além das importâncias teóricas e praticas pode se dizer que há também a importância econômica, pois quando se trabalha com material em mídia digital, torna-se muito fácil esta ser copiada, compartilhada, e, portanto, está em vários lugares ao mesmo tempo, estando suscetíveis de serem adulteradas (caso não tenha algum dispositivo de segurança como criptografia) vendidas de forma ilegal (pirateadas), ou seja, cometendo crimes em relação a Lei nº 9.610 / 98 que trata-se dos Direitos Autorais, trazendo prejuízos não só para os autores

mas também para o Estado, que diminuem a arrecadação em relação as vendas de musicas, softwares, livros. Também é possível a invasão a contas de email de funcionários de grandes empresas e obterem de forma ilícita dados sigilosos.

No 1º capítulo será apresentado uma visão da importância do Direito Eletrônico para sociedade que está cada vez mais conectada adquirindo novos hábitos, costumes, novas formas de se comunicarem. Com todas estas transformações que acaba refletindo socialmente, traz preocupações aos profissionais do Direito em garantir a ordem social e o Estado Democrático de Direito. Nada obstante ao gigantesco benefício da internet para a sociedade moderna, porém o lado negativo existe, é este ponto que será abordado. Ainda neste capitulo abordará os principais crimes contra bens jurídicos cometidos por meio de sistemas de computador, a evolução do judiciário, e o uso do processo em meio eletrônico.

No capítulo seguinte tendo a preocupação apresentada no capítulo anterior, e diante deste cenário inovador se faz necessário o estudo dos aspectos jurídicos e adaptações ao Direito que esteja em consonância com este novo e promissor território virtual, sem fronteiras, chamado Ciberespaço. Serão apresentadas também soluções de conflitos entre indivíduos conectados bem como a união pacifica entre os membros em conquistar novos horizontes com o devido respeito aos limites virtuais nas relações ali existentes. Ainda neste, serão comentados sobre a Lei n.º 12.737/12, suas implicações e o que revela o Direito Estrangeiro.

No capítulo de número 3, o assunto norteador é sobre a privacidade e intimidade na era tecnológica, neste o estudo será sobre a liberdade de expressão e o direito a privacidade que com o acesso fácil a informações atualizadas e disponíveis a qualquer cidadão deram origem a mutações sociais, educacionais, políticas e econômicas como nunca visto antes. A proteção constitucional em meio ao uso da comunicação eletrônica, que com todas estas modernidades tecnológicas catalisam a preocupação sobre a invasão da privacidade. Tendo estas situações qual é a tutela jurisdicional no ciberespaço? Segue se o estudo.

1. DIREITO ELETRÔNICO: UMA VISÃO INICIAL

A sociedade tem vivenciado profundas e significativas mudanças sobre questões que envolva a tecnologia digital mais especificamente as inseridas na internet, esclarecendo algumas lacunas objetivas, as quais são objetos de estudos do direito que procura entender e, se necessário, propor normas que venham a preencher estes espaços 'abertos' com a crescente popularização da grande rede (CORRÊA, 2000).

Sobre as fascinantes informações disponibilizadas na internet o escritor Corrêa fez a seguinte projeção:

> A ciência jurídica, por conseguinte, não pode abstrair-se de algo assustadoramente grande, e que até o ano 2010 chegará a uma marca superior a 600 milhões de usuários, pessoas conectadas a um ponto comum, relacionando-se entre si, das mais diversas localidades do globo, não havendo limites de passagem e expressão. O grande desafio para o direito é a compreensão e o acompanhamento dessas inovações, garantido assim a pacificação social, e o desenvolvimento sustentável dessas novas relações e, acima de tudo, a manutenção do próprio Estado Democrático de Direito (CORRÊA, 2000, p. 3).

É difícil estabelecer uma correta projeção sobre a quantidade estimada de usuários conectados a internet ainda mais quando se tem um espaço de dez anos, como o que foi feito pelo escritor citado anteriormente. Segundo a União Internacional de Telecomunicações (UIT) organização internacional destinada a padronizar e regular os assuntos relativos ao uso das ondas de rádio e telecomunicações internacionais, divulgou que no final de 2010 o número de usuários da internet chegou a 2,08 bilhões, contra 1,86 bilhão um ano antes (UIT, online). O importante a destacar da citação é a preocupação em que o direto deve acompanhar as inovações garantindo a ordem social e o Estado Democrático de Direito.

A forma de comunicação entre as pessoas se transformou e a cada dia se torna mais popular, pois o acesso facilitado muitas das vezes pelo o governo como a redução do Imposto sobre Produto Industrializado (IPI) fez com que mais pessoas adquirissem dispositivos eletrônicos, que permitem o acesso rápido a internet, que também está cada vez mais rápida com a concorrência das operadoras e a disponibilização da chamada banda larga. Fazendo com que mais pessoas estejam conectadas e por mais tempo submetidas aos benefícios decorrentes do acesso rápido a informações.

Nada obstante ao gigantesco benefício da internet para a sociedade moderna, porém o lado negativo existe, é este ponto mais interessante ao direito (CORRÊA, 2000).

O agente que comete um delito no meio eletrônico difere dos demais, pois não utiliza nenhum armamento a não ser seu intelecto e dos conhecimentos técnicos, para executar seu ato infracional a distancia (ANDRADE, 2009).

A dificuldade de se relacionar os crimes cometidos via internet esta em encontrar as evidências que cheguem ao autor. Uma invasão a sistema alheio realizado por alguém que detenha prestigioso conhecimento técnico poderia alterar arquivos e eliminar rastos de vestígios que o em criminaria. "Um crime perfeito, sem traços, e, portanto, sem evidências" (CORREIA, 2000). Em princípio o crime eletrônico não é crime fim, por natureza, e sim um crime de meio, ou seja, utiliza - se de um meio virtual para ocorrer (ZANATTA, 2010). Os crimes eletrônicos tiveram suas primeiras referencias por volta de 1960 tendo maiores incidências nos casos de manipulação e sabotagem de sistemas de computadores (CARNEIRO, 2011). Estes crimes podem ser destacados em dois tipos: os que são cometidos por meio do computador, e os contra os sistemas de computadores (ANDRADE, 2009). Dessa forma pode – se classificar os delitos eletrônicos em duas grandes categorias, a saber:
crimes cometidos contra um sistema de computador; crimes contra outros bens jurídicos, por meio de um sistema de computador.

Crimes cometidos contra um sistema de computador: trata–se, dos crimes virtuais/eletrônico propriamente dito onde o agente utiliza de um dispositivo eletrônico (computador, tablet, celular) para ter acesso a sistemas de outros dispositivos eletrônicos sem que o sujeito passivo tenha autorizado. Dessa forma o computador, segundo ensina Adeneele Garcia Carneiro:

> ...é meio para execução do crime nessa categoria de crimes está não só a invasão de dados não autorizados mais toda a interferência em dados informatizados como, por exemplo, invasão de dados armazenados em computador seja no intuito de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o software ou hardware do computador e só podem ser concretizados pelo comutador ou contra ele e seus periféricos... (CARNEIRO, 2011, online).

Os crimes eletrônicos cometidos contra um sistema de computador atacam a maquina em se, com o objetivo de causar dano a vitima ou obter vantagem ilícita que pode ocorrer por introdução de dados falsos ou alteração de resultados.

Seguindo este mesmo raciocínio se posiciona Damásio de Jesus apud (CARNEIRO, 2011, online):

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

Crimes contra outros bens jurídicos, por meio de um sistema de computador: trata-se dos crimes em que o agente utiliza o computador como meio para produzir alguma conduta ilícita já tipificada, ameaçando ou lesando outros bens, não computacionais ou diversos da informática (ARAS, 2001).

Devido, sobretudo ao anonimato que a internet proporciona aos seus usuários somados com algumas brechas nos sistemas computacionais torna o ambiente muito propício aos "delinquentes virtuais" (TEXEIRA, 2007) fazendo com que potencializa o surgimento dos mais variados formas de crimes tais como estelionato eletrônico, calúnia, injuria, difamação, racismo, pedofilia, invasão de privacidade, subtração de dados bancários, uso não autorizado de imagem de pessoas, Cyberbulling, Cyber Terrorismo, dentre outros a ser dissecados a seguir.

"Ocorre que frente à importância da identificação do autor do crime e a dificuldade desta identificação, surgiu à necessidade de se traçar um perfil denominando grupos que praticam determinados crimes virtuais, dentre essas denominações temos a figura do hacker" (CARNEIRO, 2010, online).

Pode ser considerado um hacker aquela pessoa que detém conhecimentos atilados sobre sistemas computacionais e que usa de suas habilidades técnicas para 'ganhar' acesso a sistemas privados. Existem empresas que contratam hackers para proteção de seus sistemas, banco de dados, seus segredos profissionais (ANDRADE, 2009). "Contudo, no submundo virtual, a terminologia "hacker" dificilmente é associada a fins criminosos, sendo correlacionada tão somente a um indivíduo extremamente hábil no campo informático" (NETO, 2003). Com o passar dos tempos hacker tornou - se gênero e as espécies de hackers podem variar de acordo com as práticas, uma das espécies são os crackers;

O Cracker é aquele hacker que utilizam seus conhecimentos com motivação criminosa agindo com o objetivo de se obter vantagens ilícitas (CARNEIRO, 2010). São como os hackers não éticos, ou "maus", que atuam invadindo sistemas com interesses patrimoniais ou danosos (NETO, 2003);

Os Phreakers também são hackers, mas com especialidades em telefonia móvel ou fixa que comentem crimes específicos voltados para a área de telecomunicações;

Os Piratas são "Indivíduos que clonam programas fraudando direitos autorais" (NETO, 2003);

Os Distribuidores de Warez são "webmaters que disponibilizam em suas páginas softwares sem autorização dos detentores dos direitos autorais" (NETO, 2003).

A técnica do phishing que é um termo oriundo do inglês (fishing) e quer dizer pesca, trata-se de um tipo de fraude eletrônica, consiste em enviar vários e-mails (span) para um publico diversificado de pessoas, utilizando algum fator surpresa com conteúdo apelativo para chamar a atenção. Como o e-mail é geralmente enviado com conteúdo que chame muita atenção se passando por empresas renomadas, a vítima acredita ser real e clica ou baixe arquivos anexados, assim captura informações pessoais sensíveis como senhas de acesso ou número de cartões de crédito e envia para os fraudadores que com base nestas informações passam a cometerem os delitos como acesso não autorizados em sistemas computacionais, furtos nas contas bancárias ou cartões de créditos. Os usuários de Lan House devem ficar atentos ao acessar sites de comércio eletrônico ou de internet banking, pois pode ter programas espiões especificamente voltados para a captura de dados pessoais (VALLOCHI, 2004).

Os chamados 'Cavalo de Tróia', também conhecida por Trojans Horse, é um programa que se passa como um arquivo no computador da vítima, tem o objetivo de controlar o sistema. Em geral é instalado em decorrência de um phishing scan. "O nome cavalo de Tróia deriva do famoso episódio de soldados gregos escondidos em um cavalo de madeira dado como presente aos troianos durante a guerra entre os dois povos" (VALLOCHI, 2004).

Diferente dos vírus, o cavalo de Tróia não tem o poder de se replicar, tem espaços de tempo definido para atuarem e captura dados em uma única máquina.

Segundo o doutrinador Artur José Concerino (apud TEIXEIRA, 2007):

> A partir de uma pesquisa da empresa Attrition, soube-se que o Brasil é o país que está em primeiro lugar quanto aos ataques de delinquentes virtuais realizados no mundo com 3,56% à frente dos Estados Unidos que teve 2,65%. Essa organização diz que uma possível explicação para isso é o fato de que os hackers americanos possuem maior prática, não deixando pistas e impedindo o rastreamento do crime, diminuindo o registro de ataques. A mesma pesquisa revelou que, de 4.573(quatro mil quinhentos e setenta e três) ataques feitos nos Estados Unidos, mais de 45% foram à empresas comerciais; 6,91% à organizações não governamentais; 5,71% à redes de provedores e 4,77% à organizações educacionais. A Nasa recebeu 39 ataques, as redes militares 65 e as policias nove (TEIXEIRA, 2007, p. 49).

Da citação do parágrafo anterior pode abstrair-se o quanto é significativo à quantidade de delitos eletrônicos. O criminoso eletrônico é aquele que usa a maquina computadorizada de forma ilegal, traiçoeira, não ética, de forma a executar praticas delituosa remotamente a atingir o sujeito passivo. Ocorre que frente à necessidade de se identificar o autor do crime e a complexidade de chegar ao sujeito ativo, fez se atinente a definição de perfis classificando em grupos conforme as praticas de determinadas condutas no submundo virtual. Sendo assim classificam-se os principais:

Clonagem de cartões de crédito: As operadoras de cartões de crédito frequentemente alertam seus clientes sobre a existência destas fraudes, o que não tem sido suficiente para inibir esta pratica delitiva, fazendo com que os prejuízos sejam reduzidos por meio do aumento das taxas de anuidade, de juros, dentre outras despesas repassadas para os clientes, que com receio passam a se recusar a internet com forma de efetuar compras com cartão (CORRÊA, 2000). Este delito consiste geralmente em ataques feitos por crackers a servidores de empresas que desenvolve atividade mercantil pela internet (e-commerce) subtraindo informações sensíveis tais como: nome e números de cartões de créditos de seus clientes. Tendo este fato gerado inúmeros prejuízos econômicos para a empresa envolvida, bem como danos e incômodos aos clientes (TEIXEIRA, 2007).

Lavagem eletrônica de dinheiro: O crime organizado em especial o tráfico de drogas movimenta diariamente volumosos numerários econômicos tendo o dinheiro passado por uma complexa rede de intermediários e por uma igualmente complexa série de contas e investimentos bancários. "Tais divisas ilegais entram pela internet ou por outra rede de contas de companhias e empresas, e em seguida, são transferidas rapidamente para outras contas, e assim sucessivamente" (CORRÊA, 2000, p. 54). E desta forma realizando a "lavagem" do dinheiro.

Cyber Terrorismo: Trata-se de um ataque em geral destrutivo contra uma rede de computadores com o intuito de destruir bens e prejudicar vidas humanas. Como exemplo pode-se destacar ataques a sistemas que controla aviões, possibilitando controlar remotamente a aeronave, deixando que o piloto tenha informações importante tais como: direção, altitude, velocidade. Tornando - se assim possíveis ataques sem suicidas (ANDRADE, 2009).

Racismo na Internet: Racismo é uma tendência de pensamento com o intuito de majorar as diferenças entre seres humanos tendo como base conjunto de opiniões pré-concebidas. Pessoas que tem por este hábito encontraram na internet, mas especificamente nas redes sociais fonte de disseminação destes pensamentos sórdidos. Em geral estes

posicionamentos racistas e discriminatórios são contra negros, indígenas e judeus (ANDRADE, 2009).

