UNIVERSIDADE FEDERAL DO MARANHÃO

CENTRO DE CIÊNCIAS SOCIAIS

CURSO DE DIREITO

ANGELO SOUSA LIMA

CIBERCRIMES E SUA CONFIGURAÇÃO NO PLANO JURÍDICO NACIONAL E INTERNACIONAL

São Luís

2017

ANGELO SOUSA LIMA

CIBERCRIMES E SUA CONFIGURAÇÃO NO PLANO JURÍDICO NACIONAL E INTERNACIONAL

Monografia apresentada ao Curso de Direito da Universidade Federal do Maranhão como requisito obrigatório para conclusão do curso e obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Cássius Guimarães Chai.

São Luís

2017

ANGELO SOUSA LIMA

CIBERCRIMES E SUA CONFIGURAÇÃO NO PLANO JURÍDICO NACIONAL E INTERNACIONAL

Monografia apresentada ao Curso de Direito da Universidade Federal do Maranhão, como requisito obrigatório para a conclusão do curso de Direito e obtenção do título de Bacharel.

São Luís, ____ de _____ de _____.

BANCA EXAMINADORA

Prof. Dr. Cássius Guimarães Chai (Orientador)

1º Avaliador

2º Avaliador

DEDICATÓRIA

Dedico este trabalho a cada uma das pessoas que me apoiou durante esses cinco anos de curso, em especial aos meus pais, Cândido e Elieide, à toda minha família, à minha noiva, Camila, e ao Mestre Cássius Chai, sem os quais eu não teria conseguido atingir os meus objetivos.

AGRADECIMENTOS

Ao estimado professor Cássius Guimarães Chai, cuja orientação constante, desde o terceiro ano de faculdade, foi imprescindível na busca de novas indagações e objetivos. Seus estudos e suas reflexões que, aliadas ao seu humanismo incomensurável, me incentivaram durante todo esse período pelas diversas vertentes do Direito e da vida.

Ao meu amado pai, Cândido, que além de meu herói, foi o responsável pela pessoa que eu me tornei e esteve comigo durante todos os momentos importantes da minha vida. À minha amada mãe, Elieide, que mesmo diante das dificuldades nunca deixou de acreditar em mim e na minha capacidade de conquistar os meus objetivos. À minha adorada família, que sempre esteve presente torcendo pelo meu sucesso.

À minha querida noiva, Camila, que me apoiou e esteve comigo durante todo o tempo de elaboração deste trabalho, sabendo lidar com todas as dificuldades e momentos de estresse, mas nunca deixando de me apoiar e torcer pelo meu êxito.

A todos e todas que de qualquer forma contribuíram na minha formação acadêmica, em especial aos meus amigos que sempre desejaram o melhor por mim.

RESUMO

A *Internet* constitui um dos maiores avanços da história da humanidade. O surgimento do Direito Cibernético, dos ciberespaços e dos cibercrimes traz consequências que atingem todos os ramos do Direito, em especial o Direito Constitucional e o Direito Penal. Novos conceitos, novos paradigmas e, em consequência, uma nova modalidade de delitos que ultrapassam o Direito Penal tradicional. A elaboração da Convenção de Budapeste ocorreu na busca de uma regulamentação jurídica a este novo espaço, principalmente no que tange à cooperação internacional penal entre os países, fator fundamental no combate aos cibercrimes e na definição de conceitos e jurisdições, bem como na imposição de estratégias para a melhoria das investigações e repressão a esta nova modalidade de delitos.

Palavras-chave: *Internet*. Direito Cibernético. Cooperação Internacional. Convenção de Budapeste. Cibercrimes.

ABSTRACT

The internet is one of the most great advances in the history of humanity. The arising of Cyberlaw, cyberspaces and cybercrimes brings consequences that affects all the branches of law, specially Constitucional and Criminal Law. New concepts, new paradigms and, consequently, a new type of criminal offenses that go beyond the tradicional Criminal Law. The creation of Budapest Convention took place in pursuit of a legal regulation in this new space, particularly with regard to international cooperation between countries, fundamental factor in the fight against cybercrimes and in the definitions of concepts and jurisdition, as well in the imposition of strategies to improve investigations and fight this new type of crimes.

Key-words: Internet. Cyberlaw. International Cooperation. Budapest Convention. Cybercrimes.

SUMÁRIO

1. INTRODUÇÃO

A *Internet* constitui um dos maiores avanços da história da humanidade, sendo a ferramenta mais utilizada no mundo atualmente, capaz de interligar cidades, estados e nações, desenvolver o intercâmbio cultural, social e comercial, bem como sendo um espaço para construção de histórias de vida e relacionamentos interpessoais.

Apesar de toda a importância desta ferramenta, o seu surgimento gerou diversas implicações no universo jurídico, levantando uma série de questionamentos a respeito de sua regulamentação legal. Com o advento da *Internet* vieram à tona também os chamados "cibercrimes" ou "crimes virtuais", ou seja, são aqueles crimes que são praticados diretamente contra um sistema ou meio informático ou através dele.

Destarte, mesmo após a consolidação da rede mundial de computadores algumas questões ainda permanecem obscuras. Como surgiram os cibercrimes? Qual a regulamentação jurídica oferecida pelo Brasil e os meios de combate a este novo tipo de delitos? Como se configuram os cibercrimes no plano jurídico internacional? Quais os principais mecanismos de repressão aos delitos virtuais? Como os países atuam em termos de cooperação internacional em direito penal em relação aos delitos virtuais? Quais os instrumentos jurídicos regulamentadores e sancionadores em relação aos cibercrimes?

Nesta esteira, verifica-se que o principal problema no que se refere ao surgimento dos cibercrimes diz respeito a como o Direito vai encarar esse novo espaço de cometimento de delitos, ou seja, se através da criação de um novo ramo específico, o Direito Cibernético ou Direito Digital, e quais vão ser os mecanismos oferecidos para o combate e repressão deste novo tipo criminal.

O presente trabalho visa à realização de um estudo bibliográfico, na expectativa de expor e demonstrar os principais aspectos e características referentes ao cibercrimes, enquanto instituto do Direito Cibernético, e suas relações com outros ramos do Direito, baseando-se principalmente nas leis do cenário jurídico nacional, na Convenção de Budapeste e na Cooperação Internacional em matéria de Direito Penal.

Também é importante destacar os efeitos dos cibercrimes (ou da cibercriminalidade) no plano jurídico internacional, visto que através dessa ferramenta de interação e comunicação globalizada que é a *Internet* as condutas e atuações no ciberespaço deixam de ser nacionalmente territoriais e passam a ser consideradas transfronteiriças, dada a enorme facilidade de acesso a sítios e domínios ao redor de todo o globo, estando estes localizados em diversos países.

Neste bojo, se faz mister uma análise do contexto de surgimento da Convenção de Budapeste e o seu papel do Direito Penal Internacional e na Cooperação Internacional, sendo hoje o principal instrumento de combate à cibercriminalidade, mas que ainda não fora assinado e ratificado pela grande maioria dos países, já que muitos sequer consideram o Direito Cibernético como um verdadeiro ramo autônomo do Direito, ou mesmo como uma realidade social capaz de modificar de fato o panorama jurídico de um país. .

2. A INTERNET E OS CIBERCRIMES

A *Internet*, indubitavelmente, representa hoje um dos meios mais importantes de comunicação, transmissão de notícias, intercâmbio de dados e informações, e, principalmente, espaço propício para o estabelecimento de relações transnacionais e interpessoais, bem como no que se refere ao *e-commerce*, consolidando-se como a ferramenta mais importante de uso mundial nos dias atuais. Entretanto, o caminho percorrido por essa ferramenta, até atingir os níveis nas quais a conhecemos hoje, é longo e remonta ao tempo da Guerra Fria, nos anos que sucederam a Segunda Grande Guerra.

2.1 Aspectos históricos

No decurso da Segunda Guerra Mundial, em fevereiro de 1945, no momento em que as forças armadas russas haviam atingido o rio Oder (fronteira entre a Polônia e Alemanha), e os exércitos americanos e ingleses se encontravam perto das margens do rio Reno (fronteira entre França e Alemanha), os presidentes dos países aliados reuniram-se em Yalta, na península russa da Crimeia, para estabelecerem as regras referentes à divisão do território alemão e seus aliados, na Europa Oriental.

O resultado da reunião foi considerado insatisfatório, principalmente por Estados Unidos e Inglaterra, visto que o poder do território russo se mostrou muito superior que ao poder dos territórios americanos e ingleses juntos. Esse evento é considerado o marco inicial do que viria a ficar conhecido como “Guerra Fria”.

A Guerra Fria, uma guerra ideológica travada entre Estados Unidos e a antiga União Soviética (URSS), foi responsável por diversos avanços no campo da ciência, tecnologia e, inclusive, no campo espacial.

Em 04 de outubro de 1957 a Rússia lança para o espaço o primeiro satélite artificial da história da humanidade, denominado “Sputnik”, que completava a órbita ao redor da terra a cada 90 (noventa) minutos e emitia sinais de rádio que podiam ser captados por quaisquer pessoas que utilizassem um rádio receptor.

O lançamento do primeiro satélite artificial ao espaço por parte da Rússia levou os Estados Unidos a criar a *ARPANET – Advanced Research Project Agency*, cujo principal objetivo era o desenvolvimento de programas espaciais. Criada em 1969, buscando atender às demandas do Departamento de Defesa Americano, no auge da Guerra Fria, ela veio a ser o embrião do que se tornaria a maior rede de intercomunicação do planeta, a *internet*.

O surgimento da *ARPANET* se deu em um período marcado pela utilização de macrocomputadores, existentes apenas em centros de pesquisas avançadas, predominantemente nos Estados Unidos, época em que os microcomputadores ainda não existiam.

Inicialmente, o objetivo de sua criação era a elaboração de uma rede que seria imune aos ataques soviéticos, possibilitando a interconexão de pontos de localização estratégicos, quebrando com o modelo tradicional de pirâmide, ou seja, uma localização principal que fosse se ramificando até atingir as localizações secundárias. Buscava-se um projeto que pudesse equilibrar todos os pontos a serem interligados, de forma que estes tivessem o mesmo "status" estratégico e organizacional. Inicialmente foram interligados 03 (três) pontos no território americano: Universidade da Califórnia (UCLA), o Instituto de Pesquisas de Stanford, e a Universidade de Utah.

O fim da Guerra Fria, entretanto, fez com que os militares já não considerassem importante a manutenção da *ARPANET*, visto que a mesma se mostrava completamente inútil para seus fins.

Destarte, a inexistência da ameaça da Guerra Fria também representou um importante marco para o avanço da *internet*, visto que com a não manutenção da *ARPANET* por parte dos militares americanos, esta passou às mãos dos cientistas em geral, que cederam as redes para as universidades, que, sucessivamente, passaram os estudos para universidades de outros países, facilitando o desenvolvimento e a expansão da rede.

O sucesso das primeiras experiências foi responsável pelo rápido avanço das junções e interconexões entre diversos pontos de localização ao redor de todo o país. Em 1981, quando ocorreu o batismo oficial da *internet*, os EUA contavam com 200 pontos interconectados através de uma mesma rede.

A partir da década de 80, os microcomputadores passaram a custar bem menos do que normalmente custavam, havendo maior difusão das aplicações de informática, embora a utilização tenha se mantido muito mais voltada a ambientes de corporações do que aplicações domésticas ou pessoais.

A década de 90 representou uma verdadeira explosão de difusão da rede, que ultrapassou a marca de mais de 01 (um) milhão de usuários e tendo início a utilização comercial da rede.

A invenção propiciada por Tim Berners-Lee, um físico do Centro de Estudos de Energia Nuclear (CERN), em Genebra, na Suíça, quando o mesmo propôs uma extensão *Gopher*, utilizando o conceito de hipertexto, onde as partes do texto "marcadas", ao serem selecionadas através de um clique, levam a maiores informações sobre o assunto em destaque, criando um conceito que hoje ficou conhecido como "navegar".

A essência da invenção de Tim Berners-Lee foi o desenvolvimento de um programa conhecido como *browser*, que fazia a leitura das informações codificadas em linhas de programação e as exibia em interface gráfica, como em um computador pessoal, e essa inovação ficou conhecido como *World Wide Web (WWW)*.

2.2 Aspectos históricos no cenário brasileiro

No Brasil, as primeiras conexões referentes ao uso da *Internet* foram estabelecidas no ano de 1988, e ocorreram entre o Laboratório Nacional de Cooperação Científica – LNCC, localizado no Rio de Janeiro, e a BITNET, que era a rede mantida pela Universidade de Maryland, localizada nos Estados Unidos.

Naquele mesmo ano, a Fundação de Amparo à Pesquisa do Estado de São Paulo estabeleceu conexão com o Laboratório de Física de Altas Energias, que estava em Chivado, também nos Estados Unidos. Em 1989, o Ministério de Ciência e Tecnologia (MCT) criou a Rede Nacional de Pesquisa (RNP), responsável pela elaboração do primeiro *"backbone"* nacional.

Contudo, naquela época o Brasil dispunha de uma política protecionista em relação aos produtos informáticos, que foi responsável por um grande atraso nos avanços do país dentro desse campo. Visava-se a proteção de empresas nacionais que eram voltadas ao desenvolvimento de produtos de informática, dificultando o acesso aos produtos de tecnologia provenientes de outros países, o que representou uma enorme demora no que se refere à conjugação de conhecimentos que pudessem viabilizar o avanço nos setores tecnológicos.

De mais a mais, insta ressaltar que, neste momento inicial, a finalidade da utilização da *Internet* no Brasil era exclusivamente acadêmico-científica, conforme destaca Takahashi:

> Uma primeira versão de serviços Internet com pontos em 21 estados no País foi implantada pela Rede Nacional de Pesquisa (RNP) de 1991 a 1993, a velocidades baixas. Entre 1995 e 1996, esses serviços foram atualizados para velocidades mais

> altas. Paralelamente, a partir de junho de 1995, uma decisão do Governo Federal definiu as regras gerais para a disponibilização de serviços Internet para quaisquer interessados no Brasil.

