INSTITUTO VALE DO CRICARÉ

FACULDADE VALE DO CRICARÉ

CURSO DE DIREITO

JEFFERSON GONÇALVES SANTOS

SÃO MATEUS – ES

2015

JEFFERSON GONÇALVES SANTOS

CRIMES VIRTUAIS NO CONTEXTO HISTORICO

Monografia apresentada como pré-requisito para obtenção do título de Bacharel em ....., da Faculdade Vale do Cricaré, elaborado sob a orientação do Prof.

SÃO MATEUS – ES

2015

Agradeço primeiramente a Deus por me sustentar espiritualmente para poder estar aqui terminando minha graduação em Direito, somente ele sabe pelos sacrifícios e vitorias conquistadas ao decorrer desses 5 anos, agradeço meus amigos de turma que contribuíram com auxílios em vários casos, são muitos para tratar de todos nesse momento, mas em especial queria agradecer a certas pessoas que conheci durante esses 5 anos espero que todos conquiste seus sonhos porque todos já somos vencedores, enfim minha amiga do peito me ajudou muito durante esses anos Maria Virginia aprendi com ela que não existe dificuldades, que não se pode superar , Luiz Felipe um cara espetacular gente fina, que sempre alegra a turma com suas palhaçadas, Nicolas Cozer viajante nas aulas mas um amigo pra qualquer ocasião, Rhayza Bassi ela e uma mulher incrível cheia de loucuras mas uma amiga e tanto, por fim mas não esquecido agradeço demais aos meus pais por financiar meus estudos e sempre acreditar na minha capacidade principalmente a minha mãe e friso com todo orgulho a frase que ela sempre fala, " Por traz de um grande homem sempre há uma grande mulher" ou seja ela me deu a base do meu conhecimento e ate hoje aprendo com ela.

Por tanto nessa minha jornada conheci professores espetaculares, alunos e vivenciei muitas alegrias e comedia, a Faculdade Vale do Cricare e uma grande instituição de ensino espero que continue crescendo e se aperfeiçoando.

Dedico não somente esse trabalho como também os 5 anos que passou a minha mãe pela força incentivo e disposição porque sem ela não teria alçando meus objetivos e sonhos

“ QUE OS VOSSOS ESFORÇOS DESAFIEM AS IMPOSSIBILIDADES, LEMBRAI-VOS DE QUE AS GRANDES COISAS DO HOMEM FORAM CONQUISTADAS DO QUE PARECIA IMPOSSÍVEL.” (CHARLES CHAPLIN”)

JUSTIFICATIVA

O tema em questão que escolhi para minha conclusão do curso e um tema que venho pesquisando durante meu ano letivo todo, e um tema não novo ou com vertentes diversificadas, mas um tema de grande impacto para sociedade, para mim um tema que ira evoluir muito mais com trasnceder dos anos pois trata de um problema atualmente de grande proporcionalidade, os crimes virtuais ainda e um crime jovem no mercado Brasileiro nosso ordenamento júridico pátrio não consegue acompnhar a velocidade do crescimento do uso desta importante tecnologia, há muitos projetos de lei que aguardam serem sancionados enquanto isso os criminosos se aperfeiçoam. O resultado que comprova esse fato, e o grande número de casos de pessoas lesadas e de indivíduo responsabilizados por tais crimes cometidos nesse ambiente em questão.

SUMARIO.

INTRODUÇÃO

A presente pesquisa visa mostrar uma reflexão sobre o tema abordado.Atualmete, a internet se tornou indispensável para grande parte da população mundial, nesse ambiente e possível pesquisar, estudar, namorar e até trabalhar. Mas como tudo possui dois lados ,o bom e o ruim, a internet tambem possui o lado ruim, pessoas ultilizam esse ambiente para cometer crimes, com ituito de obter para si, vantagem em proveito dos outros internautas.

O grande coringa dessa problematica nesses delitos praticados nesse ambiente é a ausencia quase total de punibilidade pelo Estado, uma vez que, a criminalidade avançou mais rapidamente do que nossa legislação e as tecnicas para se chegar ao autor do crime ainda estão em fase de aprimoramento.

Esse crimes virtuais vem se tornando normal em nosso país, infelizmente , devido a lentidão do poder legislativo em tipificar essas modalidades de crimes, vem criando um clima de “terra sem lei” na internet, pois os criminosos sabem que suas identificações são quase impossíveis e mesmo que estes sejam identificados, não a lei que defina esses crimes a lentidão do judiciário ao punir essas condutas.

Por conta dessa facilidade o legislador precisa se ater aos fatos e criarem urgentemente tipificação para essas condutas, para retirar essa sensação de impunidade nesse ambiente vasto e cheio de informações pessoais dos internautas.

E de conhecimeto que possui projetos de lei em tramitação no Congresso Nacional, mas como e visto, essse orgão para aprovar novas leis, necessita de alguns anos de estudos para por em pratica.

1. PARECIMENTO DOS CRIMES VIRTUAIS.

Conforme o tempo fora passando surgiram ferramentas para facilitar a integração das etnias tanto ligando as nações como sua população, surgindo como exemplo os computadores para facilitar nosso dia a dia, tarefas de longo prazo termina quase instantaneamente com a utilização do mesmo, o computador e uma maquina que armazena e transforma em informações, toda disponibilizada em um ambiente que podemos denominar atualmente de nuvem ou seja na internet.

2. HISTORIA

Desde as grandes revoluções da humanidade até os dias atuais, o homem vem transformando a tecnologia de informação desenvolvendo novas máquinas e ferramentas que ligam os quatro cantos do mundo e torna as atividades do dia a dia mais fáceis .

Podemos dizer que citar um período que teve uma grande evolução, que ocorreu no período da Revolução Industrial, iniciando primeiramente no Reino Unido, por volta do século XVIII, trazendo grande avanço para modo de vida da população, com a criação das maquinas movida a carvão mineral principal fonte de energia para que as máquinas daquele período.[1]

As cidades começaram a se desenvolver, trabalhadores que trabalhavam de forma braçal e artesanal começaram a operar máquinas, as fabricas passaram a produzir cada vez mais, e novas invenções começaram a surgir, como navios e locomotivas a vapor, fizeram com que a circulação de mercadorias se tornasse cada vez mais rápido, fazendo com que as matérias primas chegassem mais rapidamente às pessoas, sendo assim começando a surgir de forma mais expressiva os inventores que iriam mudar o mundo, podendo citar grandes invenções, como por exemplo, a fotografia (1839), Telefone (1876), Luz Elétrica (1879), Televisão (1924), muitas invenções mudaram e mudam ate hoje o cotidiano de cada pessoa pelo mundo.

Deste modo o primeiro computador eletrônico foi o ENAIC (Eletronic Numerical Integrator and Calculator), criado por volta do ano de 1946, o qual fora desenvolvido por parte do exército norte-americano, pesando em media umas 30 toneladas, e media 5,50 metros de altura e 25 metros de comprimento e ocupava 180 m² de área foi construído sobre estruturas metálicas com 2,75 metros de altura e contava com 70 mil resistores e 17.468 válvulas a vácuo ocupando a área de um ginásio desportivo quando acionado pela primeira vez o ENAIC consumiu tanta energia que as luzes de Filadelfia piscaram.

Mas o primeiro computador com mouse e interface gráfica é lançado pela Xerox, em 1981, no ano seguinte a Intel produz o primeiro computador pessoal 286, do primeiro computador até os dias atuais a sociedade vive sempre se transformando se modificando na sociedade em que vivemos, evoluímos dos escritos em pedras para o papel, do uso da pena com tinta ao Código Morse, do e-mail para a videoconferência a com isso sempre estamos em evolução.

No meio dessas transformações surgiu a internet, na década dos anos 60 aproximadamente no ano de 1996, algumas universidades se uniram para desenvolver a ARPANET (Advanced Research Projects Administrantion – Administração de Projetos e Pesquisa Avançados) necessariamente a criação da internet foi para fins militares pois naquela época estava retrado o cenário da Guerra Fria.

Conforme o ilustra definição de Zanellato, a internet e um suporte (ou meio) que permite trocar correspondências, arquivos, ideias, comunicar em tempo real, fazer pesquisas documental ou utilizar serviços e comprar produtos.

Deste modo a Internet e uma rede de computadores, ligadas por rede menores, comunicando-se entre si, os computadores se comunicam por um endereço lógico, chamado de IP, onde possui inúmeras informações que são trocadas, surgindo ai um problema, pois há muitas informações pessoais que fica disponíveis na rede, ficando a disposição de milhares de pessoas que possuem acesso a internet, quando o usuário não disponibiliza tais informações , elas são procuradas por outros usuários que buscam na rede o cometimento de crimes, os denominados Crimes Virtuais.

Levy , em sua obra Cyberdémocracie: Essai de Philosophie Politique, já se encontrava um crescente aumento por parte das

> pessoas que utilizavam a internet, e previa um aumento gradativamente tendo em vista o desenvolvimento de novas tecnologias, interface de comunicação sem fio, e uso integrado de dispositivos portáteis.

Como se pode ver atualmente o desenvolvimento da tecnologia e diária todos os dias está em transformação, o pensamento de Levy estava certo atualmente a internet está disponível em vários dispositivo portáteis das mais diferentes formas, milhares de pessoas se interagem navegando pela internet do que vivendo o mundo real, mídias sociais, leitura de livros, videoconferência, jogos online, sites de relacionamentos dentre outros, em fim, a rede mundial de computadores é acima de tudo uma rede mundial de indivíduos, onde há grande movimentação de informações, portanto como há esse grande fluxo de informação ocorrendo uma necessidade de regulamentação jurídica para sanar litígios que venham ocorrer nesse ambiente, para isso precisa de planejamento e táticas que só pode ser feita em equipe e com pessoas qualificadas para estar dando suporte e segurança no ambiente virtual.

Esse ambiente pode ser chamado de terra sem lei pois e difícil de fiscalizar tantas trocas de informações, crimes virtuais vem se modificando e dificultando ao transcorrer do tempo, na década de 70, esses crimes era voltado ao sistema de segurança das empresas, com foco principal nas instituições financeiras, esses crimes eram feitos por pessoas aptas, especialistas em informática, atualmente o perfil dessas pessoas são usuários comuns qualquer pessoa que tenha um conhecimento mínimo sobre a informática, com acesso a internet pode praticar algum crime de informática, o usuário domésticos hoje possui um conhecimento vasto sobre manuseio de computadores no ambiente virtual.