Pirataria de Software: A internet propicia a violação dos direitos de propriedade intelectual do software, pois facilita a copia e/ou distribuição de programas pirateados. Infringindo a Lei da proteção da propriedade intelectual de programas de computador, lei n. 9.609 de 19 de fevereiro de 1998 (TEXEIRA, 2007). O ordenamento jurídico foi surpreendido com a celeridade em o progresso tecnológico vem se inserido na sociedade informacional, concebendo mudanças intrínsecas em relação a modelos de produção de conhecimento menos individualistas para mais colaborativos. Forçando mudanças nos paradigmas de conhecimento, evidenciando – se que cada conquista tecnológica é acompanhada do surgimento de novos desafios para a ciência jurídica (WACHOWICZ, 2010).

Sobre a proteção jurídica do software a mestre Elizabeth Dias K. Pereira diz:

> Toda a elaboração do software, além de requerer, por um período razoável de tempo, pessoas com habilidades técnicas apuradas e especializadas, requer um custo altíssimo. Daí a necessidade de o sistema jurídico proporcionar proteção, meios de defesa adequados, para que a propriedade alheia não seja devastada (PEREIRA, 2002, p. 80).

Para que as atividades no computador ocorram é necessário o uso de software ou programa computacional, que se trata de uma sequencia de algoritmos organizados logicamente e escrito em uma linguagem que o computador a intérprete. Toda esta atividade é exercida por um programador que o elabora escolhendo e organizando a informação em instruções lógicas, para isto, requer habilidade técnica, experiência, tempo, treinamento dentre outros. Por estas razões software é obra intelectual, resultado da produção da mente humana. Quando se compra um software, na verdade se adquire uma licença de uso. A compra de software 'pirateado' corrobora com a organização criminosa, diminui a arrecadação e a oferta de empregos, além de afastar investimentos de empresas estrangeiras que não se sente seguras no desenvolvimento em novos produtos.

Espionagem Industrial: Consiste em fornecer informações confidenciais ou segredos comerciais sem a autorização dos detentores dessa informação, tendo por objetivo a obtenção de vantagens econômicas de forma desleal. A Internet é uma ferramenta que facilita a espionagem e as transferências destas informações obtidas ilegalmente. Tendo esta pratica de espionagem industrial aumentada nos últimos tempos, fizeram com que as empresas revisassem as formas de acesso as informações principalmente a cerca de produtos a serem

lançados, pois não muito raro uma empresa projetar um produto e ver este mesmo produto lançado por outra que patenteou em seu nome (AGUIAR, 2009).

Pornografia Infantil: A pornografia infantil é caracterizada pela publicação de fotos de crianças pré-púberes e por isto é uma forma ilegal de pornografia. "Tais atitudes vêm sendo veementemente condenadas pela mídia e pela sociedade em geral, e erroneamente recebem a denominação de pedofilia" (AGUIAR, 2009). Embora seja diferente da pedofilia, de uma forma ou de outra acaba se relacionando, pois quando se publica fotos de crianças contendo senas de sexo, se atribui a ocorrência de violenta exploração. A palavra pedofilia vem do grego atração ou afinidade por criança.

De acordo com a afirmação do estudioso Daniel Pedrosa Aguiar:

> ... pode-se definir que um pedófio nem sempre pode ser considerado um criminoso, mas sim um ser que necessita de tratamento psiquiátrico, porém quem comete pornografia infantil provavelmente terá como causa esta patologia. Tal conduta criminosa, porém, não isenta o autor das consequências penais existentes em nossas legislações... (AGUIAR, 2009, online).

Pedofilia é considerada distúrbio psíquico que se caracteriza pela obsessão por práticas sexuais não aceitas pela sociedade. A relação sexual ou ato libidinoso praticado por adulto com criança ou adolescente menor de 14 anos é considerada crime Conforme o artigo 241-B do Estatuto da Criança e do Adolescente (ECA). Para consumar esta prática reprovável, os pedófilos costuma usar salas de bate-papo ou redes sociais na internet.

Invasão de Privacidade: Atualmente a informação de dados pessoais tem sido intensivamente utilizada para práticas comerciais permitindo a fornecedores e produtores de mercadorias e/ou serviços alavancarem vantagens sobre concorrentes. Desta forma perfis com dados consolidados de consumidores alvos são de grande valia na rede de empresários dispostos a pagar por esta informação (LINS, 2000).

A inviolabilidade a intimidade, a vida privada, a honra e a imagem das pessoas, esta previsto no art. 5º, incisos X, XII da Constituição Federal onde é determinado ser “inviolável o sigilo da correspondência e das comunicações telegráficas de dados e das comunicações telefônicas" e assegura o direito a indenização, pelo dano material ou moral decorrente da violação (SCORZELLI,1997).

“O cruzamento de informações permite a criação de retratos que mostram os nossos principais hábitos e práticas, revelando facetas das quais o próprio indivíduo muitas vezes não se apercebe. Podem ser elaborados por empresas privadas, para fins comerciais, ou por órgãos do governo, inclusive para fins de investigação criminal” (LINS, 2000, online).

Celso Ribeiro Bastos e Ives Gandra da Silva (apud TEIXERA, 2007) dizem que à reserva da intimidade e da vida privada trata-se de uma faculdade de cada pessoa, que deve impedir a intromissão de alheios a sua vida privada e familiar.

1.1 A Evolução do Judiciário

O governo brasileiro, no ano de 1984, sancionou a lei n.º 7.232/84 que dispõe sobre a Política Nacional de Informática, tendo estabelecido princípios, objetivos e diretrizes, cria o Conselho Nacional de Informática - CONIN e também a Secretaria Especial de Informática - SEI que desde 1990 com uma reestruturação que houve nos órgãos e nos Ministérios através da Lei n.º 8090 de 13 de novembro de 1990, deixou de existir tendo transferido a competência para a Secretaria da Ciência e Tecnologia que é subordinada ao Ministério da Ciência e Tecnologia (PEREIRA, 2002). O que chama a atenção é a preocupação que já existia no Governo em relação ao avanço Tecnológico que estava entrando no Brasil, nesta época computador e internet eram poucos que tinham, devido ao custo em se adquirir. Como a internet no Brasil estava 'engatinhando' era cedo para se ter uma preocupação em relação aos delitos que poderia surgir por intermédio da grande Rede. A preocupação quanto ao controle não alcançou a mesma proporção dos avanços tecnológicos, não se trata da mesma severidade quanto ao controle Chinês em relação aos acessos a Internet, pois lá o que querem é coibir a disseminação de informação ilegal na rede.

Quanto à censura a disseminação de informações, não cabe aqui fazer nenhum comentário, mas em relação ao controle quanto aos delitos cometidos na Internet, que também existe, este sim é digno de elogios. Esse cerceamento sistemático da internet pelo Governo chinês é conhecido como "the great firewall of China". Veja o que determina o artigo 14 da política oficial da República Popular da China (RPC) de 2000, em relação ao uso e gestão da internet: "os provedores devem manter esses registros por até 60 dias e disponibilizá-los aos órgãos policiais e de segurança e à Procuradoria do Povo para fins de manutenção da segurança nacional e para investigação de delitos" (CHINA).

A conferência organizada pelas Nações Unidas em Túnis, capital da Tunísia que ocorreu em novembro de 2005 revelou mundialmente o que muitos já sabiam sobre o controle americano sobre a Internet. Tudo bem que desde a sua criação há quase 50 anos os Estados Unidos merecem o reconhecimento por ter sido a nação que desenvolveu a web. Porém já é passada da hora de este controle ser compartilhado ente as nações. A ONU tem-se movimentado no sentido de chamar para se controle da internet, que é louvável, mas não

deixa de ser suspeita tendo em vista a manipulação que este organismo sofre por parte dos americanos, que alias tem sua sede em Nova Iorque (GUEIROS, 2009).

Os governos mundiais não entendiam a Internet no início de seu desenvolvimento, atualmente com a maturidade da Web isto gerou uma série de novos interesses, principalmente pelo poderio econômico que se traz dela. Assim as autoridades do mundo inteiro desejam ter o controle da internet, os países como a China o Irã e Arábia Saudita por terem regimes autoritários temem o poder que a Internet confere ao cidadão comum. Eles não veem com bons olhos o controle dos Estados Unidos dentro da Rede, monitorando e rastreando informações, bloqueando sites e até o desligamento virtual de uma conexão eletrônica (GUEIROS, 2009). Enquanto não exista um real consenso sobre uma governança compartilhada internacionalmente de forma multilateral sobre a internet, deve-se adotar 'soluções caseiras' para mitigar e solucionar possíveis problemas advindos do crescimento vertiginoso, da única verdade, que é o sucesso da internet.

O maior problema é a ausência quase total de punibilidade pelo Estado sobre delitos eletrônicos, que proteja o usuário, e que caso ocorra algum ato infracional que chegue ao autor do crime e o puna com base em legislação específica. Sobre legislação específica que trata dos crimes eletrônicos vários países já criaram, tais como: Espanha, Portugal, Argentina e recentemente o Brasil.

Há muito tempo projetos de lei objetivando a regulamentação dos crimes eletrônicos tramitavam no congresso nacional, destacamos: o projeto de Lei n.º 2126/2011, que institui o Marco Civil da Internet, conseguinte à recente aprovação aos 07/11/2012, dos Projetos de Lei n.º 2793/11, de autoria do Deputado Paulo Teixeira (PT/SP) e 84/99, do Deputado Eduardo Azeredo (PSDB/MG). O texto aprovado do Projeto de Lei n.º 2793/11, vulgarmente conhecido como "Lei Carolina Dieckmann" a atriz teve (36) fotos de seu arquivo pessoais furtadas por hackers e divulgadas na internet. Este fato repercutiu no Congresso Nacional fazendo com que os legisladores aprovassem o projeto de lei n.º 2793/11 que já tramitava o assentindo em regime de urgência. A nova lei n.º (12.737/12) passou a especificar e punir os delitos tais como: violação de senhas, invasão de computadores e devassa de outros dispositivos de informática (LEMOS, 2012).

A lei n.º 12.737 de 30 de novembro de 2012, publicada no diário oficial da união no dia 03 de dezembro de 2012, passou há vigorar 120 dias após a publicação, ou seja, no dia 02 de abril de 2013. Esta lei trouxe para o ordenamento jurídico penal brasileiro o crime de “invasão de dispositivo informático” que consistente na conduta de “invadir dispositivo

informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita"(BRASIL).

A lei aprovada "a toque de caixa" é limitada, mas o que importa neste momento é que foi dado o primeiro e importante passo rumo a construção de um conjunto de leis que proteja os usuários de internet e dispositivos de informática contra crimes eletrônicos (LEMOS, 2012). Outro projeto mais antigo e abrangente o PL 84/99, de autoria do deputado Luiz Piauhylino Monteiro, do Estado de Pernambuco (CORRÊA, 2000) que no Senado Federal está com a numeração PL nº 89/03, tem por objetivo acrescentar nova redação para tipos penais já existentes em nosso sistema criminal. Este projeto é considerado um dos mais importantes, sobre os crimes eletrônico, tendo por objetivo principal, preencher as lacunas na legislação brasileira no que diz respeito às responsabilidades dos agentes envolvidos em irregularidades no meio eletrônico (ZATTA, 2005). No momento este projeto esta tramitando na casa de leis tendo como relator o deputado Eduardo Azeredo (PSDB/MG).

A expectativa, após a *vacatio legis* de 120 dias, é que os infratores tenham mais receio, pois agora os delitos cometidos no meio eletrônico são tipificados como crime, o que antes era feito por analogia. O crime é comum e formal, consuma com a mera invasão ou instalação de vulnerabilidade, e qualquer pessoa (física ou jurídica) podem figurar como sujeitos ativos ou passivos (CABETTE, 2013).

1.2 A Reforma do Poder Judiciário e a Evolução Para o Processo em meio Eletrônico

As inquietudes humanas em buscar evolução nos mais diversos cenários não ocorreram sem passar por modificações. As maiores mudanças que impactaram positivamente a sociedade ocorreram pelas chamadas revoluções como: revolução agrícola; revolução industrial; e a revolução a qual a sociedade atual se insere conhecida, com a revolução da informação ou do conhecimento. Diante dessa terceira e não menos importante revolução social fez crescer o interesse por meios alternativos de obtenção de conhecimento. Fazendo surgir relações contratuais intersistêmicas, as contratações eletrônicas. A fim de atingir essa sociedade "*hi-tech*" o judiciário e sua estrutura (compreende aqui os humanos que utilizam o sistema) devem passar por mudança cada vez mais constante para que se possa atuar frente a essa nova realidade.

Diante deste cenário eletrônico fazem surgir grandes desafios físicos, principalmente no sentido de romper paradigmas. O Direito como instrumento regulador da sociedade é responsável pelo equilíbrio da relação comportamento e poder, que para obter se, deve antes interpretar a fotografia social do momento (PINHEIRO, 2010).

O direito que estuda estas transformações e soluções adequadas para a contemporânea sociedade "sem papel" é o Direito Eletrônico ou Digital. Este direito visa acompanhar esta sociedade que se molda a cada "*clique*", buscando analisar leis genéricas por um lado, mas ao mesmo tempo técnicas por outra "*face*".

> O direito digital traz ainda a possibilidade de aplicar uma série de princípios e soluções que já vinha sendo usada de modo difuso princípios e soluções que estão na base do chamado direito costumeiro. Essa coesão de pensamento possibilita efetivamente alcançar resultados e preencher lacunas nunca antes resolvidas, tanto no âmbito real quanto no âmbito virtual, uma vez que é a manifestação de vontade humana em seus diversos formatos que une esses dois mundos no contexto jurídico. Logo, o direto digital estabelece um relacionamento entre o direito codificado e o direito costumeiro, aplicando os elementos que cada um tem de melhor para a solução das questões da sociedade digital (PINHEIRO, 2010, p. 372).

Nesse liame, é mister citar as principais características do Direito Eletrônico, que são as seguintes: dinamismo, autorregulamentação, celeridade, uso da analogia, solução por arbitragem. Muito embora o Direito Eletrônico seja relativamente novo, suas características não as são, pelo contrario estão embutidas nos mais variados ramos do direito. "A mudança está na postura de quem a interpreta e faz sua aplicação" (PINHEIRO, 2010).

O filósofo da informação o francês Pierre Lévy, discípulo de Deleuze, observa, com maestria, que é importante entender que a virtualização não é uma "desrealização".

> A transformação de uma realidade num conjunto de possíveis não é uma desrealização, mas uma mutação de identidade, um deslocamento do centro de gravidade ontológico do objeto considerado: em vez de se definir principalmente por sua atualidade uma solução, a entidade passa a encontrar sua consistência essencial num campo problemático. Virtualizar uma entidade qualquer consiste em descobrir uma questão geral à qual ela se relaciona, em fazer mutar a entidade em direção a essa interrogação e em redefinir a atualidade de partida como resposta a uma questão particular (Levy, 1999, p. 18).