Entre os estados nos quais foram implantados o serviço de *Internet*, destaca-se o Estado da Paraíba, cujo ponto de principal fora estabelecido na cidade de Campina Grande, dando suporte à instalação da Rede Paraibana de Pesquisa – RPP, que reuniu várias instituições do meio acadêmico paraibano.

Em dezembro de 1994, a EMBRATEL, ainda como empresa pública, deu início aos primeiros testes realizados com linhas discadas, elegendo um montante de 5 (cinco) mil usuários para a efetuação de testes naquele ano.

Em junho de 1995, através de uma Portaria do Ministro da Ciência e Tecnologia, fora criado o Comitê Gestor da *Internet*, composto por membros do Ministério das Comunicações, Sistema Telebrás e Conselho Nacional de Pesquisa e Desenvolvimento Tecnológico, e que tinha como atribuições principais a fomentação ao desenvolvimento dos serviços de *Internet*, recomendação de padrões e procedimentos técnicos para o uso da *Internet*, a coordenação e atribuição de endereços, registro de nomes de domínios e a interconexão de espinhais dorsais para o funcionamento da *Internet*.

Neste momento, a relevância da *Internet* já era perceptível, destacando-se como um meio revolucionário de comunicação e acesso a uma diversidade de informações, havendo, inclusive, grande demanda nos meios comerciais, que eram dificultadas pela EMBRATEL e pelo Ministério de Comunicações, em função das dúvidas acerca de como tarifar o produto, e da falta de infraestrutura para suprir essa nova demanda.

Entretanto, a partir de 1996, quando grandes grupos comerciais, como o Grupo Abril e o RBS (do Rio Grande do Sul) passaram a vender serviços de assinatura e acesso de conteúdo, e, consequentemente, as demandas comerciais começaram a serem atendidas, havendo notável melhora na infraestrutura e velocidade dos serviços.

Em 1997, a *Internet* foi consolidada no cenário brasileiro. Bancos, empresas e universidades passaram a manter pontos constantes de presença na rede, bem como o alcance do conteúdo que atingiu centenas de pessoas. Novas revistas foram lançadas sobre o tema, o conteúdo em língua portuguesa tornou-se bastante significativo na rede, e o enorme crescimento de usuários dentro da população brasileira, todos estes foram fatores responsáveis para o estabelecimento definitivo da *Internet* no país.

Em 1998 havia uma estimativa que de o número de usuários havia crescido em torno de 130% (cento e trinta por cento) em relação ao ano anterior. Aliás, importa ressaltar

que desde o ano de 1995 a estimativa de crescimento de usuários da *Internet* em relação ao ano anterior sempre ultrapassou o percentual de 100% (cem por cento), ou seja, sempre dobrou.

O final do século passado foi marcado pelo crescimento e consolidação da *Internet* ao redor do globo, sobretudo pelo crescimento exponencial e penetração em diversos meios como entretenimento, educação, comercial e governamental.

Inicialmente, não é difícil perceber que a *Internet* era restringida a poucas pessoas, consequentemente aquelas representantes das classes média e alta, principalmente em função de fatores como o alto custo dos microcomputadores, restrições ao uso da rede devido a problemas no setor de telecomunicações e de provedores de serviços em locais distantes dos grandes centros urbanos. Todos estes fatores, aliados ao cenário de crise econômica mundial, que possuía seus desdobramentos no Brasil, representavam obstáculos à popularização da *Internet*.

As dificuldades iniciais da rede também afetaram o setor do *e-commerce*, visto que havia grande desconfiança por parte dos usuários em relação às compras virtuais, e também em função da crise econômica e do *crash* das empresas ponto com, que ficou conhecido como "o estouro da bolha".

Neste momento, o número estimado de usuários da rede era de 5 (cinco) milhões e, neste ponto, já eram perceptíveis as primeiras atuações de criminosos na *Internet*. Apesar de muito restrita e com atuações pontuais, a incidência de cibercrimes começou a ocorrer, limitando-se a atuações de certos tipos de criminosos conhecidos como "*defacers*", ou seja, eram espécies de *hackers* do mal que desfiguravam páginas da internet deixando mensagens ou até mesmo subtraindo informações de sistema de banco de dados.

A partir de 2002, a estabilidade econômica proporcionou oportunidade de acesso à rede pelas classes menos favorecidas. As medidas de incentivo fiscal concedidas pelo governo à indústria de computadores e a estabilidade econômica, que gerou crescimento na renda das classes mais baixas da sociedade, tornaram os computadores (PCs) um objeto de uso comum.

Importa destacar também a grande evolução na infraestrutura das telecomunicações, grande parte em função das privatizações ocorridas no Brasil durante o governo Fernando Henrique Cardoso.

Atualmente, experimenta-se no Brasil um momento de inclusão digital sem precedentes, com o constante crescimento do número de usuários e possibilidade de acesso à rede por uma grande escala de pessoas. Hoje, de acordo com a ANATEL, são registrados no Brasil 26,6 milhões de acessos à banda larga fixa, sendo que deste número, cerca de 50%

(cinquenta por cento) estão concentrados em 37 cidades brasileiras. Ademais, com o surgimento das mídias sociais, o acesso à rede e a difusão de informações se ampliou cada vez mais, não sendo mais necessárias a presença obrigatória de um computador como requisito para conexão à rede.

Ainda de acordo com a ANATEL, pela primeira vez, houve redução na proporção dos usuários de internet via computador, embora tenha aumentado o acesso. Foram 31,4 milhões de lares com computador em 2015 (46,2% do total), menos que os 48,5% medidos em 2014. O acesso a internet subiu de 54,4% para 57,5%, com cerca de 102,1 milhões de pessoas de 10 anos ou mais de idade – crescimento de 7,1% (ou 6,7 milhões de usuários), tendo crescido também o número de usuários que preferem utilizar o telefone móvel para acesso à *Internet*, do que o computador. (ANATEL, 2015).

Destarte, em meio a todo esse universo de usuários, rede de dados, telecomunicações, difusão de informações e serviços, não seria surpreendente imaginar a existência de uma parcela significativa de pessoas e organizações criminosas dispostas a desafiar as ações do Estado do ciberespaço, mediante a prática de diversos crimes (estelionato, espionagem industrial, subtração de informações, dano moral, racismo etc.).

2.3 Direito cibernético: um novo ramo do direito?

O mundo evoluiu bastante com o passar dos anos, e através da informática essa evolução tem se tornado uma marca cotidiana, visto que as pessoas estão cada vez mais *online* (conectadas à rede) e buscando resolver os problemas de suas vidas ao passo de um clique. Destarte, em função de tal processo evolutivo, se faz necessário que o Direito passe a atender às novas demandas sociais, passando a olhar cada vez mais para as tecnologias informáticas, de modo a regular o uso do ciberespaço e prestar atenção na sua utilização para o cometimento de crimes e atividades ilícitas.

O Direito é um fenômeno cultural universal e, por isso, deve seguir a realidade temporal e geográfica em que se desenvolve, tendo em vista que as evoluções do mundo social, político e econômico são refletidas diretamente nos aspectos jurídicos.

O avanço da tecnologia na área da informática causa imensa transformação e impacto nas relações sociais, em função das facilidades conquistadas por meio do uso do computador e da *Internet*, modificando a vida moderna, no que se pode denominar "era da Informática".

Importante também ressaltar que com o advento da "era da Informática" passam a surgir questionamentos acerca de um novo ramo do Direito, por onde são processadas as

informações jurídicas complementares ao trabalho dos juristas. Este ramo é denominado Informática Jurídica e, de acordo com Kaminski (2002), é quase unânime o uso desta nomenclatura pelos juristas desta área, definindo-a da seguinte forma:

> A Informática Jurídica é o processamento e armazenamento eletrônico das informações jurídicas, com caráter complementar ao trabalho do operador do Direito; é o estudo da aplicação da informática como instrumento, e o consequente impacto na produtividade dos profissionais da área. E também a utilização do computador como ferramenta na Internet.

Some-se também a existência do Direito Cibernético, que também pode ser chamado de Direito Digital, Ciberdireito, Direito Eletrônico, Direito de Informática etc., e que cuida de valores éticos e das relações que surgem através da informática em sentido amplo, e que ainda estuda os efeitos jurídicos que surgem com a tecnologia, principalmente seus reflexos dentro do ciberespaço.

Cientificamente, a palavra cibernética tem surgimento no ano de 1948, momento no qual Norbert Wiener (matemático), escreveu a obra: "Cibernética: controle e comunicação no animal e na máquina", embora a primeira utilização do termo não tenha sido feita pelo matemático.

Segundo Roque Antônio Carrazza, a definição de cibernética é:

> Cibernética é definida como sendo a ciência que trata das matérias, do cérebro, do sistema nervoso do homem, buscando descobrir seu funcionamento, analisando, de forma crítica e profunda, o modo de realização das coisas (CARRAZZA apud CRESPO, 2011, p. 45).

Segundo Colli (2010, p. 21), "a cibernética possui como um de seus fundamentos a interatividade entre sistemas de controle e processamento de informações, máquinas, seres vivos e sociedade".

Fernando Jose da Costa defende que:

> "[...] enquanto o computador é um processador de dados, a cibernética é a ciência dos sistemas de informática. Não se pode com precisão definir seu campo de estudo, já que se encontra em constante transformação". (2011, p.17)

Desta forma, percebe-se que a cibernética é o ramo que estuda as relações informáticas e seus sistemas, que estão em constante inovação e atualização, sendo um objeto de estudo mutante e evolutivo ao decorrer do tempo.

Dentro desse panorama, surge o conceito de Direito Cibernético ou Direito Digital, que, segundo Patrícia Peck, uma das especialistas nesse ramo, se traduz como:

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal e Direito Internacional etc). (PECK, 2002, p. 25).

Destarte, conforme depreende-se dos ensinamentos da autora, não há que se falar na criação de um novo ramo do Direito, mas sim em um novo espaço de direitos cujas peculiaridades devem ser observadas por todos os ramos jurídicos.

O Direito Cibernético, embora ainda não possa ser classificado como um ramo do direito autônomo para muitos autores, seguramente introduz no ordenamento jurídico uma nova visão e forma de pensar o Direito, visto que estabelece uma quebra de paradigmas, dado que suas relações ocorrem em um espaço relativamente novo, no caso, o ciberespaço.

Na Europa, seguindo um caminho oposto ao brasileiro, o Direito Cibernético ou Direito Digital foi reconhecido oficialmente pela Comunidade Europeia em 1980 e, em 1992, recebeu expressa recomendação para que fosse ensinado como disciplina autônoma nas Faculdades de Direito.

No Brasil ainda persiste largo desconhecimento desse campo de estudo por substancial parcela da comunidade jurídica, que ignora sua existência e razão de ser, ou descarta liminarmente qualquer cogitação sobre seu lugar na taxonomia do Direito.

Contudo, mesmo que a doutrina majoritária brasileira ainda não o considere um ramo específico do Direito, é importante que sejam destacadas algumas considerações sobre o papel deste novo meio, visto que o Direito Digital apresenta peculiaridades metodológicas, acervo normativo próprio e substancial e importante função social.

A peculiaridade metodológica caracteriza-se por um método indutivo de pensamento, visto que parte-se de especificidades informáticas próprias até o enquadramento de seus aspectos no âmbito jurídico, em contraposição ao tradicional raciocínio dedutivo, que parte de abstrações jurídicas, moldadas por um momento histórico bastante diferente do atual.

O acervo normativo próprio, por sua vez, é considerável e de crescimento exponencial, na medida em que convergem para a Informática as preocupações contemporâneas com privacidade, segurança, responsabilidade civil, propriedade intelectual etc.

A função e importância social são manifestas, visto que é extremamente interessante à sociedade o estudo e o tratamento integrado das múltiplas facetas jurídicas do desenvolvimento, exploração e uso da Informática, as quais hoje alcançam a todas, seja direta ou indiretamente.

Destarte, ainda que para a doutrina majoritária no Brasil este não possa ser considerado um ramo específico do Direito, cumpre ressaltar que o mesmo possui todas as condições formais e materiais para tanto.

2.4 Cibercrimes: conceito e classificação

Os crimes cometidos dentro do ambiente virtual ou contra dados e sistemas de funcionamento de uma máquina informatizada, são consequência da evolução dos equipamentos de comunicação eletrônicos e da *Internet*.

Os crimes cometidos por meios eletrônicos surgiram na década de 1960, época em que surgiram na imprensa e na literatura os primeiros casos de crimes envolvendo o uso do computador, caracterizados principalmente por manipulações, sabotagens, espionagem e uso abusivo dos computadores e dos sistemas, sendo denunciados principalmente em matérias jornalísticas. (FERREIRA, 2001, p. 209).

Primeiramente, antes de tudo, importa destacar que a figura do crime dentro do Direito Penal possui certas particularidades, sem as quais não que se falar em conduta criminosa. Não existe crime sem lei anterior prévia que o defina, ou seja, para que uma sanção possa ser praticada a um indivíduo por uma conduta tida como ilícita, é necessário que uma lei anterior exista e defina essa conduta como criminosa.

O Código Penal não define de forma exata o que seria a conduta criminosa, conforme podemos depreender do seu art. 1º, que faz apenas uma explicação do fato considerado criminoso e sua previsão legal, afirmando que uma conduta humana só é punível aos olhos da lei se esta lesar bem jurídico importante, e restar prevista na lei penal antes do fato típico ser cometido.

É importante mencionar também que a Lei de Introdução ao Direito Penal (Decreto-Lei n. 3.914/41) também não define o conceito de crime, limitando-se apenas a diferenciar crime de contravenção penal.

O conceito de crime, hoje, emana da doutrina, não existindo um conceito definido fornecido pelo legislador, restando apenas a conceituação doutrinária. Os conceitos mais difundidos são: formal, material e analítico.

