ASSOCIAÇÃO CARUARUENSE DE ENSINO SUPERIOR E TÉCNICO

FACULDADE ASCES

BACHARELADO EM DIREITO

A APLICAÇÃO DA LEI BRASILEIRA NOS CRIMES CIBERNÉTICOS E SUA PERSECUÇÃO PENAL

VINÍCIUS ARAGÃO MELO

CARUARU

2015

ASSOCIAÇÃO CARUARUENSE DE ENSINO SUPERIOR E TÉCNICO

FACULDADE ASCES

BACHARELADO EM DIREITO

A APLICAÇÃO DA LEI BRASILEIRA NOS CRIMES CIBERNÉTICOS E SUA PERSECUÇÃO PENAL

VINÍCIUS ARAGÃO MELO

Trabalho de Conclusão de Curso, apresentado a FACULDADE ASCES, para obtenção do grau de bacharel em Direito, sob a orientação da Professora Paula Rocha Wanderley.

CARUARU

2015

BANCA EXAMINADORA

Aprovada em: ___/___/___.

_____

Presidente:Prof. Paula Rocha Wanderley

_____

Primeiro Avaliador: Prof.

_____

Segundo Avaliador: Prof.

DEDICATÓRIA

Dedico esse trabalho primeiramente a Deus, razão da minha existência; a meus pais, Silvano Osvaldo da Silva Melo e Milka Valéria Aragão Melo, os quais sempre estiveram ao meu lado em todos os momentos da minha vida; aos meus avós por sempre me incentivarem e apoiarem.

AGRADECIMENTOS

Meus agradecimentos à Professora Paula Rocha Wanderley, que com sua dedicação e seu amor ao trabalho me orientou com excelência, sempre com sua paciência e dividindo seus conhecimentos; à Faculdade ASCES, por proporcionar um curso com uma qualidade impressionante; e aos meus amigos por dividirem momentos de preocupação e alegria ao meu lado.

RESUMO

O presente trabalho visa abortar o tema dos crimes virtuais com o enfoque na persecução penal e no ordenamento jurídico vigente tratando do assunto, uma vez que ainda é muito raso e escasso, de maneira tal que não é possível garantir uma proteção eficaz para aqueles que se utilizam dessas ferramentas que atualmente são de suma importância na vida das pessoas, quais sejam, o computador e a internet. Isso se deve ao fato de que o direito brasileiro ainda não conseguiu acompanhar, de forma equivalente, o desenvolvimento da sociedade, assim como dos criminosos que elevaram a mais um patamar a categoria de crimes cibernéticos, sendo hoje recorrente o número de vítimas de tais delitos. Sendo assim, o legislador adotou medidas protetivas para tentar combater as infrações digitais, como por exemplo estender a aplicação do Código Penal para ser utilizado como regra a tipicidade ali contida e abordá-las na seara digital quando possível. Ademais, há ainda leis que visam garantir a segurança jurídica dos usuários da web tanto de forma isolada como a Lei que combate à pornografia infantil na internet, como de forma generalizada, a exemplo da lei "Carolina Dieckman" e da Lei n°12.735/12. Contudo, não obstante, tais medidas tenham iniciado o encaminhamento do Brasil para o rol de países que lutam contra a violência digital, é importante ressaltar que ainda existem lacunas no ordenamento jurídico pátrio que devem ser sanados e preenchidos com urgência, pois os infratores estão cada mais numerosos e as vítimas também aumentam, fazendo-se necessária uma reforma no direito digital brasileiro para que o crime virtual seja combatido, processado e julgado como se deve, possibilitando uma utilização mais segura por parte da população desse instrumento tão benéfico para aqueles que o usam para o bem.

ABSTRACT

The present work has the goal to approach the cybercrimes with focus in criminal prosecution and present National Law about the subject, which one remains shallow and scarce, in a way that is not possible ensure solid protection to those who makes use of these tools that currently are very important in people's life, namely, computer and internet. This is because the Brazilian law could not follow, in an equally way, the society's development, as so the criminals that had leveled up the category of cybercrimes, being often the number of victims of those crimes. Therefore, the legislator adopted protective measures to try to combat the digital offenses, for example extend the application of the Criminal Code to be used as rules for the typicality present there e approach them on the virtual zone when possible. Furthermore, there are laws that have the destination to protect the law safety of the web users, in an isolated way, like the decree that fights against the child pornography on internet, such as in a general way, applying here de law Carolina Dieckman and the law number 12.735/12. However, such measures have started the walking of Brazil to the list of countries that fight cyber violence, is important to say that still are blind spots in Brazilian Law that must be resolved and filled in with urgency, because the criminal are each day bigger in number and the victims also rise up, being necessary a change in the digital law to the combat the cybercrimes, and also prosecute and judge them as is shall, enabling the possibility of use the internet in a risk free way to those who use to the great good.

SUMÁRIO

INTRODUÇÃO

Sabe-se que a Guerra Fria foi um conflito que deixou o mundo dividido e de luto devido aos confrontos entre os Estados Unidos da América (EUA) e a União Soviética (URSS). Deixando de lado as mortes sofridas pela nação mundial, a guerra possibilitou o desenvolvimento do planeta em várias áreas como a política, econômico-financeira e bélica, pois o que ocorreu de fato foi uma corrida armamentista no sentido de que se um polo criava algo novo e que estava um passo à frente dos demais o outro polo conseguia ainda desenvolver algo mais original e melhor que o do adversário.

Partindo dessa ideia de competição onde um sempre cria algo melhor que o anterior, não foi diferente com a rede de computadores e internet, pois foi a partir dessa luta que os Estados Unidos passaram a se utilizar das máquinas digitais para armazenamento de dados e compartilha-Los com outros computadores, a fim de proteger a informação caso a base militar de operações fosse atacada e o aparelho destruído, uma vez que essa mesma informação estaria a salva em diversos dispositivos compartilhados, sendo assim o início da evolução dos computadores.

A globalização permitiu aos aparatos tecnológicos continuarem a evoluir e se desenvolverem ao ponto de cada vez mais ingressarem nas vidas das pessoas, sendo impensável a sua “não-utilização”. Desta feita, com os computadores crescendo em quantidade e, principalmente, qualidade, foi possível alcançar lugares antes nunca atingidos, aumentar a interação social podendo se comunicar quase que de maneira ao vivo e em tempo real com pessoas de qualquer lugar do planeta, assim como crescer o número de relações e transações comerciais entre países que jamais haviam realizado qualquer tipo de conexão.

Entretanto, não se pode deixar iludir pela falsa ideia de que apenas coisas benéficas foram agregadas com a globalização, uma vez que as inovações também ocorreram no polo ilícito. Com isso, os criminosos trataram logo de utilizar a nova ferramenta humana mais comum para propósitos cruéis e torpes, afim de vitimar inocentes que ainda não estavam habituados àquela tecnologia. Eles elevaram o padrão de crimes, incorporando nesse rol já extenso, os chamados crimes virtuais.

Os delitos virtuais ganharam força no território brasileiro, pois não há no ordenamento jurídico vigente normas suficientes para garantir uma segurança a quem se utiliza dos computadores. Ainda não adentrou no patamar daquilo que se entende por necessário e adequado, restando várias lacunas, das quais os infratores se valem para escapar à justiça e saírem impunes de seus crimes, trazendo para a sociedade um sentimento de impunidade quanto aos delitos informáticos.

Contudo, desrespeitoso seria afirmar que o Brasil está desamparado quando da proteção aos crimes cibernéticos, uma vez que o poder legislativo, em parceria com o judiciário, foram muito felizes ao adotarem medidas, a curto prazo, para proteger os cidadãos de se tornarem vítimas. O código penal, valendo-se da analogia, poderá ser aplicado em certas circunstâncias aos crimes na seara digital; foram criadas leis mais especificas e outras de caráter geral, inclusive trazendo para a realidade o processo virtual ao judiciário.

Resta evidente que, como dito anteriormente, a curto prazo essas medidas protetivas funcionam, mas para um período de maior duração, não o fazem, pois ainda deixam brechas na lei, as quais são passiveis de exploração por parte dos criminosos. Faz-se necessária, no atual cenário em que se vive o Brasil, uma reforma na legislação pátria vigente, afim de aprimorar o direito cibernético para ampliar a área de atuação e proteção contra esses delitos, favorecendo os usuários de boa-fé e aumentando o arsenal de armas para combater não apenas os criminosos, mas também o crime na sua raiz e essência.

CAPÍTULO 1: OS APARATOS PRINCIPIOLÓGICOS, BREVE HISTÓRICO DA INTERNET E SEGURANÇA CIBERNÉTICA

O homem sempre buscou melhorar e evoluir, superando a cada dia o seu próprio limite, seja no intelecto ou na forma física. O ser humano está em uma constante corrida contra ele mesmo, onde não se permite ficar para trás, de tal modo que o surgimento da internet se ocasionou devido a uma disputa de poder entre duas grandes potências mundiais.

Pois bem, o mundo se desenvolveu com a ajuda da globalização e arrolado a ele veio a internet, que possibilitou avanços nas mais variadas áreas e beneficiou as relações exteriores entre povos e nações. No entanto, evoluir não necessariamente significa melhoria, o homem aprendeu a usar a internet como uma arma para atender a suas vontades ilícitas.

Mas, como para todo problema há uma solução, neste caso não seria diferente, tendo sido criados diversos meios e instrumentos de combate e proteção contra os ataques virtuais, garantindo assim uma maior segurança para aqueles que se utilizam desta importante ferramenta que é a internet.

1.1 Aparato Principiológico

Antes de adentrar na seara principiológica, é mister entender porque esses princípios são de vital importância para uma legislação, tanto já efetivada no tempo e espaço como também para uma recente.

Os princípios servem como balizadores, guias, para um determinado comportamento adotado por uma nação, sendo de tal forma indispensável para a direção que o país tomará em determinadas situações. Eles não somente conduzem, como servem, muitas vezes, de base para uma legislação ou tomada de decisões do judiciário, uma vez que não poderá ferir um determinando princípio adotado.

1.1.1 Princípio da Reserva Legal e Tipicidade

O princípio da reserva legal aponta que a conduta realizada, seja ela ação ou omissão, precisar estar tipificada e esteja de acordo com o modelo descrito na legislação específica. É possível reforçar esse entendimento através de jurisprudência do STJ:

> "Em Direito Penal tem exponencial relevo o princípio da reserva legal, do qual emana o princípio da tipicidade, que preconiza ser imperativo que a conduta reprovável se encaixe no modelo descrito na lei penal vigente na data da ação ou da omissão" (STJ, REsp. 300092/DF, Rel. Min. Vicente Leal, 6ª T., DJ 22/4/2003, p. 277).

Resta claro, pois, a necessidade de haver uma subsunção, que se configura no enquadramento da conduta realizada à norma legal, para que o Direito Penal possa se interessar e reprovar a ação ou omissão praticadas.

1.1.2 Princípio da Dignidade da Pessoa Humana

É o princípio base. Uma qualidade de todo ser humano, inerente à crença, raça, sexo ou ideologia. Todos têm que ser respeitados, até o mais cruel dos homens. É uma atribuição íntima, gravada na pessoa desde o seu concebimento, não podendo, dessa forma, ser violado em virtude de qualquer argumento.

Ao se falar do princípio da dignidade, vem à mente a questão: quem é titular de tal direito? A resposta se encontra no artigo 1º da Declaração dos Direitos do Homem e Cidadão, onde afirma que "todos os homens nascem livres e iguais em dignidade e direito". Logo, a interpretação correta é a de que todo ser humano é possuidor desse direito, haja vista que lhe é assegurado o mínimo de decência para que se possa viver e desempenhar suas atividades sem prejuízo moral e ético.

1.1.3 Princípio da Territorialidade

Tal princípio encontra-se no artigo 5º do Código Penal e versa sobre a aplicabilidade da lei penal brasileira apenas aos crimes cometidos em nosso Estado, determinando também, em seus incisos I e II, as extensões do território brasileiro, como por exemplo as embarcações e aeronaves brasileiras. Ao ler o artigo

supramencionado, nota-se que o Brasil adotou uma teoria chamada de “temperada” acerca da territorialidade. Isso porque o Estado brasileiro pode abrir mão de sua capacidade de julgar e condenar em razão de tratados e convenções dos quais o Brasil seja signatário. É de suma importância delimitar até onde chega o território brasileiro para fins de determinar de quem é a competência para processar e julgar o delito ali cometido, encerrando assim conflitos de competência

1.1.4 Princípio da Extraterritorialidade

Este encontra-se no artigo 7º do Código Penal Brasileiro e aduz acerca da sujeição à lei brasileira aos crimes cometidos em território estrangeiro, cominado com o princípio que determina a aplicação da lei penal brasileira face aos crimes perpetrados por estrangeiros contra brasileiros fora do Brasil.