Nota-se que a Sociedade da Informação, que tem como átomo fundamental o conceito de Tecnologia da Informação (T.I) que abrange uma gama de produtos de *hardware* e *software* bem como toda sua estrutura de armazenamento, processamento, acesso instantâneo de um número cada vez maior de processos de trabalho e que permitem conectar pessoas a se

interagir de diversas formas, que também envolve a inteligência artificial e os sistemas peritos ou sistemas especialistas. Devido ao acesso a informação ter atingindo crescimento cada vez maior fizeram com que órgãos reguladores e de apoio como Anatel e o Ministério da Ciência e Tecnologia a buscar por melhorias na tecnologia da infraestrutura de comunicação e informações com o intuito de adequá-la a eficiência de outros países, instalando rede nacional de fibra ópticas e assim melhorando a qualidade dos serviços (FILHO, 2001).

"Demonstra o fato não só que o governo está atento a esta nova realidade advinda da sociedade informacional, como também que está se estruturando para atender às suas exigências e demandas básicas" (FILHO, 2001).

> Nos últimos anos, por exemplo, as decisões judiciais foram se aprimorando no tocante aos temas relacionados ao direito digital, isso porque houve um amadurecimento do próprio assunto dentro da sociedade e por parte dos estudiosos do direito, que passaram a refletir as grandes mudanças culturais e comportamentais vividas pela sociedade e interpretar as leis já existentes dentro desta nova visão e trazer soluções às necessidades trazidas pela evolução tecnológica (PINHEIRO, 2010, p.374).

Importante é ter se em mente que a tecnologia da informação não é a solução que resolverá o problema do judiciário, mas será de grande ajuda, e uma delas é o processo judicial eletrônico.

Alguns problemas enfrentados pelo judiciário brasileiro tais como: lentidão na tramitação dos processos; dificuldade na pesquisa e no armazenamento de processos físicos; obsolescência administrativa, estes problemas estão sendo gradativamente superados pela utilização do Processo Judicial Eletrônico (PJe). O PJe trata-se da informatização e da tramitação do processo, criado para minimizar ou até mesmo por fim aos autos em papel no Poder Judiciário.

A possibilidade da utilização de recursos eletrônicos em processos no Poder Judiciário Brasileiro, foi através da Lei nº. 9.800 de 26 de maio de 1.999, que permitiu aos profissionais do direito, a interposição de recursos por meio de 'fac-símile' ou outro meio similar como o e-mail. Permitindo às partes e ao Juiz, a utilização de sistemas informáticos para realização de atos processuais (TONHÁ, 2006).

Sobre o uso do meio eletrônico para tramitação de processo a Lei n.º 11.419 de 19 de dezembro de 2006, dispõem sobre a informatização do processo judicial em seu artigo 1º está previsto:

> Art. 1º O uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais será admitido nos termos desta Lei.
> § 1o Aplica-se o disposto nesta Lei, indistintamente, aos processos civil, penal e trabalhista, bem como aos juizados especiais, em qualquer grau de jurisdição.
> § 2o Para o disposto nesta Lei, considera-se:
> I - meio eletrônico qualquer forma de armazenamento ou tráfego de documentos e arquivos digitais;
> II - transmissão eletrônica toda forma de comunicação a distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores;
> III - assinatura eletrônica as seguintes formas de identificação inequívoca do signatário:
> a) assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica;
> b) mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos (BRASIL).

O artigo supracitado foi posto na integra, neste trabalho, para chamar a atenção à quantidade de termos técnicos inseridos nesta Lei que na data da promulgação poucos já tinham ouvido ou lidos algo a respeito, tais como: transmissão eletrônica, assinatura digital, certificado digital, autoridade certificadora.

O Processo eletrônico está elucidado no artigo 8 º da Lei em tela que concede ao "Poder Judiciário autonomia em desenvolver sistemas eletrônicos de processamento de ações judiciais por meio de autos total ou parcialmente digitais, utilizando, preferencialmente, a rede mundial de computadores e acesso por meio de redes internas e externas" (BRASIL).

Seguindo a leitura na mesma lei em seu artigo 16 trata do livro cartorário que poderão ser, junto com os demais repositórios do poder judiciário armazenados em meio totalmente eletrônico.

> Este é mais um grande passo para a diminuição do tempo de duração dos processos. Além disso, também haverá grande economia relacionada ao custo de produção e encadernação de livros, bem como de espaço físico para armazená-los, desde que respeitada à segurança necessária (BALDAN, 2011, online).

Para se adequar a esta realidade fizeram surgir várias empresas, que detenham competência em desenvolver soluções, que possibilitem a acessibilidade a todos que utiliza ou utilizará o sistema. Nesta relação de parceria entre publico e privado possibilitou um incremento que alavancou ainda mais o aproveitamento de oportunidades que visam levar à modernização do País, beneficiando outras grandes áreas tais como: educação à distância, telemedicina, teletrabalho, dentre outros (FILHO, 2001).

> Nos últimos anos, por exemplo, as decisões judiciais foram se aprimorando no tocante aos temas relacionados ao direito digital, isso porque houve um amadurecimento do próprio assunto dentro da sociedade e por parte dos estudiosos do direito, que passaram a refletir as grandes mudanças culturais e comportamentais vividas pela sociedade e interpretar as leis já existentes dentro desta nova visão e trazer soluções às necessidades trazidas pela evolução tecnológica (PINHEIRO, 2010).

"A onda reformista experimentada pelo Estado brasileiro não se limitou ao Poder Executivo. O Poder Judiciário também foi alvo de uma extensa reforma, a qual alterou, não apenas alguns procedimentos judiciais, mas também a própria estrutura deste poder" (SENA, 2012).

Com todas estas transformações que assolam o mundo contemporâneo pouco se tinha notado no intuito da modernização do Poder Judiciário, após a emenda constitucional n.º 45 de 30 de dezembro de 2004, já tem sido realidade, e a cada dia se torna mais presente a tão esperada reforma no judiciário.

O que marcou o início desta profunda reforma em andamento foi à criação do Conselho Nacional de Justiça, órgão com poder de fiscalizar a atuação do Poder Judiciário.

"No contexto da reforma do Judiciário, o tema transparência teve lugar de destaque. Este destaque decorreu da própria conjuntura histórica brasileira, a qual guarda fortes resquícios do patrimonialismo, do clientelismo, nepotismo e da corrupção" (SENA, 2012).

> A autoridade exercida pelo Conselho Nacional de Justiça deve ter em vista suprir as necessidades dos diversos órgãos que compõem o Poder Judiciário brasileiro, considerando, como premissa inafastável, que tais órgãos são os primeiros responsáveis por seus próprios destinos. Somente diante de sua inegável insuficiência ou deficiência, é que deverá o órgão central atuar. Incumbe, asssim, ao Conselho Nacional de Justiça responder aos desafios da modernização e às deficiências oriundas de visões e práticas fragmentárias da administração do Poder Judiciário (MENDES, online).

Como pode ser observado o caminho para a transparência neste ambiente globalizado foi aberto e reconhecido pelos poderes constituídos, é neste contexto é que se justificam o interesse absoluto e o crescimento das empresas de base tecnológica bem como o crescimento de operações mundiais de fusões e incorporações. Por outro lado, o conteúdo das informações assim como a imposição por padrões disseminados indiscriminadamente por agrupamentos empresariais, poderá ocorrer em discriminação étnica ou religiosa. Assim sendo o conteúdo das informações trafegadas na rede ou nas estradas informacionais, devem passar por analise de ordem cultural ou religiosa antes de serem publicadas no ciberespaço.

2. ASPECTOS JURÍDICOS E O CIBERESPAÇO

A forma célere que o processo tecnológico se insere no corpo social é inédita na historia da humanidade e fez com que o ordenamento jurídico fosse surpreendido com a dinâmica estimulada pelos avanços provocados pelas inovações eletrônicas, cuja capacidade de gerar dados novos prende o legislador que torna incapaz de acompanhá-las (WACHOWICZ, 2010).

Diante deste cenário inovador e vigoroso é necessário que se imprima adaptações ao Direito que esteja em consonância com este novo e promissor território virtual, portanto sem fronteiras, chamado Ciberespaço. O Termo Ciberespaço "vem do inglês cyberspace foi criado pelo escritor norte-americano William Gibson, e foi popularizado em seu livro de ficção científica Neuromancer, de 1984" (FILHO, 2010).

O exponencial crescimento da tecnologia digital propiciou o que se denomina sociedade da informação que constantemente transitam no Ciberespaço, local onde a informação, o conhecimento e os bens intelectuais trafegam ou são compartilhados sem dificuldades pela internet.

Os bens intelectuais estão atualmente globalizados indicando um iminente esgotamento dos limites territoriais do tradicional Estado-nação, que vem se tornando inábil por si só, em regulamentá-lo (WACHOWICZ, 2010), e consequentemente controlar e protegê-lo na sociedade conectada ou cibernética.

Em sociedade é comum o desenvolvimento de termos e linguagens próprios inerentes a um perfil que se imprime aos seres que dela façam parte. Fazendo surgir o neologismo "internetês" linguagem utilizada pelos internautas com o objetivo de se comunicar mais rápido, por quem "navega livremente em busca de informações comerciais, curiosidades sobre países distantes, informações bancárias, esportivas, culturais, consultas a médicos, bibliotecas, museus e assim por diante" (SCORZELLI, 1997).

Segundo ensinamento da mestre Galli:

> A linguagem da Internet tem seus pressupostos que, naturalmente, estão caminhando para um novo modelo de comunicação. A Internet já se transformou num veículo de comunicação com uma linguagem acessível à maior parte dos hiperleitores. Desse modo, há uma exploração dos termos dessa área, os quais são transferidos para o contexto social e divulgados como uma linguagem global (GALLI, online).

Por estas e outras razões a Internet atualmente é considerada uma anarquia, por não serem administradas por governos específicos estando submetidas a regras claras, leis específicas, pois são os próprios usuários que se revestem de tentativas e controle e padrões próprios de comportamentos éticos e técnicas estritamente apolíticas (SCORZELLI, 1997). Desta forma o direito que existe neste ambiente "é muito mais costumeiro de autorregulementação e de uso de mecanismos de mediação e arbitragem para a solução de conflitos" (PINHEIRO, 2010).

A busca por soluções de conflitos entre indivíduos conectados bem como a união pacifica entre os membros em conquistar novos horizontes com o devido respeito aos limites virtuais nas relações ali existentes, tem tornado uma preocupação recorrente entre os estudiosos do direito, magistrados, advogados em responder a estes problemas ao mesmo tempo em que não diminua o padrão de qualidade da internet.

Com o intuito de melhor administrar e tomar decisões mais acertadas sobre o uso da internet no Brasil o Ministério das Comunicações em uma ação conjunta com o Ministério da Ciência e Tecnologia em 31 de maio de 1995 criaram o Comitê Gestor da Internet no Brasil – CGI.br, foi alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003. Composto por membros do governo, comunidades acadêmicas, entidades operadoras e gestoras das espinhas dorsais (backbone) que são linhas de distribuições de acesso a internet. O CGI é uma realidade e representa um modelo pioneiro de governança na internet, tendo por principais atribuições (CORRÊA, 2000): fomentar o desenvolvimento de serviços ligados à internet; recomendar padrões e procedimentos técnicos e operacionais para a internet; o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil; a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>; a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.

Quanto à questão da administração e governança da internet em território brasileiro não se tem mais o que abordar neste trabalho, pois cumpre os objetivos e determinações que motivaram a sua criação, porem se faz necessário o controle repressivo aos usuários que infringem normas e boas praticas na internet. Em outros países como: Estados Unidos, Canadá e Japão são signatários de convenções internacionais como a convenção de Budapeste.

A Convenção de Budapeste que ocorreu no dia 23 de novembro de 2001 em Budapeste Hungria, nesta ocasião 43 Países participantes firmaram acordo que passou a

vigorar desde 2004 e trata "da punição e prevenção a crimes de ofensa a confidencialidade e a integralidade de dados dos computadores, como invasões de hackers a sistema de computadores, e a crimes praticados com o uso de sistema de dados e computador como pornografia infantil, racismo dentre outros..." (GATTO, 2011).

Segundo os estudiosos em relações internacionais Souza e Pereira:

> Segundo seu Preâmbulo, a Convenção prioriza "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional" e reconhece "a necessidade de uma cooperação entre os Estados e a indústria privada" (SOUZA, online).

A convenção é composta de quatro capítulos que juntos somam 48 artigos organizados por títulos de fácil compreensão e aborda assuntos como: tipificação do cibercrimes; infrações relacionadas à pornografia infantil, direitos autorais; dentre outros não só relativos a direito material, mas também processual, e prever até mesmo a extradição que é previsto no artigo 24.

O título 2 da convenção de Budapeste trata da conservação expedida de dados informáticos armazenados em seu artigo 16 que é composto por 4 incisos dispõem sobre "a guarda criteriosa das informações trafegadas nos sistemas informatizados, e sua liberação para as autoridades, de forma a garantir a efetiva aplicação da lei Penal" (GATTO, 2011).

O Brasil não é signatário da convenção de Budapeste e há varias controvérsias sobre as vantagens e desvantagens em se aderir. O Artigo 37 da convenção em tela trata da adesão de países que não participaram da elaboração, quando convidado pelo comitê de ministros do conselho europeu (SOUZA, 2009).

A leitura do artigo 9º da convenção, que trata das Infrações relacionadas com pornografia infantil, relembra um caso emblemático que ocorreu em 2008, nesta ocasião, envolveu uma empresa 'mundial' em Tecnologia da Informação (TI), por ter negado a fornecer dados de supostos pedófilos para a CPI da Pedofilia que foi instalada em 2008 na Câmera dos Deputados para investigar sítios virtuais. A princípio a empresa se negou a fornecer as imagens que comprometeriam seus clientes, alegando se tratar de informações confidenciais e por não esta sujeita a legislação brasileira, pois seus servidores ficam em outros países. Poderia ter sido mais célere se o Brasil fosse membro da convenção (SOUZA, 2009).

Estudiosos criticam a convenção por atribuírem poderes à polícia que comprometeriam a preservação da liberdade na internet, como vários países já criaram leis

autorizando empresas de segurança monitorarem a internet, eles temem que esses poderes sejam ampliados nos países signatários (DANTAS, 2008).

> ...condutas delituosas controvertidas, tais como o jogo ilegal pela internet e o terrorismo cibernético, foram deixadas de fora da Convenção para que cada Estado pudesse decidir criminalizá-las ou não. Já em relação à responsabilidade de pessoa jurídica, a Convenção se restringe apenas a dizer que ela poderá ser responsabilizada criminal, civil ou administrativamente (MAZONI, online).