Formalmente crime é aquele resultante da inclusão de uma conduta ao texto legal, ou seja, tudo que o legislador diz ser conduta criminosa, será, sem ater-se ao conteúdo ilícito. Para Capez, "considerar a existência de um crime sem levar em conta sua essência ou lesividade material afronta o princípio constitucional da dignidade da pessoa humana". (CAPEZ, 2012, p. 134).

Materialmente, o conceito de crime confunde-se com o pensamento da sociedade a respeito do que pode ou deve ser proibido, visto que quando ofende o bem jurídico protegido por alguém, essa conduta merece penalização. (NUCCI, 2012, p. 174).

Para Capez (2012, p.134), o crime sob esse aspecto (material) é aquele que busca entender a razão de determinado fato humano ser considerado criminoso ou não.

Ressalta Nucci (2012, p. 175), que o crime formal nasceu a partir do conceito material de crime, só que formalmente previsto em lei.

Para Zaffaroni, pode-se conceituar delito como:

> delito é uma conduta humana individualizada mediante um dispositivo legal (tipo) que revela sua proibição (típica), que por não estar permitida por nenhum preceito jurídico (causa de justificação) é contrária ao ordenamento jurídico (antijurídica) e que, por ser exigível do autor que atuasse de outra maneira nessa circunstância, lhe é reprovável (culpável). (ZAFFARONI, 1996).

Francisco de Assis Toledo, adepto do conceito tripartido de crime, assim escreve:

> Substancialmente, o crime é um fato humano que lesa ou expõe a perigo bens jurídicos (jurídico-penais) protegidos. Essa definição é, porém, insuficiente para a dogmática penal, que necessita de outra mais analítica, apta a pôr à mostra os aspectos essenciais ou os elementos estruturais do conceito de crime. E dentre as várias definições analíticas que têm sido propostas por importantes penalistas, parece-nos mais aceitável a que considera as três notas fundamentais do fato-crime, a saber: ação típica (tipicidade), ilícita ou antijurídica (ilicitude) e culpável (culpabilidade). O crime, nessa concepção que adotamos, é, pois, ação típica, ilícita e culpável. (TOLEDO apud GRECO, 2013, p. 143).

Desta maneira, conclui-se que a maioria doutrinária segue o conceito analítico na forma tripartida de crime, visto que nele são verificados com clareza os três elementos que o crime deve possuir de forma particular, sendo estes inseparáveis, quais seja, fato típico, ilícito e culpável, sem os quais não pode haver conduta criminosa ou delito.

2.4.1 Crime cibernético ou cibercrime

O conceito atribuído aos crimes que se utilizam dos dispositivos informáticos para cometer ilícitos penais, com ou sem o auxílio da rede de transmissão de dados, varia de acordo com o entendimento de cada doutrinador acerca desses ilícitos e do seu meio de execução, tendo por isso várias nomenclaturas esparsas na doutrina.

A fenomenologia criminal no que concerne às TIC (Tecnologias de Informação e Comunicação) é cada vez mais profunda e diversa, e sua presença muda sempre, adaptando-se às novas potencialidades tecnológicas e sociais. (CASABONA apud CRESPO, 2011, p. 46).

Conforme Costa (2011, p. 51), "trouxe a internet um novo mundo, denominado digital. Nele as pessoas navegam, se comunicam e de um mundo virtual praticam condutas e consequências em um mundo real." Deste modo, vê-se que com base na afirmação do autor

acima citado, a internet pode ser muito útil, mas a partir dela muitas condutas efetuadas virtualmente poderão ter efeitos exteriorizados no mundo natural.

Klaus Tiedemann denomina "criminalidade informática" todas as formas de comportamento ilegal que venham a, de qualquer forma, provocar danos sociais, por intermédio de um computador. (TIEDEMANN apud LIMA, 2011, p. 9).

"Crime de computador" é a nomenclatura utilizada por Paulo Lima, pois entende que o computador é a ferramenta básica para o cometimento desses crimes. Do mesmo modo, diz que se o computador for usado como um instrumento facilitador da prática criminosa, também há de ser considerado um crime deste tipo. (LIMA, 2011, p. 8).

Ricardo Martin entende de forma diferente sobre o conceito de crime informático, usando esta nomenclatura por acha-la simples e porque para ele é a expressão que mais equivale ao termo inglês *computer crimes*, dizendo ser este tipo de crime toda ação investida de dolo, que seja prejudicial a pessoas ou entidades, usando para essa efetivação, os dispositivos usados rotineiramente para realizar tarefas de informática. (MARTIN apud LIMA, 2011, p. 10).

Crespo (2011, p. 50-51) adota o nome de "crimes digitais", apesar de haver muitas contrariedades na doutrina, fundamentando sua nomenclatura ao fato de que ser a informática uma das coisas a serem reguladas ou ainda porque a informática é um pressuposto de outro meio onde se cometem ilícitos hodiernamente – a telemática.

Contudo, apesar de ser adepto da nomenclatura crimes digitais, Marcelo Crespo concorda com o nome delitos informáticos, dos quais são adeptos Rossini e Bonilha, dizendo que às condutas praticadas por meio da informática não se pode atribuir ligação unicamente ao computador, uma vez que se verificam delitos cometidos com o uso das telecomunicações, da telemática. Contudo, já que a telecomunicação precisa da informática, não há equivoco quanto a nomenclatura "*delitos informáticos*" em vez de dizer "*delitos telemáticos*". (CRESPO, 2011, p. 49, grifo nosso).

Ivette Senise Ferreira, usando o nome crime da informática, diz ser este "toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão." (FERREIRA apud COSTA, 2011, p. 51).

Segundo Peritos convidados pela OCED (Organização para a Cooperação Econômica e Desenvolvimento da Organização das Nações Unidas – ONU) para Paris, em maio de 1983, "o termo *crimes de computador* define, como qualquer comportamento antijurídico, não ético ou não autorizado, relacionado com o processamento de dados e/ou

transmissão de dados". (COMPUTER RELATED CRIMINALLITY apud LIMA, 2011, p. 12). Opera-se aqui, uma similitude com o conceito acima trazido pela doutrinadora Ivette Senise Ferreira.

Sandra Gouvêa tem preferência pelo uso da expressão "crimes por meio da informática", dando como justificativa a sua escolha a razão de que os computadores não são os únicos instrumentos capazes de serem usados nas práticas criminosas. (GOUVÊA apud CRESPO, 2011, p. 48).

Por fim, conforme muito bem explicado por Ivette Senise Ferreira, não há um consenso acerca do conceito de crime cibernético entre os estudiosos porque:

> As várias possibilidades de ação criminosa na área informática, assim entendida em seu sentido lato, abrangendo todas as tecnologias da informação, do processamento e da transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais fornecem um denominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores. (FERREIRA 2001, p. 208).

Destarte, percebe-se que não existe nomenclatura consensual entre os doutrinadores para a qualificação dos crimes cibernéticos. Contudo, a diferença é a apenas a forma de se nomearem as condutas, posto que o importante é que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda, deve a conduta ser típica, antijurídica e culpável.

2.4.1.1 Bem Jurídico

O bem jurídico protegido no âmbito cibernético geralmente confunde-se com aquelas protegidos pelo Direito penal tradicional, apesar de apresentarem peculiaridades específicas. A proteção deve ser conferida da mesma forma, entretanto, devem ser observados as características do ciberespaço e do *modus operandi* nesse meio.

Para o Direito Penal, o conceito de bem jurídico possui características mais específicas, devendo ser considerado o caráter de última *ratio* do Direito Penal, que deve ser o instrumento final de atuação e proteção dos bens mais importantes nas relações em sociedade. (LIMA, 2011, p. 2).

O Direito Penal só é legítimo para privar alguém de sua liberdade, se cumprir uma série de requisitos impostos pela legislação. Primeiramente, o limite do poder de punir do Estado se acha no princípio da legalidade, ou seja, para que haja cerceamento do direito de

liberdade de algum indivíduo, é necessário que a conduta tida como criminosa esteja prevista por lei como ilícita e esteja vigente à época da execução do crime (LIMA, 2011, p. 1).

Existem várias interpretações para o que se chama de "bem jurídico", mas a doutrina majoritariamente entende que este é uma limitação do poder de punir do Estado. (CRESPO, 2011, p. 54).

A evolução grandiosa da informática estabeleceu um importante ponto de referência na história da comunicação e das relações sociais, buscando novas ideias no que tange a bens jurídicos, até mesmo influenciando nas classificações sobre os fatos que sejam crimes digitais. (CRESPO, 2011, p. 56).

Os crimes realizados por meio de dispositivos informáticos afetam não só os bens que já eram juridicamente amparados pelo Direito Penal, como alcança uma enormidade de bens jurídicos novos. Nesse sentido, são as palavras de Crespo (2011, p. 56), que diz:

> Ao considerarmos as condutas ilícitas por meio da informática, verificamos a possibilidade de lesão a outros bens jurídicos. Assim, pode-se falar em condutas dirigidas a atingir não só aqueles valores que já gozam de proteção jurídica, como a vida, a integridade física, o patrimônio, a fé pública, mas, também as informações armazenadas (dados), a segurança dos sistemas de redes informáticas ou de telecomunicações.

No entendimento de Lima (2011, p. 3) "há de ser considerado, de um lado, que parte da nova criminalidade informática somente tem utilizado meios computadorizados para a prática de infrações penais comuns, com ataques a bens jurídicos já tradicionalmente protegidos pelo ordenamento penal (...)".

Por outro lado, ainda segundo Lima (2011, p. 4) nem todas as ações ou práticas ilícitas realizadas por meios de computadores recaem sobre bens jurídicos tradicionalmente conhecidos, visto que a nova delinquência, esta referente aos crimes informáticos, recai também sobre elementos da própria informática, como os *hardwares*, programas, dados, documentos eletrônicos, etc.

Desta forma, da acepção trazida pelo autor supracitado nos dois parágrafos anteriores, pode-se perceber que os criminosos na área informática usam deste meio para atingir tanto bens jurídicos tradicionais, quanto bens jurídicos novos, (a própria máquina e seus artefatos que fazem parte de sua composição).

Consoante Roriva Del Canto, o principal bem jurídico nos crimes digitais é a informação, e de forma suplementar os dados ou os sistemas. Essa ideia, parte do fundamento de que os dados são apenas a representação eletrônica ou digital da informação, mesmo que os valores variem, e os sistemas são os mecanismos materiais de funções automáticas de armazenamento, tratamento e transferência. (CANTO apud CRESPO, 2011, p. 57).

Desta forma, é importante observar quais os bem jurídicos lesados quando se trata de crimes cometidos por meios eletrônicos contra dados ou sistemas de meios informáticos.

2.4.2 Classificação dos cibercrimes

A classificação dos crimes cibernéticos não é uníssona em toda a doutrina, variando de acordo com cada autor ou estudioso sobre o tema. A informática é uma área que vive em constante processo de evolução, onde sempre há uma novidade tecnológica capaz de deixar os equipamentos informáticos cada vez melhores e visado pelos criminosos.

Ferreira (2001, p. 214-215) adota a classificação de crimes informáticos elaborada por Hervé Croze e Yves Bismuth, adotada por diversos doutrinadores, na qual os autores fazem uma distinção entre duas categorias de crimes informáticos, quais sejam: atos dirigidos diretamente contra sistemas informáticos, não importando a motivação; e atos que atentam contra valores sociais ou outros bens jurídicos tradicionalmente conhecidos, mas cometidos utilizando o sistema de informática como meio, e não como alvo.

Vicente Greco Filho compartilha o mesmo entendimento, tendo em vista que para ele:

> (...) focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da Internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo (...). (GRECO FILHO apud LIMA, 2011, p. 22).

Esta também é a classificação seguida por Crespo (2011, p. 63) visto que o autor entende ser a mais objetiva e sujeita de se enquadrar às condutas ilícitas mais atuais. Também é a classificação adotada por Ferreira e Greco, assim representada: a) condutas perpetradas contra um sistema informático. b) condutas perpetradas contra outros bens jurídicos.

No bojo do que a doutrina atualmente vem considerando como crimes cibernéticos, adota-se a nomenclatura de crimes próprios (aqueles contra a própria internet e dados) e crimes impróprios (cometidos por meio de computadores). No caso dos crimes próprios o presente trabalho explanará apenas sobre a conduta criminosa de invasão de dispositivo informático e as modificações ao Código Penal, trazidas pela Lei 12.737/12.

2.4.2.1 Crimes próprios

Crimes informáticos próprios são, consoante Castro (2003, p. 10), aqueles que para serem realizados necessitam da informática. Sem o meio informático é impossível a

execução e consumação da infração. Na verdade, os crimes informáticos próprios nasceram com a evolução desta ciência, são caracterizados por serem tipos novos, que afetam a informática, sendo esta última o bem juridicamente resguardado.

Existem muitas opções de ataques que podem ser realizados contra um computador. Dentre as muitas áreas vulneráveis, existem aquelas em que a ação delitiva atua na unidade por onde entram os dados, na saída dos dados eletrônicos, na unidade centralizada onde são processados os dados, num dispositivo de armazenamento ou ainda na transmissão dos dados. (LIMA, 2011, p. 32).

Segundo entendimento de Crespo (2011, p. 57), "não há como negar que, além da informação, os dados, a confiabilidade e segurança dos sistemas e redes informáticas e de comunicação sejam novos paradigmas de bem jurídicos a serem tutelados pelo Direito Penal".

2.4.2.2 Crimes impróprios

Os crimes informáticos impróprios são, consoante Castro (2003, p. 10), "aqueles que podem ser praticados de qualquer forma, inclusive através da informática".

O uso da internet não é por si só um meio novo de que se valem os criminosos para delinquir, mas é uma ferramenta que associada aos dispositivos informáticos pode ser usada por qualquer pessoa sem habilidades especializadas, que usam esses dispositivos cometendo ilícitos no meio virtual, afetando bens jurídicos comuns, diferentes do mundo informático.