3 CONCEITOS DE CRIMES VIRTUAIS.

São crimes cometidos por outrem através de computadores, praticados no ambiente virtual utilizando a internet, condutas de acesso não autorizado a informações, essas ações podem ser, interceptação de comunicações, modificações de dados, extravios de endereço, divulgação de pornografia infantil, terrorismo, entre outros.

Sendo esse tipos de crimes no ambiente virtual, difícil de se denominar para os delitos que se relacionam com a tecnologia, como, crimes de computação, delitos de informática, abuso de computador, fraude virtual, os conceitos não engloba todos crimes ligados a tecnologia, portanto, torna difícil tendo em vista que existem muitas situações complexas no ambiente virtual.

Apesar de muita divergência doutrinarias no que se concerne, a esses crimes, uma grande parte de doutrinadores conceitua-os como “crimes digitais” a denominação desse delitos deve ser feita de acordo com o bem jurídico protegido, conforme Fragoso:

> “A Classificação dos crimes na parte especial do código é questão ativa, e é feita com base no bem jurídico tutelado pela lei penal, ou seja, a objetividade jurídica dos vários delitos ou das diversas classes de intenções”.

Sendo assim a analise do crime primeiramente deve averiguar se o mesmo é um crime digital ou não, e aplica-lo ao tipo penal certo, tendo analogia ao Direito.

4. DA CATEGORIA DOS CRIMES VIRTUAIS.

Atualmente o numero de pessoas que utilizam a internet cresce rapidamente pela facilidade de manuseio, existindo em media inúmeros websites na internet, e a cada dia cresce o numero de homepages por dia, no ambiente virtual ultimamente encontramos de tudo como compras de qualquer tipo de bem como também, concluir curso obter formação acadêmica para trabalho profissional.

Deste modo os usuários do ambiente virtual estão expostos a diversos tipos de crimes, estes, dificilmente encontram soluções, lesando os usuários de boa fé que utilizam a internet.

A descoberta de um crime digital (virtual) de certa forma não e uma tarefa fácil pelo vasta informação que habita na nuvem, ou seja, ambiente virtual não obtendo uma forma ágil de encontrar os possíveis criminosos e aplicar de forma rápida uma possível punição pelo crime cometido, e para complicar ainda mais uma possível forma de combater esses crimes e o avanço extraordinário que a tecnologia obtém a cada dia, e a opinião dos doutrinadores mudando conforme segue a evolução tecnológicas.

As formas de variação dessas condutas que ora utilizam computadores como meio para cometer delitos, e também a casos que sem o uso do sistema informático não seria possível à consumação de determinados crimes.

Deste modo existem crimes que utilizam os computadores como meio para o cometimento de delitos no ambiente virtual, e casos em que sem o uso do sistema informático não seria possível a consumação de determinados crimes.

Tiedemann formulou em 1980 a seguinte classificação dos delitos informáticos:

> a)Manipulações: podem afetar o input (entrada), o output (saída) ou mesmo o processamento de dados;
>
> b) Espionagem: subtração de informações arquivadas abarcando-se, ainda, o furto ou emprego indevido de software;

> c) Sabotagem: destruição total ou parcial de programas;
> d) Furto de tempo: utilização indevida de instalações de computadores por empregados desleais ou estranhos.

Greco filho adota a seguinte divisão condutas inflacionárias no sistema informático, e , condutas contra outros bens jurídicos, segue observação do autor. (GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000)

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou.

O Dr. Vladimir Aras21 tem sua classificação da seguinte forma:(ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: . Acesso em: 18 mar. 2014.)

> a) uma primeira, onde estão substancialmente unidos pela circunstância que o computador constitui a necessária ferramenta de realização pela qual o agente alcança o resultado legal;

b) a segunda categoria de crimes do computador, poderia incluir todos aqueles comportamentos ilegítimos que contestam os computadores, ou mais precisamente, seus programas;

c) a última categoria deveria juntar todas as possíveis violações da reserva sobre a máquina. aqui entram em consideração as habilidades de colheita e elaboração de todo tipo de dados.

Em todas as classificações há de se considerar pontos em comum, algumas posições defende os meios eletrônicos como objeto protegido, outras, como meios eletrônicos como instrumento que pode danificar outros bens, esta está classificação torna-se uma das mais oportunas, tendo em vista que abarca mais opções a cerca das praticas. (CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2011.p.63)

5. Tipificação dos crimes virtuais ou cibernéticos.

Tais crimes são cometidos em um ambiente aonde e impossível de se prever o que pode ocorrer por ter uma vasta extensão de informações sendo trocadas a todos momento sem pausa ou interrupção, portanto e considerado como um crime fim, por sua natureza pois só ocorre em ambientes virtuais, com ressalva dos crimes cometidos por hackers, que suas condutas tem a probabilidade de se definir como estelionato, extorsão, falsidade ideológica, fraude e diversos outros equiparados, diante do exposto o comportamento criminoso pode ser virtual mais em algumas ocorrências, o crime não.

Para demonstrar com mais clareza tais situações, podemos expor como exemplo o julgamento pelo ministro Sepúlveda Pertence, do STF, do habeas corpus (7668/PB 22-9-1998) sobre crime de computador.

EMENTA: "Crime de Computador": publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte.

> 1. O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" - ao contrário do que sucede, por exemplo, aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realiza- lá pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum. (SEPÚLVEDA, 1998, p. 3).

Portanto a internet surge como facilitador, principalmente pelo anonimato que ajuda o criminoso a cometer vários tipos de delitos e ficarem impunes, as questões ao conceito do crime sobre, delito, ato ou efeito são as mesmas, quer que sejam aplicadas para o Direito Penal ou para o Direito Virtual, a vertentes atuais trazem a tona ao respeito da territorialidade e á investigação, bem como a tipificação de algumas modalidades de possuir seu titulo penal próprio.

O Principio da territorialidade e a que possui maior importância pois, com sua solução ficaria fácil distinguir a competência , pois ainda não há uma legislação especifica tornando escassa as modalidades dos delitos cometidos em tais ambientes, na ausência de legislação, aquele que praticou um algum crime virtual deverá ser julgado dentro do próprio Código Penal. Podendo dar como exemplo, um determinado indivíduo de uma empresa X foi pego pela gerente extraviando, dados de clientes, dados estes que estavam salvos no computador da empresa, tal individuo será acusado por ter infringido o artigo 163 do Código Penal, que é destruir, inutilizar ou deteriorar coisa alheia: pena – detenção, de um a seis meses, ou multa.

Mesmo sem uma lei especifica os crimes virtuais podem ser julgados pela lei brasileira. Como crimes citados a seguir.

a) Pirataria: Copiar dados em CDs, DVDs ou qualquer base de dados sem prévia autorização do autor é percebido como pirataria em conformidade com a Lei 9.610/98. De acordo com o art. 87 da referida lei, "o titular do direito patrimonial sobre uma base de dados terá o direito exclusivo, a respeito da forma de expressão da estrutura da mencionada base". As penas possuem uma variação de 2 meses a 4 anos, podendo haver aplicação ou não de multa, a estar sujeito se houve reprodução parcial ou total, venda ou disponibilização ao público via cabo ou fibra óptica; b) Dano ao patrimônio: Previsto no art. 163 do Código Penal. O dano pode ser simples ou qualificado, sendo estimado qualificado quando "o dano for contra o patrimônio da União, do Estado, do Município, de empresa concessionária de serviços públicos ou de sociedade de economia mista". Nota-se que para ser qualificado, o objeto do dano deverá ser da União, do Estado, do Município, de empresa concessionária de serviços públicos ou de sociedade de economia mista, podendo ser aplicado, por exemplo, àqueles crimes de sabotagem dentro de repartições públicas. A mesma lógica é utilizada quando se trata de vírus, por ser considerado como tentativa (perante comprovação) de dano. A punição para dano simples é de detenção, de um a seis meses, ou multa. Já para dano qualificado, a pena prevista é detenção de seis meses a três anos e multa; c) Sabotagem informática: A sabotagem, no tocante aos termos econômicos e comerciais, será a invasão de determinado estabelecimento, objetivando prejudicar e/ou roubar dados. Segundo Milton Jordão, "versa a sabotagem informática no acesso a sistemas informáticos visando a extinguir, total ou parcialmente, o material logo lá contido, podendo ser cometida por meio de programas destrutivos ou vírus". A lei apenas prevê punição de 1 a 3 anos de prisão e multa, porém não inclui a sabotagem informática em seu texto; d) Pornografia infantil: O art. 241 do ECA (Estatuto da Criança e do Adolescente) veda "apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, de modo inclusivo na rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito abrangendo criança ou adolescente". Esse tipo de conduta é denominado como exclusivamente crime virtual, pois ele só ocorre única e exclusivamente através do uso da internet. A punição para quem contravenha este artigo do estatuto é de detenção de 2 a 6 anos e multa; e) Apropriação indébita: O Código Penal faz

referência apenas à apropriação indébita de bens materiais, como por exemplo CPU, mouse e monitor, sendo afastada a forma de apropriação de informações. Não obstante, se a apropriação ocorrer através de cópia de software ou de informações que legalmente concernem a uma instituição, podem-se aplicar punições por pirataria. A pena para apropriação indébita está prevista no artigo 168 do referido código, sendo de reclusão de 3 a 6 anos e multa para quem praticar ato fraudulento em benefício próprio; f) Estelionato: Nesta tipificação de crime, o Código Penal pode ser aplicado de acordo com o seu artigo 171, de forma que o crime tenha sido executado plenamente. Segundo Da Costa, o estelionato "consuma-se pelo alcance da vantagem ilícita, em prejuízo alheio. É também admissível, na forma tentada, na sua amplitude conceitual, porém é de ser buscado o meio utilizado pelo agente, uma vez que impunível o meio inidôneo". A pena é de reclusão de 1 a 5 anos e multa; g) Divulgação de segredo: O Código Penal nada menciona em referência caso o segredo seja revelado via computador, sendo tratado da mesma 17 forma que se fosse divulgado por documento, por se tratar de uma forma de correspondência; h) Crimes contra a liberdade individual: São os tipificados no Código Penal como crimes de ameaça (artigo 147), de inviolabilidade de correspondência (artigos 151 e 152), de divulgação de segredos (artigos 153 e 154) e de divulgação de segredos contidos ou não em sistemas de informação ou bancos de dados da Administração Pública (artigo 153, § 1º-A). O crime de interceptação telefônica e de dados, que tem como bem jurídico tutelado os dados, pois o que se tem como objetivo é proteger a transmissão de dados e restringir o uso dessas informações para fins fraudulentos. O tipo penal citado protege igualmente o tema da inviolabilidade das correspondências eletrônicas, o que já é garantido na própria Magna Carta(Constituição Federal de 1988), no seu artigo 5º, XII, assim como ocorre a sua remissão ao paragrafo art. 1º, parágrafo único da Lei nº 9.296, de 24 de julho de 1996, onde regula o inciso XII, parte final já citado. XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução

> processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática. i) Difamação, injúria e calúnia: São os crimes de calúnia (artigo 138), de difamação (artigo 139) e de injúria (artigo 140). Os criminosos são estimulados pelo quesito do anonimato, podendo ocorrer em locais virtuais tais como chats, blogs, pelo envio de spams e por meio de publicações em homepages, entre outros meios de postagem eletrônica. Outro exemplo a ser citado que pode acontecer nas redes sociais, é se alguém divulgar informações falsas que lesem a reputação de outra pessoa ofenda a dignidade do outro ou de má-fé acusem alguém de criminoso, desonesto ou perigoso; j) Falsa identidade: Sucede quando alguém apresenta nome ou dado diverso do qual consta em seu documento de identificação, tais como idade, estado civil, sexo e outras características com o desiderato de conseguir alguma vantagem ou prejudicar outra pessoa. O crime do artigo 151 do CP, denominado como crime de violação de correspondência, é um tipo inteiramente aplicável à conduta de interceptação e violação de e-mails, pois os tipos previstos na Lei 6.538/78 são inaplicáveis, pois essa dispõe sobre os serviços postais explorados pela União, por meio de empresa pública vinculada ao Ministério das Comunicações. Neste tipo, o bem jurídico tutelado é a integridade dos Serviços Postal e de Telegrama nacionais, devendo a correspondência se dar por meio da via postal ou por telegrama, proposições nas quais o e-mail não se encaixa. (OLIVEIRA, 2002, p. 73).

Essas modalidades citadas de crimes virtuais demonstra como está ultrapassada a legislação que regula esse tipo de delito para os dias atuais, nosso sistema judiciário não acompanhou a evolução de tais crimes deixando as famosas “brechas” na lei que sempre beneficiam os infratores.

Uma modalidade de crime que vem se tornando muito comum no ambiente virtual é o envio de e-mail simulando ser de algum órgão estatal da União conhecido, como o caso da Receita Federal, TSE (Tribunal Superior Eleitoral), na qual o individuo tem o objetivo enganar, enviando uma mensagem declarando que

há uma pendência como órgão em que a vitima deve clicar no link para obter o acesso do boleto ou ate mesmo para mais detalhes.

Ao clicar no link, a vitima e redirecionado para uma pagina que instala sem permissão um Ransomware um tipo de Spyware, programa espião que rouba informações e danifica seu computador, o criminoso começa receber dados sigilosos, outra modalidade bastante praticada que utiliza dos mesmo artifícios do e-mail, mas, não usa remetentes de órgãos estatais sim instituições financeiras.

Há crimes cujo intuito é demonstrar a fragilidade de sistemas, como é o caso das recentes invasões às páginas de órgãos oficias. Existe uma infinidade de crimes muito ainda nem possuem um modus operandi conhecido e outros ainda nem foram descobertos.

> **Spyware** consiste em um programa automático de computador, que recolhe informações sobre o usuário, sobre os seus costumes na Internet e transmite essa informação a uma entidade externa na Internet, sem o conhecimento e consentimento do usuário.
>
> Diferem dos cavalos de Tróia por não terem como objetivo que o sistema do usuário seja dominado, seja manipulado, por uma entidade externa, por um cracker.
>
> Os spywares podem ser desenvolvidos por firmas comerciais, que desejam monitorar o hábito dos usuários para avaliar seus costumes e vender este dados pela internet. Desta forma, estas firmas costumam produzir inúmeras variantes de seus programas-espiões, aperfeiçoando-o, dificultando em muito a sua remoção.
>
> Por outro lado, muitos vírus transportam spywares, que visam roubar certos **dados confidenciais** dos usuários. Roubam dados bancários, montam e enviam registros das atividades do usuário, roubam determinados arquivos ou outros documentos pessoais.
>
> Com frequência, os spywares costumavam vir legalmente embutidos em algum programa que fosse shareware ou freeware. Sua remoção era por vezes, feita

quando da compra do software ou de uma versão mais completa e paga.

Traduzindo ao pé da letra, Spyware significa "aplicativo ou programa espião"

Os **Ransomwares** são softwares maliciosos que, ao infectarem um computador, criptografam todo ou parte do conteúdo do disco rígido. Os responsáveis pelo software exigem da vítima, um pagamento pelo "resgate" dos dados
. Ransonwares são ferramentas para crimes de extorsão e são extremamente ilegais. O PC Cyborg Trojan, foi o primeiro código de um ransomware conhecido. Nomes de alguns Ransomwares conhecido: Gpcode-B e PGPCoder. fonte(https://pt.wikipedia.org/wiki/Spyware acesso 2014).

6 DOS CRIMES VIRTUAIS PRÓPRIOS E IMPRÓPRIOS.

Os crimes virtuais próprios são aqueles que utilizam o sistema informático do computador (a rede) como ferramenta, para meio de execução do crime, que não só esta ligada, somente na invasão de dados não autorizados, mas em toda interferência de dados informatizados como, por exemplo, invasão de dados armazenados em computador, seja no intuito de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o software ou hardware do periféricos(saídas ou entradas), deixando evidenciado para alguns doutrinadores como Dámasio de Jesus:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. (DAMÁSIO, 2003).

Da mesma forma são os crimes virtuais impróprios utilizam do computador como meio de praticar condutas ilícitas, mas com uma diferença, não e necessário o sistema informático para cometer tais crimes seus componentes são dispensável para concretização do ato criminoso que pode se dar de outras formas e não necessariamente pela informática como no caso da pedofilia.

Como o ilustre Damásio discorre:

> [...] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não computacionais ou diversos da informática. (2003).

Greco Filho (2000) adere à seguinte divisão: condutas perpetradas contra um sistema informático e condutas perpetradas contra outros bens jurídicos. Segue a observação do autor.

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticadas por meio da internet e crimes ou ações que merecem incriminação, praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, como, por exemplo, o homicídio. O crime, no caso, é provocador, do resultado morte, qualquer que tenha sido o meio ou a ação que o causou. (2000, p. 3).

Conforme fora analisado, as classificação são questionáveis precisando de uma analise a fundo sobre algumas posições que ora atribui os meios eletrônicos como objeto protegido (bem jurídico), ora meios eletrônicos como meio de se atingir outros bens.

7 ASPECTOS PENAIS DO SUJEITO ATIVO E PASSIVO NOS CRIMES VIRTUAIS

A comprovação do sujeito nos crimes cometidos na internet e extremamente difícil, uma vez que para identificar tal sujeito seja quase impossível fazendo com que seja traçada um perfil para tais indivíduos denominados de hacker entende-se como: “[...] pessoa que usa seu conhecimento técnico para ganhar acesso a sistemas privados”[1]. São pessoas com conhecimento vastos e únicos sobre informática, podendo haver conhecimento também positivo não somente negativo, pois eles ajudam a criação de ferramentas para ajudar no manuseio do sistema.

Deste modo o hackers em si e um gênero, e as espécies tendem a se variar, uma espécie a ser citada são os crackers, criado em 1985 por hackers que discordavam do termo generalizado pois a imprensa definia técnicos em Informática ou usuários de computadores que cometessem ações ilegais ou que causassem transtornos para outras pessoas. Podem ser citadas também outras espécies de hackers, como os, lamers chamados de wannabes ou script-kid, são pessoas que atuam em pequenos atos não trazendo tanto perigo para outros usuários do ambiente virtual, considerados leigos pelos hackers podendo também citar os phreakers, que atuam em crimes específicos direcionados para área de telecomunicações e os defacers, esses registram sua marca ao invadirem paginas na internet e desfigura-las.

Diante do exposto, podemos traçar os perfis dos criminoso e imaginar como aonde, que eles agem e o que pretende fazer de uma forma universal, porém não a como identifica-los antes ou ate mesmo quando cometem condutas ilícitas, desta forma torna muito difícil descobrir o sujeito ativo sabemos ate como identificar e endereço falsos ou ate mesmo copiados para retardar a rapidez da identificação.

[1]Disponível em: < http://michaelis.uol.com.br/moderno/ingles/definicao/inglesportugues/hacker%20_455080.html>. Acessado em: 27.nov.2014.

Já no caso do sujeito passivo o referencial especifico seria aquela pessoa que está sendo prejudicada, assim de forma genérica, pode se garantir que será realizada

através de uma pessoa física ou jurídica ou uma entidade titular , publica ou privada. Portanto o sujeito passivo da violação penal pode ser qualquer pessoa normal, ou jurídica, o que e de se espantar e que a maioria dos crimes cometidos no ambiente virtual não e divulgado em rede, pela não dispersão das devidas informações ou pela pura simplesmente falta de haver a denúncia concreta, podendo ser citado as grandes empresas que evitam divulgar sobre prováveis ataques virtuais sofridos, para não demonstrarem fragilidade quanto sua segurança no sistema operacional.

No caso de pessoas físicas, que por falta da punibilidade aos infratores e falta de uma estrutura de denuncia, as vitimas acabam não denunciando assim facilitando bastante a proliferação das diversas espécies de crimes virtuais.

8.TIPOS DE CRIMES REALIZADOS NO AMBIENTE VIRTUAL.

As condutas criminosas realizadas nesse ambiente tem uma tarefa difícil que e analisada rigorosamente por ser complicado de ser verificar onde o criminoso se encontra realmente, nesse ambiente não há barreiras para impedir a punição devida de seus praticantes. Esses delitos cometidos nesse ambiente ocorrem também no ambiente cotidiano do nosso dia a dia ou seja os crimes possui algumas peculiaridades, o que faz necessário uma adequação quanto a sua tipificação penal, veremos adiante crimes da virtuais e outros já existente que passaram a ser executados virtualmente.

8.1 FRAUDE VIRTUAIS

Esses tipo de crime no território brasileiro está habitual, em sites , provedores, e-mail ,tentativas de fraudes com objetos financeiros envolvendo o uso de cavalo de Tróia, notificação de direito autorais possíveis violações dentre outras.

O criminoso pratica uma conduta de invasão, modificação ou alterando,ou seja, uma possível adulteração em programas, dados eletrônicos tirando proveito .