O Senador Eduardo Azeredo, autor do projeto de Lei sobre Crimes Cibernéticos, respondeu no XVII Congresso Latino-Americano de Auditoria de Sistemas, algumas indagações sobre a inclusão do Brasil na convenção. Na resposta foi taxativo "A adesão do Brasil não está interligada à aprovação do PL que tipifica os crimes na Web no país pelo Congresso Nacional". E afirmou também que trata de decisão do poder executivo em aderir ou não a convenção (online, 2008).

2.1 Lei 12.737/12 e Suas Implicações

Em princípio com a ausência de legislação específica aqui no Brasil, que tratasse sobre crimes eletrônicos, estes eram considerados pela doutrina como um incidente econômico com solução na área penal. Com as inovações trazidas pela Lei n.º 12.737/12 que acrescentou dois artigos 154-A e 154-B no código penal brasileiro, a penalização será mais específica.

O artigo 154-A trata do crime de invasão de dispositivo informático, que consiste em acessar dispositivo eletrônico alheio conectado ou não à rede de computadores, mediante violação a mecanismos de segurança com o fim de obter, adulterar, ou destruir dados ou informações sem autorização do proprietário do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (BRASIL).

O parágrafo primeiro prevê a pena para quem produzir, oferecer, distribuir, vender ou difundir dispositivos ou programa de computador com o intuito de permitir a conduta descrita no caput do artigo. O parágrafo segundo qualifica a pena de um sexto a um terço se da invasão ocasionar prejuízo econômico. O parágrafo terceiro qualifica a pena para os casos em que a conduta prevista no caput resultar em obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, neste caso a pena salta para 6(seis) meses a 2 (dois) anos, e multa, se a conduta não constituir crime mais grave. No parágrafo quarto e penúltimo deste artigo prever aumento de pena para os casos previstos no parágrafo terceiro que tenha havido divulgação, comercialização ou transmissão

a terceiro. No parágrafo quinto aumenta se a pena em um terço até a metade, se o crime foi praticado contra uma destas autoridades pública: presidente (a) da republica, governador (a) e prefeito (a); presidente (a) do Supremo Tribunal Federal; presidente (a) do poder legislativo e das autarquias de cada uma das esferas (federal, estadual, municipal).

O artigo 154-B trata da regra da ação penal do crime de Invasão de Dispositivo Informático definidos no artigo 154-A. O sujeito que tenha sofrido crimes conforme previsão no 154-A deverá apresentar representação, salvo se cometido contra "a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos" (BRASIL).

O objetivo dos artigos acrescido pela Lei n.º 12.737/12 é a tutela à liberdade individual, eis que o tipo penal está posicionado no capítulo que regula os crimes contra a liberdade individual (artigos 146 a 154 do código penal brasileiro) (CABETTE, 2013). Também é tutelada a privacidade das pessoas em sua intimidade e privacidade, vale lembrar que está tutela é albergada pela Constituição da República Federativa do Brasil (CF/88), no seu artigo 5º, X que traz "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL). "Percebe-se, portanto, que a tutela é individual, envolvendo os interesses das pessoas (físicas e/ou jurídicas) implicadas, nada tendo a ver com a proteção à rede mundial de computadores e seu regular funcionamento." (CABETTE, 2013).

Os sujeitos envolvidos neste crime comum e formal, recentemente tipificado, é qualquer pessoa, inclusive pessoa jurídica, neste caso na modalidade passiva. Não há previsão de aumento de pena, para os casos que o autor seja funcionário púbico (CABETTE, 2013). O tipo subjetivo é doloso, não há previsão para o tipo culposo. O crime se consuma "com a mera invasão ou instalação de vulnerabilidade, não importando se são obtidos os fins específicos de coleta, adulteração ou destruição de dados ou informações ou mesmo obtenção de vantagem ilícita" (CABETTE, 2013).

A lei em comento alterou os artigos 266 e 298 do Código Penal. O Artigo 266 antes da alteração apresentava o seguinte texto:

"Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa" (BRASIL).

Com a nova lei em análise a aplicabilidade do artigo supramencionado ficou ampliado, e passou a contar com dois parágrafos a saber:

“§1º. Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento” (BRASIL).

Esta redação visa sancionar os sujeitos ativos que interromperem impedirem ou dificultarem o restabelecimento da tecnologia, de transmissão de dados ou voz, utilizados pela população (CABETTE, 2013).

“§ 2º. Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública” (BRASIL).

Este segundo parágrafo apresenta como objetivo a majoração da sanção penal na hipótese do crime previsto no caput ter sido praticado por ocasião de calamidade publica (CABETTE, 2013).

Como o artigo 266 o 298 também sofreu alteração em seu texto, antes era assim:

“Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa” (BRASIL).

O Legislador inseriu no texto do artigo supracitado equiparando a documento particular o cartão magnético bancário, passando a fazer parte ao artigo o parágrafo único abaixo:

“Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito” (BRASIL).

> A informação supracitada justifica-se, pois a equiparação do cartão magnético bancário, seja ele de débito ou crédito ao patamar de documento particular viabiliza a aplicação da sanção prevista pelo artigo 298 CP (reclusão de 01 a 05 anos e multa), pena esta mais grave se comparada às demais ora estudadas, pois o acesso a dados sigilosos na esfera bancária não colocam em risco apenas a esfera moral, mas também o patrimônio da vítima, que poderá vir a ser subtraído de forma célere por intermédio de simples transação pactuada no ambiente virtual(CABETTE, 2013, online).

A inclusão e modificação dos artigos, supramencionados, com o advento da lei n.º 12.737/12, embora ainda insuficiente veio em boa hora, enriquecer nosso ordenamento jurídico penal no que tange a fraudes eletrônicas. Punindo com mais rigor condutas até então frequente nos grandes centros como a falsificação (clonagem) de cartão de débito/crédito.

2.2 A Efetividade e Direito Estrangeiro

Apresentado o conteúdo da lei federal sobre a invasão de dispositivos informático, faz surgir uma indagação, do quanto essa norma que está posta a disposição do poder público trará de resultado efetivo para a população brasileira.

Há um princípio fundamental no ordenamento jurídico brasileiro, o princípio da legalidade, que está presente no artigo 5º, inciso XXXIX da Constituição Federal de 1988, bem como no artigo 1º do Código Penal e também no artigo 1º do Código Penal Militar que diz: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal" (BRASIL). Em outras palavras para que se condene um agente ativo pela prática de um delito, deve antes da ocorrência do fato existir a tipificação da conduta como sendo crime, ou seja, é condição *sine qua non* (que significa sem o qual não). Assim o réu poderá ficar impune caso não haja no ordenamento uma lei que permita por analogia aplicar a hipóteses semelhantes.

Como diz um ditado popular “antes tarde do que nunca” traduz bem o sentimento daqueles que aguardavam a aprovação do projeto que se postergava de 1999, mas embora reacionário veio a contribuir com o início da modernização do código penal brasileiro. No mesmo dia (30 de novembro de 2012) foi sancionada pela presidenta Dilma Rousseff duas importantes leis para os crimes eletrônico-informáticos, além da lei em estudo conhecida como “lei Carolina Dieckmann” foi aprovada a lei n.º 12.735/12 conhecida como “lei Azeredo”, esta última “... entre outras determinações, prevê em seu artigo 4º a necessidade de estruturação dos órgãos da polícia judiciária para o combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado” (OLIVEIRA, 2012).

A aprovação destas leis vai contribuir com a desmotivação ou inibição daqueles que sentiam se livres para acessar indevidamente equipamentos eletrônicos de pessoas (física/jurídica) com a intenção de conquistar ilegalmente alguma vantagens, mediante a revelação de segredos ou imagens privadas. Desta forma garantirá ao usuário certa segurança informática, no que diz respeito a confidencialidade, integridade e disponibilidade da informação que há um bom tempo necessitava de proteção jurídico-penal (OLIVEIRA, 2012).

Infelizmente as notícias sobre a efetividade da lei, não são das melhores, pois uma série de questionamento tem contribuído para essa dificuldade, nada que o tempo e algumas adaptações, principalmente quanto à jurisprudência que se formará possam resolver as lacunas que a lei não obturou.

Há um detalhe importante a ser ressaltada a lei não protege qualquer dispositivo informático, mas somente aquele que teve o sistema invadido mediante violação indevida de mecanismo de segurança (antivírus, firewall, senhas, etc.). É requesito para esta cominação

punitiva a "violação indevida de mecanismo de segurança", o seja o acesso a sistemas desprotegido é fato atípico (CABETTE, 2013).

Devem-se alertar os usuários para que se protejam ao máximo, com uso de senhas complexas, antivírus, firewall (sistema que bloqueia o acesso remoto não autorizado), não fazer downloads de qualquer programa ou e-mail suspeito, pois o mesmo pode ter sido enviado por algum cracker para que o próprio usuário desabilite o(s) sistema de proteção de seu dispositivo (BRITO, 2013). Na tentativa de que se descoberto for, o dispositivo estava desprotegido e que, portanto não cabe aplicar a lei.

> Não parece justo nem racional presumir que quem não instala proteções em seu computador está permitindo tacitamente uma invasão, assim como deixar a porta ou o portão de casa abertos ou destrancados não significa de modo algum que se pretenda permitir a entrada de qualquer pessoa em sua moradia (CABETTE, online).

Ao criar a lei o legislador poderia ter considerado somente a invasão ou instalação de vulnerabilidades, sem entrar no mérito da violação de mecanismo de segurança, que neste caso poderia ser uma qualificadora para aumento à pena. Tal como ocorre no caso de furto qualificado por rompimento de obstáculo (CABETTE, 2013). Porém mesmo com a critica a lei vem satisfazer a necessidade de criminalização de condutas ilícitas que comumente ocorre nos dispositivos informáticos conectados ou não no ciberespaço.

Embora o Brasil tenha legislação que tipifica criminalmente delitos informáticos esta ainda é esparsa, pouco abrangente e, por ser recente desconhecida. E ainda não se formou uma cultura de informática jurídica, de direito eletrônico, e da importância da regulação do Estado no ciberespaço (ARAS, 2001). Para complementar e buscar soluções mais abrangentes para caso específico é conveniente estudar o ordenamento jurídico estrangeiro, aplicando por analogia uma melhor solução, formando desta forma o Direito Comparado.

> Direito comparado é expressão que resulta, claramente, da junção de dois termos: direito, que, no caso, se refere a sistema jurídico, e comparado, que tem a ver com a comparação, na busca por semelhanças e diferenças entre objetos comuns pesquisados, sejam eles um sistema jurídico sejam eles um instituto jurídico (SIQUEIRA, 2012, online).

Os Estados Unidos da America (EUA) país de notáveis recursos econômicos e tecnológicos foi pioneiro em difundir o computador na vida social de seus habitantes, e também o primeiro a ver nascer um novo ramo do direito: *Computer and the Law* (computador e a lei). Mas a frente em 1983 os europeus perceberam o surgimento deste novo

ramo do direto e que já incidia profundamente na prática profissional nos EUA. Não é de causar espanto que além dos europeus outros países absolveram a experiência americana já consolidada e amadurecida neste novo ramo jurídico que desde o começo teve dimensão transnacional. (PAESANI, 1998).

Os meios de comunicações interligados mundialmente sobre tudo pela internet tem proporcionado incremento nos números de delitos eletrônicos além das fronteiras e das jurisdições territoriais. Causando virtualmente prejuízos reais em dispositivo informático alheio, esteja em que parte do mundo estiver bastando para isto que o cracker tenha obtido acesso remoto ao dispositivo da vitima, assim ele pode copiar/alterar o que quiser. "Se os legisladores pretendem criar um código para a supervia da informação devem, lembrar-se que estão policiando uma estrada que fisicamente não vai a lugar nenhum" (PAESANI, 1998).

Os nichos mais preciosos da privacidade tais como contas correntes, declarações do Imposto de Renda, números e transações de cartões de crédito, endereços pessoais bem como outras informações sensíveis, que também ficam armazenados nos computadores dos usuários que utilizou para fazer a declaração ao "leão", por exemplo, poderão ser devastados por pessoas que detenham conhecimento técnico e que esteja fora de alcance das legislações brasileira (PAESANI, 2003).

Devido às transformações principalmente de ordem política-econômica que vem sendo enfrentado em âmbito mundial por vários países, e frente a este cenário levaram lhes a buscar a prevenção e retribuição punitiva, assim atualizaram seus ordenamentos jurídicos e se adequaram ao novo contexto mundial/atual (MAZONI, 2009).

Para inovar seus ordenamentos jurídicos é preciso ter regras claras e que não afastam investimentos de empresas na rede. Normas do Direito penal devem ser vistas como *última ratio*, ou seja, o último recurso, e que para isto devem ser criadas a partir de experiências e conhecimento extraído das normas civis, sobre pena de elevarem os custos de investimento no setor. Assim sendo o melhor caminho é debater em audiências publicas através do estabelecimento do marco civil para verificar o que teve efeito ou não e regular a rede com base na experiência adquirida. Países que são signatários da convenção de Budapeste fizeram antes o a regulamentação do ponto de vista civil e após isso que estabeleceram parâmetros punitivos para os infratores da rede (LEMOS, 2005).

Segue alguns exemplos de legislações estrangeira relativo a crimes eletrônico em geral: na Alemanha é tratado em seu código penal na Seção 202 a, Seção 263 a, Seção 269, Seção 270 a 273, Seção 303 a, Seção 303b e na lei contra Criminalidade Econômica de 15 de

maio de 1986. Na Áustria é tratado no código penal desde 1987 onde é contemplado os delitos e fraude informática nos artigos 126 e 148 respectivamente. Na China é especificado um regulamento para proteção da segurança da informação no decreto 147 do Conselho da República Popular da China. Em Cuba existe um regulamento desde 1996 emitido pelo Ministério da Indústria Mecânica e Eletrônica. Na Dinamarca os delitos informáticos são tratados no código penal local na seção 263. Nos EUA os crimes de informática são tipificados na seção 502 do código penal local, é dado aos Estados independência para legislar sobre o assunto. Na Noruega os delitos informáticos estão tipificados no código penal nos parágrafos 141, 151, 261, 291 (SILVA, 2000).

Além destes supracitados tem-se também a Lei da República Portuguesa nº. 109 de 15 de setembro de 2009, publicada no diário oficial português nº. 179. A referida lei ratifica o protocolo adicional à convenção sobre o cibercrime relativo à incriminação de atos de natureza racista e xenófobos praticados através de sistemas informáticos. Esta lei portuguesa é composta de cinco (5) capítulos que juntos somam trinta e dois (32) artigos muito bem dispostos e redigidos em português claro e de fácil assimilação. O artigo 4º trata do Dano relativo a programas ou outros dados informáticos que dentre outras punições prevista nos seis (6) incisos, estabelece pena de prisão de até três (3) anos ou multa para aquele que sem permissão legal do proprietário do dispositivo informático, "apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso" (PORTUGUAL). Os Artigos 6º e 7º dispõem respectivamente sobre acesso ilegítimo e interceptação ilegítima que prever pena de até (três) 3 anos de prisão ou multa podendo ser majorada até (cinco) 5 anos se deste acesso o agente tiver tido conhecimento de segredo comercial ou industrial ou de dados confidenciais protegidos por lei. O capitulo terceiro trata das disposições processuais e em seu artigo 16 º estabelece como se procederá com a apreensão de dados informáticos, que devido à relevância esta disposta na integra, e sem tradução, logo abaixo:

> 1 — Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.
> 2 — O órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.