Neste sentido Crespo (2011, p. 94) escreve que há dois tipos de crimes digitais: os próprios e os impróprios. No que tange aos delitos classificados como impróprios, não há grandes diferenças quanto ao *modus operandi*. Em outras palavras, embora o modo pelo qual se realiza a ação criminosa seja outro, a saber, o meio informático, não são exigidos conhecimentos e técnicas específicas para tanto.

Ressalta Peck (2002, p. 125) que a maioria dos crimes realizados na rede também acontecem fora do universo virtual. A internet surge apenas como um facilitador, especificamente por proporcionar que a pessoa não seja identificada.

Merecem destaque os crimes contra a honra, que encontram-se previstos nos artigos 138 a 140 do Código Penal, e versam sobre a conduta de caluniar, difamar e injuriar uma pessoa. Atualmente, com o surgimento das redes sociais, estas condutas tornaram-se cada vez mais típicas e, embora não sejam crimes próprios do meio informático, a utilização da *Internet* para o cometimento de tais delitos é cada vez mais constante.

Outra espécie de crime bastante típica no meio informático é a pornografia infantil, que nada mais é que a divulgação na rede de transmissão de dados, de fotografias, imagens, figuras que exponham as crianças e menores de idade, ligados a atos obscenos, que motivem o desejo sexual. (LIMA, 2011, p. 34).

Os principais crimes que englobam a pornografia infantil restam previstos no Estatuto da Criança e do Adolescente, nos artigos 240 e seguintes. O nosso Código Penal também pune condutas envolvendo relações sexuais com menores, como exemplo o estupro de vulnerável, constante do artigo 217-A. (CRESPO, 2011, p. 90).

Outro crime que pode ser cometido pelo meio informático é o crime de ameaça. Consoante Crespo (2011, p. 88), "é crime intimidar, amedrontar alguém mediante a promessa de causar-lhe mal injusto e grave. A lei brasileira, no art. 147 do Código Penal busca proteger a liberdade da pessoa no que toca a paz de espírito, ao sossego e ao sentimento de segurança".

No Código Penal existem diversos crimes que o indivíduo poderia também, em tese, executá-los através do meio informático, quais sejam: estelionato (art. 171), falsificação de documento público (art. 297), falsidade ideológica (artigo 299), etc. (LIMA, 2011, p. 27-28).

3. CIBERCRIMES: uma análise no plano jurídico brasileiro

O Direito Cibernético ou Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.).

Atualmente, o mundo conta com ferramentas como o *Internet Banking*, DVD, MP3, HDTV — *High Definition Television* —, TV Interativa, TV Digital, Banda Larga, WAP, VoIP. O que todas essas siglas significam para o mundo jurídico atual? Significa que os profissionais do Direito são os responsáveis por garantir o direito à privacidade, a proteção do direito autoral, do direito de imagem, da propriedade intelectual, dos *royalties*, da segurança da informação, dos acordos e parcerias estratégicas, dos processos contra *hackers* e muito mais. Para isso, o Direito Cibernético deve romper paradigmas, de modo a criar novos instrumentos capazes de atender a esses anseios.

Da criação do *chip* ao lançamento do primeiro computador com interface gráfica para utilização doméstica se passaram quase vinte anos. Desde então, os câmbios são constantes, culminando na convergência de várias tecnologias, criando uma rede única de comunicação inteligente e interativa que utiliza vários meios para transmitir uma mesma mensagem, em voz, dados ou imagem. É importante compreender que a ressaca tecnológica traz uma relação de dependência, atingindo pessoas, empresas, governos e instituições.

As relações comerciais migram cada vez mais para a Internet. Nesta esteira, surgem também os riscos inerentes à acessibilidade, tais como segurança da informação, concorrência desleal, sabotagens por *hackers*, dentre outros. Destarte, na mesma velocidade da evolução da rede, em virtude do relativo anonimato proporcionado pela Internet no Brasil, crescem os crimes, as reclamações devido a infrações ao Código de Defesa do Consumidor, as infrações à propriedade intelectual, marcas e patentes, entre outras.

Historicamente, todos os veículos de comunicação que compõem a sociedade informatizada passaram a ter relevância jurídica a partir do momento em que se tornaram instrumentos de comunicação de massa, pois a massificação do comportamento exige que a conduta passe a ser abordada pelo Direito, sob pena de criar insegurança no ordenamento jurídico e na sociedade. Foi assim com a imprensa, o telefone, o rádio, a televisão e o fax. Não poderia ser diferente com a *Internet*.

Cada um deles trouxe para o mundo jurídico particularidades e desafios: a questão dos direitos autorais, a liberdade de imprensa, as restrições à programação por ofensa a valores ou moral, as encomendas por fax, as compras por telefone, a licença do humorista para não cair na calúnia e na difamação, a proteção das fontes, os contratos dos anunciantes, os seguros de transmissão, entre outros. Com a Internet não há diferença: não existe um Direito da Internet, assim como não há um direito televisivo ou um direito radiofônico. Há peculiaridades do veículo que devem ser contempladas pelas várias áreas do Direito, mas não existe a necessidade da criação de um Direito específico.

3.1 Aspectos constitucionais relacionados ao direito cibernético e crimes virtuais

O direito cibernético surgiu a partir da facilitação no desempenho de atividades cotidianas proporcionadas pelo uso de ferramentas informatizadas. Esses mecanismos eletrônicos guarnecem inúmeros bens jurídicos de suma importância para o ser humano, a exemplo da saúde, intimidade, segurança, liberdade e outros.

Desse modo, a sociedade se vê vinculada às tecnologias da informação, tendo, a criminalidade, passado por esse mesmo processo. Aparecem os crimes virtuais e, com eles, novos bens jurídicos, devendo estes serem protegidos pela ordem constitucional. Há um impacto do direito cibernético na ordem constitucional, gerando consequências na esfera penal. (MONTEIRO NETO, 2008, p. 6; OLIVEIRA, 2013, p. 11).

No bojo deste impacto paradigmático, a Constituição, enquanto mecanismo regulador de toda a ordem política e jurídica do Estado, abarcou a responsabilidade de dar contornos jurídicos à nova realidade social, cultural e econômica que surge. Consequentemente, a Carta Magna estendeu laços protetivos aos novos bens e valores jurídicos, resultados da chamada revolução informacional. (MONTEIRO NETO, 2008, p. 9)

Esta revolução deixa evidente a importância e o papel da informação, que se torna, então, um bem jurídico importante frente à globalização operada, principalmente, pelos meios informáticos. No pensamento de Beneyto (1997, p. 15), “para considerar-se plenamente cidadão, o homem contemporâneo precisa dispor de fontes informacionais que lhe permitam conhecer o que se passa e, em seguida, formar juízos sobre os acontecimentos”.

Destarte, o direito à informação é um direito fundamental do homem, de forma que está vinculada à democracia moderna. A implantação dos demais direitos se materializa a partir da garantia constitucional da liberdade de informação. Mormente, importa salientar que a ordem jurídica constitucional brasileira reservou em seu texto pétreo um Título destinado

aos direitos e garantias fundamentais, ligados à ideia de pessoa humana e seus atributos de personalidade, como a liberdade, por exemplo, não podendo, o titular de tais direitos, dispor deles. (MONTEIRO NETO, 2008, p. 57, 60)

O direito à informação, que é um tipo de direito à liberdade, encontra-se previsto no *caput* do artigo 5º e em alguns de seus incisos, todos da Constituição Federal (Brasil, 1988), conforme se verifica abaixo:

> *"Art. 5 – Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*
> *IV – é livre a manifestação de pensamento, sendo vedado o anonimato;*
> *V – é assegurado o direito de resposta, proporcional ao agravo, além de indenização por dano material, moral ou à imagem;*
> *IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;*
> *XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício ao exercício profissional;*
> *XXXIII – 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 pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade de do Estado;*
> *LXXII – conceder-se-á habeas data:*
> *a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constante de registros ou banco de dados de entidades governamentais ou de caráter público;*
> *b) para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;"*

Todas essas garantias estão diretamente ligadas à liberdade informática, que consiste no direito que dispõe cada cidadão de utilizar-se dos instrumentos da informação para informar e informar-se. Para Paesani (2006, p. 21), tal entendimento encontra respaldo no artigo 220 da Constituição Federal (BRASIL, 1988): “A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição”.

Verdade é que o dispositivo supracitado não faz restrição aos meios de difusão de informação, sendo amplo seu alcance. (MONTEIRO NETO, 2008, p. 65-66)

Mister se faz salientar que é crescente a necessidade de intervenção do Estado na fruição dos meios tecnológicos de produção e difusão da informação, como preconizado na Constituição Federal. No entanto, tal intervenção não pode ser desordenada, sob pena de ferir o princípio da intervenção mínima. Desse modo, tal intervenção deve ser focada na fiscalização e inibição de práticas nocivas. (Ibidem, p. 68)

Por conseguinte, coube ao Direito Penal a obrigação de estruturar mecanismos que viessem a prevenir e punir de forma efetiva as condutas lesivas a esses novos bens e valores jurídicos, tudo isso com respaldo nos ditames constitucionais. Tais condutas, em sua maior parte, ainda se encontram carentes de regulamentação específica, favorecendo o entendimento de que o mundo virtual é um ambiente sem leis. (Ibidem, p. 10)

No entendimento de Bobbio (1992, p. 34), "(...) o desenvolvimento da técnica, a transformação das condições econômicas e sociais, a ampliação dos conhecimentos e a intensificação dos meios de comunicação poderiam produzir mudanças na organização da vida humana e das relações sociais, criando condições favoráveis para o nascimento de novos carecimentos".

A Carta de 1988 destaca o princípio da dignidade da pessoa humana como norteador do Estado Democrático de Direito. Nesse ínterim, partindo da premissa de que o Direito Penal amolda-se ao perfil traçado pela Constituição, destacam-se princípios constitucionais-penais, como os princípios da legalidade ou da reserva legal, da anterioridade, da taxatividade e da territorialidade. (MONTEIRO NETO, 2008, p. 85; SOUZA NETO, 2009, p. 58)

O princípio da legalidade ou da reserva legal é uma vertente penal do princípio da intervenção mínima e, segundo Bittencourt (2012, p. 14), "constitui uma efetiva limitação ao poder punitivo estatal". Destarte, o Estado deve estar alerta às novas condutas que surgem através do ciberespaço, devendo intervir somente em último caso, em caso da efetiva lesão de bens jurídicos considerados de fato relevantes

Outro princípio constitucional do Direito Penal é o princípio da anterioridade da Lei penal, enunciado no artigo 5°, XXXIX da Constituição Federal e no artigo 1° do Código Penal. Para que haja crime e a ele seja cominada uma pena, primeiro se faz necessário que o fato tenha sido praticado em momento posterior à criação da norma incriminadora. (MONTEIRO NETO, 2008, p. 87) Assim, o crime cibernético somente estará caracterizado caso a conduta praticada esteja prevista anteriormente em lei, ou seja, antes do momento de sua execução.

Já o princípio da taxatividade impõe que a norma penal incriminadora seja exata. Ou seja, deve detalhar e pormenorizar a conduta tipificada, sob pena de perder a eficácia. No caso dos crimes virtuais equivale a mesma regra, devendo todas as condutas consideradas ilícitas serem caracterizadas de forma detalhada e esclarecedora, jamais de forma abstrata.

O princípio da territorialidade versa sobre um dos maiores desafios para acabar com o crime virtual, por possuir, a internet, caráter global. Nesse sentido, o artigo 5º do Código Penal Brasileiro dispõe que aos crimes cometidos em território brasileiro aplicam-se a lei brasileira. Com relação aos crimes cometidos pela internet, aplica-se a lei brasileira quando o site utilizado for brasileiro. Contudo, uma exceção a este dispositivo é o princípio da extraterritorialidade, contido no artigo 7º do mesmo diploma legal. Assim, estando o agente localizado fora do país, aplica-se a lei brasileira nos casos do supracitado artigo ou nos casos em que houver acordo ou tratado nesse sentido. (SOUZA NETO, 2009, p. 58-60)

Por fim, vale ressaltar que o Direito Penal vem acompanhando, ainda que de forma lenta e gradual, as mudanças ditadas pela explosão tecnológica, operada desde a última metade do Século XX. Tais mudanças já estão preconizadas na Constituição da República do Brasil, de forma que se buscou proteger os interesses envolvidos contra os avanços da utilização dos meios informáticos em práticas que ferem a dignidade da pessoa humana, assimilando os nuances da nova realidade social. Assim, a tutela penal de tais interesses faz-se extremamente necessária, vez que a falta de regulamentação que reprima atos que vão de encontro à nova ordem social torna instável a sustentação desse novo modelo.

3.2 Legislação nacional e projetos de lei referentes aos cibercrimes

Hoje, no Brasil, existem algumas leis e projetos de lei que visam regulamentar certos tipos de condutas ou atividades dentro do meio virtual ou informático, visando proteger direitos fundamentais dos cidadãos, principalmente a honra e a privacidade, mas não exclusivamente.

Quanto à privacidade e os crimes a ela relacionados, veremos que nossa legislação elaborou a Lei 12.737/2012. Esta lei foi elaborado após o ocorrência de um vazamento de fotos pessoas de uma famosa atriz nacional, chamada de Carolina Dieckmann (nome também utilizado para se referir à lei).

No ano de 2013 ouve outra invasão de servidor, este chamado de NUVEM, no qual várias celebridades dos Estados Unidos e de ouros países guardavam suas fotos pessoais, as quais foram expostas após a invasão.

Enfatizando o caso da atriz brasileira Carolina Dieckmann, àquele que deu causa à Lei 12.737/2012, cumpre destacar que esta última dispõe sobre a tipificação criminal de delitos informáticos, tipificando condutas que não eram previstas, de forma específica, como infração penal.

A Lei alterou alguns artigos do Código Penal, o 154-A e 154-B no CP, bem como acresceu os artigos 266 e 298 a este mesmo Código - Decreto N° 2.848/1940.

O antigo artigo 154-A do Código Penal dispõe que:

> 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: Vigência 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: Vigência Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (VADE MECUM. 14ª Ed. São Paulo. Saraiva, 2012.p.526).