A fraude consiste em um dado não solicitado que pode ser feito através de um e-mail não solicitado que passa uma informação de uma grande instituição conhecida que as vezes a pessoa ate tem algum vinculo com essa tal instituição, exemplo banco, procurando induzir o usuário ao fornecimento de dados pessoais, antes esse tipo de mensagem induzia o usuário a abrir paginas fraudulentas na Internet. Nos dias atuais eles utilizam tal artifícios para fazer com que o usuário instale um programa malicioso um possível spyware que ira sem sua permissão extrair dados de contas, fotos, imagens, vídeos, contas de facebook, hotmail. Conforme Paulo Marco, o mesmo define as fraudes virtuais como:

> Fraudes eletrônicas – invasão de sistemas computadorizados e posterior modificação de dados, com o intuito da obtenção de vantagem sobre bens, físicos ou não, por exemplo, a adulteração de depósitos bancários, aprovações em universidades, resultados de balanços financeiros, pesquisas eleitorais, entre outros. (Crimes de computador e segurança computacional. Campinas, SP: Ed. Millennium, 2005.p.60).

As fraudes eletrônicas crescem, cada vez mais e nosso ordenamento jurídico decai a cada ano, sendo tipificado à modalidade de furto mediante a fraude (artigo 155 do Código Penal), a qual caracteriza pelo envio de um e-mail falso com a intenção de capturar dados pessoais de usuários ate mesmo dados de contas bancarias mediante a instalação de um spyware em seu computador.

Este tipo de crime há duas vertentes de origens: Interna – praticadas por empregado ou terceiro que se encontra dentro do local a ser fraudado; Externa – o criminoso não possui vinculo com local que será fraudado, mas isso não significa que o agente não possa um dia ter tido relação co a vitima.

O usuário é induzido a fornecer dados importantes, na maioria das vezes em paginas duvidosas, ou ate mesmo em rede sociais, tentam roubar dados pessoais. Um crime que ocorrer diariamente é o furto de dados, este crime esta conceituado o artigo 155 do Código Penal como sendo “subtrair para si ou para

outrem, coisa alheia móvel”, a questão é que se poderia se enquadrar o furto de dados como sendo furto conforme o artigo 155 supra citado porque tendo em vista que tal conduta não se configurar subtração pois ele pode apagar os dados ou ate mesmo, levar os mesmo mediante cópia e não elimina-los ou seja não configurando crime.

8.2 ESTELIONATO

Este crime está presente tanto no ambiente virtual como fora conforme artigo 171 caput do Código Penal o ramo do direito virtual e uma sistemática nova, alguns autores separam as condutas delituosas em face dos computadores, como elemento físico, e contra os dados os quais encontram neles.

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa. (vade mecum 2014 sariva)

No caso da aplicação do estelionato no ambiente virtual seria a conduta de induzir ou manter a vitima em erro, e com isso, obtendo vantagem ilícita, são varias as formas de estelionatos praticadas nesse meio difícil e tipificá-las como estelionato, dessa forma o legislador previu, como meio executório a fraude com objetivo de persuadir a vítima a erro.

Tais criminosos utilizam e-mails com conteúdo criptografados de sites verdadeiros, os usuários acabam acessando essa pagina basta clicar e pronto, aparece uma copia idêntica do site original que persuadi o usuário a preencher desta forma distribui suas informações para o criminoso. Um exemplo claro desse tipo de conduta são e-mails, que chegam com remetente de Banco pedindo para entrar em contato por sites para saber sobre informações de empréstimos e acaba preenchendo um formulário falso que rouba seus dados e transfere os valores disponíveis em sua conta, para sua posse.

Uma maneira de se proteger e instalando um antivírus adequado, configurado que exclua e-mails tidos como possíveis ataques a dados de seus

computador, á exclusão pode ser feita antes de ser recebida no computador, ou, efetuar a configuração de segurança do *firewall,*tal ferramenta servi como uma barreira para bloquear possíveis intrusos. O Firewall e o antivírus funcionam no monitoramento das portas de entrada, saída de pacotes de dados.

8.3 INVASÃO DE PRIVACIDADE

Com avanço da tecnologia na estrutura mundial de informática, pessoas passam a disponibilizar muitas informações na rede, desde informações que são lançadas em sites específicos, até perfis de rede sociais o uso extraordinários dessa ferramenta possibilita realizar inúmeras questões, podendo trazer penalidades para o usuários tanto pessoas físicas quanto pessoas jurídicas, que sem autorização devida propagam um certo tipo de material que muitos desejam ter , essa privacidade constitui um limite natural ao direito à informação.

Diante do exposto podemos observar que a internet por ser uma rede de troca de informação grande acaba sendo alvo de pessoas que utilizam da mesma de forma errada para tirar proveito para si próprio, ou para atingir outras pessoas, o que se procura na realidade é resguardar o cidadão com relação aos seus dados que estão disponibilizados na rede, sejam aqueles disponível em órgão públicos, entes privados, ate mesmo porque os dados pessoais dos cidadãos não podem ser tratados como mercadoria, tendo que e dever do Estado resguarda os direitos da pessoa, e o cidadão deve por si só requisitar as empresas, que seus dados, sejam armazenados e guardados em segurança não deixando exposto na rede virtual.

8.4 CRIMES CONTRA HONRA

Tais crimes estão previsto em lei vide artigos 138, 139 e 140 do Código Penal, comum ver eles no ambiente virtual já que há uma grande quantidade de usuários que navegam na rede.

Tipificar a honra e fácil pois são qualidades de um individuo que seja, física, moral, intelectual, no que se diz respeito a sua autoestima, a honra pode se dizer que e um patrimônio que cada pessoa tem e deve ser protegido, tendo invista que

seu atributo como pessoas em sociedade fará uma escolha,que seria definir a sua aceitação ou não para viver em um determinado grupo social.

Um dos crimes cometidos contra honra seria o crime expresso no artigo 139 do Código Penal, nele contem a seguinte texto, “difamar alguém, imputando-lhe fato ofensivo à sua reputação”, tal crime vai contra a honra objetiva da pessoa algo que venha constranger a reputação da pessoa realizada por terceiros. Esse crime praticado na internet nas mais diversas formas, seja por e-mails enviados a pessoa diversas ou publicado em redes sociais ofensas a sua honra objetiva, nesse crime a pessoa jurídica não poderá ser o sujeito passivo, pois o artigo 139 do CP e direcionada a pessoa humana, mas quando , praticado mediante imprensa, pode-se aplicar a Lei n° 5.250/67 – Lei de Imprensa.

Portanto basta ter, a perpetuação de algo que venha ferir sua reputação perante a sociedade, que o crime irá se consumir, por exemplo, quando alguém espalhar um ato ofensivo a uma pessoa pelas redes sociais, e os usuários presentes fizeram a leitura do fato ofensivo.

Outro crime contra honra e o de Calunia previsto no artigo 138 do Código Penal, que traz em seu texto o seguinte argumento, “Caluniar alguém, imputando-lhe falsamente fato definido como crime” nesse crime a honra da vitima e abalada, ou seja sabe-se que a imputação e falsa, assim, abala sua reputação mediante a sociedade.

O crime de Injúria consiste na propagação de uma mentira negativa sobre a qualidade da vítima por um terceiro, estando ligadas a atributos morais, intelectuais, físicos, afetando de forma significativa a honra subjetiva da vítima, o tipo penal desse crime tem previsão legal no artigo 140 do Código Penal: “ Injuriar alguém, ofendendo-lhe a dignidade ou o decoro”.

8.5 ESPIONAGEM ELETRÔNICA.

Este tipo de crime vem crescendo, pois a quantidade de pessoas acessando ambiente virtual e empresas se alocando e divulgando seus produtos nesse ambiente faz com que, fiquemos mais conectados a rede de computadores, inclusive ela grande disseminação de redes sociais grupos que liga pessoas de

vários países e regiões,tudo isso faz com que necessitamos cada vez mais de segurança e proteção de informações nesse ambiente, seja, prevenindo, seja monitorando.

Há várias formas de espionagem eletrônica, mas a que se destaca mais no ambiente virtual e a chamada Sigint (signals intelligence), responsável por interceptar e decodificar dados, tradução e analise de mensagens por um terceiro, pensava-se que a espionagem seria feita por empresas para burla o sistema de segurança das concorrentes com fim de desmoralizar a concorrência, mas e ao contrario pessoa da empresas envolvidas permitem o acesso ao ambiente, ou agirem como coletoras ou causadoras de sabotação.

Portanto o crime de espionagem eletrônica não possui uma tipificação penal exata, sendo utilizada os artigos 154 e 184 – " crime de violação de segredo profissional e crime de violação de direito autoral.

> Violação do segredo profissional
>
> Art. 154 – Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
>
> Pena – detenção, de três meses a um ano, ou multa.
>
> Parágrafo único – Somente se procede mediante representação
> (vade mecum saraiva 2014 p. 541)
>
> 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. (vade mecum p. 546).

Assim deve-se haver um investimento em segurança no ambiente virtual pela empresa para assegurar as informações pessoais dos seus clientes, tendo como maior dificuldade seria a ameaça interna pela grande dificuldade em encontrar o agente causador pelo fato de ser interno e a disponibilidade de recurso para camuflar seus atos e apaga os registros não deixando rastro para que possa ser apanhado.

Patrick Peck salienta que para combater esse tipo de crime devendo ser aplicada medida em três níveis: Físico, Lógico e Comportamental, devendo considerar seguintes matérias: (Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.385 – 386)

> a) Criação de controles mais rígidos na área de Recursos Humanos, pois a maioria dos Insiders possui

um histórico de violação a políticas corporativas e/ou prática de crimes, mas há também informações sobre atividades extratrabalho, como família e mesmo Orkut e Blog da pessoa que revelam muitas vezes o que está acontecendo;

b) Fazer segregação de função, mas rever com freqüência os acessos e, se possível, amarrar não apenas o login do usuário com uma senha, mas também a uma identidade de máquina; c) Criação de equipes com atividades especificas, a fim de que determinada tarefa que envolva confidencialidade ou risco não fique atrelada a somente um indivíduo, e sim a um grupo, a fim de cada um exerça uma fiscalização sobre o outro;

d) Uso de software de monitoramente eletrônico, pois vigiar é essencial;

e) Desenvolvimento e aplicação de Políticas de segurança da Informação;

f) Regulamentação do uso de dispositivos móveis, com bloqueio de portas USB, por exemplo, restrições de uso de determinadas mídias;

g) Execução de ações de conscientização que englobem todos os funcionários, terceirizados e gestores (de nada adianta chefes não serem conscientizados, pois cabe a eles dar o exemplo;

h) Criação de um canal de denúncia anônimo; i) Preparar o terreno para a adequada coleta das provas. Nesse sentido, é fundamental guardar os logs da rede, guardar os emails originais (eletrônicos), dados de acesso entre outros; j) Seguir o “princípio do menor privilégio”, ou seja, garantir acesso ao que é estritamente necessário;

k) Ter classificação da informação bem definida e aplicada;

l) Realizar testes de vulnerabilidade e simulações de Black bag.