Como bem ensina o Cavalhido (2209):

> “O crime cometido, no estrangeiro, contra brasileiro, ou por brasileiro, é da competência da Justiça brasileira e, nesta, da Justiça Federal, a teor da norma inserida no inciso IV do art. 109 da Constituição Federal, por força dos princípios da personalidade e da defesa que, ao lado do princípio da justiça universal, informam a extraterritorialidade da lei penal brasileira (Código Penal, art. 7º, inciso II, alínea *b*, e $3º) e são *ultima raio,* expressões da necessidade do Estado de proteger e tutelar, de modo especial, certos bens e interesses. O atendimento dessa necessidade é, precisamente, o que produz o interesse da União, em detrimento do qual o crime é cometido, no estrangeiro, contra ou por brasileiro é também praticado. Por igual, compete à Justiça Federal julgar os crimes ‘previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente’ (Constituição Federal, art. 109, inciso V). (STJ, HC, 18307/MT, Rel. Min. Hamilton Cavalhido, 6ª T., DJ 10/3/2009, p. 313).”

O supramencionado artigo expressa as situações onde, mesmo tendo sido cometido fora do país, o autor do crime será processado e julgado pela lei penal brasileira.

1.1.5 Princípio da Justiça Universal

A Justiça Universal não é um princípio que se encontra explicito, mas traz consigo a ideia de que o indivíduo fica sujeito àquela lei penal vigente no país em que for encontrado, não importando onde o crime foi praticado ou contra quem. Trata, normalmente, de crimes que o Brasil se obrigou, por meio de tratados e convenções,

a reprimir, como por exemplo o tráfico internacional. Nas palavras do jurista brasileiro Hildebrando Accioly, em seu Manual de Direito Público, 20ª edição, afirma que:

> *A competência universal põe-se como mecanismo adicional efetivo, no sentido de prevenir a impunidade dos crimes internacionais, em que se assinala que a competência dos estados, para processar crimes cometidos no território de outro estado, por pessoas que não tenham a nacionalidade daquele estado, deve ser regida por normas claras, a fim de não comprometer a segurança jurídica e a utilização razoável de tal competência (ACCIOLY, 2012, p. 79)*

Isto posto, ratifica-se a importância de tal princípio, pois determina uma reprovação de grau elevadíssimo por parte dos Estados em razão de alguns crimes de nível hediondo e cruel, ensejando no processamento e julgamento em qualquer país signatário que se encontre o criminoso, não importando se ali foi ou não efetuado o crime. Ademais, a justiça universal fortalece os preceitos trazidos por um outro princípio, qual seja, o da dignidade da pessoa humana, onde todos devem ser tratados com respeito e de maneira honrosa.

1.1.6 Princípio da Nacionalidade

Associado ao princípio da territorialidade, esse princípio expressa a ideia de que a legislação do pais ao qual o sujeito pertence irá acompanha-lo para onde for, ou seja, mesmo estando em outro Estado. Isso se deve ao fato de que o pais policia e protege seus nacionais, punindo-os quando cometem crimes e defendendo-os quando são lesados no exterior. Esse princípio apresenta dois polos: o ativo, que ocorre quando o indivíduo comete o delito; e passivo, quando ele é atingido ou um bem jurídico seu. Este princípio tem por base a relação de fidelidade entre o indivíduo de um Estado com este, ainda que esteja fora de seu território nacional. Em sua origem, o princípio foi justificado pelas diferenças de civilização dos países e pela circunstância de coexistir vários povos em um mesmo Estado.

1.2 Origem e Evolução da Internet

Foi necessário realizar esse rápido percurso principiológico, para nos debruçarmos agora, sobre a origem e evolução da internet e sobre a sua importância no mundo contemporâneo.

O mundo está todo interligado, seja nas relações comercias, financeiras ou ideológicas. Hoje, pessoas de um lado do planeta podem ter contato diário, e praticamente ao vivo, com outras que se encontram do outro lado do globo. Tudo isso foi permitido graças à globalização. Ela, nada mais é, do que o processo de cunho social e econômico que permite a interação entre seres humanos e também entre países de maneira acelerada. Tal processo possibilita a diminuição de distâncias, facilitando assim a comunicação entre povos e nações.

Zygmund Bauman, capta de maneira peculiar o significado de globalização:

> O significado mais profundo transmitido pela ideia da globalização é o do caráter indeterminado, indisciplinado e de auto propulsão dos assuntos mundiais; a ausência de um centro, de um painel de controle, de uma comissão diretora, de um gabinete administrativo. A globalização é a 'nova desordem mundial. (BAUMAN, 1999, p.58)

O processo de globalização não atinge apenas um grupo pré-determinado de pessoas ou nações, ele abraça a todos, por isso é chamado de fenômeno mundial contemporâneo. A globalização não pertence a um pais só, ela tem ramificações que circulam o planeta inteiro, daí a ideia supramencionada de "a falta de um centro, de um painel de controle", porque não há maneiras de controlar, de comandar. É um processo que aconteceu de maneira natural devido às necessidades da época, pois, como se sabe, a globalização se iniciou nos séculos XV e XVI durante as Grandes Navegações e Descobertas Marítimas, onde o homem teve os primeiros contatos com outros povos de diferentes raças e costumes. Ganhou força no fim do século XX com a derrota da URSS e do socialismo e a ascensão do capitalismo, quando a partir desse momento, os países buscaram novas formas de melhorar seus produtos utilizando-se das novas tecnologias, bem como de comercializar esses produtos com outros países. Com isso houve o início do uso da internet, computadores e outros meios de comunicação.

Milton Santos acrescenta ao debate outro ponto de vista acerca do tema, quando aduz em sua obra:

> “Globalização seria o resultado das ações que asseguram a emergência de um mercado dito global, responsável pelo essencial dos processos políticos atualmente eficazes. Os fatores que contribuem para explicar a arquitetura da globalização atual são: a unicidade da técnica, a convergência dos momentos, a cognoscibilidade do planeta e a existência de um motor único na história, representado pela mais-valia globalizada” (SANTOS, 2001, p.24)

Com isso, ele ratifica a ideia de que a globalização surgiu pela necessidade se tornar as distâncias mais curtas para melhorar e beneficiar as relações antes praticamente impossíveis, assim como afirma que ela é fundamental para o aprimoramento mundial nas mais variadas áreas, haja vista que proporciona o desenvolvimento de países e povos.

Nos dias atuais, vive-se muito rápido, o ser humano está sempre querendo ganhar tempo, pois há muito o que fazer. Com isso, passou a utilizar cada vez mais o recurso da internet, seja para se atualizar dos acontecimentos globais ou mesmo para comunicar-se com outras pessoas. A internet ao longo dos anos conseguiu se tornar algo de valor essencial na vida do homem, muitas pessoas possuem internet em suas casas, celulares e laptops. Ela nada mais é do que uma rede de computadores ligada ao redor do planeta, o que proporciona a interação de pessoas de lugares distantes como se perto estivessem.

A internet surgiu por volta de 1960, durante a Guerra Fria, onde havia uma espécie de corrida entre os Estados Unidos (EUA) e a União Soviética (URSS) para ver qual delas seria a nação mais poderosa. Essa disputa ocorreu principalmente na área bélica, haja vista que a cada arma criada por um dos polos do conflito, o outro tentava superar. No entanto, os EUA, em uma tentativa estratégica de proteger informações valiosas criou o que atualmente se conhece por “internet”. A ideia principal era descentralizar as informações de um só lugar para que caso aquele ponto fosse atacado e destruído, as informações ali contidas não se destruíssem também. Com isso, criou-se uma forma de passar esses dados para outros receptores conectados, pois assim, caso o Pentágono, por exemplo fosse alvejado, os dados que ele possuísse estariam seguros em outro computador.

Como bem expressa Manuel Castells (2000, p.82) resumindo de maneira contundente o surgimento da internet, ao afirmar que:

> “A criação e o desenvolvimento da internet nas três últimas décadas do século XX foram consequência de uma fusão singular de estratégia miliar, grande cooperação científica, iniciativa tecnológica e inovação contracutural (...) Quando mais tarde, a tecnologia digital permitiu o empacotamento de todos os tipos de mensagens, inclusive de som, imagens e dados, criou-se uma rede que era capaz de comunicar seus nós sem usar centros de controle. A universalidade da linguagem digital e a pura logica das redes do sistema de comunicação geraram as condições tecnológicas para a comunicação global horizontal”

A primeira rede criada foi a ARPAnet, idealizada pela ARPA (sigla para Advanced Research Projects Agency). Inicialmente a ARPA realizou o estudo de interligação de computadores através de uma rede e desenvolveu, na década de 70, o TCP/IP, que são os protocolos utilizados até hoje. Considerado por muitos como um dos pioneiros no conceito de internet, J.C.R. Licklider trabalhava no Instituto Tecnológico de Massachusetts (MIT) e foi quem começou a falar em uma conexão galáctica entre computadores, ou seja, um sistema que concentraria todos os computadores do mundo em uma única forma de compartilhamento. Em 1990, houve um salto na história da internet, pois foram criados conceitos que estão vigentes até hoje e que funcionam para o melhor desempenho dela, como por exemplo o protocolo HTTP (Hyper Text Transfer Protocol), da linguagem HTML (Hyper Text Markup Language) que possibilita a navegação de um site para outro, ou de uma página para outra. A empresa World Wide Web (www) também deu sua contribuição ao mundo virtual, pois abriu a internet para todos quando simplificou a sistematização de documentos *online*, podendo ser esses em vídeos, fotos ou textos, sendo assim executados e interligados pela internet, contribuindo para um compartilhamento de dados e informações mais eficiente (CASTELLS, 2000)

A internet hoje faz parte do cotidiano da maioria das pessoas, estando presente em seus lares, escolas, faculdades e empregos. Não é mais possível imaginar um mundo onde não haja a internet conectando todos. Ela possibilita uma interação entre os seres humanos mesmo quando esses estão longe uns dos outros, ela aproxima e diminui a distância. Outra característica da internet é favorecer a liberdade de expressão, onde cada um é livre para ser e falar o que deseja, dentro da limitação do bom senso, sem sofrer retaliação. Porém, como está se tornando um costume da população, há algumas pessoas que se utilizam desse meio de interação e compartilhamento de dados para praticar atos ilegais, torpes e prejudiciais a outrem, ou seja, usam a internet para praticar crimes, uma vez que estando dentro dela, o

indivíduo não tem um rosto ou sequer um nome, possuindo apenas pseudônimos ou “apelidos”, na linguagem cibernética.

1.3 Segurança Virtual

A informática e a internet possibilitaram aos seus usuários diversos benefícios, no entanto, na mesma proporção, nasceram os perigos provenientes destes recursos, onde cada vez mais a solução para estes problemas tem se tornado complexa.

Navegam na internet todo o tipo de informações, sendo elas em formato de imagem, vídeo, áudio, ou até mesmo contas bancárias, e-mails, segredos e confidencias pessoais. Com isso, tem sido essencial a segurança cibernética, visando proteger o indivíduo de ter sua privacidade violada e sua vida exposta em toda rede.

Sabe-se que com o avanço tecnológico os crimes no âmbito virtual também cresceram. Particulares e empresas, hoje, procuram bancar um investimento maciço em segurança virtual para proteger as informações ali presentes. Crimes como roubo de dados de cartão de crédito, invasão à contas bancárias, *hackeamento* de computadores pessoas, estão fazendo cada dia mais vítimas entre os usuários da rede.

Segundo informa Mikko Hypponen, o diretor-executivo da F-Secure, uma companhia que atua na área de segurança virtual, em uma entrevista ao site *www.tecmundo.com.br:*

> Se olharmos o cenário de cibercrimes de dez anos atrás, encontraríamos “amadores” distribuindo malwares por métodos que atualmente seriam considerados um tanto antiquados e ineficazes. Hoje, os inimigos mudaram bastante – não lidamos mais com programadores amadores”

Tal afirmação ratifica a ideia de que não apenas a internet, em seu polo positivo, cresceu e se desenvolveu, mas ao seu lado, e na mesma proporção, se modificaram e tornaram-se mais árduos os perigos trazidos consigo. O binômio internet-segurança anda lado a lado numa relação de proporção direta, ou seja, a medida que um se eleva, o outro assim também o faz.

As maiores ameaças cibernéticas dos dias atuais são compostas por três pilares: os criminosos organizados, conhecidos como *crackers*, os webativistas e os

governos de várias nações por todo o mundo. Os primeiros são os mais perigosos e seus ataques são motivados pelo dinheiro, com isso, se utilizam de *banking trojans*, que é uma ferramenta que se infiltra no computador da vítima e rouba o acesso ao *internet banking,* fazendo com que o criminoso tenha acesso ao saldo e possa furtar a quantia que desejar sem que seja possível rastrear de volta para seu próprio computador, sem o conhecimento da vítima; também usam o *keylogger,* que é uma chave que tem o intuito de copiar tudo que é digitado no teclado da vítima, com isso o sujeito tem acesso a senhas de redes sócias e contas bancárias.