O novo artigo 154-B dispõe:

> Art. 154-B - Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionarias de serviços públicos. (VADE MECUM. 14ª Ed. São Paulo. Saraiva, 2012.p.527).

O artigo 226 diz:

> 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. Parágrafo único - Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública. § 1° Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. § 2° Aplicam-se as penas em dobro se o crime e cometido por ocasiao de calamidade pública. (VADE MECUM. 14ª Ed. São Paulo. Saraiva, 2012.p.539).

Por sua vez, o artigo 298 estabelece que:

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa. Falsificação de cartão. Parágrafo único**.** Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (VADE MECUM. 14ª Ed. São Paulo. Saraiva, 2012.p.542).

Destarte, legislar sobre a matéria de crime cibernético em plena era digital é extremamente difícil e delicado. Isso porque sem a devida redação do novo tipo penal corre-se o risco de se acabar punindo um inocente. Também importa frisar desde logo que em computação forense, as testemunhas automatizadas (máquinas), não possuem a capacidade de diferenciar "culpa" de "dolo", ou seja, são incapazes de captarem a existência ou não de intenção em certos tipos de ações.

Desta maneira, um computador não traz informações de contexto a respeito de uma situação, tampouco consegue dizer se houve ou não vontade de se realizar aquele ato.

O crime eletrônico pode ser, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual. Em outros casos, pode ser um crime-fim, ou seja, ataca-se o próprio ambiente virtual ou sistema de dados informáticos. Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual; contudo, em certos casos, não é.

Para elucidar esta corrente de pensamento, deve-se trazer à baila o julgado do STF, de relatoria do Ministro Sepúlveda Pertence, *Habeas Corpus* (76689/PB 22-9-1998), sobre crime de computador:

> EMENTA: "Crime de Computador": publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte. 1. O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" - ao contrário do que sucede, por exemplo, aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial.

Dando continuidade a essa reflexão, temos que a maioria dos crimes cometidos na rede ocorre também no mundo real, segundo Pinheiro:

> A Internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória, bem como às necessidades de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio. (PINHEIRO, 2010, p. 296-297).

Os crimes eletrônicos ou cibernéticos têm modalidades distintas, dependendo do bem jurídico tutelado. Como exemplo, podemos citar o crime de interceptação telefônica e de dados, que tem como bem jurídico tutelado os dados, ou seja, o que se quer é proteger a transmissão de dados e coibir o uso dessas informações para fins delituosos. Esse tipo penal protege também a questão da inviolabilidade das correspondências eletrônicas, como vemos na CRFB/88, em seu artigo 5º, XII, bem como o art. 1º e o parágrafo único da Lei nº 9.296/96, o qual regula o inciso XII, parte final já citado.

> XII - 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. Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Um dos maiores problemas jurídicos dos crimes virtuais é a falta de denúncias. Ainda que seja possível realizar o registro da ocorrência pela *Internet*, são poucas as unidades e pessoas qualificadas e preparadas para proceder na investigação de um crime virtual. Se o Brasil fosse membro da Convenção sobre o Cibercrime, as cooperações entre autoridades com mais conhecimento e preparo poderiam acelerar as formas de localização e repressão aos criminosos cibernéticos.

Portanto, é importante ressaltar que os criminosos da *Internet* já não são criminosos incomuns, ou seja, aquela imagem de um sujeito extremamente inteligente e com vasto conhecimento técnico já não corresponde à realidade, pois atualmente é muito fácil encontrar na própria Internet o código fonte aberto de um vírus ou trojan, ou mesmo páginas que ensinem ou expliquem detalhadamente como se proceder para práticas delituosas.

Dessa forma, segundo Pinheiro:

> O combate a esses crimes torna-se extremamente difícil por dois motivos: a) a falta de conhecimento do usuário, que, dessa forma, não passa às autoridades informações relevantes e precisas; e b) a falta de recursos em geral das autoridades policiais. (PINHEIRO, 2010, p. 300).

O maior estímulo aos infratores é a percepção de que, na maioria das vezes, a *Internet* resulta como um meio marginal, alheio à fiscalização, devido à inexistência de preparo adequado e recursos por parte das autoridades que possibilitem a rápida identificação e localização dos criminosos.

Tal sensação é fruto da certeza por parte da sociedade de que o meio virtual não é devidamente vigiado, além de muitas vezes a falta de informação ser fundamental nessa caracterização, visto que grande parte das vítimas em crimes virtuais sequer conseguem detectar que foram alvos de um crime.

Desta forma, o conjunto norma-sanção se mostra imprescindível também no universo digital ou informático. Caso contrário, enquanto houver essa falta de crédito na capacidade punitiva da sociedade digital, os crimes tenderão a aumentar e os negócios virtuais a serem desestimulados.

Ademais, no Brasil, a quase inexistência de legislação a respeito dos cibercrimes, a falta de conhecimento ou informações de grande parte da população brasileira continuam sendo os principais aspectos a motivarem os criminosos No Brasil, as principais punições realizam-se por meio do Direito Penal tradicional, ou seja, quando um indivíduo utiliza-se de um sistema de dados para furtar certa quantia monetária de outrem, ele geralmente é punido pelo furto, mas não penalizado pela invasão ou quebra de sistema.

3.3 O Projeto de lei nº 84 /99

Atualmente, tramita no Legislativo, entre outros da mesma índole, o Projeto de Lei nº 84/99, que tem como objetivo principal o combate aos crimes virtuais ou cibercrimes.

Contudo, desde o momento de sua apresentação o projeto apresentava falhas enormes, que deixam o Brasil anos-luz atrás dos ditames da Convenção de Budapeste ou Convenção sobre o Cibercrime. E mais, o referido projeto pretende implantar um Estado permanente de vigilantismo, pondo fim à navegação anônima na *Internet*, fato que deixa dúvidas a respeito dos reais interesses desta proposta.

Dessa forma, o Senador Eduardo Azeredo, defendendo o projeto de sua autoria, relatara que em algum momento os criminosos seriam prejudicados pela ausência de anonimato e cadastramentos irrastreáveis na rede, e que os únicos prejudicados seriam os internautas.

O projeto conta com muitas falhas e é importante que se ressaltem os vários pontos de incongruência e obscuridade presentes na proposta. E mais, a manutenção do Marco

Civil da Internet (Lei 12.965/2014) são fundamentais na busca por segurança na rede, evitando-se assim a discriminação de dados *online* e trazendo proteção aos usuários da rede.

A Lei n. 12.965/2014 trouxe proteção à privacidade dos usuários, obrigando que a atuação das empresas na web seja cada vez mais transparente e trazendo a proteção dos dados dos usuários como garantia fundamental, que só pode ser quebrada mediante ordem judicial e, com isso, as empresas não poderão mais repassar seus dados para terceiros sem a autorização de um juiz. Outra inovação é a garantia de privacidade das comunicações. Assim, percebe-se que o Marco Civil representa enorme avanço aos direitos dos usuários, tornando quase impossível a aprovação do Projeto de Lei nº 84/99.

O Projeto de Lei n° 84/99, embora seja o mais antigo, é também o mais criticado desde sua criação. Importa frisar que a proposta em discussão costumeiramente é comparada ao Ato Institucional nº 5, que remonta ao período da Ditadura Militar brasileira. Isso ocorre em função do estado de vigilância constante pretendido pelo projeto, que acabaria com uma das principais características do meio virtual, a privacidade.

Destarte, a liberdade e privacidade que levaram anos para serem conquistadas estariam totalmente ameaçadas caso o referido projeto fosse aprovado, contudo, com o advento do Marco Civil da Internet essa aprovação resta bem mais difícil e complicada, mas, devido a atual conjuntura política brasileira pós-*impeachment* da presidente Dilma Rousseff, não se pode descartar nenhuma possibilidade.

> "O Ato Institucional Nº5 ou AI-5 foi o quinto de uma série de decretos emitidos pelo regime militar brasileiro nos anos seguintes ao Golpe militar de 1964 no Brasil. O AI-5, sobrepondo-se à Constituição de 24 de janeiro de 1967, bem como às constituições estaduais, dava poderes extraordinários ao Presidente da República e suspendia várias garantias institucionais. Redigido pelo ministro da justiça Luís Antônio da Gama e Silva em 13 de dezembro de 1968, entrou em 40 vigor durante o governo do então presidente Artur da Costa e Silva, o ato veio em represália à decisão da Câmara dos Deputados, que se negara a conceder licença para que o deputado Márcio Moreira Alves fosse processado por um discurso onde questionava até quando o Exército abrigaria torturadores ("Quando não será o Exército um valhacouto de torturadores?") e pedindo ao povo brasileiro que boicotasse as festividades do dia 7 de setembro. Mas o decreto também vinha na esteira de ações e declarações pelas quais a classe política fortaleceu a chamada linha dura do regime militar. O Ato Institucional Número Cinco, ou AI-5, foi o instrumento que deu ao regime poderes absolutos e cuja primeira consequência foi o fechamento do Congresso Nacional por quase um ano".

O principal ponto de ataques e críticas da proposta em questão foi o art. 22, que trata sobre as obrigações dos provedores de acesso à Internet no Brasil:

> Art. 22. Manter em ambiente controlado e de segurança, pelo prazo de 03 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial. Estes dados, as

> condições de segurança de sua guarda e o processo de auditoria à qual serão submetidos serão definidas nos termos de regulamento. (PL 84/99 Acesso em: 10 dez. 2016).

Os provedores não poderiam negar o fornecimento de informações, sobretudo porque isso ocorreria apenas por meio de decisão judicial, contundo, o armazenamento de informações e dado dos usuários por um período de 03 (três) anos é o ponto mais surreal da proposta, visto que não existe qualquer seguro para os usuários a respeito do sigilo e da forma de manutenção dos dados. Contudo, com a sanção do Marco Civil, o prazo de armazenamento de informações fora reduzido para 01 (um) ano, praticamente pondo fim à questão, conforme o deputado Alessandro Molon:

> "Outro ponto importante é a definição de um ano para o tempo de guarda dos registros de conexão. Esse tempo permite que esses dados sejam utilizados em uma eventual investigação policial e, ao mesmo tempo, não onera demasiadamente os provedores de Internet". (POSSETI, acesso em 20 de dez. 2016).

No dia 13 de julho de 2011, aconteceu uma audiência pública na qual foi debatido o Projeto de Lei n° 84/99, oportunidade na qual foram expostas algumas alterações em relações a alguns termos, como "dispositivos de comunicação" e "redes de computadores" de diversos artigos. O deputado Azeredo, "argumentou que a proposta deve valer apenas para sistemas informatizados", que seriam todos os sistemas capazes de capturar, processar, armazenar ou transmitir dados digitalmente". (ANITA, acesso em 10 de dez. 2016).

Importa ressaltar que a referida proposta dificilmente terá aprovação após a sanção do Marco Civil da Internet, contudo, o Brasil vive um momento político caótico nos anos 2016/2017, caminhando cada vez mais para o cerceamento de liberdades, na contramão da expansão de Direitos promovida por países desenvolvidos como o Canadá e a Alemanha e, embora seja difícil a prospecção da referida proposta, atualmente, não se pode descartar nenhuma possibilidade por parte do momento político vivido, razão pela qual se faz imprescindível os relatos e críticas acerca do supracitado projeto.

Desta forma, se existe algum ponto realmente positivo de proposições como essa, esse ponto reside na iniciativa, visto que se faz mister que o Brasil comece cada vez mais a caminhar na busca por uma regulamentação do ciberespaço e combate aos cibercrimes, não podendo olvidar que esses avanços jamais podem ocorrer à custa dos direitos dos usuários e de suas garantias.

3.4 Direito processual penal e a jurisdição dos cibercrimes

O Direito Processual Penal ocupa-se da prestação jurisdicional relativa ao combate dos crimes, entre eles os crimes cibernéticos ou cibercrimes, de forma que alguns requisitos são essenciais na definição de tais questões. Entre eles, o primeiro requisito a ser observado é o local onde ocorreu a ação, ou seja, o território em que a conduta criminosa fora cometida, conforme dispõe Patrícia Peck, uma das especialistas na área:

> "O problema é que na internet fica muito difícil estabelecer uma demarcação de território, as relações jurídicas que existem podem ser entre pessoas de um país e outro, e entre diferentes culturas, as quais se comunicam o tempo todo, e o direito deve intervir para proteger os litígios que eventualmente vierem a acontecer". (PINHEIRO, Patrícia Peck. Direito Digital. 4°. Ed. São Paulo: Saraiva, 2010.p.80).

Na *Internet* é comum que os usuários se registrem em domínios diversos de países diversos, não é a toa que se costuma afirmar que "a *Internet* não têm barreiras", assim como pessoas de outros países podem acessar livremente um site registrado no Brasil ou em qualquer outra parte do globo, restando difícil se fazer um controle preciso dos locais nos quais os delitos são efetivamente cometidos.

> "Na atualidade existem diversos princípios para se determinar qual será a lei aplicável a cada caso, há o principio do endereço eletrônico, o do local em que a conduta se realizou ou exerceu seus efeitos, o do domicílio do consumidor, da localidade do réu, o da eficácia na execução judicial". (PINHEIRO, Patrícia Peck. Direito Digital. 4°. Ed. São Paulo: Saraiva, 2010.p.82).

Destarte, conforme os ensinamentos da autora acima, vários são os princípios ou regras que podem ser utilizados para definir o local de um crime e quem possui a competência para processamento e julgamento de tais delitos, sendo possível eleger tanto o local onde está registrado o endereço eletrônico, o local onde a conduta fora de fato realizada, o local onde a conduta gerou plenamente os seus efeitos, o domicílio do consumidor, nas relações de consumo etc.

No ordenamento jurídico brasileiro, aplicam-se os artigos 5° e 6° do Código Penal Brasileiro, no que tange a competência para processar e julgar os crimes praticados na internet:

> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
>
> Art. 6º - 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. (VADE MECUM, 2012, P. 509).