Quando e realizada uma conduta regularizada por normas a tendência e de obter um controle mais eficaz para que possa reduzir a capacidade de exerce um ato de espionagem, aumentando assim a possibilidade de descobrir o infrator, seja por meio de evidências material ou pelo uso de pericia digital.

8.6 CRIMES CONTRA PROPRIEDADE INTELECTUAL.

Nesse crime veremos também o artigo 184 do Código penal como tipificação, o bem jurídico que procura ser preservado é o direito autoral, os reflexos que a obra ira gerar, ou seja os direitos conexos à mesma.

Na no ambiente virtual há uma grande carência de tipificação de condutas impróprias, e também, ausência de fiscalização, e territorialidade, permitindo assim uma grande quantidade de circulação de informação, sem as devidas regulamentações, assim o acesso de qualquer um a qualquer documento ocorrendo varias copias de materiais disponibilizados, onde muitas das vezes o criador e desrespeitado, tendo em vista que não há qualquer respaldo aos seus direitos como autor da obra que está sendo duplicada.

O artigo 184 e 186 do Código Penal versa:

> 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. Art. 186 - Procede-se mediante:

> I – queixa, nos crimes previstos no caput do art. 184; II – ação penal pública incondicionada, nos crimes previstos nos §§ 1º e 2º do art. 184; III – ação penal pública incondicionada, nos crimes cometidos em desfavor de entidades de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo Poder Público; IV – ação penal pública condicionada à representação, nos crimes previstos no § 3º do art. 184.

Também não a uma tipificação exata quanto a violação de programas de computadores, somente se limitando a obras fonográficas e cópias de obras intelectuais, ademais, o artigo 12, caput, da Lei n° 9.609/98, versa sobre os direitos do autor de programa de computador dependendo da violação para meios de divulgação sem autorização, pra fins de comercio sem as devidas autorização do autor sobre aquela disseminação.

> Art. 12. Violar direitos de autor de programa de computador: Pena - Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena - Reclusão de um a quatro anos e multa.
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
> § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:

> I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
>
> II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo. § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

Um exemplo de como se precaver dessas situações são os Softwares possuem forma de compartilhamento de duas formas primeira as Livres que pode ser atualizada e modificada por vários autores, esse tipo e o gratuito o usuário pode e livre para fazer o que desejar, e os Softwares que possui bloqueio para copias e atualizações não podendo assim modificar o mesmo não podendo efetuar a distribuição podendo optar pela distribuição desde que seja paga pela cópia.

O termo utilizado para tipo de conduta se chama pirataria que, se consuma numa cópia não autorizada, feita por usuários ou até mesmo empresas, há vários tipos de pirataria como veremos a seguir.

A Pirataria de Usuário Final – são aquelas cópias adicionais realizadas sem autorização, efetuadas eventualmente por indivíduos que por exemplo copiam um software comprado de uma empresa onde laboram.

Venda não autorizada – acontece quando vendedores distribuem cópias de um único pacote para diversas pessoas, ou quando copiam sem autorização de um software original que deveria.

Pirataria na Internet – Possíveis sites falsos que disponibilizam downloads gratuito de software, distribuindo cópias falsas, ou desviadas.

Cracking – Toda vez que houver a quebra de acesso de um software original protegido.

Portanto podemos observar que há grande necessidade de proteção da propriedade intelectual, pois e um grande valor para sociedade, dessa forma podemos obter a seguinte conclusão e dever da lei proteger determinada obra intelectual para que, o individuo possa gozar dos benefícios resultante da exploração de suas criação, impondo um enorme desafio aos operadores do Direito.

8.7 DANOS INFORMÁTICOS.

O dano informático não e tipificado claramente em lei temos sim um artigo o 163 do Código Penal versa, destruir inutilizar ou deteriorar coisa alheia: Pena – detenção de um a seis meses, ou multa.

Em seu texto o legislador não pensou de forma clara no ambiente virtual sim no ambiente físico protegendo a coisa, seja ela móvel ou não, o seja material, não levando a consideração a conduta do dano informático à época da elaboração do artigo supracitado se encaixando perfeitamente, por exemplo, a danos que possa ser causado em dispositivos como CDs-Rom, diquetes, pen drives, hard disk, enfim nos equipamentos informáticos.

Portanto atualmente se alguém praticar um dano informático em terceiros seja, ela culposa ou dolosa não haveria punição concreta no código penal recorrendo assim ao dispositivo da legislação Cível.

Existe atualmente o Projeto de Lei 84/99, o qual se aprovado, o art. 163 do Código Penal passará a ter a seguinte redação:

> Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio. Parágrafo único. Nas mesmas penas incorre quem apaga, altera ou suprime os dados eletrônicos alheios sem autorização ou em desacordo com aquela fornecida pelo legítimo titular.

Dessa forma o legislador abarca não somente as coisas tangíveis sim também as intangíveis também, certamente irá resolver a questão no que diz a

respeito dos danos informáticos sanando a lacuna que havia no artigo 163 do Código Penal Brasileiro.

8.8 PORNOGRAFIA INFANTIL.

Atualmente o aumento da pornografia infantil esta sem rédeas não havendo uma forma de conter tal fato com a evolução da internet e massificação de redes social e as conexão com o mundo, torna ainda mais difícil controlar o Brasil está entre os 5 grandes países com índice alarmante de pornografia infantil.

O elemento subjetivo dessa conduta e o dolo, quando a finalidade do criminoso e de expor ao publico, ou comercializar, não e necessário ter acesso ao material para que o crime possa ser consumir, basta a disponibilização do material e a possibilidade de que alguém venha a ter acesso ao mesmo.

Devemos fazer uma distinção da Pornografia Infantil,e a Pedofilia Infantil, a pedofilia e quando há um sentimento erótico daquele adulto com uma criança ou adolescente, diferente da pornografia infantil não há um sentimento sim a comercialização de fotografias e vídeos eróticos envolvendo crianças e adolescentes.

O Estatuto da Criança e o Adolescente, Lei 8.069/90, dita penalidades para o pedófilo e aquele que divulga ou comercializa imagens, vídeos envolvendo criança em cenas de sexo.

> Art. 240 – Produzir ou dirigir representação teatral, televisiva ou película cinematográfica, utilizando-se de criança ou adolescente em cena de sexo explícito ou pornográfica: Pena – reclusão de 1 (um) a 4 (quatro) anos, e multa. Parágrafo único. Incorre na mesma pena que, nas condições referidas neste artigo, contracena com criança ou adolescente.
>
> Art. 241 – Fotografar ou publicar cena e sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão de 1 (um) a 4 (quatro) anos. (Vade Mecum Saraiva 2013 p. 1041)

O crime tipificado no artigo 241 e entendido como norma aberta, e o Supremo Tribunal Federal já entende que sua aplicação também se consuma mediante o ambiente virtual, no ato de sua publicação, divulgou e pronto o delito está consumado vejamos o entendimento da Colenta Primeira do STF:

> **ESTATUTO DA CRIANÇA E DO ADOLESCENTE** – Art. 241 – Inserção de cenas de sexo explícito em rede de computadores (Internet) – Crime caracterizado – Prova pericial necessária para apuração da autoria. “Crime de computador”; publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores atribuída a menores – Tipicidade – Prova pericial necessária à demonstração da autoria – Habeas Corpus deferido em parte. 1. O tipo cogitado – na modalidade de “publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente” – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma normal aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta incriminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da Lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a

> autoria da inserção incriminada do conhecimento do homem comum, impõe se a realização de prova pericial.

Para se localizar os criminoso dos artigos citados, geralmente precisa de quebra de sigilo, tendo em vista que necessita de rastreamento daquele individuo que praticou o ilícito, e após conseguir localizar o culpado, e necessário muitas das vezes que sejam as provas eletrônicas analisada por uma pericia técnica rigorosa para que sejam aceitas em processos.

9.SOBRE A LEGISLAÇÃO EM VIRGO NO BRASIL.

Diante do que vem sendo exposto no transcorrer da apresentação sobre o crimes virtuais, podemos mencionar outros crimes cometidos na internet como, lavagem de dinheiro, invasões de privacidade, pichações em sites oficiais do governo, sabotagem, crimes contra honra, paz pública, lesões ao direito humano (terrorismo, crimes de ódio, racismo, etc), destruição de informações, jogos ilegais, falsidade ideológica, modificação ou alteração não autorizada de sistema de informação, violação de sigilo funcional, dentre outros, todos sem uma tipificação adequada ocorrendo muitas brechas e livrando os criminosos dos mesmos. Tais crimes utilizam a internet como meio de lesar outras pessoas obtendo vantagem do usuário desse ambiente virtual ou atacar a honra deste usuário.

O ilustre autor Marcelo Baeta Neves Miranda [2], discorre o seguinte sobre crimes virtuais.

> Por não encontrar amparo na lei penal vigente é o crime de hacking, consistente no acesso a um determinado sistema por particular sem autorização. Conforme o autor, em outros países já existem leis que visam coibir o ataque dos hackers, quais sejam: a) Copyright, Designs and Patents Act (Inglaterra-1988); b) Computer Fraud and Abuse Act (E.U.A. - 1986) e c) Communication Decency Act (E.U.A. – 1996).

A imputação desse crimes resulta em grande escala de individuo utilizar tais ferramentas para causar dano a usuários em toda rede informática, mas o

importante será como nosso ordenamento jurídico irá se adequar a tais formas de delitos.

10. NATUREZA JURIDICA DO ASPECTO PENAL.

Como esmaltado no nosso ordenamento jurídico, o homem vive e coexiste em grupos, regularizado pelo Direito, assim assegura o convívio social, e as condições mínimas de existência.