O Brasil segue uma rota perigosa, haja vista que é muito atrativa para os hackers. O especialista e chefe da divisão de Riscos Cibernéticos do *Willis Group* (Grupo Willis) de Londres, Peter Armstrong, afirma que o Brasil, por ter um sistema bancário desenvolvido e uma legislação nova e com brechas, chama a atenção dos criminoso virtuais pois o "custo-benefício" de cometer o crime e conseguir não ser pego (devido as leis escassas que o país ainda tem) é muito bom. De acordo com Armstrong, os ataques virtuais sofreram um aumento de 48% no ano de 2014, segundo a pesquisa "Gerenciando riscos cibernéticos em um mundo interconectado", pela Pricewaterhouse Coopers (pwC). Ademais, tal pesquisa demonstrou que a violação virtual elevou-se para 42,8 milhões em comparação ao ano de 2013, o que equivale a 117.339 novos ataques ao dia.

Para se proteger das ameaças há alguns componentes que auxiliam o usuário no combate as invasões. Tem-se o *Firewall*, que pode ter fora de *hardware* ou *software*, que tem a finalidade de bloquear o acesso a páginas maliciosas na internet, ajudando a navegar por sites e páginas mais seguras.

Outro instrumento defensivo é a criptografia. Seu nível de segurança é muito alto pois ela tem a função de processar as informações em linguagem matemática onde a leitura daquela mensagem só será possível se o indivíduo possuir a chave para a tradução da mensagem, que consiste em reorganizar os números e tornar clara a informação. A criptografia é de suma importância na autenticação e assinatura digitais.

O *antispam* também protege o computador contra ataques virtuais. Seu uso é mais comum e de fácil acesso. Sua função é filtrar correspondências eletrônicas (*e-mails)* e identificar quais são maliciosos (contém *spam*) e quais são seguros abrir, possibilitando ao usuário um controle melhor de suas notificações bem como garantindo a segurança do seu aparelho.

É possível hoje se utilizar de proteção contra *spyware* e outros *softwares* mal-intencionados através dos programas *antispyware*, que ficam fazendo buscas no computador verificando arquivos e dados para detectar alguma informação prejudicial camuflada e que possa corromper a máquina. De tal forma, ao ser detectado o mal, o próprio programa anula e não permite que o vírus se infiltre. É preciso cautela, nesse caso, pois o spyware se pega de maneira muito simples e básica, bastando ao usuário entrar em determinados sites – cuja finalidade é unicamente lhe transferir o vírus – ou baixar programas que trazem consigo a ameaça.

Há diversas medidas protetivas que as pessoas podem e devem tomar para tornar o acesso ao seu computador mais seguro e de difícil penetração: Nunca abrir arquivos anexados a e-mails de pessoas ou empresas desconhecidas, e mesmo que o remetente seja conhecido, passe um bom anti-vírus antes de abrir o arquivo; manter em seu computador um bom anti-vírus, sempre atualizado, deixe o firewall do windows sempre ativado; fazer sempre as atualizações necessárias do seu sistema operacional; nunca instalar programas piratas em seu computador, pois eles podem trazer vírus ou outros programas perigosos; não abrir *pen drives* ou CDs de outras pessoas sem antes passar o anti-vírus; não colocar dados pessoais (endereço, nome completo, endereço, CPF) em redes sociais; seguir sempre as orientações de seu banco para acessar sua conta pelo Internet Banking; não digitar as senhas e dados pessoais em computadores públicos; não criar senhas com datas de aniversários, sequências numéricas fáceis ou nome de pessoas; ter cuidado ao utilizar o cartão de crédito em compras *online*, tenha certeza que a loja virtual é segura; não clicar em links mostrados por e-mails desconhecidos, pois eles costumam instalar vírus ou cavalos-de-Tróia (programas que roubam dados do computador); não divulgar dados pessoais (endereços, números de documentos).

Como exposto, todos estão sujeitos a ataques virtuais. A linha que separa violação e segurança é muito tênue, devendo a vítima chamar para lhe defender o direito. Este deverá regulamentar o processo de utilização da rede para que seja garantida uma segurança maior ao usuário na hora de usar a máquina e que seja respeitado o direito de privacidade de cada ser humano.

CAPÍTULO 2: CONCEITO DE CRIME E SUAS CARACTERÍSTICAS, VULNERABILIDADE NA REDE E PRINCIPAIS CRIMES VIRTUAIS

2.1 – Vulnerabilidade Na Rede

Atualmente é comum ouvir que o mundo está vivendo na “era da informática”, devido a importância que foi atribuída à internet na vida das pessoas. A web se tornou um dos principais meios de propagação de notícias, de comunicação e interação entre os usuários.

Uma das funções mais usadas da internet é aquela de mascarar alguns usuários que acham que por estrem atrás de uma tela de computador ou celular eles são inatingíveis e portanto podem fazer qualquer coisa. Isso se deve ao fato de que as pessoas estão utilizando a rede para expor suas vidas, funcionando como um verdadeiro "diário Online" onde todos têm acesso a conteúdo privado que é fornecido pelo próprio dono por livre e espontânea vontade. Indivíduos se expõem abertamente pra qualquer um que esteja interessado em saber da vida alheia e não mede as consequências das suas ações, pois se sente protegido pela internet e não raciona acerca dos riscos aos quais está trazendo consigo. Ao abrir sua vida pessoal no mundo cibernético a pessoa está automaticamente convidando invasores para dividir histórias e experiências bem como dar munição para aqueles mal intencionados que utilizam daquelas informações para chegar na vítima, fingir uma interação benéfica e atraí-la para alguma armadilha.

Há de entender que embora a internet traga consigo coisas maravilhosas, ela também transforma os usuários em pessoas sem nome e sem rosto, podendo esta fingir sem alguém completamente diferente do que na realidade é. Com isso, não há como ter certeza se aquele sujeito é de verdade quem ele alega ser, de tal maneira que os criminosos se usam dessa inocência por parte de alguns internautas para começar conversas e distorcer pontos da realidade afim de ludibriar a vítima fazendo-a crer que está dividindo informações com alguém, quando de fato está com um completo estranho.

As pessoas estão abusando da boa-fé de outras afim de obter vantagem pessoal ou apenas usar aquela informação para humilhar outrem. Tem-se que ter uma

mentalidade mais desenvolvida no sentido de perceber que os tempos mudaram e, nesse quesito, infelizmente, para pior, de maneira tal que os usuários da rede estejam atentos e mais inteligentes para que não acabem se tornando alvos fáceis e ampliando assim sua segurança e proteção.

2.2 – Conceito de Crime e suas Atribuições

Antes de ingressar na área cibernética é necessário entender o que de fato é crime, como se configura e quais seus elementos. Com isso, tem-se o estudo do Direito Penal que possibilita o entendimento de tais aspectos e proporciona uma melhor compreensão acerca do tema.

Como normalmente acontece no direito, há sempre várias correntes debatendo um mesmo assunto, ou vários estudiosos que defendem pontos de vistas divergentes. Na seara criminal, no diz respeito ao conceito de crime e suas atribuições tem-se por pacificado tal entendimento.

O direito brasileiro, no âmbito penal, adotou a teoria tripartida do crime, ou seja, crime é toda conduta que seja, simultaneamente, um fato típico, antijurídico e culpável. É necessária a comprovação de todos os três institutos acima mencionados, não se configurando crime no caso de ausência de um deles.

Welzel, sua obra intitulada *Derecho penal alemán,* faz uma breve consideração acerta do tema, e aduz que:

> A tipicidade, a antijuridicidade e a culpabilidade são três elementos que convertem uma ação em um delito. A culpabilidade – a responsabilidade pessoal por um fato antijurídico – pressupõe a antijuridicidade do fato, do mesmo modo que a antijuridicidade, por sua vez, tem de estar concretizada em tipos legais. A tipicidade, antijuridicidade e a culpabilidade estão relacionadas logicamente de tal modo que cada elemento posterior do delito pressupõe o anterior (WELZEL, 1997, p. 57)

Tal explanação esclarece que os três elementos do crime estão ligados uns aos outros de certa maneira que para se entender um deve-se, previamente, saber do outro. Com isso, faz-se do conceito de crime algo indivisível e único, sendo impossível

a atribuição de apenas dois desses elementos, haja vista que estão unidos e em uma relação de dependência de um para com o outro para que se tenha, de maneira completa, a classificação do crime.

Zaffaroni, em *Manual de Derecho Penal- Parte General,* ajudando a enriquecer o debate, ensina que:

> 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, p. 324).

De tal maneira, faz-se necessário um breve estudo acerca dessas três atribuições do crime para que se possa determinar se determinada ação, ou omissão, pode ser classificada como crime.

O fato típico é composto por conduta, (dolosa ou culposa, comissiva ou omissiva), nexo de causalidade, resultado e tipicidade. A conduta teve seu conceito estudado e modificado ao longo dos tempos, sempre acrescentando algo ao anterior. Anteriormente, a ação era tida como voluntária que trouxesse modificações no mundo exterior. Após, a conduta englobou o sentido da omissão, ou seja, tanto uma ação (comissão) como uma omissão voluntárias manifestadas no mundo exterior; Welzel (*1997)* afirmava que a ação era direcionada sempre a uma atividade fim, podendo ser ilícita ou licita. Por fim, no ponto de vista de Daniela de Freitas Marques, em Elementos subjetivos do injusto, “o conceito jurídico de comportamento humano é toda atividade humana social e juridicamente relevante, segundo os padrões axiológicos de uma determinada época, dominada ou dominável pela vontade” (MARQUES, 2001, p. 67). Ajudando a renomada autora, Johannes Wessels, em *Derecho Penal – Parte General,* defende que:

> O conceito de ação, comum a todas as formas de conduta, reside na relevância social da ação ou da omissão. Interpreta a ação como fator estruturante conforme o sentido da realidade social, como todos os seus aspectos pessoais, finalistas e causais e normativos (WESSELS, 1980, p. 23-24).

A ação (ou conduta) possui quatro variações: dolosa, culposa, comissiva ou omissiva. A conduta dolosa é aquela em que o autor da infração tem o dolo, ou seja, a intenção de causar o dano a outrem; a culposa é aquela em que mesmo que o infrator não tenha a intenção de diretamente causar o prejuízo a terceiros, mas ele assume o risco através da imprudência, negligencia ou imperícia. A ação comissiva é o agir, é o "fazer“ de fato, sendo uma conduta positiva; a omissiva é aquela na qual o agente deixa de agir, se nega a realizar tal ato que deveria, legalmente, prestar. Nesse caso, tem-se uma conduta de cunho negativo.

O nexo causal, por sua vez, é o liame que une a ação ao resultado, sendo assim necessário comprovar que houve uma relação de causalidade para se imputar o crime. O artigo 13, do Código Penal Brasileiro, em seu *caput*, expressa que “o resultado, de que depende a existência do crime, somente é imputável a quem lhe deu causa. Considera-se causa a ação ou omissão sem a qual o resultado não teria ocorrido”.

O STJ, em sua jurisprudência tratou do tema da seguinte maneira:

> Mesmo em se tratando de crimes societários, é indispensável a indicação de uma conduta que se ligue minimamente ao resultado, não bastando a referência À condição de sócio, sob pena de responsabilização de caráter objetivo (STJ, HC 50804/SP, Rel.ª Min.ª Maria Thereza de Assis Moura, 6ª T., DJe 1º/12/2008).

Resta claro pois que em todo crime se faz importante determinar que há uma conexão entre a conduta e o resultado por ela efetivado para que se possa falar em crime. Como bem assevera Guilherme de Sousa Nucci, em sua obra, Manual de Direito Penal:

> Nexo causal é o vínculo estabelecido entre a conduta do agente e o resultado por ele gerado, com relevância suficiente para formar o fato típico. Portanto a relação de causalidade tem reflexos diretos na tipicidade. Causalidade significa sucessão no tempo(...) Por outro lado, *causa* é toda ação ou omissão que é indispensável para a configuração do resultado concreto, por menor que seja o seu grau de contribuição (NUCCI, 2014, p. 157)

Desta forma, se torna fácil entender que a causalidade tem uma importância de grande valor para a configuração do delito, haja vista que sem ela, não importando o

tamanho da sua intervenção, seja direta ou indiretamente, não poderá ser imputado tal ato como crime.