Como se pode verificar, o ordenamento jurídico pátrio adotou a teoria da ubiquidade, conforme versa o art. 6° do CP, sendo que aos delitos que são praticados por brasileiro, tanto no país quanto no exterior, ainda que transnacionais, será aplicada à lei brasileira, tendo em vista ainda o que dispõe o art. 7° do CP, o qual sujeita a lei brasileira a alguns crimes praticados no estrangeiro. (Crimes digitais. São Paulo: Saraiva, 2011.p.118).

4. CIBERCRIMES NO PLANO INTERNACIONAL: convenção de Budapeste

O esforço da União Europeia para constituição de um instrumento jurídico hábil a combater o cibercrime tem como precursores os trabalhos desenvolvidos pela OCDE (Organização para Cooperação Econômica e Desenvolvimento) e pelo G8, e também, de outros estudos viabilizados pelas Nações Unidaes e pelo Conselho da Europa. A Convenção de Budapeste resultou assim, como fruto destes estudos e recomendações que se fizeram prementes, principalmente a partir da construção do ideal de cooperação em matéria penal que já amadurecido neste espaço comunitário.

Estes trabalhos desenvolvidos pela OCDE foram muito significativos uma vez que contribuíram para a implementação de novas medidas, ainda nos idos de 1982 quando em Paris "[...] decidiu sobre a nomeação de uma comissão de peritos para discutir a cibercriminalidade e a necessidade de mudança nos Códigos Penais". No caso do G8 estas atividades iniciais datam de 1998 com a criação de um grupo de especialistas para atuar no combate ao crime organizado transnacional, principalmente com o objetivo de assegurar que nenhum criminoso recebesse refúgio em qualquer lugar do mundo.

Reforçando este ideal, bem antes, a Interpol se firma como primeira organização internacional a enfrentar os crimes cibernéticos e discutir os aspectos legais quando, em 1979, realizou uma conferência em Paris, firmando a preocupação de que "A natureza da criminalidade informática é internacional, devido ao constante aumento das comunicações por telefone, satélites, etc. entre os diferentes países. As organizações internacionais, como a Interpol, deveriam dar mais atenção a este aspecto".

Entretanto a primeira iniciativa internacional para debater o cibercrime na Europa foi do Conselho da Europa, em uma conferência especial sobre aspectos criminológicos da criminalidade econômica em Estrasburgo, em 1976, quando vários cibercrimes foram descritos. Soma-se a esta, outras iniciativas abordadas em 1985 e em 1989 com a definição de uma lista que incluía uma série de cibercrimes como falsificação de computador, danos aos dados em computadores ou programas de computador, sabotagem, acesso não autorizados, a intercepção não autorizada e a reprodução não autorizada de programas de computador (pirataria de softwares).

A emergente preocupação levou os líderes europeus a reunirem-se em um evento especial, a Cimeira de Tampere, em 1999, com o objetivo de estabelecer definições, incriminações e sanções comuns relacionadas aos "crimes de alta tecnologia", como relata Chawki.

Fixaram-se nessa linha uma série de recomendações no âmbito do Conselho da União Europeia. Desta forma temos as Recomendações do Comitê de Ministros Nº R (85), que relacionavam tanto à aplicação prática da Convenção Europeia sobre Auxílio Judiciário Mútuo em Matéria Penal, quanto às cartas rogatórias para a intercepção de telecomunicações. Do mesmo modo as Recomendações de Nº R (88) sobre as medidas destinadas a combater a pirataria no domínio do direito de autor e dos direitos conexos; N.º R (87) que disciplina a utilização de dados de caráter pessoal na área policial; N.º R (95) relativa à proteção de dados de carácter pessoal no setor das telecomunicações e a Recomendação N.º R (89) sobre a criminalidade informática que estabelece diretrizes para os legisladores nacionais referente à definição de certos cibercrimes.

No vácuo destes acontecimentos seguiram-se ainda: a Recomendação Nº R (95) relativa a problemas processuais penais relacionados com as tecnologias da informação; Resolução n.º 1 adotada pelos Ministros Europeus da Justiça na sua 21ª Conferência (Praga, 10 e 11 de Junho de 1997), que estabelecia ao Comitê de Ministros apoio para o trabalho desenvolvido pelo Comitê Europeu para os Problemas Criminais (CDPC) em face da criminalidade, objetivando aproximar as legislações penais nacionais, permitindo a utilização de meios de investigação eficazes.

Merece destaque a Resolução n.º 3, adotada na 23ª Conferência dos Ministros Europeus da Justiça (Londres, 8 e 9 de Junho de 2000), que incentivava as partes intervenientes nas negociações a seguir esforços para viabilizar soluções coerentes. Permitia cooperação para que o maior número possível de Estados participasse do encontro que viria a culminar com a Convenção de Budapeste. Houve também o reforço no sentido de efetivar um mecanismo ágil e eficaz para a cooperação penal internacional, com enfoque para os cibercrimes.

Tendo igualmente em conta um plano de ação adotado pelos Chefes de Estado e de Governo do Conselho da Europa, por ocasião da sua Segunda Cimeira (Estrasburgo, 10 e 11 de Outubro de 1997), para procurar respostas comuns face ao desenvolvimento das novas tecnologias da informação, com base nas normas e princípios do Comitê de Ministros do Conselho da Europa que estabeleceu neste mesmo ano um comitê de peritos intitulado "Comité de Peritos sobre a criminalidade no ciberespaço (PC-CY)", assumindo as negociações sobre um projeto de convenção internacional sobre a cibercriminalidade. Estes trabalhos perduraram por aproximadamente quatro anos, merecendo destacar que entre abril de 1997 e dezembro de 2000, o PC-CY realizou 10 reuniões plenárias e 15 reuniões do seu grupo aberto de redação. Tendo os trabalhos sido finalizados em abril de 2001.

De acordo com Delgado:

> Além dos Estados-membros do Conselho da Europa, também os Estados Unidos, Canadá, Japão e África do Sul contribuíram com o referido Comitê para a elaboração da Convenção sobre o Cibercrime, tendo sido convidados a participar do processo de sua elaboração na qualidade de "observadores externos". O seu texto final, juntamente com o respectivo "Relatório Explicativo", foram submetidos à aprovação e adoção pelo Comitê de Ministros do Conselho da Europa, em sua 109ª Sessão, em 8 de novembro de 2001, e a Convenção foi aberta à assinatura pelos Estados-membros do Conselho da Europa e os não-membros, mas que também participaram do seu processo de elaboração, na cidade de Budapeste, em 23 de novembro de 2001.

Desde sua adoção em 23 de novembro de 2001, em Budapeste, Hungria, um total de 54 Estados já assinaram a Convenção sobre Cibercrime (Convenção de Budapeste), sendo que deste total, atualmente, 28 nações já a ratificaram, incluindo países que não integram a União Europeia: Canadá, Costa Rica, República Dominicana, Japão, México, Filipinas África do Sul e com destaque os Estados Unidos, berço da internet (a Convenção foi ratificada em 2006 e entrou em vigor em 1 de janeiro de 2007). Quanto ao Brasil, cumpre informar que até hoje o país não assinou a Convenção de Budapeste.

Destaque-se ainda, quanto aos aspectos essenciais da Convenção, que em 01 de março de 2006, passou a vigorar o Protocolo Adicional à Convenção de Budapeste, que visa criminalizar condutas de cunho racista e xenofóbicas, através de ameaças, insultos e condutas congêneres, praticadas através da internet e redes de computadores.

Nesta dimensão a Convenção de Budapeste sobre Cibercrime é o primeiro tratado internacional que busca abordar a cibercriminalidade e harmonizar as legislações nacionais, melhorar técnicas e aumentar a cooperação entre as nações. Representa ainda uma nova era na cooperação penal entre as nações, oferecendo uma regulamentação supranacional "a fim de efetivamente combater infrações relacionadas aos cibercrimes facilitando a detecção, investigação e repressão de tais delitos, tanto a em âmbito nacional quanto internacional, e fornecendo mecanismos de rápida e confiável cooperação internacional".

4.1 Tratamento legal do cibercrime na convenção de Budapeste

Como se depreende de todo contexto formado, isto é, ainda que os principais fundamentos tecnológicos que embasam o funcionamento das novas tecnologias encontrem raízes num momento anterior à década de 90, foi apenas com a popularização da internet que os conceitos tradicionais entraram num processo de mutação. Um novo componente iria

possibilitar que espaço e tempo passassem a ter novos contornos, numa supressão de escalas, de forma a fazer com que sejam indiferentes os conceitos de território e lugar do crime.

Conceitos tradicionais foram revistos, da mesma forma a sociedade passou a sofrer os efeitos da prática de condutas que durante muito tempo permeavam as ideias humanas, como se ficção científica fosse.

Os novos fenômenos assim denominados de cibercrime, têm um novo território – o ciberespaço, mas seus efeitos se materializam na vida humana sob muitas formas, o que requereu, pois, a construção de novos instrumentos jurídicos que pudessem fazer frente ao fenômeno em escala global, solução apenas viabilizada mediante a cooperação penal internacional.

Não interessa desta forma, que se estabeleçam leis rígidas, mas com amplitude limitada, e, é isto que os doutrinadores tem compreendido, pois, não há possibilidade jurídica de que tais instrumentos tenham alcance além das fronteiras, já que a própria noção de soberania irá limitá-los:

> As novas tecnologias existentes irão desafiar os conceitos jurídicos. Informação e comunicação fluir mais facilmente em todo o mundo. Fronteiras não são mais limites para este fluxo. Os criminosos estão cada vez mais localizadas em locais diferentes do que os seus actos produzir os seus efeitos. No entanto, as leis são geralmente confinado a um território específico. Assim, soluções para os problemas devem ser abordados pela legislação internacional, que requeiram a adopção de adequados instrumentos jurídicos internacionais. A presente Convenção visa enfrentar este desafio, com o devido respeito aos direitos humanos na nova sociedade da informação.

Neste sentido, o tratamento legal do cibercrime na Convenção de Budapeste foi fruto de amplo debate, cuja formulação requereu anos de maturação e emprego de toda experiência proporcionada pela vivência no direito comunitário europeu.

Desta forma, o próprio preâmbulo da Convenção de Budapeste, estabelece:

> Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e confiável; [...]de modo a tornar mais eficazes as investigações e as acções penais relativas a infracções penais relacionadas com sistemas e dados informáticos, bem como permitir a recolha de provas em forma electrónica de uma infracção penal.

Destarte, a Convenção de Budapeste sobre o Cibercrime significa avanço formidável no combate à criminalidade cibernética, só possível, em escala global, mediante a cooperação dos Estados, através de suas instâncias policiais e judiciais, sem que seja preciso

esquecer que há medidas que podem ser tomadas no âmbito do direito nacional no Estados, pois nem todas as condutas delituosas são transfronteiriças.

4.2 Convenção e sua estrutura normativa

A Convenção de Budapeste sobre o Cibercrime está estruturada em quatro Capítulos, compreendidos como linhas centrais a estruturar o instrumento jurídico. Por questões de ordem metodológica e para melhor compreensão de sua estrutura, faz-se necessário a apresentação de seus elementos essenciais.

O Capítulo I, trata de terminologias, constando apenas um artigo.

O Capítulo II estabelece medidas a se tomar em nível nacional, com a fixação de aspectos referentes ao direito penal material, processual e competência, assim estabelecida:

> Secção 1 – Direito penal material
> Título 1 – Infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos
> Título 2 – Infracções relacionada com computadores
> Título 3 – Infracções relacionadas com o conteúdo
> Título 4 – Infracções relacionadas com a violação do direito de autor e direitos conexos
> Título 5 – Outras formas de Responsabilidade e Sanções
> Secção 2 – Direito Processual
> Título 1 – Disposições comuns
> Título 2 – Conservação expedita de dados informáticos armazenados
> Título 3 – Injunção
> Título 4 – Busca e Apreensão de dados informáticos armazenados
> Título 5 – Recolha em tempo real de dados informáticos Secção 3 – Competência(com destaques do autor).

O Capítulo III, da Convenção apresenta-se como o mais significativo ao presente estudo, uma vez que trata da cooperação internacional, compondo este, duas seções, com os seguintes dispositivos:

> **Secção 1 – Princípios gerais**
> Título 1 – Princípios gerais relativos à cooperação internacional
> Título 2 – Princípios relativos à extradição
> Título 3 – Princípios Gerais relativos ao auxílio mútuo
> Título 4 – Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis
> **Secção 2 – Disposições específicas**
> Título 1 – Auxílio mútuo em matéria de medidas provisórias
> Título 2 – Auxílio mútuo relativamente a poderes de investigação
> Título 3 - Rede 24/7 (grifo nosso).

No capítulo IV, são expostas as disposições finais, com destaque para os artigos que tratam da adesão à Convenção, da aplicação territorial e de seus efeitos.

A Convenção tem como escopo principal, numa visão geral: (1) harmonizar o direito penal interno (de cada país) e harmoniza-lo com as previsões relativas ao cibercrime; (2) prover o direito processual penal interno de poderes necessários para a investigação e repressão de delitos como bem como outros crimes cometidos por meio de um sistema de computador ou obtenção de provas em relação ao que está em formato eletrônico e (3) a criação de uma rápido e eficaz regime de cooperação internacional.

É preciso fazer o registro de que o texto original da Convenção, traduzido do inglês para o português, não representa com exatidão o sentido e expressão de termos utilizados nas Tecnologias da Informação e da Comunicação, ou mesmo, puramente no cotidiano da informática. Por exemplo, no artigo 1º, que trata das definições, o texto em original em inglês prevê a definição de "*computer system*", já o texto traduzido para português e disponível indica a expressão "sistema informático", que obviamente tem um sentido muito mais amplo que "*computer system*" (sistema de computador)..

4.3 Definições essenciais

O art. 1º, da Convenção de Budapeste estabelece a definição para quatro itens: sistema informático, dados informáticos, fornecedor de serviço e dados de tráfego. Sistema informático é definido como "qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de um entre eles" desenvolve ou executa o tratamento automático de dados.