O direito penal constitui por princípios, conhecimentos e normas jurídica, que vem dar efetividade a atos praticados contra os bens do nosso ordenamento jurídico. Segundo Miguel Reale Junior, o Direito Penal constitui uma espécie de controle social, mas de caráter formal e residual, pois só atua diante do fracasso dos instrumentos informais de controle. Tal pensamento se concretiza, da seguinte forma o Direito Penal funciona como uma resposta a delitos para a sociedade sentir-se protegida, sem a pretensão de plena eficácia no impedimento da pratica de fatos delituosos. [3]

A matéria que e expressa no Direito Penal tem a visão da proteção dos bens jurídicos de caráter de proteção dos indivíduos uns contra os outros, desta mesma forma o Estado contra os indivíduos, alem de assegurar garantias como a sociedade que são tutelados pelo o mesmo. A interferência penal na vida dos indivíduos deve ser mínima por ser a forma mais gravosa de se lidar, ao que diz ser o Direito Penal a “ultima ratio”.

[2]. Acesso em: 10 maio 2015 63 Denominação proposta por MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via Internet . Jus Navigandi, Teresina, a. 4, n. 37, dez. 1999.

Tendo assim um limite para ser imposta no ambiente social, dependendo o limite material da norma incriminadora, que se visa a proteção dos valores fundamentais à convivência social, esta questão tem hoje grande ênfase diante do processo de criminalização, sendo operado por meio de uma inflação legislativa penal.

O principio da legalidade se consagra em nosso ordenamento pelas letras em latim “ nullun crimen, nulla poena sine lege, que se constitui uma limitação no poder punitivo estatal. Impondo o dever de punir ao legislador para decretar os tipos penais que seja, a fim de dar conhecimento ao destinatário da norma, do que e lícito e ilícito. Consequentemente, tal principio proíbe o uso da analogia, a

retroatividade (in mallam parte) e edição de leis penais indeterminadas e /ou imprecisas.

Quanto ao tempo do crime na internet, devemos tratar tal situação que por sua natureza torna as informações e relações instantâneas, pela analise do momento que se considera praticado o delito para aplicação da lei penal ao seu autor assim como a lei penal no espaço.

No nosso ordenamento jurídico foi adotado, a teoria da atividade, ou seja, considera o tempo do crime no devido momento da conduta.

No geral cabe o Estado, delimitar seu próprio poder punitivo em observância às regras de Direito Internacional, quando tratamos as condutas efetuadas no ambiente virtual devemos ficar atentos para não interferimos interesses de outros países, porque pode causar o conflito de soberanias, devendo recorrer aos princípios.

O ambiente virtual e um ambiente constituído de bits e bytes que por sua vez não há um local especifico, que nada mais são unidades de medida criadas através do computador, ou seja, um lugar que existe e não existe ao mesmo tempo. Não podendo resolver com exatidão possíveis conflitos nessa área , acreditamos que somente a colaboração internacional poderá resolver os dilemas territoriais do

[3]REALE JÚNIOR, Miguel. Instituições de direito penal. Rio de Janeiro: Forense, 2002. v. 1. Parte geral. p. 3.

11. POSSIVEL SOLUÇÃO

Como que já se e esperado a tecnologia vem se aperfeiçoando cada vez mais rápido com passar do tempo, o numero de conexão entre comunicação cresce, cresce também o da criminalidade neste meio, criminoso se apodera desse ambiente, pois há uma enorme dificuldade de investigação para se punir o individuo.

A ONU (Organizações das Nações Unidas) reconheceu que este tipo de delito nesse ambiente e um serio problema, já que vários países ainda não adaptaram sua legislação para tais tipos penais e procedimentos investigativos, para inibir a dissipação dos delitos eletrônicos.

Nota-se que nosso sistema de leis estão analisando com toda preocupação uma forma de regulamentar tal assunto, porque se percebe a

quantidade de delitos ocorrendo nessa área que não a uma forma eficaz de punir os infratores, atualmente há 13 (treze) projetos lei em tramitação no Congresso Nacional.

Mas o que realmente se precisa, e de um policiamento internacional que dê apoio às policias mundiais,fornecendo melhores condições de treinamento para tornarem capazes de investigar os crimes que ocorrem no ambiente virtual, alem de interligar as nações para assegurar a investigação e a coleta de provas destes crimes, por guardarem características peculiares, observando a grande possibilidade de ser objeto de execução à distancia, envolvendo diversos países.

A impunidade nesse ambiente e consequência da impossibilidade de rastreamento do individuo que cometa tais condutas não da falta de legislação especifica. Pela grande extensão do ambiente virtual e as lacunas que há no mesmo, tornando difícil de fiscaliza-la e impor limites. Os dados são transmitidos livremente e veloz pela internet, trocando de países instantaneamente tais dados são traduzidos em bits, facilmente manipulados pelos experts.

O primeiro decreto condenatório por crime eletrônico no Brasil foi proferido pela juíza da 3ª Vara da Justiça Federal de Campo Grande (MS), Janete Lima Miguel. Isso apenas vem confirmar que nossa legislação vigente pode ser aplicada aos crimes cibernéticos. (Neste sentido ROSSINI, 2004.)

Porem alguns autores, dizem que deveria ser formulada uma lei prevendo todas as ações danosas na Internet, mesmo que o bem jurídico tutelado seja o mesmo já tutelado pela lei previamente existente assim sendo excluindo possíveis lacunas as famosas brechas na legislação existente.

Devemos não só se focar na criação de uma lei para regulamentar tal ambiente sim numa forma de proteger a informação e a proteção de dados pessoais, para que os bens jurídicos tutelados por leis seja aplicada no mundo físico tenham eficácia no ambiente virtual e vice-versa.

Atualmente vivenciamos um período que há uma inflação legislativa, ou seja, uma lei penal sobre crimes virtuais só iria aumentar os dígitos das leis já editadas e que não tem eficácia, exemplo desta ineficácia seria a situação da Lei dos Crimes Hediondos que não fez diminuir os crimes da espécie.

Nas palavras do professor Saulo de Carvalho:

> A alternativa ao Estado providência, portanto, passa a ser um Estado penitência, configurando uma máxima que parece ser a palavra de ordem na atualidade: Estado social mínimo, Estado penal máximo. Gesta-se, no interior dessa ideologia, uma saída plausível para aqueles que foram destruídos ou que nunca chegaram a ter cidadania: a marginalização social potencializada pelo incremento da máquina de controle social, sobretudo carcerária. [...] Exigiu-se da estrutura liberal (genealógica) do direito penal algo que dificilmente terá capacidade resolutiva, projetando severos índices de ineficácia. Desde esta perspectiva, pode-se afirmar a existência de uma 'Constituição Penal', idealizadora/instrumentalizadora de um Estado Penal, plenamente realizada.

O grande problema da jurisdição no ambiente Virtual seria aplicação da lei, e um problema geográfico de desterritorialização, pois não há barreiras físicas, e por isso, o conceito clássico de soberania do Estado acaba relativizada, assim como e o do tempo. Os criminosos estão munidos com tecnologias de mais modernas, e isso tudo cria um espaço no qual as prescrições jurídicas nacionais são insuficientes, pois apenas a cooperação global pode sanar tal carência.

Providencias devem ser tomadas para que seja possível a regulamentação do ambiente virtual assim diminuindo os crimes cometidos, e tais providencias devem ser tomada individualmente, ou por diferentes nacionalidades em âmbito global, pois a internet traz resultados positivos eficiente e duradores. Somente o trabalho conjunto em nível internacional e interdisciplinar eficiente para o ambiente virtual.

O problema e a base de função de prevenção e investigação que nosso pais se encontra pois temos o exemplo do FBI que já há alguns anos vem treinando equipes chamadas de Cybercops, policiais especialmente treinados e, principalmente, equipados para combater esses delitos que se figuram como desafio criminal do próximo século. O enfoque esta sendo na ampliação da cooperação entre países, alertando para a carência e a forma totalmente dispersa da Internet.

Portanto, os crimes virtuais encontra-se espalhado pelo Código Penal a contrario do que alguns doutrinadores afirmam, a aplicação da lei já existe à essas condutas não e o caso de analogia, pois não são crimes novos, não são bens

jurídicos novos necessitando de tutela penal, a novidade fica por conta do modo operandi, de como o criminoso tem feito uso das novas tecnologias, com foco na Internet, fazendo com que os estudiosos e os aplicadores do Direito tenham que renovar o seu pensamento.

12. LEGISLAÇÃO NACIONAL TIPIFICANDO OS CRIMES VIRTUAIS.

As relações que ocorre no ambiente virtual pode-se dizer que esta interligada inteiramente ao Código Penal pois, cabe ao Direito disciplinar e regulamentar as condutas entre os usuários que ali se encontram, sendo já de grande valor suas normas que já constam mas não sendo suficiente para punir alguém que cometi crimes nesse ambiente havendo muitas brechas e desacordo entre aplicadores do Direito na nossa sociedade .

Mas para que venha ser aplicado o sistema do Código Penal nos crimes praticados no ambiente digital é necessário que o tipo penal venha a se adequar as normas já existentes, e as lacunas que por ventura ainda há de ser preencher, sendo extremamente necessária a tipificação clara sobre conceitos de informática na legislação atual.

As primeiras normas começaram a aparecer com advento do Plano Nacional de Informática e Automação (Conin), Lei n. 7.232/84, o qual versava sobre as diretrizes no âmbito da informática em solo Brasileiro, depois veio a Lei n. 7.646/87, a qual

foi revogada pela Lei n. 9.609/98, sendo que esta foi o primeiro ordenamento a descrever as infrações de informática, a qual podemos citar alguns artigos:

> Art. 12. Violar direitos de autor de programa de computador:
> Pena – Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena – Reclusão de um a quatro anos e multa.
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
> § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
> I – quando praticados em prejuízo de entidade de direito público,
> autarquia, empresa pública, sociedade de economia mista ou
> fundação instituída pelo poder público;
> II – quando, em decorrência de ato delituoso, resultar sonegação
> fiscal, perda de arrecadação tributária ou prática de quaisquer dos
> crimes contra a ordem tributária ou contra as relações de consumo.
> § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do
> tributo, ou contribuição social e qualquer acessório, processar-se-á
> independentemente de representação.

Podemos citar também algumas normas do Código de Defesa do consumidor – Lei 8.078/11 (VADE MECUM. 11ª Ed. São Paulo. Saraiva, 2011.p.855)

> Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
> Pena – Detenção de seis meses a um ano ou multa.
> Art. 73. Deixar de corrigir imediatamente informações sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata:
> Pena – Detenção de um a seis meses ou multa.