Resultado é quando o objetivo pretendido pelo agente é alcançado, sendo assim, ocorre o chamado crime consumado. De acordo com o Código Penal Brasileiro, em seu artigo 1º, inciso I, “Diz-se o crime consumado quando, quando nele se reúnem todos os elementos de sua definição legal”.

Sabe-se que cada crime é diferente do outro, cada um tem suas particularidades e não se confundem. Logo, para se consumar e ter-se alcançado o resultado almejado, faz-se necessário que cada uma dessas especificidades seja realizada. Com isso, o tempo da consumação – ou do resultado – irá variar de acordo com cada tipo penal, haja vista que nem todos possuem o mesmo instante consumativo.

Há de se falar também em crime tentado, que segundo o inciso II do artigo 14 do diploma acima mencionado se dá “quando iniciada a execução não se consuma por circunstâncias alheias à vontade do agente”. A tentativa é caracterizada por três elementos:

I. A conduta dolosa, ou seja, uma vontade voluntária e consciente do agente de praticar a infração;
II. O agente deve estar na fase de execução;
III. O agente deve ser interrompido por um fator alheio a sua vontade, não alcançando a consumação

Para que se tenha uma conduta classificada como criminosa, tem-se que observar a chamada tipicidade, que nada mais é do que a subsunção da conduta à norma. Ou seja, é a adequação daquele comportamento ao que está estabelecido na lei.

Rogério Greco, em obra Curso de Direito Penal – Parte Geral, traz o seguinte ensinamento:

> Por imposição do princípio *nullum crimen sine lege*, o legislador, quando quer impor ou proibir condutas sob a ameaça de sanção, deve, obrigatoriamente, valer-se de uma lei. Quando a lei em sentido estrito descreve a conduta (comissiva ou omissiva) com o fim de proteger determinado bem cuja tutela

> mostrou-se insuficiente pelos demais ramos do direito, surge o chamado *tipo penal* (GRECO, 2014, p. 163)

A antijuridicidade, por sua vez, diz respeito à contrariedade à norma, seria o que se chama de ilicitude. Quando uma conduta afronta o que está na norma, diz-se que essa ação é ilícita, pois não aconteceu do modo como a lei permite, autoriza ou proíbe. Contudo, para analisar a antijuridicidade, tem-se que antes estudar a tipicidade. Ou seja, primeiro verificar se a conduta é típica ou não, se incorrer na negativa, não há que se falar em ilicitude pois não configurará crime em primeira análise; porém, se a resposta for positiva, então se passará para o exame da ilicitude. Para Fernando Capez, todo fato que for penalmente ilícito é, antes de mais nada, típico, porque se assim não o fosse, não existiria a necessidade de se preocupar em aferir sua ilicitude. Entretanto, um fato típico pode não ser ilícito devido à concorrência de causas excludentes de ilicitude.

Tais causas excludentes são aquelas que como o próprio o nome aduz, anulam a ilicitude de modo que mesmo tendo efetuado tais condutas elas não serão tidas como ilícitas pois estavam acobertadas pela lei, autorizando o seu uso em determinadas situações; são conhecidas como causas legais de excludentes de ilicitude, e elas são: estado de necessidade, legítima defesa, exercício regular de um direito, estrito cumprimento de um dever legal.

O estado de necessidade é aquela situação na qual o indivíduo se encontra em perigo e sua saída é praticar o ato ilícito, desse modo, sacrificando um bem em prol de outro. Como dispõe o artigo 24 do Código Penal Brasileiro, *caput*, parágrafo 1º:

> Considera-se em estado de necessidade quem pratica k gato pra salvar de perigo atual, que não provocou por sua vontade, nem podia de outro modo evitar, direito próprio ou alheio, cujo sacrifício, nas circunstâncias, não era razoável exigir-se (...) Não pode alegar estado de necessidade quem tinha o dever legal de enfrentar o perigo.

Isto posto, nota-se que são necessários requisitos para que configure o estado de necessidade:

I. Perigo atual;
II. Não provocado pelo agente;
III. Direito próprio ou alheio;

IV. Não haver dever legal de enfrentar o perigo;
V. A conduta adotada ser a única viável;

A legítima defesa se configura quando o agente repele ação injusta, contra direito seu ou de outrem, usando dos meios moderados e necessários. No entanto, há divergências quanto a quais bem jurídicos esta causa abraça. Há quem defenda, como Zaffaroni e Pierangeli (1999) , que afirmam que todo e qualquer bem jurídico é passível de ser defendido por meio da legítima defesa; outros, a exemplo de Muñoz Conde (2000), retiram os bens jurídicos comunitários de tal benefício. Para que se possa falar em legítima defesa é preciso verificar a ocorrência de certos elementos extraídos do *caput* do artigo 25 do CP, como bem ensina o mestre Rogerio Greco:

I. Injusta agressão;
II. Meios necessários;
III. Moderação no uso dos meios necessários;
IV. Atualidade e iminência da agressão;
V. Defesa de direito próprio ou de terceiros;

O supramencionado autor, ainda acrescenta o fator subjetivo, além desses objetivos acima citados:

> Para que se possa falar em legítima defesa, não basta somente a presença de seus elementos de natureza objetiva, descritos no art. 25 do Código Penal. É preciso que, além deles, saiba o agente que atua nessa condição, ou, pelo menos, acredita agir assim, pois, caso contrário, não se poderá cogitar de exclusão da ilicitude de sua conduta, permanecendo está, ainda, contrária ao ordenamento jurídico (GRECO, 2014, p. 80)

Há também casos onde ocorre o excesso da legítima defesa. Nessa hipótese, o agente ultrapassa os limites dos "meios necessários" e passa a agir mediante desnecessariedade, de tal forma que deixará de ser abraçado pela causa excludente de ilicitude tendo que responder pelo excesso cometido.

Segundo entendimento do TJMG:

> Não se afasta a legítima defesa tão somente porque o réu não mediu, com racionalidade, a proporção do revide, haja vista que, no calor da discussão, não se exige a mensuração matemática dos meios a serem utilizados como forma de afastar a agressão injusta e iminente. (TJMG, AC 0005220-28.2005.8.13.0628, Rel. Des. Evandro Lopes da Costa Teixeira, DJe 13/7/2012)

É certo que o tribunal foi feliz em sua decisão pois no momento da agressão injusta cada pessoa tem uma maneira diferente de reagir, não se podendo medir o quanto a pessoa poderá repelir, pois é correto afirmar que quando sua mente está tomada por sentimentos como raiva ou ira, derivados de uma ação injusta contra você, não há um controle total sobre o corpo

O exercício regular de direito ficou a cargo da doutrina explicar, uma vez que seu conceito é bastante subjetivo. Esta causa excludente de ilicitude se dá quando o ordenamento jurídico confere àquela conduta uma prerrogativa de fato típico, ou seja, o agente se encontra acobertado ao cometer determinado ato pois a própria lei lhe atribuiu essa possibilidade.

A última excludente se dá através do estrito cumprimento de dever legal, que, assim como a outra causa acima citada, também é uma prerrogativa, porém desta vez é atribuída a algum cargo ou profissão exercida pelo agente. Nesse caso, para se ter, de fato, a excludente, faz-se necessário que o autor se prive ao limite do seu poder estabelecido na lei. Greco (2014) traz dois requisitos para que se instaure o estrito cumprimento do dever legal: o dever legal, fornecido pela lei; em segundo lugar, é preciso que esse cumprimento a esse dever se dê nos específicos termos impostos pela lei, não podendo ultrapassar o limite por ela trazido.

Culpabilidade é o terceiro pilar da conceituação de crime. Ela é o juízo de reprovação atribuído ao agente realizador do ato, bem como a caracterização de culpa pelo fato ocorrido. Ocorre nesse caso uma censurabilidade por parte da sociedade e do legislador, um sentimento de repulsa e reprovabilidade

Integram a culpabilidade a imputabilidade, a potencial consciência sobre a ilicitude do fato e a exigibilidade de conduta diversa. A primeira, diz respeito a capacidade que possui o agente de ser responsabilizado pelo fato típico e ilícito por ele praticado. Nas palavras de Sanzo Brodt, em sua obra nomeada “Da consciência da ilicitude no direito penal brasileiro”:

> A imputabilidade é constituída por dois elementos: um intelectual (capacidade de entender o caráter ilícito do fato), outro volitivo (capacidade de determinar-se de acordo com esse entendimento). O primeiro é a capacidade (genérica) de compreender as proibições ou determinações jurídicas. *Bettiol* diz que o agente deve poder 'prever as repercussões que a própria ação poderá acarretar no mundo social' deve ter, pois, 'a percepção do significado ético-social do próprio agir'. O segundo, a 'capacidade de dirigir a conduta de acordo com o entendimento ético-jurídico'. Conforme *Bettiol,* é preciso que o agente tenha condições de avaliar o valor do motivo que o impele à ação e, do outro lado, o valor inibitório da ameaça penal. (SANZO BRODT,1996, p. 46)

Na contrapartida da imputabilidade há as exceções, chamadas de inimputabilidade, que são exatamente o contrário, ou seja, a impossibilidade de se atribuir a responsabilidade de determinado fato para o indivíduo caso este incorra em duas hipóteses, quais sejam: inimputabilidade por doença mental; e inimputabilidade por imaturidade natural.

Tal entendimento se mostra claro e eficaz ao examinar o texto do Código Penal Brasileiro que traz as duas supracitadas hipóteses:

> Art.26 – É isento de pena o agente que, por doença mental ou desenvolvimento mental incompleto ou retardado, era, ao tempo da ação ou da omissão, inteiramente incapaz de entender o caráter ilícito do fato ou de determinar-se de acordo com esse entendimento (BRASIL, 2014)

O STJ, ratificando o artigo acima, entendeu que:

> Em sede de inimputabilidade (ou semi-imputabilidade), vigora, entre nós, o critério biopsicológico normativo. Dessa maneira, não basta simplesmente que o agente padeça de alguma enfermidade mental, faz-se mister, ainda, que exista prova (v.g., perícia) de que este transtorno do caráter ilícito do fato (requisito intelectual) ou de determinação segundo esse conhecimento (requisito volitivo) à época do fato, i.e., no momento da ação criminosa (STJ, HC 33401,RJ, Min. Felix Fischer, 5ª T., DJ 3/11/2004, p. 212).

Rogério Greco (2014) interpretando o artigo, aduz que o legislador se valeu de dois critérios para a caracterização do *caput* do artigo 26. O primeiro é a existência de uma doença mental ou desenvolvimento mental incompleto ou retardado; a segunda é a incapacidade absoluta por parte do agente de entender que aquela ação ou omissão possuía uma índole ilegal.

Para que possa incorrer em culpabilidade é necessário que se observe se o infrator tinha conhecimento de que aquele ato por ele praticado era ilícito ou não. É a chamada potencial consciência sobre a ilicitude do fato que se dá devido ao erro de proibição, o qual não se confunde com erro do tipo. A Lei de introdução as normas do direito brasileiro, em seu artigo 3º diz que ninguém pode deixar de cumprir a lei alegando que não a conhece, e o artigo 21 do Código Penal aduz que o desconhecimento da lei é inescusável, o que quer dizer que em alguns momentos poderá haver um equívoco acerca de uma situação ser ou não uma infração penal.

O erro de tipo acontece quando o indivíduo se equivoca nas condutas tipificadas, a situação presente lhe é interpretada de modo diferente de como realmente é. Por outro lado, o erro de proibição é justamente a consciência equivocada de que aquele ato é ilícito, ele entende a situação como ela se apresenta de fato, mas o seu erro está em supor que aquela ação é justa, quando na verdade é injusta.

É de suma importância tratar de que o legislador tomou o cuidado de usar o termo “potencial” consciência, haja vista que com isso ele reduziu o risco de abuso dessa excludente de culpabilidade. Ora, com essa expressão não basta apenas que o infrator não saiba, ele terá que se encontrar em uma situação onde não exista também a possibilidade dele ter conhecimento de que a conduta por ele adotada é rejeitada pela legislação. Ou seja, mesmo que ele não saiba da ilicitude do fato, mas tenha a chance de o saber ele será imputável.

Por fim, é preciso que a atitude tomada pelo agente seja, naquela situação, o último recurso passível de utilização. Se ele tivesse outra opção e mesmo assim adotou o caminho contrário ao direito, este será responsabilizado, pois para que se aplique a inexigibilidade de conduta diversa é preciso que seja interpretada de tal maneira que o homem médio na visão da sociedade agiria de maneira igual.

2.3– Principais Crimes Cibernéticos

No exame dos delitos virtuais, com a finalidade de estipular se houve de fato o cometimento de crime, deverá ser analisado todos os aspectos acima tratados, sob pena de incorrer em erro. Não é uma tarefa fácil, pelo contrário, possui uma

complexidade muito larga, haja vista a dificuldade de conseguir estabelecer quando e onde foi exercida a conduta ilícita. Sem contar que em face do direito penal, cada crime possui uma peculiaridade própria, que significa que cada crime é diferente do outro em todos os aspectos.