No ponto seguinte, alínea "b", do artigo 1º, se esclarece o próprio instrumento jurídico, a definição para "dados informáticos", como sendo "qualquer representação de fatos, de informações ou de conceitos, incluindo um programa" que possibilite um sistema informático executar uma função. Nos termos da Convenção, alínea "c", é fixada a definição para "fornecedor de serviço" que seria a entidade de caráter público ou privado que possibilite a utilização de seus serviços de forma a viabilizar comunicação através de um sistema informático e ainda "qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores desse serviço.

De acordo com o disposto na alínea "d", tráfego de dados significa:

> [...] todos os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Desta forma, são definidos, em síntese, o sistema, ou seja, o conjunto de equipamentos empregados para atividades na área de informática, incluindo computador, impressoras e scanners.

O conjunto de equipamentos, da forma como descrita, não representa risco potencial, pois sem acesso à rede internacional de computadores seu alcance fica restrito ao lar de seu proprietário.

Outro ponto chave definido, diz respeito aos softwares utilizados, bem como o produto da utilização do sistema, que pode, por exemplo, ser um texto digitado ou até mesmo um programa de computador, ou seja, esse conjunto de informações armazenadas no "sistema informático" irão constituir os dados informáticos.

Quanto à definição das entidades públicas ou privadas que fornecem ou disponibilizam o serviço de provedor, ou seja, a pessoa que irá possibilitar a conexão do interessado à rede mundial de computadores ou ainda a pessoa que armazena tais informações – espécie de provedor de conteúdo.

Ao tratar de "dados de tráfego", a Convenção quer indicar todas as informações que transitam na rede, de forma que se possa estabelecer uma lista de parâmetros que são essenciais para identificação da origem e do destinatário, consequentemente, seus possíveis remetentes e destinatários, uma vez que se prioriza os aspectos referentes a origem, destino, trajeto, hora, data, tamanho e duração ou tipo do serviço.

As redes de computadores surgiram com a necessidade humana de compartilhar informações que, a princípio, estavam isoladas em computadores. Esse compartilhamento de informações é viabilizado quando dois computadores ou mais são conectados, fazendo com que exista uma interação entre eles.

Neste sentido, Mangueira assevera que "A interligação de computadores possibilita o compartilhamento de arquivos, periféricos (impressoras, leitoras de discos óticos, discos rígidos, *plotters*, etc.) e conexões com outras redes (é aqui que reside o perigo!), como a internet".

O grande segredo da internet é a capacidade de colocar em conexão diferentes redes de computadores, fazendo com que haja uma interação global. Essa conectividade só é possível graças à existência de um protocolo de global de informações, o que torna possível diferentes redes e sistemas se comunicarem entre si.

Essa linguagem universal é conhecida como TCP/IP (*Transmission Control Protocol/Internet Protocol*), que foi desenvolvido na década de 70. Dessa forma, conforme ensina Mangueira:

> O TCP/IP envia informações divididas em pacotes e possui camadas (níveis) com funções bem específicas, para o nível físico, para o transporte, para a rede interna (internet) e para a aplicação. Ao transferir uma mensagem de uma aplicação de uma máquina a uma outra aplicação localizada em uma outra máquina, o protocolo transmite a mensagem do nível de aplicação até o nível físico, daí a mensagem é transmitida pela rede até o outro computador, que transporta a mensagem da camada física até a aplicação.

Podemos dizer, então, que cada computador que esteja conectado à *web* possui um endereço IP (Protocolo de Internet). Protocolo IP "é o protocolo da Internet, que permite a interconexão de diferentes redes para transmissão de pacotes de dados." Cada computador que esteja conectado a uma rede com acesso à internet possui um endereço IP, e isto funciona como se fosse uma impressão digital, que torna determinada máquina única na rede, o que facilita, por conseguinte, o rastreamento e localização de computadores que foram utilizados por pessoas que estejam conectadas à rede para praticar crimes.

4.4 Previsão de delitos e medidas a serem adotadas no âmbito do direito material

A Convenção também traz recomendações para que no direito interno, dos países signatários, sejam estabelecidas condutas delituosas para os atos de acesso ilegítimo intencional (total ou parcial com violação de medidas de segurança, cujo objetivo seja a obtenção de dados informáticos ou outra intenção ilícita); interceptação ilegítima de dados informáticos; interferência em dados; interferência em sistemas e uso abusivo de dispositivos.

In casu para os atos de acesso ilegítimo, interferência de dados informáticos, interferência em sistemas e uso abusivo de dispositivos estariam compatíveis com a ideia de elaboração de novas tipificações penais, visto que a descrição das condutas presentes na Convenção não encontram tipos penais semelhantes em nosso ordenamento jurídico penal.

Por outro prisma, quanto à conduta de interceptação ilegítima de dados informáticos, há disposições presentes a partir do próprio texto constitucional que dispõe em seu art. 5º, inciso XII, sobre a inviolabilidade do "[...] sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas [...]" a própria Carta Magna excetua as hipóteses de ordem judicial, para fins de investigação criminal ou instrução processual penal.

A partir da tutela prevista na própria Constituição Federal, há previsão de punição para essa conduta presente na Lei 9.296/96, que regulamenta o art.5º, inciso XII, tratando da definição do crime de interceptação não autorizada de comunicação informática ou telemática de dados.

4.4.1 Infrações penais relacionadas com computadores

A Convenção do Conselho da Europa sobre Cibercrime dispõe em seu Título 2, das infrações relacionadas a computadores. Especificamente as condutas de falsidade e burla informática. Esta duas hipóteses previstas na Convenção já encontram regulamentação penal no ordenamento jurídico penal brasileiro, pois a Lei n º 9.983/2000, inseriu os artigos 313-A e 313-B, estabelecendo punição para as condutas de "inserção de dados falsos em sistema de informações" e "modificação ou alteração não autorizada de sistema de informações".

Há ainda disposições de ordem penal constantes no Código Eleitoral, ou seja, no art. 72 da Lei n. 9.504/97276, que cuida das infrações relacionadas com acesso indevido ao sistema de voto eletrônico ou dano aos equipamentos utilizados na votação, que em nosso caso realiza-se através de urnas eletrônicas.

4.4.2 Infrações penais relacionadas com o conteúdo

O art. 9º, da Convenção de Budapeste, trata especialmente da conduta das infrações relacionadas com a pornografia infantil na internet. Estas condutas durante os três últimos anos provocaram uma espécie de comoção social no Brasil, em face dos comportamentos mais perversos, contendo cenas de sexo explícito com crianças e adolescentes.

O alerta surgiu quando a empresa Google Inc. passou a disponibilizar no Brasil o site de relacionamentos Orkut. O que seria um espaço para estreitamento de laços sociais, rapidamente converteu-se num espaço para práticas de disseminação de cenas de sexo explícito envolvendo menores e maiores de 18 anos, o que gerou a instalação de uma Comissão Parlamentar de Inquérito (CPI) no Senado Federal.

A pressão social, bem como a grande repercussão internacional que os fatos geraram, potencializaram a tramitação de projeto legislativos, culminando com rápida aprovação no parlamento e sanção presidencial da Lei nº 11.829/2008, que alterou a Lei nº 8.069/1990 - Estatuto da Criança e do Adolescente, objetivando aprimorar "o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet".

Como se depreende das disposições acima fixadas, o Brasil estipulou em sua legislação nacional, a punição para condutas de pornografia infantil, inclusive na internet, mas ressalte-se, que a edição dessa medida legislativa não decorreu de adesão à Convenção, mas

da pressão exercida pela sociedade e pelos debates parlamentares com o advento da CPI da pedofilia.

4.4.3 Infrações penais relacionadas com o direito do autor e direitos conexos

Um dos aspectos mais significativos do impacto da internet na sociedade relaciona-se com o direito autoral. Em duas conferências que subsidiaram o presente estudo - SPCI 2008 (*1st International Conference on Security, Privacy and Confidentiality Issues in Cyberlaw*), Cairo, Capital do Egito e Cyberspace 2008 (*6th Internatinal Conference Cyberspace 2008*), na cidade de Brno, República Tcheca, a temática foi abordada com ênfase por especialistas da Índia e da União Europeia.

No direito brasileiro duas leis regulam a matéria relacionada aos direitos autorais e direitos conexos, a Lei nº 9.609/98, que dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no País e a Lei nº 10.695/2003, que alterou as disposições constantes no Código Penal Brasileiro, referente aos direitos autorais e direitos conexos. As duas legislações contemplam a previsão de providências constantes na Convenção de Budapeste e, em aderindo à Convenção, em termos de direito material, a legislação brasileira pouco careceria de ajustes.

4.4.4 Outras formas de responsabilidade criminal e sanções

No título 5, art. 11, a Convenção de Budapeste dispõe sobre as medidas necessárias para responsabilizar e punir a forma tentada dos delitos que nela estão dispostos, bem como as práticas que forem perpetradas mediante cumplicidade, cujas disposições de ordem penal, encontram-se estabelecidas no art.14 e no art. 29, do Código Penal Brasileiro e, neste caso, também não seriam necessários ajustes.

Merece observação o disposto no art. 12º, que se refere à responsabilidade penal da pessoa jurídica em face de crime praticados, ainda que individualmente (desde que a pessoa exerça poder de direção), e de forma omissiva, quando tenha negligenciado a supervisão e o controle de atividades exercidas por seus empregados.

Quanto às sanções e medidas, previstas no art.13, o instrumento jurídico internacional de combate ao cibercrime prevê que os Estados signatários tomem medidas "necessárias para assegurar que as infrações penais verificadas em aplicação dos Artigos 2º a 11º sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo penas

privativas da liberdade". Prevê, inclusive, a necessidade de imposição de sanções pecuniárias quando se tratar de pessoa jurídica.

5. CONCLUSÃO

Destarte, percebe-se que o surgimento da Informática e, consequentemente, da *Internet* representaram uma verdadeira revolução no mundo contemporâneo, com impactos em todas as esferas possíveis, sejam elas políticas, sociais ou econômicas, alterando permanentemente todas as formas de relações existentes ao redor do globo.

A *Internet* é a ferramenta hoje mais utilizada pela população mundial, sendo responsável pela absorção para si de todos os fenômenos sociais existentes fora do mundo real. Atualmente, todas os tipos de interações e contatos existentes no cotidiano podem ser substituídas ou encontradas no meio virtual. As mídias sociais foram criadas e com isso toda aquela interação social característica de ambientes como escolas, universidades, barzinhos e festas migrou para o mundo virtual. Dificilmente será possível encontrar alguém que não esteja presente em pelo menos uma rede social sequer.

A *Internet* também revolucionou o comércio mundial, pois o chamado *e-commerce* trouxe inúmeras facilidades para o universo das compras. Hoje é possível fazer tudo ao passo de um único clique, sem a necessidade de sair de casa, visto que a maioria das empresas ou lojas que se encontra nas ruas ou nos *shoppings centers* também possuem domínios *online*, nos quais os produtos ofertados muitas vezes, inclusive, possuem um preço mais acessível ao consumidor, a comodidade de entregar em domicílio e a facilidade do pagamento através do *Internet Banking*, ou seja, a *Internet* acaba por oferecer muito mais conforto, comodidade e segurança.

Contudo, aliado a toda essa interação social e ao surgimento do ciberespaço, onde todas as relações do mundo real também encontram-se devidamente representadas, às vezes até de maior mais alargada, também surgiram as condutas maliciosas ou ilícitas, também surgiu um meio mais rápido, prático e anônimo para o cometimento de delitos e, com isso, também ficou mais difícil a persecução e captura deste novo tipo de criminosos, os criminosos virtuais.

A rede *online* oferece uma variedade infinita de opções de domínios e acesso a banco de dados, de diversos países do mundo. Alguém no Brasil pode facilmente utilizar um domínio localizado na China e inclusive burlar esse sistema para o cometimento de ilícitos, tudo a depender da capacidade de cada criminoso. E com isso, surgem os problemas, visto que, neste caso, onde uma pessoa localizada no Brasil utiliza-se de um domínio chinês para uma conduta criminosa que gerará efeitos nos Estados Unidos, quem seria competente para processar e julgar o feito? Quem seria competente para a execução da sentença? A melhor

resposta, aquela que abrange de uma forma mais larga todas as possibilidades reside na cooperação internacional.

A Convenção de Budapeste, elaborada em 2001, ou seja, 15 (quinze) anos atrás, talvez seja o instrumento mais abrangente no que se refere ao mundo dos cibercrimes ou da cibercriminalidade. Oferecendo conceitos e definições básicas, bem como diretrizes para a melhoria das investigações e processamento de crimes virtuais, além das tipificações de novas condutas enquanto crimes, a Convenção de Budapeste é o principal instrumento de cooperação internacional e combate à cibercriminalidade.

No que se refere ao Brasil, o primeiro e decisivo passo para uma mudança paradigmática no combate aos cibercrimes seria a assinatura da Convenção, e sua consequente ratificação, visto que, desta maneira, seria instaurada uma nova visão e maneira de pensar a respeito da cibercriminalidade, aceitando-se a sua relevância social e fornecendo base para um novo modelo de legislação e combate aos crimes no ciberespaço.

REFERÊNCIAS BIBLIOGRÁFICAS

_____. Código Penal (1940). *Decreto-Lei nº 2.848*, de 7 de dezembro de 1940. Brasília, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decretolei/del2848compilado.htm>. Acesso em 19 nov. 2016.

_____. Lei de Introdução ao Código Penal. *Decreto-Lei nº 3.914*, de 9 de dezembro de 1941. Vade Mecum OAB e concursos. São Paulo: Saraiva, 2015.

_____. Lei nº 12.737/12, de 30 de novembro de 2012. *Dispõe so*bre 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: Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011 2014/2012/lei/l12737.htm>. Acesso em 19 nov. 2016.