Cabe também um breve resumo sobre as condutas já tipificadas no ordenamento jurídico pátrio que são criminalizada.

> Art. 153, § 1° - A do Código Penal – Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública.
> Pena – detenção de 1 a 4 anos, e multa.
> Art. 313 – A do Código Penal – Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir

indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.
Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.
Art. 313 – B do Código Penal – Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.
Pena – detenção de 3 (três) meses a 2 (dois) anos, e multa.
Art. 325, § 1°, incisos I e II - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitarlhe a revelação:
Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.
§ 1 Nas mesmas penas deste artigo incorre quem:
I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública;
II – se utiliza, indevidamente, do acesso restrito.

Art. 2°, V – Lei n. 8.137/90 – utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública.

Art. 72 da Lei n. 9.504/97 – Constituem crimes, puníveis com reclusão, de cinco a dez anos: I – obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; II – desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; III – causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

Há muito projetos Lei em andamento para regulamentar delitos tecnológicos, destacando o PL n°84/99, que ao longo dos anos foi incorporado inúmeros artigos, de seus apenas seis artigos iniciais, recebendo inúmeras emendas que ampliaram, as alterações que este projeto lei trará a legislação.

a) O art. 2° prevê a inclusão do Capítulo IV do Título VIII, da Parte Especial do Código Penal, com a redação dos arts. 285- A (acesso não autorizado a sistemas informáticos), 285-B (obtenção e transferência ilegal de dados) e 285-C (ação penal);
b) O art. 3° prevê a inclusão do art. 154-A no Título I, Capítulo VI, Seção IV, que trata da divulgação ou utilização indevida de informações e dados pessoais;

> c) O art. 4° trata da alteração do art. 163, inserido no Título II, Capítulo IV, para que inclua no crime de dano a destruição, inutilização ou deterioração de dado alheio.
> d) O art. 5° trata da inclusão do art. 163-A no mesmo Título II, Capítulo IV, que incrimina a disseminação de vírus computacional;
> e) O art. 6° altera o crime de estelionato para que conste no art. 171, § 2°, VII, a difusão de vírus que vise destruir, copiar, alterar, facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado, para obter vantagem econômica para si ou para outrem, em detrimento de outrem;
> f) O art. 7° altera os crimes dos arts. 265 e 266 do Código Penal para que constem como crime contra a segurança dos serviços de utilidade pública os de informação e telecomunicações;
> g) O art. 8° altera o art. 297 do Código Penal para que dentre as falsificações de documentos públicos incluam-se os dados;
> h) O art. 9° altera o art. 298 do Código Penal para que dentre as falsificações de documentos particulares incluam-se os dados;
> i) O art. 10 muda o Código Penal Militar para que o art. 251 do Capítulo IV, do Título V da Parte Especial do Livro I do Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), passe a vigorar acrescido do inciso VI ao seu § 1°, e do § 4°, incriminando-se o estelionato eletrônico;
> j) O art. 11 altera o caput do art. 259 e o caput do art. 262 do Capítulo VII, do Título V, da Parte Especial do Livro I do Decreto-Lei n. 1001, de 21 de outubro de 1969 (Código Penal Militar), para que deles conste destruição a dados sob administração militar;
> k) O art. 12 altera o Capítulo VII, do Título V, da Parte Especial do Livro I do Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), que fica acrescido do art. 262-A, prevendo a disseminação de vírus em sistemas militares;
> l) O art. 13 altera o Título VII da Parte Especial do Livro I do Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), que fica acrescido do Capítulo VII-A, que prevê crimes contra a segurança dos sistemas informatizados;
> m) O art. 14 altera o caput do art. 311 do Capítulo V, do Título VII, do Livro I da Parte Especial do Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), para que a falsificação
>
> de documentos inclua os dados;
> n) O art. 15 altera os incisos II e III do art. 356, do Capítulo I, do Título I, do Livro II da Parte Especial do Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), para que conste do crime de favorecer o inimigo a entrega de dados;
> o) O art. 16, um dos mais polêmicos, traz definições do que devem ser considerados dispositivo de comunicação, sistema informatizado, rede de computadores, código malicioso, dados informáticos e dados de tráfego;

Podemos citar um caso separado do artigo 16, sendo que o mesmo define como dispositivo de comunicação, por exemplo, um pen-drive, disco rígido, CD,DVD, o que não se encaixa com a realidade, por isso há uma discussão sobre tal artigo.

> p) O art. 17, cuja supressão da redação é recomendada pela proposta do substitutivo, dispõe que para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado;
> q) O art. 18 estabelece que os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializados no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado;
> r) O art. 19 altera a redação do inciso II do § 3º do art. 20 da Lei n. 7.716, de 5 de janeiro de 1989 (crimes de racismo e preconceito), para permitir a cessação de transmissões 38 radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio de condutas descritas na lei;
> s) O art. 20 prevê que o caput do art. 241 da Lei n. 8.069, de 13 de julho de 1990, tenha redação que coíba o recebimento e o armazenamento de imagens e fotos com conteúdo de pornografia infantil;
> t) O art. 21 pretende alterar a Lei n. 10.446/02, que dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme, para os fins do disposto no inciso I do § 1° do art. 144 da Constituição, para que os crimes digitais sejam da competência da Justiça Federal;
> u) O art. 22 obriga os que provêem o acesso a rede de computadores mundial, comercial ou do setor público, e também as prestadoras de serviço de conteúdo, sejam obrigados a diversas condutas, que dizem respeito, por exemplo, que as responsáveis pelo provimento, deverão manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, destino hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória e ao Ministério Público mediante requisição. Este artigo tende a ser o mais polêmico de todos os citados do Projeto de Lei.

Notamos, que ao realizar uma analise a fundo sobre os artigos deste projeto em lei, ele possui uma grande tipologia de condutas mas em certo momentos peca, no quesito regras rígidas, para tanto os usuários que utilizam como para as empresas que exercem o papel de provedoras do serviço de acesso a internet, fazendo com que de certa forma o usuário de má-fé, tenha caminho livre para que venha praticar condutas antijurídicas, para que o mesmo venha a ser responsabilizado. Tal projeto vem se encaminhado lentamente sendo uma iniciativa do Senador Eduardo Azeredo, o qual também dispõe de crimes cometidos no meio informático, e crimes que são cometidos por meio de computadores e instrumentos de acesso a internet ou cenário digital, podemos citar pontos importantes desse projeto, como, Disseminar phishing scam (e-mails fraudulentos contendo malwares e outros códigos maliciosos), nova tipificação do crime seria Estelionato Eletrônico.

O citado projeto, faz referência a poucos institutos que os especialista da área de informática, estão acostumados a se debaterem no seu cotidiano, era de se esperar, até porque o mesmo foi colocado em discussão para a sociedade apenas depois da proposta de lei ser aprovada pela Câmara dos Deputados, e o que se observa hoje é a falta de uma equipe de profissionais da área de informática para auxiliar na ordenação dos artigos que fazem parte do Projeto, tendo em vista que o instituto é de alta complexidade até para profissionais mais experientes da área.

Atualmente está em virgo a lei 12.737/2012, que altera o Código Penal e tipifica os crimes virtuais no Brasil, que utilizar o dispositivo informático alheio (computadores,tablets,notebooks,celulares, entre outros) Disseminar phishing scam (e-mails fraudulentos contendo malwares e outros códigos maliciosos), que esteja ligada ou não a internet, criar programas de violação de dados ou divulgar e negociar informações obtidas de forma ilícita poderá ser punido com multa e ate prisão as penas variam de três meses a dois anos de reclusão.

Esta lei foi denominada de Carolina Dieckmann, pois a atriz teve 36 fotos íntimas vazadas na internet em maio de 2012, prevê pena de seis meses a dois anos se a invasão resultar na obtenção de comunicações eletrônicas privadas segredos comerciais ou industriais informações sigilosas, aumentando ate dois terço se tiver sido comercializado, e a transmissão a terceiros a qualquer título, dos dados ou informações obtidos diz, o artigo 154-A do Código Penal, essas pena pode aumentar se o crime for cometido contra, vereadores, deputados federais e estaduais, senadores e o presidente da Republica, ou se a invasão resultar em prejuízo financeiro.

Esta lei e tida como uma evolução, para nosso ordenamento jurídico ela não trouxe nenhuma revolução já que não dispõe de mecanismo para que a Policia tenha maior acesso aos dados dos provedores de serviço. O problema maior nesse ambiente informático e a investigação muito complexa, pois envolve um caminho longo, para isso deve-se obter o endereço de IP que e a identidade virtual , e necessário recorrer a justiça para liberar o provedor fornecer o IP, esse processo e demorado e como visto a punição e muito branda isso faz com que a vítima desista de procurar a Policia.

13 CONCLUSÃO

Por conseguinte a realização deste estudo, concluímos que se faz necessário à revisão em nosso ordenamento jurídico, de condutas criminosas praticadas por meio da internet sendo que, o Brasil está atrasado no aspecto jurídico e policial, mas em progresso na criminalidade realizada por meios virtuais, devendo-se igualar aos países que já possuem legislação específica para crimes virtuais, para que não sejamos um paraíso aos criminosos desse setor, nosso país se encontra entre os dez países que mais utilizam a internet, em um mercado promissor e crescente, sem uma legislação clara que puna adequadamente e classifique quantos e quais são os crimes cometidos virtualmente, para amparar os usuários desse serviço. Pela grande evidencia de crescimento desse setor ficou evidente que cada dia cresce o número de usuários que procuram no espaço virtual maneiras para aplicar golpes por exemplo, estelionatários que criam falsos, sites, de Bancos ou lojas de grande nomes no Brasil, que copiam dados como, senha, numero de conta, todos os dados digitado nessa pagina e transmitido quase que automaticamente para as mãos dos criminosos.

O tema de grande destaque nos últimos anos esta sendo o crime de pornografia infantil que esta se espalhando não só no ambiente virtual mas também no dia a dia, e no mundo todo, pela facilidade de se espalhar os dados e ser remunerado pelo mesmo sem deixar pistas e um ambiente gracioso para pessoas que gostam de cometer delitos e ficar impune, porque e quase impossível fazer um rastreamento de endereço IP imediatamente principalmente no Brasil, pois não a

fiscalização descente por parte do poder publico nas relações entre diversos usuários na rede.

Toda essa pesquisa realizada teve com objetivo maior apresentar as diversas formas as quais pode, realizar um delito através do mundo virtual, sendo da forma punitiva mais branda até a sua restrição de liberdade. Foram apresentadas ainda lacuna referente a áreas deixada pela legislação brasileira ,apesar da grande evolução no século 21 ainda esta muito atrasada em comparação a outros países.