Os crimes virtuais tiveram sua primeira aparição na década de 1960 quando infratores usaram a rede para manipular e espionar outros computadores e sistema, e desde então foi-se cada vez mais evoluindo não só a quantidade de crimes no mundo virtual, mas também a gravidade de tais delitos.

Como dito anteriormente, essa evolução se deve, em parte, à globalização, que possibilitou a redução de distâncias antes jamais percorridas. Através dela, qualquer pessoa, de qualquer país, pode praticar uma infração penal onde quer que se encontre no planeta bastando ter acesso a um computador.

No Brasil, houve mais de 28 milhões de vítimas de crimes cibernéticos de acordo com a empresa de segurança Symantec. Esse número representa 14,5% da população nacional, no entanto os dados da pesquisa dizem que 56% dos brasileiros já sofreram algum ataque na rede, de acordo com o *site* “www.tecnologia.ig.com.br”

A RSA Anti-Fraud Command Center (AFCC) pertencente à divisão de segurança da empresa EMC2 Corporation, após uma pesquisa, comprovou que o Brasil se encontra em 4º lugar na lista dos 5 países onde mais há ataques na seara cibernética. Na sua frente se encontram outros países como Estados Unidos da América, Reino Único e Índia, nesta ordem, como indica o endereço eletrônico “www.em.com.br”.

Os crimes recorrentes são os de pornografia infantil, injúria, difamação, calunia, fraudes e crimes contra a propriedade intelectual, comumente conhecido como “pirataria”

A pornografia infantil consiste em divulgar fotos ou vídeos com conteúdo sexual envolvendo crianças e adolescentes, logo, menores de idade. Tornou-se uma prática comum no Brasil o consumismo desse tipo de pornografia, haja vista que é muito difícil de localizar e identificar a vítima bem como seu agressor.

O presidente da SaferNet Brasil, Thiago Tavares, falou a respeito do tema para o *site “www5.tjba.jus.br* :

> São 700 mil páginas diferentes de pornografia infantil circulando na rede, que podem ter sido postadas a partir de qualquer lugar no mundo. Por isso, embora o material encontrado seja prova concreta de crimes cometidos, as

> autoridades não conseguem identificar nem o local, e muito menos a vítima, a não ser que alguém faça esse reconhecimento e denuncie. A expectativa, entretanto, é que com o uso de tecnologias avançadas essas identificações venham a ser feitas. São tecnologias capazes de coletar as informações das fotos anexadas, os chamados meta dados.

O presidente ainda afirmou que o número de vítimas identificadas é de menos de 1%, sendo 0,65%, o que é preocupante, haja vista os outros 99% que continuam no anonimato sofrendo abusos de seus infratores. É um dado alarmante, pois isso mostra a ineficiência do combate a esses crimes e o quanto é preciso melhorar, inovar e se empenhar em lutar contra esse mal.

O perigo é tão grande que em 2014 foi feita uma pesquisa pela Folha de São Paulo e constatou que a pornografia infantil era líder em denúncias na internet. O interessante destacar aqui, é uma linha de raciocínio derivada dessa pesquisa, qual seja: se o número de denúncias é assim tão amplo, imagine-se os casos que persistem no anonimato. Sim, sabe-se que nem todos os abusos são denunciados, sendo o principal motivo o medo das vítimas para com seus agressores. Muitas vezes elas sentem medo, vergonha, desprezo por si mesmas e isso impede que elas ajam da maneira correta e reportem as autoridades o que lhe ocorreu.

A pesquisa anteriormente citada, ainda foi capaz de determinar que no site da SaferNet na Central Nacional de Denúncias de Crimes Cibernéticos havia mais 8 categorias de infrações: incitação a crimes contra a vida (com 19,2% das denúncias), racismo (9,4%), intolerância religiosa (7,9%), maus tratos contra animais (7,6%), neonazismo (7,1%), xenofobia (3,9%), homofobia (3,4%) e tráfico de pessoas (0,1%)

Por ser um crime de difícil julgamento, os indivíduos estão dia-a-dia se tornando mais ousados e covardes. Ousados no sentido de criarem páginas e mais páginas na *web* com matéria pornográfica infantil sem medo de serem processados e julgados, pois sabem que o Brasil ainda não possui uma legislação forte suficiente para localizar e sentenciar tais atos; e covardes, pois mesmo com toda a ousadia citada anteriormente, eles continuam escondidos sob o anonimato que só a internet é capaz de proporcionar e com isso podem fazer *uploads* de dados ilegais tendo a noção de que uma vez postos na rede, é impossível deletá-los, estarão lá para sempre.

No caso da pornografia infantil, visa-se a proteção do bem jurídico vida, dignidade da pessoa humana e respeito ao ser humano, não sendo conivente em permitir que crianças e adolescentes tenham suas vidas marcadas por atrocidades cometidas por monstros que já renunciaram a esse direito há tempos atrás.

Outros crimes bastante comuns na internet são os de calúnia, difamação e injúria, todos esses classificados como crimes contra honra. O Código Penal trata de cada um destes em seus artigos 138, 139 e 140, respectivamente.

> "Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos
> § 3º - Admite-se a prova da verdade, salvo:
> I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
> II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
> III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.
>
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.
>
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena:
> I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II - no caso de retorsão imediata, que consista em outra injúria.
> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.
> § 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:
> Pena - reclusão de um a três anos e multa"

As redes sociais se tornaram um instrumento poderoso nas mãos dos criminosos, facilitando o cometimento de delitos. As pessoas acham que estão seguras porque se encontram atrás de um computador e começam a denegrir a imagem alheia, com o intuito de diminuir e machucar a outra parte. Desta feita, se valem de *Facebook, Twitter, Tumbler, Instagram* para ofenderem a honra de um desafeto seu.

A calúnia importa um fato não verídico que é tipificado na lei como crime. O que esses indivíduos não sabem é que aquela rede social é vista não apenas pela pessoa que ele almeja atacar, mas todos os seus familiares, amigos e colegas de profissão, de tal modo que acarreta em um grande prejuízo na sua vida, uma vez que ao ler

aquilo as pessoas próximas à vítima não acreditarão pois conhecem sua índole, porém aos mais distantes no relacionamento pessoal, poderão acreditar naquela mentira e, no caso do âmbito de trabalho, acarretar em uma possível demissão, desmoronando assim a vida da caluniada.

A linha que separa liberdade de expressão e respeito ao outro é muito tênue, sendo muitas vezes invisíveis para alguns. Logo, o uso de *blogs* e páginas de exteriorização de ideias se tornou uma arma para poder caluniar desafetos lhe atribuindo crimes que não foram cometidos se valendo da argumentação de que o país é livre e nele há a liberdade de falar o que quiser. O TRF, em uma Apelação Criminal, julgou:

> PENAL. PROCESSO PENAL. CRIME CONTRA HONRA. CALÚNIA. DIVULGAÇÃO DE NOTÍCIA VIA INTERNET. MEDIDA ASSECURATÓRIA. RETIRADA DE CONTEÚDO OFENSIVO DA REDE MUNDIAL DE COMPUTADORES. DECISÃO REFORMADA. APELAÇÃO PROVIDA.
> 1. Inicialmente, excluo a apelada Cláudia Soares Ribeiro do pólo passivo da presente medida assecuratória por faltar-lhe legitimidade para impedir a veiculação, na rede mundial de computadores, da matéria que se aponta como ofensiva.
> 2. "A internet é o espaço por excelência da liberdade, o que não significa dizer que seja um universo sem lei e infenso à responsabilidade pelos abusos que lá venham a ocorrer" (STJ, REsp 1117633/RO, Rel. Ministro Herman Benjamin, Segunda Turma, julgado por unanimidade em 09/03/2010, DJe 26/03/2010).
> 3. Uma vez que, a teor do noticiado pelo d. Ministério Público Federal, a notícia que se aponta como ofensiva continua sendo veiculada em sítios da internet, impõe-se seja determinado aos provedores, sites de busca e, ao Comitê Gestor da Internet no Brasil que cessem a veiculação da notícia que ora se aponta como ofensiva e criminosa.
> 4. Não há de se falar, outrossim, que tal determinação poderia vir a implicar em afronta ao princípio da liberdade de expressão, pois o egrégio Supremo Tribunal Federal, por ocasião do julgamento da ADPF nº 130, reconheceu a supremacia da liberdade de informação jornalística, como expressão da liberdade de imprensa. Porém, como mecanismo constitucional à calibração de tal princípio, reconheceu a aplicabilidade dos seguintes incisos do art. 5º da Constituição Federal: vedação do anonimato; direito de resposta; direito a indenização por dano material ou moral à intimidade, à vida privada, à honra e à imagem das pessoas; livre exercício de qualquer trabalho, ofício ou profissão, atendidas as qualificações profissionais que a lei

> estabelecer; direito ao resguardo do sigilo da fonte informação, quando necessário ao exercício profissional.
> 5. Apelação provida (Res 320958, RN 2001/0049583-4 – STJ).

Fica claro, pois, que a calúnia existe tanto no mundo real, quanto no mundo virtual, não podendo se desprender daquele estando neste. Tal entendimento se expande e abraça também a ideia de que no mundo virtual as leis continuam a vigorar para todos, com todas as consequências trazidas pelos atos infracionários, não estando acobertados por apenas estarem em uso de máquinas.

O mesmo se aplica aos casos de difamação e injúria na internet, onde o único motivo para que isso ocorra é simplesmente destruir a honra, a imagem e a dignidade da vítima, lhe adjetivando com palavras torpes. O Tribunal de Justiça do Distrito Federal julgou uma Ação Cível do Juizado Especial:

> Juizado especial. Civil. Injúria e difamação. Sítio da internet. Violação da dignidade. Dano moral configurado. Indenização razoável e proporcional. Recurso desprovido. 1.a regra inscrita no art. 333 do CPC impõe ao autor o ônus de comprovar os fatos constitutivos do seu direito e ao réu o dever de demonstrar a inexistência desses fatos ou a presença de outros que lhes sejam impeditivos, modificativos ou extintivos. 2.no caso em exame, o autor comprovou a exibição de palavras ofensivas à sua honra no "blog" do requerido, enquanto esse se limitou a negar que tal fato violou a dignidade do requerente. 3.a injúria e a difamação atingem a honra objetiva e subjetiva da vítima, bem como ensejam a indenização por dano moral, sobretudo quando as ofensas são irrogadas em sítio da rede mundial de computadores. 4.o dano moral é *in re ipsa*, ou seja, decorre do próprio fato ou ato causador da lesão, não havendo que se falar em prova da alteração do estado anímico do agente. 5.se no arbitramento do valor da reparação observaram-se os princípios da razoabilidade e da proporcionalidade, não há razão para a sua revisão pela instância ad quem. 6.recurso conhecido e desprovido. 7.decisão tomada nos termos do art. 46, da lei nº 9.099 /95, servindo a ementa de acórdão. 8.condeno o recorrente no pagamento das custas e honorários advocatícios, os quais arbitro em 10% (dez por cento) do valor da condenação, cuja exigibilidade resta suspensa em face da gratuidade de justiça, nos termos da lei n. 1.060 /50 (ACJ 1049443520108070001 DF 0104944-35.2010.807.0001 – TJ-DF).

Sendo assim, nota-se que o bem jurídico protegido nesses casos é a honra, a dignidade e a imagem da vítima, se perfazendo o crime com a simples indicação de alguma negativa a seu respeito infringindo sua moral.

Atualmente, pode-se dizer que os crimes de calúnia, difamação e injúria se unificaram, no meio ambiente digital, e tornaram-se conhecidos como *cyberbullying*. É uma variação do nome *bullying*, que deriva da raiz *bully* cujo significado é “valentão”,

logo, pode-se extrair a ideia de que há um assédio por parte, na maioria das vezes, de alguém mais forte contra um ser mais frágil, onde a primeira pessoa abusa e cruza o limite da sua vantagem para tentar diminuir e ofender a outra parte mais fraca. É muito ordinário nos dias de hoje, devido à larga propagação das mídias sociais, assim como de um ideal de como o ser humano tem que ser fisicamente, como deve agir e em que deve acreditar, afetando, dessa maneira, a mente da vítima.

Em se tratando da esfera financeira, o crime mais comum no ciberespaço é o furto digital, os hackers e crackers invadem, manipulam e furtam dados com *login* e senha de contas de correspondências eletrônicas (*e-mails)* ou até mesmo bancárias. É costumeiro o indivíduo ser ludibriado achando que está acessando determinado conteúdo quando na verdade está caindo na armadilha do criminoso e, sem querer, acaba por fornecer dados pessoais que serão usados para obtenção de vantagem econômica. Isso se dá através do *Phishing,* que consiste em criar uma página na rede falsa, onde a vítima equivocadamente supõe estar em uma página legal, mas se encontra em uma adulterada e falsa cujo único propósito é roubar informações pessoais.