> 3 — Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto. 4 — As apreensões efectuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.
> 5 — As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária estão sujeitas, com as necessárias daptações, às regras e formalidades previstas no Código de Processo Penal e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista.
> 6 — O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.
> 7 — A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes:
> a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura;
> b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;
> c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou
> d) Eliminação não reversível ou bloqueio do acesso aos dados.
> 8 — No caso da apreensão efectuada nos termos da alínea b) do número anterior, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital (PORTUGUAL, online).

O artigo 27 º estabelece que a aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses segundo o referido artigo

> ... salvo tratado internacional, a lei penal portuguesa é aplicável aos factos cometidos por Portugueses, se não lhes for aplicada outra lei penal; aos fisicamente praticados em território português ou que visem sistemas informáticos localizados em território português; e também cometidos em benefícios de pessoas colectivas com sede em território português (nº 1). Em caso de conflitos de jurisdição positivos entre Estados membros a decisão cabe aos órgãos e mecanismos instituídos da União Europeia (nº 2). A decisão de aceitação ou transmissão do procedimento deve ser tomada tendo em conta o local da prática dos factos, a nacionalidade do autor e o local onde este foi encontrado (nº 3) (DIAS, 2010, online).

A lei portuguesa sobre o cibercrime deu inicio após Portugal assinar a Convenção sobre Cibercime do Conselho da Europa em 2001. Tendo sido ratificado por seu parlamento em maio de 2009. Que fornece ao sistema processual penal português normas a obter dados de tráfego e a realização de interceptações de comunicações para prosseguir com a

investigação de crimes no ambiente virtual. Esta lei traz uma experiência positiva as nações que busca inovar nesta área cuja demanda é tendente ao crescimento.

3. PRIVACIDADE E INTIMIDADE NA ERA TECNOLÓGICA

A liberdade de expressão compreende a faculdade de expressar livremente ideias, pensamentos e opiniões, está consagrada na constituição federal, e é compreendido como um fundamento para as sociedades democráticas. Porém esta liberdade não é completa, pois não se pode manifestar opinião de preconceito racial ou que estimule a destruição social por exemplo.

"É um direito assegurado não só no ordenamento jurídico brasileiro, como também além de nossas fronteiras, uma vez que está previsto em normas supranacionais, como acontece no pacto de São José de Costa Rica, art. 13" (TEIXEIRA, 2007).

> A proteção Constitucional da Liberdade de opinião pode ser divisada no inciso IV do artigo 5º da CF/88, segundo o qual "é livre a manifestação do pensamento, sendo vedado o anonimato", ao passo que a liberdade de expressão, gênero que é, vem garantida por diversos dispositivos, constitucionais, a saber, o próprio inciso IV do artigo 5º e mais os incisos VII, segunda parte, IX, além dos artigos 215 e 220 caput e respectivos parágrafos (ABDO, 2011 p. 32,33).

A constituição estabelece alguns limites à liberdade de expressão tais como: a vedação do anonimato, o direito de respostas, indenização por danos morais e materiais além dos direitos a honra e a privacidade. Antes de utilizar o direito da liberdade de expressão o agente deve antes escolher o meio que será utilizado para manifestar sua opinião visando atingir o publico esperado, envolvendo, ao menos, três elementos: o emissor, a mensagem, e o receptor (ABDO, 2011). A mídia frequentemente mais utilizada devido ao alcance global com custo quase zero e a internet, sobre tudo as redes sociais que permite que pessoas e grupos por mais distantes que estejam possam se fazer ouvi (FURST, 2012).

Na internet acontece quase que indiscriminadamente a violação da privacidade devido à facilidade de se dados sobre os usuários, o que permite ao emissor enviar inúmeras mensagens não desejadas. A privacidade de tão importante é considerada direito fundamental tendo previsão na Constituição Federal de 1988 no artigo 5º inciso X, porém com a popularização da internet tem encontrado grandes problemas de violação de privacidade nesta crescente rede de comunicação (TEIXEIRA, 2007).

> A situação é de perigo constante, pois grande parte dos usuários da internet registram, na rede, dados específicos de sua privacidade. Em muitos casos, a própria qualificação pessoal do indivíduo, seus hábitos, costume e preferências ficam expostos em navegações, podendo ser captadas para fins de procedimentos de marketing, ou para spam (expressão genericamente utilizada para designar as mensagens eletrônicas não solicitadas, ou a mesma mensagem que é enviada para uma multiplicidade de destinatários) (BARROS, 2005, p. 281).

O direito à privacidade ou direito de estar só é tutelado pelo Estado e tem por fundamento a defesa da personalidade humana contra intromissões alheias. Também é resguardada pela ONU desde 1948 com a Declaração Universal dos Direitos Humanos em seu artigo 12, que preceitua uma proteção à pessoa contra intromissões arbitrarias tanto em sua vida privada bem como na sua família, no seu domicilio, em suas correspondências além de ataques a sua honra e reputação. Porém cabe a cada ser humano estabelecer o limite a ser preservado em sua privacidade e intimidade, pois se admite o consentimento implícito, quanto à própria pessoa divulga aspectos da própria vida privada (PAESANI, 2003).

A doutrina apresenta vários posicionamentos a cerca do direito à privacidade e às vezes, considera implicitamente como sinônimo ao direito à intimidade, porém a própria Constituição estabelece diferenças ao separar a intimidade de outras manifestações da privacidade tais como a vida privada, a honra e a imagem. Neste sentido pode se dizer que intimidade é espécie do gênero privacidade (LEYSER, 1999).

A intimidade relaciona ao modo de ser de cada pessoa tem a ver com o mundo intrapsíquico, com a "vida secreta do indivíduo" tais como aspectos particulares, ou que atingem sua autoestima, autoconfiança, seu ego, sua sexualidade, compreendendo também seu lar, a sua família e a sua correspondência. Neste sentido corrobora ao entendimento do direito a inviolabilidade do domicílio, o sigilo da correspondência, o segredo profissional, direito à imagem, tutela do nome e da obra intelectual (SCORZELLI, 1997).

> O direito à intimidade tem estreita relação com outros direitos da personalidade, como, por exemplo, a honra, a imagem, embora não se confundam, podendo um fato lesivo repercutir nos demais. Porém cada um destes direitos tem suas particularidades e diferenças os que fazem distinguir uns dos outros (LEYSER, 1999, p.28,29).

Tanto a privacidade quanto a intimidade são direitos personalíssimos e apresentam algumas características tais como: vitaliciedade, intransmissibilidade, imprescritibilidade e irrenunciabilidade.

Dotti apud Teixeira diz que: os aspectos da vida privada e da personalidade vêm sendo ameaçados com a evolução da informática o que acaba permitindo o acesso de curiosos a informações relativas à vida privada e a imagens das pessoas.

> Na internet as pessoas que detêm o seu acesso se expõem demasiadamente, a ponto de muitas vezes sentirem-se desprotegidas. Os usuários da internet têm um livre trânsito de informação e junto com esta liberdade, vem a periculosidade do seu mau uso, quando a internet é acessada de forma indevida por um usuário. Deve-se, portanto, ficar atento para que não deixe a privacidade ser invadida (SCORZELLI, 1997, p.28).

Com o advento da informática a percepção a cerca da privacidade vem mudando e de certa maneira a vida íntima deixou de ser "reservada" passando a ser um livro aberto com informações acessíveis a qualquer um da sociedade que se interesse. Desta forma o individuo esta por perder, a cada dia, a privacidade sobre seus dados e informações pessoais presentes na web que poderão ser manipulados facilmente, por terceiros, que detenham poder de processar estas informações sem o seu consentimento. O que é mais preocupante é que as pessoas estão ficando cada vez mais vulnerável a sofrer invasão de privacidade eletrônica.

> O que foi até aqui exposto diz respeito a temas que envolvem provedores, sites e usuários, associados ao fato da velocidade com que os dados são colhidos, armazenados e, eventualmente, comercializados. Acontece que, uma vez comercializados os dados, pode haver violações de direitos, o que frequentemente ocorre ao se considerar que as comunicações via internet também transmitem informações sigilosas e privativas. Todo esse fenômeno, de certo modo recente, cria uma situação de insegurança jurídica quanto ao uso da internet e a garantia de uma proteção da privacidade dos usuários e dos dados sigilosos transmitidos (TEIXEIRA, 2007, p.69,70).

A liberdade aparente que a internet passa a seus usuários, com a falsa ideia de anonimato, tem sido palco de diversos crimes, acarretando mudanças no comportamento dos indivíduos. Com todo o aparato tecnológico cada vez mais acessível tem feito surgir à sociedade "sem papel" que tem gerado cada vez mais documentos eletrônicos e convivem na era do processo eletrônico e do fisco eletrônico (PINHEIRO, 2012, p.368). Estando numa era da comunicação eletrônica, onde a informação é o "ativo financeiro", que migra numa velocidade incrível percorrendo todo o universo num "piscar de olhos", tornando numa forma universal de se comunicar deste modo poderia existir uma legislação mais eficiente e igualmente universal que estabelecesse o controle de todos os países com possibilidades de intervenção supranacional de organismos internacionais. (MARTINS, 2011).

> Art. 5º, XII, CF - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL).

Atualmente o termo "correspondência" nos remete a outras formas de comunicação não somente ao modelo retrógrado da carta escrita manualmente ou impressa, mas também a comunicação eletrônica tais como: e-mail, spam, mala direta, mensagens instantâneas que muitas vezes abarca textos sigilosos e que por isto necessita da mesma proteção constitucional.

Quanto ao uso da comunicação eletrônica nem sempre faz uso da proteção constitucional, pois como exemplo o empregador pode de forma moderada, generalizada, impessoal, controlar as mensagens do trabalhador, enviadas e recebidas pela caixa de email profissional com o objetivo de se evitar abusos que possa causar prejuízos a instituição privada. Porém questões como a apresentada que versa sobre privacidade não há entendimento unificado, pois norma infraconstitucional não pode sobrepor a previsão constitucional que proteja a privacidade assim “a inserção do empregado no seu ambiente de trabalho não lhe retira os direitos da personalidade, dos quais o direito a intimidade constitui uma espécie” (DONEDA, 2008).

Não coaduna este entendimento quando se diz respeito a órgãos públicos, pois há outro direito também constitucional que preceitua a afirmativa: "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo" texto do artigo 5º, Inciso XXXIII CF/88.

O acesso às informações públicas é essencial para a disseminação do conhecimento e da informação nas sociedades modernas. Ha experiências positivas no país no sentido de corroborar com a transparência às informações de interesse público, dentre elas aumentarem o controle e fiscalização das contas e despesas. Desta forma fez nascer o Portal da Transparência que mostra além da aplicação de recursos públicos pelo governo a remuneração mensal dos seus servidores.

> A liberdade de informação é pressuposto fundamental para garantir o direito ao respeito à vida privada “não só porque ela permite a formação de uma opinião pública esclarecida, capaz de respeitar e se posicionar ao lado de um indivíduo que, frente às admoestações da turba e da burocracia estatal, advoga um interesse legítimo; mas também, porque ele dá azo à transparência tanto nos negócios públicos quanto nas decisões sociais que podem vir a gerar efeitos sobre os direitos essenciais da pessoa humana”. A declaração Universal dos Direitos do Homem proclamou em favor de todos o direito à liberdade de opinião e expressão sem constrangimento e o direito

> correspondente de investigar e receber informações e opiniões e de divulgá-las sem limitação de fronteiras (LAYSER, 1999).

A lei complementar n.º 131 de 27 de maio de 2009 estabelece normas de finanças públicas como também execução orçamentária e financeira da União, dos Estados, do Distrito Federal e dos Municípios, com o objetivo de estimular a continua modernização da administração pública com a ampliação das divulgações de ações governamentais bem como o fortalecimento da democracia. Para isto estipulou prazos para que cada esfera pública disponibilizasse as páginas na web sobre transparência pública com informações atualizadas sobre despesas realizadas pelos órgãos e entidade da administração publica, visando o incremento do controle social sobre execução orçamentária, licitações, contratações dentre outros custos.

Com o acesso fácil a informações atualizadas e disponíveis a qualquer cidadão deram origem a mutações sociais, educacionais, políticas e econômicas como nunca visto antes, tendo em vista não ser mais necessário grande dispêndio de tempo e deslocamento a bibliotecas, para se pesquisar sobre algum fato, o que se precisa é saber filtrar e selecionar a informação de sites confiáveis que se adéquam a demanda do momento (MONTEIRO, 2007).

Com todas estas modernidades tecnológicas catalisam a preocupação sobre a invasão da privacidade sobre tudo em relação às pessoas que exercem atividades laborais em alguma esfera da administração pública. Pois com o cruzamento de informações podem revelar "retrato de toda sua vida, fazendo emergir fatos que liquidam homens públicos em momentos que são escolhidos, de forma e modo estratégicos" (RULLI, 2005).

> O conhecimento e a informação são produtores de riqueza. A sociedade da informação deve evoluir necessariamente para a Sociedade do Conhecimento. Embora seja comum designarmos a existência de uma nova era, denominada “Era do Conhecimento”, a mesma ainda não foi atingida. Informação e conhecimento são conceitos distintos. A informação existe em larga escala, embora ainda, parte da sociedade esteja excluída dessa realidade. O acesso à informação não significa acesso ao conhecimento. Conhecimento se traduz em amadurecimento, em análise da informação. Trata-se de capacidade intelectual (SIQUEIRA, 2003, p. 259).

Embora se reconheça as preocupações aplicáveis à informação (principalmente quanto aos recebíveis) transmitidas e postas à disposição na internet, porém o cidadão tem direito de ser informado. Este direito este consagrado no artigo 5º inciso XXXIII da CF/88 que dispõem: "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob a pena de

responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado" (BRASIL).

Para tutelar o direito a informação há no Brasil o remédio constitucional denominado *habeas data*. Assemelha-se a *habeas corpus* com a diferença que este propõe a liberdade do corpo, enquanto que a primeira trata de liberdade dos dados. Sobre o regulamento do direito de acesso a informações esta elencada na lei nº. 9.507/97 que garante e disciplina os direitos ao acesso, retificação e complementação das informações. "Mediante este instrumento constitucional o interessado pode exigir o conhecimento de registros e dados relativos à sua pessoa e que se encontrem em repartições públicas ou particulares acessíveis ao público" (SIQUEIRA, 2003).

