FACULDADES INTEGRADAS

"ANTONIO EUFRÁSIO DE TOLEDO"

FACULDADE DE DIREITO

A SISTEMATIZAÇÃO DOS DIREITOS FUNDAMENTAIS FRENTE SUAS CRESCENTES VIOLAÇÕES POR MEIO DO USO DA INTERNET

Guilherme Barros Martins de Souza

Presidente Prudente/SP

2013

FACULDADES INTEGRADAS

"ANTONIO EUFRÁSIO DE TOLEDO"

FACULDADE DE DIREITO

A SISTEMATIZAÇÃO DOS DIREITOS FUNDAMENTAIS FRENTE SUAS CRESCENTES VIOLAÇÕES POR MEIO DO USO DA INTERNET

Guilherme Barros Martins de Souza

Monografia apresentada como requisito parcial de conclusão de curso para obtenção do grau de Bacharel em Direito, sob orientação do Prof. Msc. Marcelo Agamenon Goes de Souza.

Presidente Prudente/SP

2013

“A justiça sustenta numa das mãos a balança que pesa o direito, e na outra, a espada de que se serve para o defender. A espada sem a balança é a força brutal; a balança sem a espada é a impotência do direito”

(Rudolf von Ihering)

AGRADECIMENTOS

Uma monografia deveria ser produto de uma atividade intelectual de caráter solitário. Entretanto, queda-se pela impossibilidade de veracidade da referida afirmação, uma vez que ninguém é tão bom ao ponto de desnecessitar de uma mão alheia.

E assim sendo, gostaria de prestar os mais sinceros e alegres agradecimentos ao meu orientador e professor Marcelo Agamenon Góes de Souza por todo o tempo desprendido à elucidação de minhas dúvidas, questionamentos e incertezas. Agradeço ainda por sempre fazer-se disponível e eficiente em seus apontamentos, resultando neste produto do qual muito contribuiu para a sua confecção.

Agradeço aos meus familiares por todo o apoio e incentivo a mim ofertados, em especial, meu pai, Mauro César Martins de Souza, pelas sábias palavras e oportunos ensinamentos que me foram passados durante todo o meu caminhar.

Agradeço às Faculdades Integradas Antônio Eufrásio de Toledo pela oportunidade dada para o pleno desenvolvimento do presente trabalho, pela sua excelente estrutura e ainda pelo seu brilhante corpo docente, coordenado de forma extremamente competente pelo fraterno Mestre Sergio Tibiriçá do Amaral.

RESUMO

Cumpre-se com o presente artigo a função de examinar e esmiuçar os problemas advindos com o avanço tecnológico da Internet em rota de colisão junto aos direitos fundamentais em especial, o direito à intimidade de seus respectivos usuários. Demonstrando-se assim, que a Internet se tornou um espaço extremamente amplo, diversificado e abrangente modo pelo qual, carece de proteção jurídica quanto aos direitos de seus usuários, que depositam inúmeros dados pessoais diariamente nestas redes.

Corroborando-se ainda, com um breve estudo acerca dos direitos fundamentais que se encontram positivados em nossa Carta Maior e possuem como premissa o estabelecimento de direitos, deveres e garantias entre os cidadãos.

Outra problemática a ser tratada reside-se no cerne da responsabilização dos agentes que se utilizam desta seara digital para o cometimento de ilícitos, haja vista que tal responsabilização criminal encontra certa dificuldade em ser estabelecida e ainda contribuem para tanto, a ausência de tipificação de algumas figuras delituosas resultando na inevitável impunidade de seus cometedores.

Abordando assim, a problemática existente entre a percepção e o respeito ao direito à intimidade e, inevitavelmente, a presença cada vez mais constante, das novas tecnologias na época em que nos encontramos. E com isso, trazendo no presente trabalho os crimes praticados por intermédio dos meios informáticos, bem como descrevendo de maneira pormenorizada seu modus *operandi.*

Palavras-chave: Direito à intimidade. Direitos e Garantias fundamentais. Vida Privada e Intimidade. Internet. Cibercrimes.