No ano de 2012, as fraudes virtuais cresceram em 61% no mesmo período que 2011, e essa porcentagem rendeu aos autores uma quantia astronômica de 1,5 bilhão de reais devido a clones de cartões de crédito e débito, assim como saques de contas bancárias, segundo o Febraban (Federação Brasileira de Bancos), como trouxe o “g1.globo.com”.

Em 2013, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil realizou um estudo onde ficou constatado que neste ano foram totalizadas 85.675 notificações de tentativas de fraudes, indicando um aumento de 23% em relação ao ano anterior; também ficou provado que o *Phishing* aumentou em 44% quando comparado a 2012 com casos de páginas falsas de bancos e sites de comércio eletrônico, como de acordo com o ***site*** *“*www.defesanet.com.br”.

Em delitos de fraude, dá-se-á sua consumação no momento em que o bem deixa posse do seu detentor, haja vista ser muito difícil saber com precisão o momento real da extração do valor.

Outra infração muito corriqueira no mundo digital é a pirataria, pertencente ao rol dos crimes contra a propriedade intelectual no artigo 184 do Código Penal Brasileiro:

> Art. 184. Violar direitos de autor e os que lhe são conexos:
> Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.
> § 1º Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 2º Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
> § 3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto

Ao longo dos anos se tornou comum o consumo de produtos que antes eram licenciados e para usufruir deles era necessário pagar e hoje com apenas um clique na internet é possível ter acesso a todo o conteúdo de graça. Isso é devido ao fato de que, atualmente, disponibilizam todo tipo de produto na rede onde basta fazer um *download* de maneira gratuita e o produto se encontra em posse do indivíduo.

Dessa forma, todas pessoas são capazes de possuir tudo sem que se tenha um controle quanto a quem pertence o direito sobre determinado produto. É muito difícil definir quem é o dono de um arquivo lançado no cibermundo, uma vez que a pessoa que o lançou pode ter adquirido de outra e relançado como se sua fosse. O Direito Penal visa proteger quem de fato é o legitimado daquele direito, como também alarga o conceito de “direitos autorais” passando a abraçar obras literárias, artísticas e cientificas

Em fevereiro de 2015 foi realizado um estudo global referente ao ano de 2014 pela consultoria TrueOptik e disponibilizado pelo *website* www.olhardigital.uol.com.br e nesse estudo ficou demonstrado que o Brasil se encontra na vice-liderança em um *ranking* mundial de pirataria com um número gigantesco de *downloads* de matérias ilegalmente gratuitas de 1,2 bilhão, bem como restou provado que o Brasil figura na

primeira colocação do *ranking* quando o assunto é o faturamento que as empresas deixaram de ganhar com a pirataria; nesse aspecto do estudo, a República Federativa do Brasil tem um valor estratosférico de US$99,6 bilhões (segue números em anexo na p. 54)

É importante ressaltar que o direito autoral possui duas vertentes a serem seguidas simultaneamente: a primeira diz respeito ao patrimônio, ou seja, deve-se respeitar o autor pela obra por ele alcançada, valorizando-o assim como a seu direito de remuneração sobre seu trabalho; a outra fala acerca da moral, a qual significa proteger o caráter e a integridade da obra.

Ao se falar em direito autoral e obra, tudo está incluído: desenvolvimento de softwares, *hardwares, artigos, blogs*, textos, montagens fotográficas, *sites* de diversos conteúdos. Portanto, há de se preservar a competência deste autor, artista, estudioso, desenvolvedor, e lhe dá o devido crédito, mas também, tão importante quanto, a proteção do que é seu por direito, através do poder legislativo, criando leis que assegurem uma maior segurança e contribuindo assim para uma maior tranquilidade no desempenho de suas funções autorais.

CAPÍTULO 3: A APLICAÇÃO DA LEI PENAL E PROCESSUAL NOS CASOS CIBERNÉTICOS

3.1 Relação da Persecução Penal nos Crimes Cibernéticos

Com a grande evolução do mundo contemporâneo trazendo consigo a internet cada vez mais para junto das pessoas, despertou-se um interesse antes adormecido pelo consumo da *web*, de forma que a sociedade incorporou esse novo instrumento em vários aspectos da sua vida. Logo, o direito não poderia ficar alheio a tais modificações e passou a se utilizar do recurso digital para aprimorar seu funcionamento e facilitar uma melhor condução do processo envolvendo os crimes virtuais.

Tem-se visto a atuação do mundo virtual mais presente no âmbito jurídico nacional, uma vez que hoje é possível se falar no uso de provas eletrônicas para serem usadas no tribunal quando no julgamento no réu, bem como se tornou uma prática comum a conservação e guarda de tais provas por parte de pessoas físicas e

jurídicas ao ponto de atualmente *e-mails,* que comprovem determinada atividade ilícita, serem aceitos em juízo.

No ano de 2006, foi criada a Lei nº 11.419/06 que significou um verdadeiro divisor de águas no direito digital, trazendo em seu artigo 1º, *caput,* a novidade da informatização do processo judicial, quando aduziu que ”O uso de meio eletrônico na tramitação de processos judicias, comunicação de atos e transmissão de peças processuais será admito nos termos desta Lei” e estendeu mais a área de atuação do processo virtual quando em seu artigo 11 determinou que "Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta lei, serão considerados originais para todos os efeitos legais".

Sendo assim, a persecução penal vem ampliando horizontes e se adentrando na seara digital para que seja alcançada uma mais completa verdade acerca das investigações nos delitos cibernéticos. Ora, persecução penal significa a junção do ato de investigar se houve de fato a configuração da infração e o momento da propositura da ação penal perante o judiciário. Como leciona o professor Nestor Távora:

> A persecução criminal para a apuração das infrações penais e sua respectiva autoria comporta duas fases bem delineadas. A primeira, preliminar, inquisitiva, e objeto do presente capítulo, é o inquérito policial. A segunda, submissa ao contraditório e à ampla defesa, é denominada de fase processual. Assim, materializado o dever de punir do Estado com a ocorrência de um suposto fato delituoso, cabe a ele, Estado, como regra, iniciar a *persecutio criminis* para apurar, processar e enfim fazer valer o direito de punir, solucionando as lides e aplicando a lei ao caso concreto (...) Em outros termos, a persecução penal estatal se constitui de duas etapas: (1) a investigação preliminar, gênero do qual é espécie o inquérito policial, objeto deste capitulo, cujo objetivo é formar lastro probatório mínimo para a deflagração válida da fase seguinte; e (2) o processo penal, que é desencadeado pela propositura da ação penal perante o judiciário.

Abrilhanta ainda mais o assunto Frederico Marques:

> A *persecutio criminis* apresenta dois momentos distintos: o da investigação e o da ação penal. Esta consiste no pedido de julgamento da pretensão punitiva, enquanto a primeira é atividade preparatória da ação penal, de caráter preliminar e informático: *inquisitivo nihil est quam informatio delict.*

Nota-se com isso, que deve-se aplicar as investigações nos casos de delitos cometidos na rede de computadores ou por meio dela, haja vista a dificuldade real de conseguir achar evidências de tais crimes, pois dificilmente o infrator terá usado dados pessoais ou até mesmo um computador do qual seja dono, valendo-se assim de outros de caráter público, encobrindo o rastro.

O ato de investigar tem por finalidade a obtenção de provas para se provar, ou não, determinado fato. A prova pericial é de suma importância nos caos de crimes virtuais, na razão de que permite ao perito criminal cibernético realizar um exame detalhado e minucioso do instrumento utilizado para a realização do crime.

Passada a primeira fase, qual seja, a investigação pericial, tem-se por fim o ajuizamento da ação penal para iniciar o processo de julgamento do criminoso pelo crime cometido e devidamente provado. Esta pode ser pública ou privada, seguindo as regras estabelecidas também pelo código penal pátrio. No entanto, não se poderá abranger todas as condutas, nem generalizá-las, devendo algumas delas ser examinadas de maneira isolada e única que lhe é peculiar, como no exemplo da intimação do provedor, busca e apreensão de computadores que deverão ser feiras por meio das normas trazidas na Lei nº 9.609/1998.

Desta forma, fica claro que algumas questões tratadas no âmbito cibernético podem ser estudadas se baseando pelo código penal, que através do uso da analogia, poderá comunicar suas regras para os crimes virtuais. No entanto, ainda se faz necessário aprimorar o ordenamento jurídico que o Brasil possui acerta do presente tema, mas também apresentar a criação de novas regras para que se preencha as lacunas ainda existentes e garanta assim um uso mais seguro da rede digital.

3.2 Consumação do Crime e Competência para processar e julgar

Para se falar em competência para processar e julgar os crimes acontecidos no âmbito virtual, necessário se faz analisar o momento da consumação desses delitos. Já foi dito anteriormente no tópico 2.2 (Conceito de Crime e suas atribuições) que a consumação do fato é o momento em que o indivíduo alcança o resultado almejado pela sua conduta, ou seja, ocorre quando o crime de fato é perpetrado e a

finalidade daquela ação ou omissão produz o efeito desejado causando danos à vítima.

Para facilitar o entendimento acerca do tema, Guilherme de Souza Nucci exemplifica da seguinte maneira:

> É o tipo penal integralmente realizado, ou seja, quando o tipo concreto se enquadra no tipo abstrato (art. 14, I, CP). Exemplo: quando A subtrai um veículo pertencente a B, como ânimo de assenhoreamento, produz um crime consumado, pois sua conduta e o resultado materializado encaixam-se, com perfeição, no modelo legal de conduta proibida descrito no art. 155 do Código Penal.

Logo, entende-se por consumação quando há a chamada subsunção da conduta à norma somando-se a isso a obtenção do resultado pretendido. Como dito acima, é importante acontecer o encaixe da conduta praticada estando ela tipificada no modelo trazido pela lei, para que se configure a consumação.

Devido à característica particular de cada crime individualmente, tendo cada um seu momento consumativo diferente do outro, há uma dificuldade ainda maior de se estipular o momento certo e especifico da configuração do delito virtual bem como definir a qual jurisdição pertence a competência para julgar tal infração cibernética, pois é um crime abrangente no sentido de o ato ser praticado em um lugar, porém o resultado ser auferido em outro completamente distante.

No Brasil, existem leis que visam combater os crimes informáticos como a Lei nº 11.829/08 que luta contra a pornografia infantil, a de nº 9.609/98 que trata da proteção da propriedade intelectual do programa de computador, entre outras. No entanto, para fortalecer a proteção dos usuários da rede contra ataques criminosos, a legislação brasileira, em conjunto com a justiça, vem utilizando-se da analogia para determinar a consumação dos delitos informáticos, pois com o advento da internet foram trazidos para o ambiente digital crimes tipificados no Código Penal, como à calúnia, injúria, difamação, ameaça. Então, para determinar a consumação desses crimes na seara virtual, se utilizou da mesma consumação dada pelo dispositivo penal, dessa maneira aumentando os meios de contra-atacar as infrações.

Tem-se aí uma decisão acertada do aplicador do direito, uma vez que a gama de instrumentos legislativos que o país dispõe não é muito variada, sendo ainda escassa, de tal maneira que qualquer outro meio que possa vir a ser utilizado para contribuição no combate a essa “nova” e moderna categoria de crime é bem-vinda. Não é de hoje que se sabe que Direito e Sociedade possuem uma relação bastante conectada de um para com outro, onde o primeiro acompanha o segundo e o segundo se amolda ao primeiro. No entanto, no ciberespaço – que consiste no âmbito virtual protagonizado pela internet dentro dos computadores - essa mutualidade ainda não aconteceu como tem que ser, tendo a sociedade se desenvolvido de uma forma assombrosa enquanto a legislação ainda não encontrou formas de proteção e combate que fossem, de fato, eficazes contra. O que se observa é um direito ainda conservador e atrasado, fraco no que diz respeito a sua eficácia e um tanto quanto leigo sobre o assunto e por causa dessa ignorância não é capaz de criar armas apropriadas para se defender.

Saber identificar o momento exato da execução do crime na esfera cibernética é o primeiro passo no combate ao crime, pois a partir disso é que se estuda onde ocorreu, quando aconteceu e quem é o legitimado para processar e julgar. São questões da maior importância, trata-se de buscar a justiça através de uma legislação inteligente e competente para reconhecer quem de fato é o causador da infração e fazê-lo arcar com as consequências dos seus atos.

Isto posto, já sabendo que a consumação dos crimes computacionais ocorre no momento disposto também pelo Código Penal, assim como pelas leis especificas de cada crime, parte-se para a análise da jurisdição e competência para realizar o processamento e julgamento do infrator penal.