> O avanço da Internet não trouxe apenas a facilidade das comunicações, mas também poderá trazer grandes transformações para os valores da sociedade. Assim, é preciso uma ponderação sobre relativizar estes direitos constitucionais: liberdade de expressão, sigilo da correspondência, direito à privacidade e ao sigilo de dados. Tais direitos, se mantidos de forma rígida, correm o risco de ser obstáculo não só para o bom funcionamento da rede mundial de computadores, como também para a sociedade atual. Na verdade, se, por um lado, a inibição de expressar-se pode significar um retrocesso nas conquistas da sociedade, por outro, a ausência de privacidade pode gerar a falta de individualidade do ser humano, entre muitas outras implicações como o congestionamento da internet pelo excesso de spams (TEIXEIRA, 2007, p.73).

O termo *spam* originou nos EUA e é usado para referir aos e-mails que geralmente tenham conteúdo publicitário e são enviados para um grande público e não solicitados pelos destinatários. Assemelha-se aos impressos publicitários deixados nas caixas de correio com a diferença de terem investimento quase zero e com o alcance em escala muito maior. Com o boom das comunicações eletrônicas os *spans* tem tornado um desafio diário aos internautas, pois não só o inconveniente de receber, mas o tempo que se perde em excluir este lixo eletrônico, que muitas vezes vem elaborado contendo dados como nome e outras informações privativas do cidadão. Desde maio de 2010 a ANATEL, órgão regulador e fiscalizador de telecomunicação, passou a determinar que as operadoras não enviem propagandas para os usuários sem a permissão dos mesmos, sobre o risco de sofrerem penalizações.

> Diante de tudo isso, torna-se evidente a necessidade de se buscar um equilíbrio para o exercício dos direitos previstos na Constituição, tendo em vista as relações estabelecidas na internet, notadamente quanto aos direitos da liberdade de expressão, da privacidade e do sigilo das correspondências das comunicações e dos dados. Um caminho para isso é deixar claro que eles serão relativos a fim de assegurar o interesse coletivo sobre o interesse

> individual. Esse é, não de modo exclusivo, mas, principalmente, um dos papéis da jurisprudência (TEIXEIRA, 2007, p.76).

Com todas estas inovações tecnológicas fortalece a importância na relação entre o Direito Penal e a Informática. Isto porque o Direito detém o poder de controle social, possuindo estrutura imperativa, atributiva e coercitiva (NETO, 2003).

> Um tema novo que gera controvérsia entre advogados é a possibilidade de dano moral pelo recebimento de spam, as mensagens eletrônicas indesejadas. No Recurso Especial (Resp) 844.736, relatado pelo ministro Luis Felipe Salomão, foi discutido se mensagens com conteúdo pornográfico recebidas sem autorização do usuário gerariam direito à indenização. Mesmo após o internauta pedir para não receber os e-mails, as mensagens continuaram chegando. O relator considerou que haveria o dano moral, que o autor do spam deveria indenizar e que existiria obrigação de remover do cadastro o e-mail do destinatário. Entretanto, o restante da Turma teve entendimento diverso. Os demais ministros levaram em conta que há a possibilidade do usuário adicionar filtros contra mensagens indesejadas. Para eles, a situação caracterizaria mero dissabor, não bastando para configurar o dano moral. A maioria da Turma considerou que admitir o dano abriria um leque para incontáveis ações. Alguns operadores do direito defendem que é necessária alteração na lei para que a jurisprudência possa avançar. Um deles é Renato Opice Blum, economista e advogado especializado em direito digital. “Nesse caso, a legislação brasileira está atrasada em relação a vários países europeus e do resto do mundo”. (STJ, 2011, online).

A ideia norteadora do crime cibernético é a utilização de *experts*, pessoas que detenham conhecimento técnico aprofundado, para utilizar de recursos com o objetivo de ocultar sua conduta, fazendo com que as ações criminosas realizadas permaneçam no anonimato. Sendo assim o Judiciário deverá agir com expertise a altura, se aperfeiçoando cada vez mais, como vem sendo feito, para vencer os desafios que a tecnologia impõe. A dificuldade é que no "mundo da internet" existe um emaranhado de jurisdições diferente, porém, apesar de os crimes serem transnacionais há mecanismos nacionais para processá-los. O que deve ser impresso para a sociedade é que no ciberespaço não há algo que possa fugir dos domínios da jurisdição do mundo físico (CORREA, 2000).

3.1 A Tutela Jurisdicional no Ciberespaço

O poder judiciário, assim como outros poderes públicos, só pode fazer o que estiver positivado é autorizado em lei, desta forma necessita de atualização e adequação no ordenamento que efetivamente possa utilizar, mas para isto deve se empregar também técnicas e procedimentos processuais conivente com a era da sociedade conectada para que o internauta possa receber a melhor prestação jurisdicional.

> Se de um lado o crime na internet evolui a passos largos e de forma sofisticada, noutro o formalismo do processo penal transforma-o, a cada dia que passa, em um peça mais antiquada e onerosa. A criminalidade cibernética jamais será contida se não for impresso ao processo penal um caráter transfronteiriço e virtual. É verdade que não é um problema exclusivamente brasileiro, pois outros países também possuem legislação como a nossa, que carece adaptar à internacionalização das redes informáticas (BARROS, 2005, p.293).

A transnacionalidade que ocorre em muitos casos faz surgir naturalmente à dúvida sobre a aplicabilidade da legislação brasileira ou estrangeira ao crime cibernético. Como uma forma de solucionar este imbróglio vem o Código Penal (CP), suprindo a lacuna legislativa específica sobre a competência do crime virtual (FILHO, 2011).

> Neste liame o CP colaciona em seu art.5º, *Ipsis literis*, que: "Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional". Constituindo, neste contexto, a aplicabilidade da lei brasileira, prevalecendo desta maneira a Soberania do Estado Brasileiro face o estrangeiro, imputando a nossa lei penal independente da nacionalidade do agente ativo ou do titular do bem lesado, já que produziu resultado no Brasil. (FILHO, 2011, online).

Sobre este assunto o doutrinador Rogério Grego (apud Filho, 2011, online) diz que: "[...] no Brasil não se adotou uma teoria absoluta da territorialidade, mas, sim, uma teoria conhecida como temperada, haja vista que o Estado, mesmo sendo soberano, em determinadas situações, pode abrir mão da aplicação de sua legislação, em virtude de convenções, tratados e regras de direito internacional [...]".

Sobre o lugar do crime o código penal dispõe em seu artigo 6º que: "Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado" (BRASIL).

No mesmo diploma em seu artigo 7º § 2º é estabelecido condições de punibilidade mesmo que o crime tenha sido cometido no estrangeiro, assim está previsto:

> "[...] a) entrar o agente no território nacional; b) o fato punível também no país em que foi praticado; estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição; d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena; e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável" (BRASIL, online).

De acordo com o principio da territorialidade temperada, como ensina Rogério Grego, não afronta nossa soberania a afastar a concepção dos crimes reais dos cibernéticos, muito pelo contrário, fortaleceria a elaboração de lei específica ou tratado internacional, assim reduzindo a problemática da competência na seara de crimes cibernéticos que iniciaram em outro Estado Soberano. O ordenamento penal brasileiro adota a teoria da ubiquidade, ou seja, o lugar do crime é tanto aquele da conduta quanto o do resultado (FILHO, 2011).

> [...] Como regra a teoria da ubiquidade (ou teoria da unidade, ou teoria mista), segundo a qual lugar do crime é tanto o lugar onde foi praticada a ação ou omissão, no todo ou em parte, como onde se produziu ou deveria produzir-se o resultado. A expressão "deveria produzir-se o resultado" refere-se às hipóteses de tentativa quando a ação foi praticada fora do território nacional. ... Diante do conceito legal de lugar do crime, em princípio não ficam sob a égide da lei brasileira os ilícitos penais quando apenas os atos preparatórios ou os efeitos secundários do crime ocorram no Brasil. O conceito de lugar do crime não é válido para o efeito de competência, uma vez que expressamente, se prevê que a competência ratione loci é determinada pelo "lugar em que se consumar a infração" (artigo 70 do Código de Processo Penal – CPP) (MIRABETE, 2011, p. 22).

A teoria da ubiquidade é em alguns casos utilizada como critério para tornar prevento o juiz e assim solucionar conflitos de jurisdição positivo entre Estados membros.

> Aos crimes virtuais praticados em nosso território nacional, importa destacar a implicação da teoria do resultado, adotada pelo CPP, em seu art.70, consagrando que, "A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução". Certa vez, nesta esteira, o STJ se posicionou a respeito da consumação do crime, sob três aspectos, quais sejam: a) envolvendo comunicação eletrônica, não ocorre no lugar do envio, e sim no lugar do recebimento; b) de furto, ocorre no momento em que o bem é subtraído da vítima, saindo de sua esfera de disponibilidade (desapossamento efetivado pelo sistema informatizado); c) de publicar cena pornográfica que envolva criança ou adolescente, dá-se no ato da publicação das imagens na internet (FILHO, 2011, online).

O crime cibernético é de natureza formal, e, portanto sem a necessidade de resultado naturalístico. Para exemplificar considere o crime de furto em uma situação real (física), um criminoso que furta certa quantia pecuniária de alguém desenvolve uma conduta que tenha por intenção vislumbrar o resultado, obter o dinheiro. Tenha este mesmo exemplo, porém, agora no campo virtual, para que o infrator atinha o objetivo ele tem que de alguma forma infectar o dispositivo informático da vítima e que com essa infecção seja capaz de capturar informações sensíveis como nome, número do cartão de crédito, tendo cumprido esta passo, o delinquente passa para o próximo. O passo seguinte é se apossar da quantia desejada,

configurando portando o furto digital. A diferença entre os casos exemplificados é que no furto digital há a necessidade de adulterar o sistema através de vírus, independentemente da obtenção do resultado esperado, pois a materialização é outra ação que podem ocorrem em momentos bem distintos.

A tecnologia é utilizada nesta modalidade de crimes contemporâneos para alavancar resultados, que para eles proporciona maior número de clientes e com baixo investimento diga se de passagem, rompendo inclusive barreiras territoriais. Para estes cibercriminosos não importa tratado ou mesmo Direito Internacional Público, o que importa é o retorno rápido e de "baixo risco".

Quem se sentir ou for vítima deverá em primeiro lugar preservar o sistema informático para preservar a respectiva prova. E assim que possível solicitar da autoridade policial a realização de exame pericial e de investigação complementar para o ajuizamento de ação penal (BARROS, 2005).

> Além da constante atualização dos peritos criminais, necessária também a atualização dos operadores do direito, para que possam atuar de forma mais segura. Implantar eventos relacionais ao tema em faculdades de Direito tornasse fundamental na busca de profissionais competentes. Os meios acadêmicos, o próprio Poder Judiciário, e também as entidades de classe devem ser alvo desta capacitação técnica. Não se olvidando da capacitação jurídica, demasiadamente importante, os operadores do direito devem se adequar à nova realidade mundial, que busca diminuir fronteiras e a celeridade (COELHO, 2008, online).

Nos crimes cibernéticos não é simples a identificação da autoria, por isto a importância de agir rápido no sentido de preservar as provas do crime. Isto porque os cibercriminosos realizam atos lesivos sob camuflagem do anonimato ou de um nickname (apelido de identificação). Com todos estes cuidados, ainda assim, mesmo que identificado o autor, não é atribuído a autoria, pois em alguns julgamentos proferidos por tribunais estrangeiros foram sustentado e aceito a negativa de autoria defendido por seus advogados particulares que impuseram dúvidas no momento de se efetivar a prestação jurisdicional. O argumento da defesa desta tese é no sentido de afirmar que o acusado também fora vítima e que o seu dispositivo informático foi "sequestrado remotamente" por vírus, não estando sobre seu controle às atividades realizadas no mesmo. A recomendação doutrinaria para caso semelhante é que o ônus da prova seja transferido para o réu, para que não comprometa irremediavelmente a atividade de persecução criminal (BARROS, 2005).

Os criminosos da web atuam em conluio com especialistas que exploram as vulnerabilidades dos sistemas computacionais instalados nos dispositivos informáticos dos

candidatos a vítima. Tendo êxito o dispositivo atacado estará submisso aos comandos a qual os seus invasores desejam realizar. O problema é que a invasão pode se dá maneira recursiva, um dispositivo que invade o outro sucessivamente até atingir um número satisfatório em que dificulta o máximo a descoberta da verdadeira autoria. A identificação dos dispositivos conectados em rede é feita pelo *Internet Protocol* - IP ou protocolo da internet, que é uma combinação numérica única fornecida pelo provedor de acesso que possibilita determinar o local em que partiu a conexão, e assim torna-se possível a identificação dos comandos da ação criminosa. Para que a prova seja o mais irrefutável possível é imprescindível o laudo pericial realizado por especialistas em direito eletrônico ou informática. Que informe detalhadamente ao juiz todos os aspectos do exame do corpo de delito do equipamento utilizado para cometer o crime, tais como os arquivos constantes no dispositivo bem como histórico de navegação na web. (COELHO, 2008).

Na atualidade os grupos mais temidos são as organizações criminosas e os ciberterroristas, que são ciberciminosos que impõe o terror numa amplitude muito maior. Os membros que compões o ciberterrorismo utilizam a internet para coordenar e dissimular suas condutas ilícitas, recrutando ou aliciando técnicos especializados, usando o cibercrime como forma de financiamento. O Ciberterrorismo tem estado em maior evidência após o ataque do dia 11.09.2001 nos E.U.A, colocando os países, principalmente aqueles ditos de primeiro mundo em alerta, pois sabe-se que alguns grupos terrorista como o Al-Qaeda, utilizada a internet como veículo para divulgar e propagar ações terroristas, espalhando o medo na opinião pública (DIAS, 2010).

3.2 A Atuação dos Órgãos Responsáveis pelo Combate ao Cibercrime

A Secretaria Extraordinária de Segurança para Grandes Eventos do Ministério da Justiça, desenvolveu um planejamento estratégico de segurança para a Copa do Mundo Fifa Brasil 2014, neste material está contemplada a segurança do espaço cibernético e atribui às Forças Armadas o papel fundamental nestas ações em parceria com as Forças de Segurança Pública (BRASIL).

> Os riscos identificados para o Brasil, relativos à Copa do Mundo de 2014, foram enumerados em função da experiência dos Oficiais de Inteligência da Agência Brasileira de Inteligência (ABIN), através da utilização do Sistema de Analise de Risco com Ênfase na Ameaça – ARENA, assim como mediante informações dos Entes Federados, levando-se em consideração, dentre outros aspectos os riscos observados em outros eventos esportivos (BRASIL, online).

Dentre alguns dos principais pontos para a elaboração da analise de ricos foram: crime organizado; criminalidade na fronteira; terrorismo e organizações extremistas; e outros crimes que engloba criminalidade de massa; fraude (pirataria, falsificação de ingressos); e traz também previsão de atuação contra os crimes cibernéticos e o uso não autorizado de sistemas de Tecnologia da Informação - TI; marketing de emboscada além de trotes e ameaças (BRASIL).