_____. *Manual de Processo Penal e Execução Penal*. 10ª Ed. rev, ampl, e atual. São Paulo: Revista dos Tribunais, 2013.

ALMEIDA FILHO, José Carlos de Araújo; CASTRO, Aldemário Araújo. *Manual de Informática Jurídica e Direito da Informática*. Rio de Janeiro: Forense, 2005.

ARAS, Vladimir. **Crimes de informática: uma nova criminalidade**. Revista informática jurídica.com. Disponível em: <http://www.informaticajuridica. com/trabajos/artigo_crimesinformticos.asp> Acesso em: 18 nov. 2016.

BARBOSA, Alexandre de Freitas (Coord**). O Mundo Globalizado**: Política, Sociedade e Economia. Contexto: São Paulo, 2006.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal*: Parte Geral. 18ª Ed. rev, ampl, e atual. São Paulo: Saraiva, 2012. Vol. I.

BOBBIO, N. **A era dos direitos.** Trad. Carlos Nelson Coutinho. 10. ed. Rio de Janeiro: Campus, 1992.

BONFIM, Edilson Mougenot. *Curso de Processo Penal*. 8ª Ed. atual. São Paulo: Saraiva, 2013.

BRASIL vive o maior "boom" de acessos residenciais à Internet. São Paulo: Convergência Digital, 2010. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=13021&sid=4>. Acesso em: 20 dez. 2016.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompila o.htm>. Acesso em 11 nov. 2016.

BRASIL. **Lei 12.965 de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 dez. 2016.

BRASIL. Ministério Público Federal. **Grupo de trabalho – crime cibernético, resultados e conclusões.** Disponível em: <http://2ccr.pgr.mpf.gov.br/docs_institucional/eventos/viiiencontro/ata_grupo_sobre_crimes_ciberneticos.pdf>. Acesso em: 16 dez.2016.

BRASIL. Presidência da República, Casa Civil - Subchefia para Assuntos Jurídicos. **Lei nº 7.170, de 14 de DEZEMBRO DE 1983. Define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L7170.htm>. Acesso em: 16 dez.2016.

BRASIL. Superior Tribunal de Justiça. **Julgados especiais**. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/1454634/carta-rogatoria-cr-438-be 2005-0015196-0-stj>. Acesso em 17 dez.2016.

BRASIL. **Supremo Tribunal Federal – RHC n. 76.689-0** – Pernambuco – Primeira Turma – Relator: Ministro Sepúlveda Pertence, DJU de 6.11.1998, p.03.

BRASIL. Supremo Tribunal Federal. **Habeas Corpus** nº. 76689. Relator: Sepúlveda Pertence, julgada em 21/09/1998, Primeira Turma, Data de Publicação: DJ 06-11-1998 PP-00003 EMENT VOL-01930-01 PP-00070. Disponível em: < http://stf.jusbrasil.com.br/jurisprudencia/740355/habeas-corpus-hc-76689-pb>. Acesso em15 nov. 2016.

BRASIL. Supremo Tribunal Federal. **Julgados especiais**. Disponível em:
BUDAPESTE, CONVENÇÃO. *Convenção sobre o Cibercrime*. Budapeste, 2001. Disponível em:<http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_Portugese.Acesso em 06 jan. 2017.

CAPEZ, Fernando. *Curso de Direito Penal*: Parte Geral. 16ª Ed. 2ª tiragem. São Paulo: Saraiva, 2012. Vol. I.

CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais*. 2ª Ed. rev, ampl e atual. Rio de Janeiro, 2003.

CAVALCANTE, Andrea de Fátima Araújo. *A Atipicidade dos Crimes Cibernéticos no Brasil e a Impunidade*: uma análise crítica. Trabalho de Conclusão de Curso (Direito). Caruaru: Favip, 2011. Disponível em: <http://repositorio.favip.edu.br:8080/bitstream/123456789/866/1/Monografia+Andrea+de+Fatima+>. Acesso em 10 dez. 2016.

CHAWKI, Mohamed. ***A critical look at the regulation of cybercrime: a comparative analysis with suggestions for legal policy***. DROIT-TIC, 11 April 2005. Disponível em: <http://www.crime-research.org/articles/Critical/. Acesso em: 10 dez. 2016.

CHAWKI, Mohamed. ***Essai sur la notion de cybercriminalité***. IEHEI, juillet 2006. Disponível em <http://www.iehei.org/bibliotheque/cybercrime.pdf> Acesso em: 20 dez. 2016.

CHAWKI, Mohamed. WAHAB, Mohamed S. Abdel. ***Identity Theft in Cyberspace: Issue and Solutions.*** Lex Electronica, vol.11 n°1 (Printemps / Spring 2006). Disponível em: <hhttp://www.lex-electronica.org/docs/articles_54.pdf>. Acesso em: 11 dez. 2016.

CIBERCRIMES E ANONIMATO: PROJETO LEI N° 84/99. SERVE A QUEM? 2008. Disponível em: <http://www.leieordem.com.br/cibercrimes-e-anonimato-projeto-de-lei-8499-serve-a-quem.html> Acesso em: 13 out. 2012.

CONVENÇÃO DE BUDAPESTE SOBRE O CIBERCRIME. Disponível em:
CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** 5. Ed. São Paulo: Saraiva, 2010.
COSTA, Fernando Jose da. *Locus Delict nos Crimes Informáticos*. Tese de Doutorado da Usp. 2011. Disponível em: <http://www.teses.usp.br/teses/disponiveis/2/2136/tde24042012112445/ptbr.php.>. Acesso dia 25 nov. 2016.

CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais*. São Paulo: Saraiva, 2011.

DELGADO, Vladimir Chaves. **Cooperação internacional em matéria penal na convenção sobre o cibercrime**. 2007. 315p. Dissertação. (Mestrado em Direito das Relações Internacionais) - Centro Universitário de Brasília. Brasília, 2007.

DOMINGUES, Antonio Carlos Iranlei Toscano Moura. **O Tribunal Penal Internacional e o combate à criminalidade econômica organizada transnacional.** Dissertação apresentada ao Programa de Pós-Graduação – CCJ – UFPB: Mestrado em Direito Econômico. João Pessoa – PB, 2007.

EUROPA GLOSSÁRIO. **Cooperação policial e judiciária em matéria penal**. Disponível em: <http://europa.eu/scadplus/glossary/police_judicial_cooperation_pt.htm>. Acesso em: 19 nov.2016.

EUROPA GLOSSÁRIO. **Eurojust**. Disponível em: <http://europa.eu/scadplus/glossary/eurojust_pt.htm>. Acesso em: 19 nov.2016.

FERNANDES, David Augusto. Crimes Cibernéticos: O Descompasso do Estado e da Realidade. *Revista da Faculdade de Direito da Universidade Federal de Minas Gerais*. Belo Horizonte, n. 62, pp. 139-178, jan./jun. 2013. Disponível em: <http://www.direito.ufmg.br/revista/index.php/revista/article/view/P.03042340.2013v62p139/248>. Acesso em 18/03/2014.

FERREIRA, Ivette Senise. A Criminalidade Informática. In: LUCCA, Newton De; SIMÃO FILHO, Adalberto (Coord.). *Direito & Internet – Aspectos Jurídicos Relevantes*. São Paulo: Edipro, 2001. p. 207-237.

FURLANETO NETO, M.; GUIMARÃES, J. A. C. Crimes na Internet: Elementos para uma Reflexão Sobre a Ética Informacional. **Revista CEJ**. Brasília, n. 20, p. 69, jan./mar. 2003. Disponível em: <http://www2.cjf.jus.br/ojs2/index.php/cej/article/viewFile/523/704>. Acesso em: 10 dez. 2016.

HAJE, L. Saiba como os crimes na internet são tratados em outros países. **Agência Câmara de Notícias**, Brasília, 08 jul. 2011. Disponível em:

<http://www2.camara.leg.br/agencia/noticias/CIENCIA-E TECNOLOGIA/199806-SAIBA-COMO-OS-CRIMES-NA-INTERNET-SAO TRATADOS-EM-OUTROS-PAISES.html>. Acesso em: 11 dez. 2016.

INTERNET ***user statistics and population stats for the countries and regions that comprise Latin American internet users*****.** EUA: Internet World Stats, 2008. Disponível em: <http://www.internetworldstats.com/stats10.htm#spanish>. Acesso em: 10 dez 2016.

KAMINISKI, Omar. A Informática Jurídica, a Juscibernética e a Arte de Governar. *Revista Consultor Jurídico*. 17 de julho de 2002. Disponível em: <http://www.conjur.com.br/2002-jul-17/informatica_juridica_juscibernetica_arte_governar>. Acesso em 26 nov. 2016.

KAMINSKI. Omar**.** Internet legal: o direito na tecnologia da informação. Curitiba: Juruá, 2007.

KOBAYASHI, Bruce H.;RIBSTEIN, Larry E. ***Multijurisdictional regulation of the internet.*** In: THIERER, Adam D.; CREWS, Clyde Wayne. ***Who Rules the Net?:Internet Governance and Jurisdiction*****.** Washington: Cato Institute, 2003.

LIMA, Gisele Truzzi de. *Redes Sociais e Segurança da Informação*. Gisele Truzzi Advogada Disponível em: <http://www.truzzi.com.br/pdf/artigo-redes-sociais-eseguranca-da-informacao.pdf>. Acesso em 26 nov. 2016.

LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. 2ª Ed. São Paulo: Atlas, 2011.

LIMA, Renato Brasileiro de. *Curso de Processo Penal*. Niterói: Impetus, 2013.

LINHA DO TEMPO DA INTERNET NO BRASIL. Disponível em <http://www.internetnobrasil.net/index.php?title=1988>. Acesso em: 10 nov. 2016.
LINS, Bernardo F. E. *Privacidade e Internet*. Consultoria Legislativa da Câmara dos Deputados. Março de 2000. Disponível em: <http://www2.camara.leg.br/documentosepesquisa/publicacoes/estnottec/tema4/pdf/001854.pdf>. Acesso em 10 dez. 2016.

MANGUEIRA, Hugo Alexandre Espínola. **Criminalidade cibernética:** estudo dos *hackers* e das implicações legais de seus ataques através da Internet. João Pessoa, 2012.

MARQUES, Helvetius. **O terrorista e os direitos humanos.** Disponível em: <http://www.juridicas.unam.mx/sisjur/internac/pdf/10-478s.pdf>. Acesso em: 21 nov. 2016.

MINISTÉRIO PÚBLICO FEDERAL. Procuradoria da República no Estado de São Paulo. *Manual Prático de Investigação, Crime Cibernético*. São Paulo, 2006. Disponível em:<mpto.mp.br/athenas/.../manual-de-atuacao-em-crimes-ciberneticosmpf>.Acesso em 30 nov. 2016.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. *Manual de Direito Penal*: Parte Geral Arts. 1º a 120 do CP. 28ª Ed. rev e atual. São Paulo: Atlas, 2012. Vol. I.

NUCCI, Guilherme de Souza. *Manual de Direito Penal*: Parte Geral e Parte Especial. 8ª Ed. rev, ampl, e atual. São Paulo: Revista dos Tribunais, 2012.

OLIVEIRA, Eugênio Pacelli de. *Curso de Processo Penal*. 15ª Ed. rev e atual. Rio de Janeiro: Lumen Juris, 2011.

OLIVEIRA, Natacha Alves de. Crimes praticados pelo sistema de informática: visão prospectiva e sistemática à luz da jurisprudência pátria. *Âmbito Jurídico*. Rio Grande, XVI, n. 115, agosto de 2013. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=13587>. Acesso em 30 nov. 2016.

PAESANI, Liliana Minard. *Direito e Internet*: liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2000.

PINHEIRO, Patricia Peck. **Direito Digital.** 5. Ed. São Paulo: Saraiva, 2010.

POSSETI, Helton. **Relator do projeto do marco civil quer apresentar seu relatório até junho.** 2012. Disponível em: <http://www.teletime.com.br/28/03/2012/relator-do-projeto-do-marco-civil-quer-apresentar-seu-relatorio-ate-junho/tt/270197/news.aspx> Acesso em: 13 out. 2012. **Projeto de Lei PL 84/99 sobre cibercrimes vai voltar à pauta na câmara.** 2011. Disponível em: <http://forum.antinovaordemmundial.com/Topico-projeto-de-lei-pl-84-99-sobre-cibercrimes-vai-voltar-%C3%A0-pauta-na-c%C3%A2mara> Acesso em: 08 set. 2012. **ROSSINI**, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2004.

TAKAHASHI, Tadao (Org.) **Sociedade da informação no Brasil : livro verde.** Brasília: Ministério da Ciência e Tecnologia, 2000.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. *Curso de Direito Processual Penal*. 8ª Ed. rev, ampl, e atual. Jus Podivm, 2013.

TOURINHO FILHO, Fernando da Costa. *Processo Penal*. 34ª Ed. rev. São Paulo: Saraiva, 2012. Vol. I.

VIANNA, Tulio Lima. *Transparência pública, opacidade privada*: o Direito como instrumento de limitação do poder na sociedade de controle. Tese de doutorado para a UFPR. Curitiba, 2006. Disponível em: <https://www.academia.edu/1911163/Transparencia_publica_opacidade_privada_o_direito_como_Acesso 26 nov. 2016.

WENDT, E.; JORGE, H. V. N. **Crimes Cibernéticos**. São Paulo: BRASPORT, 2012.

ZAFFARONI, Eugenio Raúl. *Manual de derecho penal* – Parte general. Buenos Aires: Ediar, 1996.

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Núcleo Integrado de Bibliotecas/UFMA

Sousa Lima, Angelo.
CIBERCRIMES E SUA CONFIGURAÇÃO NO PLANO JURÍDICO NACIONAL E INTERNACIONAL / Angelo Sousa Lima. - 2016.
54 f.

Orientador(a): Cássius Guimarães Chai.
Monografia (Graduação) - Curso de Direito, Universidade Federal do Maranhão, UFMA, 2016.

1. Cibercrimes. 2. Convenção de Budapeste. 3. Cooperação Internacional. 4. Direito Cibernético. I. Guimarães Chai, Cássius. II. Título.