O STJ, em sua Terceira Seção, no Conflito de Competência 97201, tem o entendimento pacificado de que o simples fato do crime ter sido cometido através de um computador, ou na rede, não torna competente a Justiça Federal para realizar o processo e julgamento do mesmo. Os juízes federais apenas terão jurisdição nesses crimes quando incorrerem nas situações elencadas pelo artigo 109, incisos IV e V da Constituição Federal de 1988, a qual traz:

> Artigo 109 – Aos juízes federais compete processar e julgar:
> IV – os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral;
> V – os crimes previstos em tratado ou convecção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;

Pode-se relacionar ao inciso IV crimes como o de guarda de moeda falsa, de tráfico internacional de entorpecentes, contra as populações indígenas, de tráfico de mulheres, de envio ilegal e tráfico de menores, de tortura, de pornografia infantil e pedofilia e corrupção ativa e tráfico de influência nas transações comerciais internacionais, que são acordados internacionalmente por meio de tratados e convenções, sendo o Brasil signatário destes. Em tais crimes, juntamente com aqueles mais do inciso V do supracitado artigo, a Justiça Federal atuará como competente.

É de suma importância apontar um fator que atua como um divisor de águas para o estabelecimento da competência nesses casos, sendo ele a internacionalidade do fato na rede, ou seja, se aquela conduta, ou acesso a uma determinada página na internet, ultrapassou os limites da fronteira nacional. Se a resposta for afirmativa, quem é competente é a Justiça Federal; sendo negativa, a conduta continuaria no âmbito nacional, sendo a competência da Justiça Estadual, bem como, mesmo o crime ultrapassando os limites do Brasil, mas não tendo sido acordado em algum tratado ou convenção internacional, nem atingindo bens relacionados à União, haja vista que não estará subsumido no artigo 109 da Constituição Federal Brasileira de 1988.

Para enriquecer o estudo, o STJ decidiu que:

> CONFLITO NEGATIVO DE COMPETÊNCIA. CRIME DE INJÚRIA PRATICADO POR MEIO DA INTERNET, NAS REDES SOCIAIS DENOMINADAS ORKUT E TWITTER.
> AUSÊNCIA DAS HIPÓTESES DO ART. 109, INCISOS IV E V, DA CF. OFENSAS DE CARÁTER EXCLUSIVAMENTE PESSOAL. COMPETÊNCIA DA JUSTIÇA ESTADUAL.
>
> 1 - O simples fato de o suposto delito ter sido cometido por meio da rede mundial de computadores, ainda que em páginas eletrônicas internacionais, tais como as redes sociais "Orkut" e "Twitter", não atrai, por si só, a competência da Justiça Federal.

> 2 - É preciso que o crime ofenda a bens, serviços ou interesses da União ou esteja previsto em tratado ou convenção internacional em que o Brasil se comprometeu a combater, como por exemplo, mensagens que veiculassem pornografia infantil, racismo, xenofobia, dentre outros, conforme preceitua o art. 109, incisos IV e V, da Constituição Federal.
> 3 - Verificando-se que as ofensas possuem caráter exclusivamente pessoal, as quais foram praticadas pela ex-namorada da vítima, não se subsumindo, portanto, a ação delituosa a nenhuma das hipóteses do dispositivo constitucional, a competência para processar e julgar o feito será da Justiça Estadual.
> 4 - Conflito conhecido para declarar a competência do Juízo de Direito do Juizado Especial Cível e Criminal de São Cristóvão/SE, o suscitado.
>
> (CC 121.431/SE, Rel. Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA SEÇÃO, julgado em 11/04/2012, DJe 07/05/2012)

Vale ressaltar também que para auxiliar na fixação de competência não importa onde está o provedor da internet, mas sim o local onde ocorreu a consumação do crime. Desta feita, faz-se mister o uso de três artigos cominados para determinar a competência, sendo eles o artigo 6º do Código Penal e artigo 70 e 88 do Código de Processo Penal, que aduzem, respectivamente:

> **Artigo 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;
> **Art. 70 –** A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
> **§ 1º** Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.
> **§ 2º** Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.
> **§ 3º** Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção.
> **Art. 88**. No processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República.

Isto posto, observa-se que há uma complexidade no que concerne à estipulação da competência e jurisdição nos casos de crimes cometidos na rede, sendo uma tarefa muito complicada e de difícil pacificação se utilizar dos requisitos certos para a determinação da mesma. No entanto, embora difícil não é impossível, e

o Brasil está se mostrando um pouco mais a cada dia ser um país não conivente com tais crimes, de tal forma que até criar um sistema de leis forte o suficiente para encarar tais desafios de igual para igual, ele se utilizará de todos os meios possíveis para proteger os cidadãos usuários da internet.

Fica claro, pois, que a internet trouxe diversos benefícios para a humanidade, encurtou distancias antes jamais percorridas pelas pessoas e aumentou, por um lado, a interação social. Contudo, não é correto afirmar que apenas coisas boas foram atraídas com o advento do uso da rede de computadores, haja vista que o fator crime se desenvolveu bastante ao ponto de, em alguns períodos de tempo, estar à frente da sociedade – e por sociedade entenda-se também o Direito – e não dispor dos meios necessários e eficazes de combate.

Por fim, mostra-se indispensável a grande necessidade de uma segurança jurídica para os usuários de computador, pois hoje, a internet é uma ferramenta comumente usada pelas pessoas para realização de diversas atividades profissionais, que na atual conjuntura da situação do País, está deixando-as vulneráveis, uma vez que não há amparo legal suficiente para garantir o uso seguro da rede.

3.3 Aplicação da Lei Penal contra os Crimes Cibernéticos

Como previamente discutido, sabe-se que a legislação brasileira carece de uma proteção maior no que diz respeito à seara criminal no âmbito virtual. Há, ainda, no atual sistema normativo do país, lacunas quando se trata da segurança que deveria ser prestada aos usuários da *web*, pois não existem leis suficientes em quantidade, e também eficácia, para combater o problema.

As normas brasileiras que tratam do presente tema são escassas porque o direito pátrio não desenvolveu-se na mesma proporção que a sociedade. E o que isso quer dizer? Significa que o corpo social evoluiu ao longo dos anos, no entanto o termo “evoluiu” deve ser interpretado por ambos os polos: o positivo e o negativo. Isso porque não se pode negar que o advento da tecnologia virtual no dia-a-dia da população trouxe consigo diversas novas vantagens antes não obtidas e favoreceu aqueles que a abraçaram; porém nem sempre evoluir quer dizer melhorar, e tal

afirmação é comprovada quando se estuda e faz a comparação entre a sociedade moderna e o direito cibernético. Infelizmente, a primeira saiu na frente com uma larga distância, visto que o legislador ainda não encontrou formas sólidas de contra-atacar essa nova categoria de crime surgida com o avanço da internet.

Sabe-se que o direito brasileiro apenas permite a revogação de uma lei por meio de outra lei, os costumes não têm eficácia normativa para abolir um dispositivo. Porém, o artigo 4º da Lei de Introdução às Normas do Direito Brasileiro diz que "quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais do direito", o que esclarece que em alguns pontos a coletividade pode influenciar no direito. Desta feita, o binômio direito-sociedade na prática deveria atuar em uma relação de mutualidade e diretamente proporcional uma à outra, na medida em que uma cresce a outra acompanha seu crescimento.

Embora o legislador brasileiro tenha se valido de alguns recursos que, de fato, agregam força na proteção jurídica contra os crimes virtuais, ainda não chegou na situação que se entenda adequada e necessária. Já foi abordado o alto índice de criminalização na área virtual aqui no Brasil e mesmo assim pouca coisa foi feita para ampliar a segurança jurídica. O *website* Opinião e Notícia falou sobre ao assunto:

> A legislação sobre o cibercrime é fraca. Aprovada em 2012, a Lei Carolina Dieckmann estabeleceu que o ato de hackear é uma ofensa criminal. Mas as penalidades fracas (de três meses a um ano de prisão e pagamento de multa) não intimidam muito (Fonte: Foreign Affairs – Brazil's Cybercrime Problem, 2015).

Isso trata bem a situação em que vive o pais. Atualmente, o Brasil possui cerca de sete leis destinadas aos crimes cibernéticos, sendo a mais conhecida a Lei nº 12.737/2012, apelidada de Lei Carolina Dieckmann, pois invasores furtaram dados do celular da atriz e divulgaram fotos privadas na internet. Somando-se a essa, há ainda a Lei nº 11.829/08, que trata da pornografia infantil na internet; a Lei nº 9.609/98, que diz respeito à propriedade intelectual do programa de computador; a Lei nº 9.983/00, que regulou os crimes correspondentes ao acesso indevido a sistemas informatizados da Administração Pública; a Lei nº 9.296/96, que disciplina a interceptação seja ela de natureza telemática ou informática; a Lei nº 12.034/09, que elencou os direitos e deveres dentro da internet durante as campanhas eleitorais; e por fim a Lei nº

12.735/2012, que trata das condutas realizadas mediante o uso de sistema eletrônico, digital ou semelhante.

Logo, vê-se que o ordenamento jurídico pátrio, embora tenha tomado medidas contra certas condutas no meio virtual, ainda se mostra pobre em quesito eficácia. O legislador adotou uma medida de se utilizar do Código Penal por meio da ampliação da área de atuação de certos tipos penais para o plano informático (cita-se a calúnia, injúria, difamação, ameaça e racismo, como exemplos) alegando que a internet é apenas mais um meio a ser usado para a consumação do ato. Tem-se por acertada a decisão do judiciário por incorrer nessas ramificações do diploma penal, haja vista a necessidade de mais e mais instrumentos para fazer justiça contra aqueles que a rompem.

Percebe-se uma negligencia por parte do legislador ao editar leis que possuam penas fracas e de pequena duração, fazendo com que gere um sentimento de impunidade no seio da coletividade. Crimes graves como furtar informações de caráter pessoal, como fica claro no artigo 154-A do diploma penal nacional, são punidos com apenas alguns meses de detenção, quando na verdade, deveriam possuir uma sanção mais severa, para que cada crime julgado servisse de exemplo para os próximos e com isso diminuir a criminalidade.

Maria Eugênia Gonçalves Mendes e Natália Borges Vieira, em seu artigo publicado pelo site GCP Advogados, discorreram:

> Diante dos avanços tecnológicos, do uso rotineiro da internet e dos meios eletrônicos no cotidiano das pessoas e, consequentemente, da propagação de crimes relacionados a esse cenário, o Brasil se mostra atrasado por ainda não possuir uma legislação específica para disciplinar os crimes cibernéticos. Vários países já apresentam legislação específica que tratam dos crimes cibernéticos, como Estados Unidos, Portugal, Inglaterra, entre outros.
> Embora já tenham sido tomadas certas medidas emergências, como a criação de normas que regulam algumas dessas condutas criminosas que ocorrem no meio virtual, como visto acima. Apesar, também, da aplicação do Código Penal para alguns crimes cibernéticos, é necessária uma legislação específica que englobe com eficiência todas essas condutas, até porque o nosso Código Penal é de 1940, época em que não existiam as tecnologias que utilizamos nos dias de hoje.
> Como vimos, os crimes cibernéticos próprios são tipos novos, e diante da falta de legislação específica, ainda existem condutas atípicas, que não podem ser punidas em decorrência do princípio da legalidade ou da reserva legal. Assim como, não é suficiente para combater os crimes cibernéticos a aplicação das legislações vigentes. Por isso, a pratica desses crimes ainda

> gera impunidade, daí surge a necessidade da legislação específica (GCP Advogados, 2013).

Fortalece o entendimento de que faz-se obrigatória uma repaginação completa no ordenamento nacional quando se tratar de leis que lidem com o espaço virtual. É necessário que o poder legislativo entenda que ao direito e à sociedade foi acrescentado um terceiro fator: o desenvolvimento também do crime.

É inviável continuar achando que o ordenamento jurídico brasileiro já está forte o suficiente para lutar de fato contra os crimes cibernéticos diante de todos esses problemas, de todas essas injustiças e de todos esses crimes e impunidades, pois é um direito de todos poder usufruir da internet com sua segurança estando garantida pelo ordenamento. Não há de permanecer retrógrado, ou estagnado no passado, uma vez que, como exposto no artigo supra, o Código Penal foi elaborado no ano de 1940, onde a internet não era utilizada como nos dias atuais.

Embora seja clara a impossibilidade da legislação em acompanhar os avanços dos crimes virtuais, primeiramente é fundamental que se entenda que a falta de legislação especifica é um grande empecilho para o desdobramento dos crimes na esfera cibernética, e essa realidade precisa mudar, mas enquanto isso não ocorre esse não deve ser o fator determinante para a impunidade dos criminosos.