Vários estados, contam com Delegacias Especializadas, a exemplo, o Tocantins que tem a Divisão de Repressão a Crime Cibernético – DRCC vinculada a Delegacia Estadual de Investigações Criminais – DEIC. Nota-se que os Estados-Membros estão criando e atuando através de órgãos incumbidos e especializados no combate e prevenção da criminalidade eletrônica, o que não pode parar é com investimentos, principalmente no que diz respeito a atualização e treinamento de seus investigadores especializados, pois o dinamismo dos infratores tecnológicos na descobertas de "técnicas do mal" são muito grandes.

Como a maioria dos crimes ocorridos na internet é de meio, as delegacias especializadas acabam sendo eficiente no combate das práticas destes delitos, através dos boletins de ocorrências. Os casos mais comuns são dos crimes de calúnia, difamação, injúria, estelionato, e outras infrações eletrônicas de dano e violações de direitos autorais.

"No âmbito da Polícia Federal, a perícia de informática teve início em 01/11/95. Posteriormente, em 96, foi criada a Unidade de Perícia de Informática da Polícia Federal - PF. Em 2003 recebeu a denominação atual de SEPFIN - Serviço de Perícia em Informática" (ONLINE). Tendo como um dos objetivos, realizar a identificação, processamento e transformar as evidências digitais em provas materiais de crimes através de métodos técnico-científicos, com a finalidade de conferir-lhes validade probatória em juízo.

Em agosto de 2005 a PF executou a "Operação Pégasus", que resultou na prisão de 105 pessoas, em pelo menos 6 Estados da Federação. Os suspeitos estavam aplicando o golpe conhecido por *pishing* (fusão de duas palavras inglesas *password* e *fishing* que significam respectivamente senha e pescaria). Os invasores visavam "pescar" as senhas das vítimas, que eram obtidos por envio de e-mails contendo de forma oculta um programa, conhecido como *trojan*. Os invasores eram tão bem orientados como os integrantes de organizações criminosas, os dinheiros obtidos nesta prática eram depositados em contas de "laranjas" ou eram utilizados no pagamento de faturas de terceiros para aquisição de produtos pela internet. Cada integrante desta organização criminosa tinha trabalhos bem divididos, os programadores

eram incumbidos de elaborarem páginas web idênticas das empresas verdadeiras e as enviavam por e-mails para vários usuários em busca de novas vitimas (BARROS, 2005).

A PF desenvolveu através dos peritos criminais federais uma ferramenta poderosa no monitoramento de redes, denominado “EspiaMule”. A utilização deste programa corroborou com o sucesso da “Operação Carrossel” em dezembro de 2007 que cominou em uma ação contra a pedofilia que atuava em (quatorze) 14 estados brasileiros e em (setenta e oito) 78 países (BRASIL).

> A pedofilia é um dos crimes que mais tem se disseminado através desta nova realidade virtual, pois os pedófilos agem através das redes de relacionamento seduzindo crianças para satisfazer aos seus desejos sexuais mais perversos. Este tipo de abuso é uma afronta a garantia de proteção integral das crianças e adolescentes preconizada na Magna Carta de 1988 e aos direitos humanos infantis tutelados na Declaração Universal dos Direitos da Criança de 1959 (SANTOS, 2010, online).

É mister relembrar um caso emblemático de grande repercussão nacional e internacional ocorrido no ano de 2000. Este caso tratava do envolvimento de dois estrangeiros acusados de engendrar uma rede de pornografia infanto-juvenil pela internet, vendendo fotos que envolvia menores. A repercussão foi ainda maior por envolver o então vice-cônsul de Israel Arie Scher, que exercia suas funções no consulado na cidade do Rio de Janeiro, e também de um professor de hebraico Georges Schteinberg. "Os dois foram denunciados por uma menina de 17 anos, que revelou detalhes comprometedores de seu relacionamento durante mais de três meses com os dois homens" (FRANÇA, 2000). Com este caso, vieram junto questões relativas à imunidade diplomática, extradição, necessidade de tratados internacionais. O caso ficou ainda mais complexo, quando o acusado deixou o país, fazendo uso da impunidade diplomática e retornando para sua terra natal. Tendo assim impossibilitado a aplicação da lei penal brasileira, pela inexistência de acordo internacional que abordasse sobre esta pratica delitiva de ojeriza mundial (SANTOS, 2010).

> ... o fenômeno da globalização, a "planificação" do mundo impulsionou a mobilidade das pessoas, facilitando, inclusive, a fuga de criminosos da persecução penal no país onde cometeram delitos. Evidencia-se aqui que o poder de dizer o direito, a jurisdição, não acompanhou, par passu, tal mobilidade. Os Estados se veem limitados a seus limites geográficos para aplicar o direito, enquanto o delito transnacional se espraia em todos os locais, especialmente no ciberespaço, de modo que autores chegam a asseverar a necessidade de criação de um novo fenômeno chamado de metaterritorialidade, reavaliando, ou mesmo afastando os conceitos tradicionais de competência internacional e extraterritorialidade (SILVA, 2012, online).

O Brasil vem gradativamente progredindo no sentido de aumentar a participação em matéria penal junto à comunidade internacional, sendo signatário de protocolos e acordos que submetem a jurisdição em Cortes Internacionais. Podem-se enumerar algumas das principais tais como: a) emenda constitucional 45/04 que incorporou tratado e convenções internacionais sobre direitos humanos, além de submeter o país a exame jurídico no Tribunal Penal Internacional; Decreto 3.468/2000 que trata do Protocolo de Assistência Mútua em Assuntos Penais entre os países do MERCOSUL (SILVA, 2012).

CONSIDERAÇÕES FINAIS

Foi visto neste trabalho a importância do Direito Eletrônico para a sociedade informacional, os crimes passíveis de os usuários sofrerem. Como são classificados estes agentes ativos destes crimes eletrônicos. Também foram apresentadas as preocupações dos profissionais do Direito em buscarem soluções para manter a ordem social e o Estado Democrático de Direito. Quais soluções adotadas em alguns países em relação ao Ciberespaço.

Quais as inovações trazidas pela Lei 12.737/12 que acrescentou dois artigos 154-A e 154-B no código penal brasileiro, com penalização mais específica para estes crimes que tende a aumentar com o aumento do tempo e da quantidade de usuários conectados a Internet.

Também fora apresentada que as pessoas devem ter em consciência, que ter um dispositivo informático plugado à internet, esta sujeita a riscos, assim como quem pretende viajar e enfrenta uma rodovia de grande movimento em um dia de feriado prolongado. Não adianta muito esta precavido, utilizando mecanismos de proteção como cinto de segurança, *aribag*, se o motorista que vem em sentido contrario estiver alcoolizado ou dormindo ao volante. De forma semelhante não adianta ter mecanismos de segurança como antivírus, *firewall* se estes estão desativados ou desatualizados. A lei que ficou conhecida como lei seca não visa acabar com os acidentes de transito, mas punir o infrator que dirigir embriagado e ao longo do tempo espera-se uma mudança cultural. O propósito da Lei sobre invasão dos Dispositivos Informáticos é semelhante, não visa por fim aos diversos delitos que podem ocorrer neste meio, mas sim iniciar uma mudança cultural dos internautas, e ao mesmo tempo deixar com mais receio os infratores.

Tendo em vista o que foi exposto neste trabalho, a grande maioria dos delitos não é abordada na Lei brasileira que trada da invasão dos Dispositivos Informáticos (Lei 12.737/12), desta forma não há que se falar em efetividade da lei. Mas há que se admitir que um importante passo foi dado para romper a inércia da falta de legislação específica sobre crimes eletrônicos ou cibernéticos. Tendo em vista que o ordenamento jurídico brasileiro adota o princípio da legalidade, assim abre caminho para aplicar melhor a pena para estes delitos e formar uma jurisprudência mais consolidada sobre estas demandas.

Foi visto que qual quer pessoa pode ser sujeito envolvido neste crime comum e formal em que pode figurar inclusive pessoa jurídica, neste caso na modalidade passiva. E que não há previsão de aumento de pena, para os casos que o autor seja funcionário púbico. Foi apresentado também que na atualidade os grupos mais temidos são as organizações criminosas e os

ciberterroristas, que são ciberciminosos que impõe o terror numa amplitude muito maior. Os membros que compões o ciberterrorismo utilizam a internet para coordenar e dissimular suas condutas ilícitas, recrutando ou aliciando técnicos especializados, usando o cibercrime como forma de financiamento.

Apresentou-se que o governo brasileiro vem fazendo esforços em se combater o cibercrime, ainda mais pela proximidade da copa do mundo em 2014 esta preocupação tem se intensificado e que no material relativo ao planejamento estratégico sobre a segurança do espaço cibernético, este controle, ficou a cargo das Forças Armadas em parceria com as Forças de Segurança Pública.

REFERÊNCIAS

ABDO, Helena. Mídia e Processo. São Paulo Ed. Saraiva, 2011.

ARAS, Vladimir Aras. Crimes de informática. Uma nova criminalidade. Disponível em: <http://jus.com.br/revista/texto/2250/crimes-de-informatica>. Acesso em 22.fev.2013.

BALDAN. GUILHERME RIBEIRO. Meio Eletrônico: Uma Das Formas De Diminuição Do Tempo De Duração Do Processo no 4º Juizado Especial Cível De Porto Velho/RO. Disponível em: < http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/8609/DMPPJ%20-%20GUILHERME%20RIBEIRO%20BALDAN.pdf?sequence=1 >. Acesso em 22.maio.2016.

BARROS, Marco Antonio. Tutela Punitiva Tecnológica. O Direito na Sociedade da Informação sobre coord. Liliana Minardi Paesani. São Paulo, Atlas, 2007.

BRASIL. http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em 29.mar.2013.

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 28.abri.2013.

BRASIL. Constituição da República Federativa do Brasil.

BRASIL. Código Penal Militar. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm>. Acesso em 05.maio.2013.

BRASIL. Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em 17.maio.2013.

BRASIL. Planejamento Estratégico de Segurança para a Copa do Mundo Fifa Brasil 2014. Disponível em < http://blog.justica.gov.br/inicio/wp-content/uploads/2012/07/ Planejamento-Estrategico-SESGE.pdf >. Acesso em 19.maio.2013.

BRASIL. Apostila desenvolvida pela Coordenação de TI da Polícia Federal - Perícia em informática: passado, presente e futuro. Disponível em < ftp://ftp.registro.br/pub/gts/gts11/02-pericia-info.pdf >. Acesso em 20.maio.2013.

BRASIL. LEI Nº 11.419, DE 19 DE DEZEMBRO DE 2006. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm>. Acesso em 21.maio.2013.

BRITO, Auriney. Análise da Lei 12.737/12 – "Lei Carolina Dieckmann". Disponível em < http://atualidadesdodireito.com.br/aurineybrito/2013/04/03/analise-da-lei-12-73712-lei-carolina-dieckmann/>. Acesso em 06.maio.2013.

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a lei 12.737/12 e o crime de invasão de dispositivo informático. Disponível em: <

http://jus.com.br/revista/texto/23522/primeiras-impressoes-sobre-a-lei-no-12-737-12-e-o-crime-de-invasao-de-dispositivo-informatico> Acesso em 29.mar.2013.

CARNEIRO, Garcia Adeneele. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529>. Acesso em 22.mar.2013.

CELLA, José Renato. Direito Digital tem muito a ser explorado. Disponível em <http://www.gazetadopovo.com.br/vida-universidade/carreira/conteudo.phtml?id=1239389&tit=Direito-Digital-tem-muito-a-ser-explorado>. Acesso 21.mar.2013.

CHINA. <http://china.org.cn/government/whitepaper/node_7093508.htm>. Acesso em 13.abr.2013.

COELHO, Ana Carolina Assis. CRIMES VIRTUAIS: ANÁLISE DA PROVA. Disponível em <http://intertemas.unitoledo.br/revista/index.php/Juridica/article/viewFile /827/804>. Acesso em 19.maio.2013.

CORRÊIA, Gustavo Testa. Aspectos Jurídicos da Internet. São Paulo. Ed. Saraiva, 2000.

DONEDA, Danilo. Privacidade e Transparência no Acesso à Informação Pública. Disponível < http://www.egov.ufsc.br/portal/sites/default/files/lefis11-09.pdf >. Acesso em 13.maio.2013.

DOTTI, René Ariel. Proteção da vida privada e liberdade de informação: possibilidade e limites. São Paulo: RT, 1980.

DANTAS, Romulo Rodrigues. Decorrências da Utilização da Internet Por Organizações Terroristas: o recurso da comunicação tecnológica como proposta de mudança não-democrática de poder. Disponível em < http://www.abin.gov.br/modules/mastop_publish/files/files_4b8d519458ebd.pdf >. Acesso em 28.abr.2013.

DIAS, Vera Elisa Marques. A Problemática da Investigação do Cibercrime. Disponível em <http://www.verbojuridico.com/doutrina/2011/veradias_investigacaocibercrime.pdf >. Acesso em 19.maio.2013.

FURST, Mariana Samos Bicalho Costa. Liberdade de Expressão na Internet. Disponível em < http://ueadsl.textolivre.pro.br/2012.2/papers/upload/97.pdf >. Acesso em 10.maio.2013.

GALLI, Fernanda Correa Silveira. LINGUAGEM DA INTERNET: um meio

de comunicação global. Disponível em <http://www.ufpe.br/nehte/artigos/LINGUAGEM%20DA%20INTERNET-um%20meio.pdf>. Acesso em 14.abr.2013

GATTO, Victor Henrique Gouveia. Tipicidade penal dos crimes cometidos na internet. Disponível em <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10065>. Acesso em: 14.abr.2011

GUEIROS, Nehemias Júnior. É chegada hora de compartilhar o controle da internet. Disponível em < http://jus.com.br/revista/texto/12966/e-chegada-hora-de-compartilhar-o-controle-da-internet>. Acesso em 13.abr.2013.

FRANÇA, Ronaldo. Inimigo externo. Disponível em <http://veja.abril.com.br/120700/p_047.html>. Acesso em 20.maio.2013.

FILHO, José Carlos de Araújo Almeida. Direito Eletrônico ou Direito da Informática? Disponível em: <http://www.ibde.org.br/docs/revista/rede08.pdf>. Acesso em 19.fev.2013.

FILHO, Jaziel Lourenço da silva. O Código e as Leis do Ciberespaço. Disponível em<http://idireitofbv.wikidot.com/lei>. Acesso em 14.abr.2013.

FILHO, Aldalberto Simão. Sociedade da Informação e seu Lineamento Jurídico. O Direito na sociedade da informação / Liliana Minardi Paesani, coordenadora. São Paulo: Atlas, 2007

FILHO, Dickson Cirilo Andrade Netto. Crime virtual: crime contra o patrimônio no âmbito da internet, suas peculiaridades e controvérsias à luz do Código Penal de 1940. Disponível em < http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12231>. Acesso em 17.maio.2013.