ABSTRACT

Will the present Article, the function to demonstrate the problems originated with the technological advancement of the Internet on a collision course with the right to privacy of their users. Thus Demonstrating that the Internet has become an extremely large space so that lacks a protection regarding the rights of its users, who are pinning countless personal data in these networks.

Being also object of the present study the systematization of fundamental rights, which are doctrines accepted in our Charter, which aims to establish Greater rights, duties and guarantees between the citizens, as well as the right to intimacy that is often violated resulting from the practices of these approaches described above, and still we will deal with the right to information.

Will also object of analysis the creation and functioning of the Internet, as well as their functions and the main services offered to its users. Since it is still of offenses from computerized means classified these as virtual crimes themselves and unfit.

Thus, Addressing the problems that exist between the perception and the respect for the right to intimacy and, inevitably, the presence increasingly constant, of new technologies in the season in which we find ourselves.

Key-Words : Right to intimacy. Fundamental Rights and safeguards. Privacy and Intimacy. Internet. Virtual Crime.

SUMÁRIO

A SISTEMATIZAÇÃO DOS DIREITOS FUNDAMENTAIS FRENTE SUAS CRESCENTES VIOLAÇÕES POR MEIO DO USO DA INTERNET

1 INTRODUÇÃO

O presente trabalho inicia-se com uma breve exposição acerca dos direitos e garantias fundamentais, que encontram amparo legal em nossa Constituição Federal de 1988.

Em seguida, passa a relatar sobre o direito à intimidade, um dos temas centrais do presente trabalho, que se trata de uma garantia de ordem constitucional à vida privada de todo cidadão, conforme o disposto no Art. 5º X, da Constituição Federal Brasileira.

Na sequência, a pesquisa irá tratar da evolução histórica da internet bem como o seu completo e amplo funcionamento. Levando em consideração, que inevitavelmente a Internet está presente de modo constante em nossas vidas, o que leva diretamente ao choque entre direitos pertencentes aos seus usuários, tendo como base que todo cidadão possui à sua vida privada, íntima e que deseja profundamente que esta jamais seja violada ou extirpada por terceiros.

Diante da necessidade e da importância do uso praticamente diário dos meios eletrônicos, entendemos assim pela Internet, pessoas estão diariamente tendo seus direitos violados, mais precisamente seu direito à intimidade, devido também a exposição de suas vidas na internet, o que muitas vezes ocorre sem o consentimento de seus titulares.

Será também objeto de analise a nova lei que tipifica os crimes virtuais, a Lei nº 12.737/12, popularmente conhecida como Lei Carolina Dieckmann, cujo nome foi dado devido às violações à intimidade sofrida por esta pessoa, que é figura pública conhecida frente à sociedade. Serão também discutidos os pontos cruciais da referida lei, bem como suas falhas e eventuais melhorias a serem pleiteadas.

E por fim, será feito uma breve exposição acerca da responsabilidade criminal e cível do autor da lesão, bem como a dificuldade de se chegar à autoria do delito, e também será analisada a responsabilidade do fornecedor do acesso à Internet.

Enfim, serão estes os principais tópicos e assuntos a serem tratados no respectivo trabalho.

2 DIREITOS FUNDAMENTAIS

2.1 CONCEITO

Em linhas gerais, direitos e garantias fundamentais seriam os direitos indispensáveis para que toda e qualquer pessoa possa vir a viver dignamente.

Direitos e garantias fundamentais possuem como finalidade primária o estabelecimento de direitos, garantias e deveres perante os cidadãos, sistematizando assim noções que servem como base para a regularização de todo aspecto social, político e histórico da vida em sociedade. Possuindo também a finalidade de resguardar a dignidade da pessoa humana em qualquer que sejam as suas dimensões.

O ordenamento jurídico brasileiro utiliza-se da expressão "direitos fundamentais", conforme disposto em nossa Carta Maior. Entretanto, a doutrina, dentre eles Luiz Alberto David Araujo que trata do tema emprega diferentes denominações, tais como: direitos humanos, liberdades assecuratórias, liberdades públicas.

Mas a doutrina, partidária em sua maioria do pensamento de Luiz Alberto David Araujo e Paulo Bonavides, tem por entendimento predominante, que a expressão "direitos fundamentais" é a mais adequada para o tratamento destas garantias.