REFERÊNCIAS BIBLIOGRÁFICAS

História e usos da Internet - Karen Cristina Kraemer Abreu*

Crimes Virtuais, Vítimas Reais - Moisés de Oliveira Cassanti Profissional de TI desde 1991, analista de sistemas, administrador de redes, programador, Policial Civil em São Paulo especializado em crimes cibernéticos.

Crimes Contra os Direitos da Personalidade na Internet - Luziane de Figueiredo Simão Lea

ACESSO à internet, provedores, internet no Brasil, avanço da Informática, computadores, história da internet, as redes sociais. Disponível em:. Acesso em: 15 nov. 2014.

BARBOSA, Denis Borges; ARRUDA. Mauro Fernando Maria. Sobre a Propriedade Intelectual. Rio de Janeiro: Campinas, 1990.

BRASIL. Código Penal. Decreto Lei n. 2.848/40. Disponível em . Acesso em: 10 abr. 2015.

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

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000

DISPONIVEL:tecnologia.uol.com.br/noticias/redacao/2013/04/02/lei-carolina-dieckmann-sobre-crimes-na-internet-entra-em-vigor.htm ACESSO 2014

FRAGOMENI, Ana Helena. Dicionário Enciclopédico de Informática. Vol.I. Rio de Janeiro: Campus, 1987.
FRAGOSO, Heleno Cláudio. Lições de direito penal: parte especial: arts. 121 a 212 do CP. Rio de Janeiro: Forense, 1983.

GIL, Antônio de Loureiro. Fraudes Informatizadas. 2 ed. São Paulo: Atlas, 1999

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

DISPONIVEL: http://www.tjmt.jus.br/noticias/29323 . ACESSO novembro 2015.

LEMOS, André/LÉVY, Pierre. O futuro da Internet: em direção a uma ciberdemocracia. São Paulo: Paulus, 2010.

LIMA, Paulo Marco Ferreira. Crimes de computador e segurança computacional. Campinas, SP: Ed. Millennium, 2005.

LIMBERGER, Têmis. O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado Editora, 2007

Disponível: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm acesso julho 2015.
FRANCO, Alberto Silva. Globalização e criminalidade dos poderosos. Revista Brasileira de Ciências Criminais, São Paulo, v. 8, n. 31, p. 102-136, jul./set. 2000. GAUER, Ruth M. Chittó. Conhecimento e aceleração: mito, verdade e tempo. In:

GAUER, Ruth M. Chittó (Org.). A qualidade do tempo: para além das aparências históricas. Rio de Janeiro: Lumen Júris, 2004. p. 1-16.

GOMES, Luiz Flávio; BIANCHINI, Alice. Globalização e direito penal. In: ESCRITOS em homenagem a Alberto da Silva Franco. São Paulo: Revista dos Tribunais, 2003. p. 264-287.

Crimes Virtuais, Vítimas Reais Moisés de Oliveira Cassanti Profissional de TI desde 1991, analista de sistemas, administrador de redes, programador, Policial Civil em São Paulo especializado em crimes cibernéticos

Diponivel www.conteudojuridico.com.br/pdf/cj037145.pdf- RAPHAEL ROSA NUNES VIEIRA DE PAIVA-Crimes virtuais acesso Janeiro 2015

ANEXOS

Anexo 1

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

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

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

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

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

“Invasão de dispositivo informático

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

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

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

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

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

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

§ 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.”

“Ação penal

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.”

Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266. § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

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

“Falsificação de documento particular

Art. 298. **Falsificação de cartão**

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

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

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

DILMA ROUSSEFF
José Eduardo Cardozo

Anexo 2

Leis existentes no Vade Mecum relacionadas a crimes virtuais

Situação 1 - A internet constitui mais uma forma de se praticar o delito do artigo 122 do Código Penal, podendo ocorrer em especial nas modalidades de, induzir e instigar quer de forma direta em conversas de salas de bate-papo ou redes sociais, quer por meio de sites específicos em ensinam a cometer suicídio.

Enquadramento viável: Art 122 - CP (Induzimento, Instigação ou Auxílio ao suicídio)

Pena: Reclusão de 2 (dois) a 6 (seis) anos (caso se consuma) Reclusão de 1 (um) a 3 (três) anos (se resultar em lesão corporal grave)
OBS: Pena duplicada se houver motivo egoístico ou se a vítima for incapaz

Situação 2 - Utilizar de MSN ou qualquer meio de comunicação on-line via internet, criar e/ou participar de Blogs ou comunidades que qualquer usuário acesso direto pelo computador, ou ainda direcionar Links (acessos) para páginas nacionais ou estrangeiras acusando diretamente pessoas que tenham cometido algum tipo de crime tipificado no Código Penal, sendo inclusive contra pessoas já falecidas. Enquadramento viável: Art 138 - CP (Caluniar alguém, imputando-lhe falsamente fato definido como crime) .
Pena: Detenção de 6 (seis) meses a 2 (dois) anos e multa.

Situação 3 - Dar forward para várias pessoas de um boato eletrônico referente a um(a)cidadão(ã) devidamente identificado(a). Este ato é comumente conhecido no mundo virtual como "repassar" por fw (abreviação de forward). Situação comum em reenvio de e-mails recebidos por outros usuários.

Enquadramento viável: Art 139 - CP (Difamar alguém imputando-lhe fato ofensivo à sua reputação)

Situação 4 - Usuário envia e-mail diretamente a uma pessoa, chamando-a de diversos adjetivos pejorativos, referindo-se as suas características pessoais, citando como exemplo feia, gorda, bruxa, etc.
Enquadramento viável: Art. 140 - CP (Injuriar alguém, ofendendo-lhe a dignidade e decoro)

Pena: Detenção de 1 (um) a 6 (seis) meses ou multa

Situação 5 - Utilizar de MSN ou qualquer meio de comunicação on-line via internet, criar e/ou participar de blogs ou comunidades que qualquer usuário acesse direto pelo computador oferecendo qualquer tipo de droga, substâncias entorpecentes ou similar ilícita, gratuita ou não, que provoque dependência química ou psíquica.
Também é punido quem oferece sem autorização e/ou em desacordo com qualquer determinação legal, qualquer tipo de produto químico ou matéria prima destinada à preparação de drogas.

Enquadramento viável: Art. 33 – Lei 11.343/06 (Importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor a venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar.
Inciso I – importa, exporta, remete, produz, fabrica, adquire, expõe a venda, oferece, fornece, tem em depósito, transporta, traz consigo ou guarda, ainda que

gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar, matéria-prima, insumo ou produto químico destinado à preparação de drogas)
Pena: reclusão de 5 (cinco) a 15 (quinze) anos e pagamento de 500 (quinhentos) a 1.500 (mil e quinhentos dias-multa)

Situação 6 - Usuário envia e-mail a terceiros, divulgando um fato de conteúdo particular de que tenha conhecimento ser secreto, seja documentos ou correspondências, cuja divulgação possa ocasionar danos Irreparáveis a pessoa física ou jurídica. Também é punido com pena mais grave pelo Código Penal Militar, se for notícia, informação ou documento, cujo sigilo seja de segurança externa do Brasil.

Enquadramento viável: Art. **153** – CP (Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor
e cuja divulgação possa produzir dano a outrem)

Art. 154 - CP (Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa provocar dano a outrem).
Art. 144 - CPM (Revelar notícia, informação ou documento, cujo sigilo seja de interesse da segurança externa do Brasil)
Pena: **Art. 153** - CP - Detenção de 1 (um) a 6 (seis) meses ou multa
Art. **154** - CP - Detenção de 3 (três) meses a 1 (um) ano ou multa
Art. 144 – COM – Reclusão de 3 (três) a 8 (oito) anos

Situação 7 - Efetuar saques e transferências em Caixas Eletrônicos Bancários, com os dados do cliente sem sua permissão ou autorização.
Enquadramento viável: Art. 155 - CP (Subtrair para si ou para outrem, coisa alheia móvel, devendo ser qualificado com o § 4º) e/ou Inciso I (destruição ou rompimento de obstáculo) e/ou Inciso II (abuso de confiança, com fraude, escalada ou destreza).

Pena: Artigo 155 - § 4º CP – Reclusão de 2 (dois) a 8 (oito) anos e multa

Situação 8 - Usuário envia vírus em qualquer situação on-line pela Internet, ou via e-mail com anexos, não importando se doloso ou culposo.

Enquadramento viável: Art. 163 - CP (Destruir, inutilizar ou deteriorar coisa alheia, podendo ser qualificado com inciso IV (por motivo egoístico ou com prejuízo considerável à vítima)
Pena: Artigo 163 CP – Detenção de 1 (um) a 6 (seis) meses ou multa.

Situação 9- Utilizar de MSN ou qualquer outro meio de comunicação on-line via internet, criar e/ou participar de Blog's ou comunidades que qualquer usuário tenha acesso direto pelo computador, ou ainda direcionar link´s (acessos) para páginas nacionais ou estrangeiras denegrindo imagem de pessoas vinculadas à religiões, credos ou crenças e/ou denegrindo-as concomitantemente.
Enquadramento viável: Art 208 - CP (Escarnecer de alguém publicamente, por motivo de crença ou função religiosa, impedir ou perturbar cerimônia ou prática de culto religioso; vilipendiar publicamente ato ou objeto de culto religioso)
Pena: Artigo 208 - CP - Detenção de 1 (um) mês a 1 (um) ano ou multa

Situação 10- Copiar conteúdos via internet, documentos não citando fontes, "baixar" arquivos de áudio e vídeo sem expressa autorização de seus autores ou de quem detenha os direitos autorais.
Enquadramento viável: Art 184 - CP (Violar direitos de autor e os que lhe são conexos). **Pena: Artigo 184** - CP - Detenção de 3 (três) meses a 1 (um) ano e multa

Se a violação acima consistir em reproduzir total ou parcialmente, objetivando lucro direto ou indireto. Enquadramento viável: Art 184 - CP (agravante com o § 1°).
Pena: § 1° do artigo 184 do CP - Detenção de 2 (dois) 4 (quatro) anos e multa

A quem aluga, vende, distribui, tem em depósito original ou cópia e delitos congêneres, sem autorização do autor.

Enquadramento viável: Art 184 - CP (agravante com o § 2°)

Pena: § 2° do artigo 184 do CP - Detenção de 2 (dois) 4 (quatro) anos e multa