LEMOS <http://veja.abril.com.br/noticia/brasil/roubo-de-fotos-de-carolina-dieckmann-acelera-tramitacao-de-projeto-de-lei-sobre-crimes-ciberneticos>. Acesso em 29.mar.2013.

LEMOS, Ronaldo, et al. Proposta de Alteração do PLC 84/99 / PLC 89/03 (Crimes Digitais) e Estudo sobre História Legislativa e Marco Regulatório da Internet no Brasil. Disponível em < http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2685/Proposta_e_Estudo_CTS-FGV_Cibercrimes_final.pdf?sequence=1>. Acesso em 09.maio.2013.

LÉVY, Pierre. Cibercultura. Rio de Janeiro: Editora 34. 1999. A inteligência coletiva: por uma antropologia do ciberespaço. São Paulo: Edições Loyola. 1998.

LINS, Bernardo F. E. Privacidade e Internet. Disponível em: http://www2.camara.leg.br/documentos-e-pesquisa/publicacoes/estnottec/pdf/001854.pdf. Acesso em 29.mar.2013.

MARTINS, Ives Gandra da Silva. Privacidade na Comunicação Eletrônica. Disponível em < http://www.scielo.br/pdf/ci/v30n1/a03v30n1.pdf>. Acesso em 12.maio.2013.

MAZONI, Ana Carolina. Crimes na Internet e a Convenção de Budapeste. Disponível em: <http://repositorio.uniceub.br/bitstream/123456789/842/1/20523632.pdf>. Acesso em 28.abr.2013.

MENDES, Gilmar. Evolução Recente do Sistema Judiciário Brasileiro. Disponível em: <http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfAgenda_pt_br/anexo/Evolucao_Recente_do_Sistema_Judiciario_Brasileiro_vPort1.pdf>. Acesso em 19.maio.2013.

MEZZAROBA, O.; MONTEIRO, C. S. Manual de Metodologia da Pesquisa no Direito. São Paulo: Saraiva, 2003.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. Código Penal Interpretado 7 ed. São Paulo: Atlas, 2011.

MONTEIRO, Jhonny Garcia Trindade. A importância do direito eletrônico no ensino superior jurídico do Brasil. Disponível em: <http://jus.com.br/revista/texto/18986/a-importancia-do-direito-eletronico-no-ensino-superior-juridico-do-brasil>. Acesso em 29.mar.2013.

MONTEIRO, Renato Leite. Cibernética: A Invasão da Privacidade e da Intimidade. Disponível em: < http://www.publicadireito.com.br/conpedi/manaus/arquivos/Anais/sao_paulo/2513.pdf >. Acesso em: 15.maio.2013.

MORAIS, Adriana, et al. Crimes Digitais e Suas Implicações. Disponível em: <http://fgh.escoladenegocios.info/revistaalumni/artigos/edEspecialMaio2012/vol2_noespecial_artigo_12.pdf>. Acesso em 19.fev.2013.

NETO, João Araújo Monteiro. Crimes informáticos uma abordagem dinâmica ao direito. Disponível em: <http://hp.unifor.br/pdfs_notitia/1690.pdf>. Acesso em 19.fev.2013.

OAB-SP Cartilha Recomendações e boas práticas para o USO SEGURO DA INTERNET PARA TODA A FAMÍLIA. Disponível em: <http://www.oabsp.org.br/noticias/2011/02/16/6753/>. Acesso em 19.fev.2013.

OLIVEIRA, Jane Resina F. "Lei Carolina Dieckmann: Antes tarde do que nunca". Disponível em: < http://www.resinamarcon.com.br/artigo/293/lei-carolina-dieckmann-antes-tarde-do-que-nunca/>. Acesso em 05.maio.2013.

ONLINE Número de usuários de internet sobe para 2 bilhões em 2010. Disponível em: <http://www.reporternews.com.br/noticia.php?cod=311078>. Acesso em 19.fev.2013.

ONLINE PL Crimes Cibernéticos - Senador Azeredo. Disponível em: < http://www.diplointernetgovernance.org/group/brasil/forum/topics/2332551:Topic:87?page=1&commentId=2332551%3AComment%3A10198&x=1#2332551Comment10198 > Acesso em 28.abr.2013.

PAESANI, Liliana Minardi. Direito de Informática: comercialização e desenvolvimento internacional de Software. São Paulo: Atlas, 1998.

PAESANI, Liliana Minardi. Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil. 2. Ed. – São Paulo: Atlas, 2003.

PEREIRA, Elizabeth Dias Kanthack. Proteção Jurídica do Software no Brasil. Curitiba: Juruá, 2002.

PINHEIRO, Patrícia Peck. Direito digital e a questão da privacidade nas empresas. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo id=2901>. Acesso em 21.fev.2013.

PINHEIRO, Patrícia Peck. O Direito Digital como Paradigma de uma Nova Era. Os "novos" direitos no Brasil: natureza e perspectivas uma visão básica dos novos conflituosidades jurídicas. 2. ed. São Paulo: Saraiva, 2012.

PORTUGUAL. Lei do Cibercrime - nº. 109/2009. Disponível em <http://dre.pt/pdf1sdip/2009/09/17900/0631906325.pdf>. Acesso em 19.maio.2013.

TEIXEIRA, Tarcisio. Direito Eletrônico. São Paulo: Editora Juarez de Oliveira, 2007.

RICCI Milena Mara da Silva. A Axiologia e a Evolução da Sociedade na Evolução do Direito de Família. Disponível em <http://www.grupointegrado.br/conccepar2011/?action=anais_resumo&id=561>. Acesso em 21.fev.2013.

TONHÁ, Herckmans Ricloarson. A reforma da lei 9.800/99. Disponível em < http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=4082>. Acesso em 21.maio.2013.

RULLI, Antonio Junior. Jurisdição e Sociedade da Informação. O Direito na sociedade da informação / Liliana Minardi Paesani, coordenadora. São Paulo: Atlas, 2007.

SANTOS, Noemi de Freitas; ROSA, Taís Hemann da. O Crime de Pornografia Infantil no Ciberespaço: Uma Abordagem sob a Égide do Direito Comparado. Disponível em < http://www.unifra.br/eventos/sepe2010/2010/Trabalhos/sociais_Aplicadas/Completo/4842.pdf >. Acesso em 20.maio.2013.

SCORZELLI Patrícia Scorzelli. A Comunidade Cibernética e o Direito. Ed. Lumenn Juris. Rio de Janeiro 1997.

SENA, Gabriel Astoni. A Reforma do Poder Judiciário no Brasil: uma análise a partir das metas do Conselho Nacional de Justiça. Disponível em < http://www.periodicos.ufsc.br/index.php/adm/article/view/2175-8077.2012v14n33p68>. Acesso em 22.maio.2013.

SIQUEIRA, Julio Pinheiro Faro Homem de. Natureza do Direito Comparado. Disponível em: <http://jus.com.br/revista/texto/23674/natureza-do-direito-comparado>. Acesso em 06.maio.2013.

SIQUEIRA, Paulo Hamilton Júnior. Habeas Data: Remédio Jurídico da Sociedade da Informação. O Direito na sociedade da informação / Liliana Minardi Paesani, coordenadora. São Paulo: Atlas, 2007.

SILVA, Remy Gama. Crimes da Informática. Disponível < http://www.cesarkallas.net/arquivos/livros/direito/00715%20-%20Crimes%20da%20Inform%E1tica.pdf >. Acesso em 09.maio.2013.

SILVA, Marcelo Mesquita. Ação Internacional no Combate ao Cibercrime e suas Influência no Ordenamento Jurídico Brasileiro. Disponível em < http://www.bdtd.ucb.br/tede/tde_busca/arquivo.php?codArquivo=1691>. Acesso em 20.maio.2013.

SOUZA, Gills Lopes Macêdo, Dalliana Vilar Pereira. A Conversão de Budapeste e as Leis Brasileiras. Disponível em <http://www.mp.am.gov.br/index.php/centros-de-apoio/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 15.abri.2013.

WACHOWICZ, Marcos Wachowicz. O "Novo" Direito Autoral na Sociedade Informacional. Os "Novos" diretos no Brasil, organizadores. Antonio Carlos Wolkmer; José Rubens Morato Leite. 2 ed. São Paulo: Saraiva, 2012.

STJ Superior Tribunal de Justiça. STJ contribui para criar jurisprudência no mundo digital. Disponível em < http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=101146>. Acesso em 16.maio.2013.

ZANATTA, O Direito Digital E As Implicações Cíveis Decorrentes Das Relações Virtuais. Disponível em: <http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2010_2/leonardo_zanatta.pdf>. Acesso em 21.fev.2013.

ZATTA, Dirciane Inês Backes. Furto de Informações. Disponível em: http://www.buscalegis.ufsc.br/revistas/files/anexos/5592-5584-1-PB.htm. Acesso em 29.mar.2013.

ANEXOS

1) - Material publicitário sobre a Lei de Combate à Criminalidade Informática de Macau.

2) Lei 109/2009 de Portugal sobre Cibercrime

ASSEMBLEIA DA REPÚBLICA

Lei n.º 109/2009

de 15 de Setembro

Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

A Assembleia da República decreta, nos termos da alínea *c*) do artigo 161.º da Constituição, o seguinte:

CAPÍTULO I

Objecto e definições

Artigo 1.º

Objecto

A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

electromagnéticos, acústicos, mecânicos ou outros;

f) «Topografia», uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;

g) «Produto semicondutor», a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica.

CAPÍTULO II

Disposições penais materiais

Artigo 3.º

Falsidade informática

1 — Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.

3) – Diário Oficial da União que saiu a publicação da Lei 12.737/12

ISSN 1677-7042

DIÁRIO OFICIAL DA UNIÃO

República Federativa do Brasil - Imprensa Nacional

Em circulação desde 1º de outubro de 1862

Ano CXLIX Nº 232

Brasília - DF, segunda-feira, 3 de dezembro de 2012

SEÇÃO 1

Sumário

Atos do Poder Legislativo

LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

A PRESIDENTA DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

Art. 2º (VETADO)

Art. 3º (VETADO)

Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 5º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

"Art. 20. .....

§ 3º .....

II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

....." (NR)

Art. 6º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.

DILMA ROUSSEFF
José Eduardo Cardozo
Paulo Bernardo Silva
Maria do Rosário Nunes

LEI Nº 12.736, DE 30 DE NOVEMBRO DE 2012

Dá nova redação ao art. 387 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, para a detração ser considerada pelo juiz que proferir sentença condenatória.

A PRESIDENTA DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º A detração deverá ser considerada pelo juiz que proferir a sentença condenatória, nos termos desta Lei.

Art. 2º O art. 387 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, passa a vigorar com a seguinte redação:

"Art. 387. .....

§ 1º O juiz decidirá, fundamentadamente, sobre a manutenção ou, se for o caso, a imposição de prisão preventiva ou de outra medida cautelar, sem prejuízo do conhecimento de apelação que vier a ser interposta.

§ 2º O tempo de prisão provisória, de prisão administrativa ou de internação, no Brasil ou no estrangeiro, será computado para fins de determinação do regime inicial de pena privativa de liberdade." (NR)

Art. 3º Esta Lei entra em vigor na data de sua publicação.

Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.

DILMA ROUSSEFF
José Eduardo Cardozo

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

A PRESIDENTA DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

"Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

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

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

4) – Página da Revista Veja que saiu uma matéria sobre a aprovação da Lei no Congresso

GUTO MAIA/BRAZIL PHOTO PRESS/AE

BELEZA ROUBADA
Fotos da atriz global nua acabaram na internet, e cinco chantagistas estão respondendo pelo crime

A LEI DA BELA CONTRA O CRIME

Depois do vazamento de fotos de Carolina Dieckmann, o Congresso aprova legislação para combater malfeitos virtuais, como o roubo de dados em invasão de computador

A terra sem lei da internet vai ficar um pouco menos insegura. O Congresso aprovou na última quarta-feira uma lei que determina punições para quem invadir computadores para obter dados, divulgar essas informações e disseminar vírus, entre outros crimes do mundo virtual *(veja o quadro)*. Até agora, a polícia e os juízes tinham de fazer malabarismos para adaptar a legislação já existente, toda ela pré-internet, para tentar enquadrar esses criminosos. O resultado, no mais das vezes, era a impunidade dos violadores. O debate sobre uma legislação específica para a internet se arrastava em velocidade de conexão discada havia mais de uma década, mas ganhou ímpeto depois da invasão do computador da atriz global Carolina Dieckmann — que acabou por batizar a nova lei. Roubadas, fotos íntimas que mostravam toda a sua beleza mignon explodiram no ibope da rede mundial de computadores no começo de maio. Logo após o vazamento, cinco homens, que haviam tentado chantagear a atriz, foram pegos e indiciados pelos crimes de extorsão qualificada, difamação e furto — mas não pela invasão de seu computador. Eles podem pegar até quinze anos de prisão. Se a Lei Carolina Dieckmann estivesse em vigor, a pena poderia ser estendida por mais quatro anos.

Outra lei, em discussão desde 1999, também foi aprovada no pacote Dieckmann e tipificou o crime de falsificação de cartões de crédito e débito por meio eletrônico. A ofensiva é positiva, mas especialistas avaliam que as novas leis já nascem com brechas. Elas não preveem punição, por exemplo, para alguém que tenta invadir um computador mas não consegue, ou o invade e não rouba nada, apenas por curiosidade. Mesmo com as falhas, o avanço é inegável. O Brasil tem a quinta maior população de usuários de internet no mundo, com 70 milhões de pessoas, que passam em média 25 horas por mês online. "Com uma movimentação dessas, já era hora de termos segurança jurídica para nossos usuários", diz Renato Opice Blum, advogado especialista em crimes de internet. ■

O QUE A NOVA LEI TORNA CRIME

■ ***Invadir computadores para obter, adulterar ou destruir dados ou informações***

Pena: **3 meses** a **1 ano** de prisão e multa. A punição aumenta de **um sexto** a **um terço** se o crime resultar em prejuízo econômico

■ ***Facilitar a invasão ou produzir, oferecer ou distribuir programas que o façam (como vírus)***

Pena: **3 meses** a **1 ano** de prisão e multa. Sobe de **um sexto** a **um terço** se o crime provocar prejuízo econômico

■ ***Obter, através da invasão, conteúdo de mensagens eletrônicas privadas, segredos comerciais e industriais, informações sigilosas ou controle remoto do computador invadido***

Pena: **6 meses** a **2 anos** e multa. Aumenta de **um** a **dois terços** se houver divulgação, comercialização ou transmissão dos dados obtidos. Se o crime for cometido contra altas autoridades, a pena aumenta de **um terço** a **50%**

■ ***Interromper ou perturbar o serviço de internet***

Pena: **1** a **3 anos.** A pena **dobra** se o crime for cometido durante calamidades públicas