Uma vez que a máquina legislativa estatal se mostra incapaz de perceber que as leis atuais se encontram ainda necessitadas de suporte, deve-se ao menos, aumentar o alcance dessas sanções e punindo mais duramente os infratores. Tomando como exemplo a Lei nº 12.767/2012 que tem por pena a detenção de três meses a um ano e as variações de acordo com o agravantes causas de aumento de pena, seria prudente estender a pena base para um montante mais árduo que cause impacto naqueles que a quem irá incorrer, bem como medo naqueles que ainda pensam em praticar tais delitos, fazendo com que pensem antes de efetuar tal conduta.

As duas leis base para a segurança informática são as já anteriormente citadas nº 12.735/12 e nº 12.737/12. São elas que norteiam o direito virtual, haja vista que as outras leis são de caráter mais especifico, abrangendo apenas aquelas situações de maneira que saindo daquela linha de raciocínio a conduta se torna atípica, logo, não haverá configuração do crime.

A aprovação de ambas as leis no ano de 2012 foi um sinal verde para a luta contra essa nova tipificação de crime e funcionou como um símbolo de esperança, haja vista que possui um conteúdo bastante importante e que disciplina atitudes que poderão ser tomadas para melhor promover a proteção no âmbito digital podendo assim serem utilizadas pelas próximas leis que vierem a ser criadas como suporte nesse entrave.

A Lei de nº 12.735/12 disciplina atos que são cometidos mediante uso de sistemas eletrônicos, digitais ou semelhantes e que são praticados contra sistemas informatizados e similares. Percebe-se aqui a amplitude que essa lei alcançou ao definir todo e qualquer meio de utilização da rede para a prática de uma infração direcionada a sistema de informática, diminuindo assim o número de espaços vagos que permitam ao sujeito escapar por falta de tipificação da norma. Ademais, ela trouxe consigo uma importante ferramenta, em seu artigo 4º onde aduz que:

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

Quer dizer que desde 2012 toda polícia judiciária do Brasil pode e deve ter um grupo de *experts* em informática para ajudar nas investigações e no combate, o que significa que o número de pessoas dispostas a ajudar e com o conhecimento exato da rede de computadores aumentou significativamente de modo que possibilita o exercício de um trabalho mais elaborado e com maior grau de acerto.

Por sua vez, a Lei nº 12.737/12 foi ainda mais além e disciplinou as condutas tipificando-as nos principais crimes informáticos relacionados a invasão de aparelhos digitais, furto e divulgação de dados na rede. Essa lei trouxe algumas mudanças no diploma penal como por exemplo a adição dos artigos 154-A e 154-B:

> **Art. 154-A**. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 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.
> **Art. 154-B**. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos

Nota-se, pois, que ambas as leis trataram de iniciar um movimento por uma internet mais segura no pais, visando proteger todas as possibilidades de violação do usuário da rede garantido um uso seguro e com proteção por meio de leis.

Torna-se evidente e clara a ideia de que ainda não é o ideal do que o Brasil precisa para combater essa espécie de crime tão comum que se desenvolveu ao longo dos anos, mas que está no caminho certo para reverter essa impunidade e garantir que todos que corrompam a privacidade, a honra, a imagem, a esfera financeira de outrem, seja devidamente punido na consequência dos seus atos, inibindo assim a criminalidade virtual, favorecendo dessa forma aqueles que tanto ganham e se beneficiam desse instrumento tão importante que é a internet.

CONSIDERAÇÕES FINAIS

Com base no que foi exposto com o estudo apresentado, teve-se por finalidade trazer à luz um problema que está ocorrendo no Brasil com demasiada regularidade fazendo numerosas vítimas e onde a tendência é continuar a aumentar se não houver uma inovação no ordenamento jurídico nacional, pois se este prosseguir inerte e vazio como hoje se encontra, não garantirá segurança para os brasileiros.

Dessa maneira, percebeu-se que a globalização foi uma das causas que abriram as portas para a entrada desses crimes no seio da coletividade, uma vez que possibilitou avançar em uma área, leia-se a digital, onde todos são anônimos e pouco fazem uso da realidade pessoal com o intuito de ludibriar e obter vantagem ilícita para si mesmo ou apenas para violentar a honra e imagem de outrem.

Comprovou-se que um dos fatores que impulsionam os criminosos a agir dessa forma, por meio de computadores, é justamente a falta de normas vigentes que regulem a matéria do direito virtual. Com isso, eles se sentem seguros para cometer crimes, pois sabem que a chance de saírem impunes possui um percentual elevado contado a seu favor, enquanto que a população sofre por causa de um legislativo omisso, fraco e preguiçoso, que não se dá ao trabalho de criar mais dispositivos favoráveis a regulamentação do presente tema, ficando a legislação pátria presa ao passado e sofrendo as consequências do presente.

Mostrou-se importante destacar o fato da persecução penal ser outra ferramenta dotada de importância vital para o combate às infrações penais cibernéticas. A capacidade de investigar e descobrir provas que poderão ser levadas a juízo através da ação penal, tendo por base uma evidencia cibernética, e uma vez lá serem aceitas de fato pelo direito, é uma vitória que acende a esperança para dias melhores

Portanto, ficou claro ao término desse trabalho que o atual sistema jurídico brasileiro ainda é incapaz de se sustentar com as próprias pernas dentro do âmbito informático, sendo de extrema urgência a ampliação do conjunto de leis que disciplinem a matéria que já começou a se encaminhar para melhor, porém ainda

precisa de um maior aperfeiçoamento. No entanto, ao criar essas leis, o Brasil poderá acreditar, com segurança e embasamento, que ocorrerá uma queda significativa na taxa de criminalidade, devido a força vinculante que tais normas irão exercer sobre o país.

REFERÊNCIAS

BAUMAN, Zygmund. Globalização - As Consequências Humanas Globalização – Tradução de Marcus Penchel. Rio de Janeiro: Ed: Zahar, 1999;

BRASIL. Consulta eletrônica de jurisprudência. Outubro de 2015. Disponível em < http://stj.jusbrasil.com.br/jurisprudencia/9833/recurso-especial-resp-320958/inteiro-teor-100019170> Acesso em 28 de outubro de 2015.

BRASIL, Decreto-Lei nº 3.689 de 3 de outubro de 1941, Código de Processo Penal, Publicado no Diário Oficial da União em 3 de outubro de 1941.

BRASIL. Lei nº 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Publicado no Diário Oficial da União em 30 de novembro de 2012.

BRASIL. Lei nº 12.735 de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Publicado no Diário Oficial da União em 30 de novembro de 2012.

BRASIL, Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Publicado no Diário Oficial da União em 7 de dezembro de 1940.

CAPEZ, Fernando. Curso de Direito Penal – Parte Geral. Rev. Att. Volume 1. Edição 11ª. São Paulo: Saraiva, 2007;

CAPEZ, Fernando. Curso de Direito Penal – Parte Geral. Edição 19ª. São Paulo: Saraiva, 2015;

CASTELLS, Manuel. A sociedade em rede – Tradução de Roneide Venancio Majer. Volume 1. Ver. Amp. 8ª Edição. Editora: Paz e Terra;

GRECO, Rogério. Código Penal Comentado, Re. Amp. Att. 7ª edição. Rio de Janeiro: Ed. Impetus, 2013;

GRECO, Rogério. Curso de Direito Penal – Parte Geral, Volume 1. Rev. Amp. Att. 16ª Edição. Rio de Janeiro: Ed: Impetus, 2014;

MARQUES, Daniela Freitas. Elementos subjetivos do injusto. Belo Horizonte: Del Rey,2001;

MUÑHOZ CONDE, Francisco. *Introducción al derecho penal.* Barcelona: Bosch, 1975;

NUCCI, Guilherme de Souza. Manual de Direito Penal, Rev. Amp. Att. 10ª Edição. Rio de Janeiro: Ed. Forense, 2014;

SANTOS, Milton. Por uma outra globalização. 6ª Edição. Rio de Janeiro: Ed: Record, 2001;

SANZO BRODT, Luis Augusto; da consciência da ilicitude no direito penal brasileiro. Belo Horizonte: Del Rey, 1996.

WELZEL, Hans. *Derecho Penal alemán* – Tradução de Juan Bustos Ramirez e Sergio Yañes Peréz. Chile: Jurídica de Chile, 1987;

WESSELS, Johannes. *Derecho penal* – Parte General. Buenos Aires: De Palma, 1980;

ZAFFARONI, Eugenio Raúl. *Manual de derecho penal* – Parte General. Buenos Aires: Del Rey, 2000;

ZAFFARONI, E. Raúl; PIERANGELI, J. Henrique. Manual de direito penal brasileiro – Parte Geral. 2. ed. São Paulo: Editora Revista dos Tribunais, 1999.

AFFAIRS, Foreign. Brasil sofre com crimes cibernéticos. Brasil – Notícia, setembro de 2015. Disponível em < http://opiniaoenoticia.com.br/brasil/brasil-sofre-com-crimes-ciberneticos/> Acesso em 17 de novembro de 2015.

ALLENDE, Fernando. Fraudes aumentam na internet. G1 Olhar Regional, novembro de 2012. Disponível em <http://g1.globo.com/sp/santos-regiao/blog-do-allende/platb/2012/11/23/fraudes-aumentam-na-internet/> Acesso em 20 de setembro de 2015.

BRASIL, Childhood. Menos de 1% das vítimas de pornografia infantil na internet são identificadas. TJBA, outubro de 2014. Disponível em <http://www5.tjba.jus.br/infanciaejuventude/index.php?option=com_content&view=article&id=335> Acesso em 15 de outubro de 2015.

DIGITAL, Redação Olhar. Brasil é vice-campeão mundial em ranking de pirataria. Home – Últimas Notícias, fevereiro de 2015. Disponível em <http://olhardigital.uol.com.br/noticia/brasil-e-vice-campeao-mundial-em-ranking-de-pirataria/46905> Acesso em 10 de novembro de 2015.

JURÍDICO, Revista Consultor. Pornografia infantil é principal denúncia na internet. Consultor Jurídico – Crimes Virtuais, novembro de 2012. Disponível em <http://www.conjur.com.br/2012-nov-05/pornografia-infantil-domina-denuncias-crime-internet-brasil> Acesso em 25 de setembro de 2015.

JUSTIÇA, Superior Tribunal de. Página 585 – 20/02/2013. Ano de 2013. Disponível em <http://www.jusbrasil.com.br/diarios/51029781/stj-20-02-2013-pg-585> Acesso em 13 de novembro de 2015.

NET, Defesa. CERT.br divulga balanço das notificações de incidentes de segurança recebidas em 2013. Cobertura Especial – Cyberwar – Tecnologia, fevereiro de 2014. Disponível em < http://www.defesanet.com.br/cyberwar/noticia/14243/CERT-br-divulga-balanco-das-notificacoes-de-incidentes-de-seguranca-recebidas-em-2013/> Acesso em 01 de outubro.

SOUZA, Aline. Brasil é o quarto país em vítimas de crimes virtuais. EM Tecnologia, Novembro de 2013. Disponível em <http://www.em.com.br/app/noticia/tecnologia/2013/11/21/interna_tecnologia,472182/brasil-e-o-quarto-pais-em-vitimas-de-crimes-virtuais.shtml> Acesso em 07 de novembro de 2015.

TOZETTO, Claudia. Brasil teve mais de 28 milhões de vítimas de crimes virtuais em 2011, diz estudo. iG São Paulo Tecnologia, outubro de 2012. Disponível em <http://tecnologia.ig.com.br/2012-10-04/brasil-teve-mais-de-28-milhoes-de-vitimas-de-crimes-virtuais-em-2011-diz-estudo.html> Acesso em 10 de novembro de 2015.

ANEXO

Número total de downloads:

1º) Estados Unidos:2,1 bilhões
2º) Brasil: 1,2 bilhão
3º) Índia: 1,1 bilhão
4º) Austrália: 1,0 bilhão
5º) Reino Unido: 939,9 milhões
6º) Canadá: 704,1 milhões
7º) Filipinas: 578,0 milhões
8º) Rússia: 531,3 milhões
9º) Paquistão: 430,3 milhões
10º) Itália: 381,5 milhões

Possível Faturamento das empresas sem a pirataria:

1º) Brasil: US$ 99,6 bilhões
2º) Índia: US$ 64,3 bilhões
3º) Estados Unidos: US$ 62,6 bilhões
4º) Itália: US$ 28,2 bilhões
5º) Reino Unido: US$ 27,3 bilhões
6º) Filipinas: US$ 24,8 bilhões
7º) Paquistão: US$ 19,2 bilhões
8º) Rússia: US$ 18,3 bilhões
9º) Turquia: US$ 17,9 bilhões
10º) Grécia: US$ 17,6 bilhões