Não podendo deixar de ser citada, a conceituação dada por Alexandre de Moraes (2012, p.132) acerca do tema:

> Os direitos fundamentais tem por finalidade básica, o repeito à dignidade do ser humano, por meio de sua proteção contra o arbítrio do poder estatal e o estabelecimento de condições mínimas e desenvolvimento da personalidade humana.

Deste modo, entende-se por direitos e garantias fundamentais, regras básicas atinentes a toda uma sociedade que almeje uma harmonia entre seus singulares, estabelecendo assim direitos e deveres que devem ser respeitados a qualquer custo.

Por fim, é de suma importância estabelecer a diferença entre direitos fundamentais e direitos humanos, haja vista que existe em caráter doutrinário certa diferenciação.

Direitos fundamentais, são aqueles direitos que encontram-se positivados, ou seja, estão devidamente previsto em lei de forma imperativa.

Já os direitos humanos, são os direitos de ordem subjetiva, ou seja, aqueles que valem por si só, não possuindo previsão legal, mas que existem no consciente de todo ser humano, mais precisamente como uma regra moral.

2.2 ORIGEM E EVOLUÇÃO DOS DIREITOS FUNDAMENTAIS

Os primeiros indícios de que surgiam mecanismos para a proteção individual deram-se no Egito e na Mesopotâmia, baseados no Código de Hamurabi, sendo assim o primeiro indício da positivação destes direitos, quais sejam: direito à vida, dignidade, propriedade, prevalecendo estes frente aos governantes da época, o que foi um tremendo avanço.

Neste período nasce a filosofia, que muito contribuiu para a positivação destes direitos, haja vista que substitui o saber mitológico pelo saber lógico da razão assim, passa o homem a ser objeto de reflexão, estabelecendo-se assim os primeiros princípios e diretrizes fundamentais de toda vida em sociedade.

O processo de positivação dos direitos humanos deu-se ainda na Idade Média, mais precisamente com a Magna Carta de 1215, que foi criada com a finalidade de acabar com os poderes ilimitados tanto dos reis quanto do papado,

cessando-se assim os inúmeros conflitos existentes na época, sendo esta a primeira fonte das chamadas Declarações de Direitos Fundamentais, que com o passar dos anos, foi deixando de serem apenas reivindicações políticas e tornaram-se normas jurídicas em razão de sua constitucionalização.

Com o fim da segunda grande guerra em 1945, já no ano de 1948 surge a Declaração Universal dos Direitos do Homem, com a finalidade de combater as atrocidades praticadas no período das batalhas contra a dignidade da pessoa humana.

Diante de todo o exposto contata-se a dificuldade de se estabelecer um marco inicial exato quanto ao surgimento dos Direitos Fundamentais, diante disso se faz por necessário a descrição dos pensamentos de BOBBIO (1992, pag. 68):

> Os direitos humanos positivados não derivam do estado de natureza, o qual foi utilizado apenas como argumento para justificar racionalmente determinadas exigências do homem. Segundo ele, o real surgimento de alguns direitos deriva das lutas e movimentos travados pelos homens cujas razões devem ser buscadas na realidade social da época, e não no estado de natureza, pois este revela a hipótese abstrata de um estado simples, primitivo, onde o homem vive com poucos carecimentos essenciais, oposto ao mundo de onde derivou toda a gama de Direitos Fundamentais que hoje conhecemos.

Conclui-se, portanto, que dizer que houve um marco inicial e específico para a criação dos Direitos Fundamentais não é tarefa fácil, haja vista uma de suas principais características, a mutabilidade.

Mas, o marco inicial mais aceito pelos historiadores do tema, trata-se de seu surgimento na Idade Média, com o cristianismo, haja vista que esta doutrina apontava a igualdade entre homem e Deus, sendo este um dos primeiros esboços da concessão de direitos aos cidadãos da referida época.

2.3 DIREITO À INTIMIDADE

2.3.1 CONCEITO

O direito à intimidade configura-se como um direito fundamental, ao qual confere ao indivíduo enquanto cidadão, o direito de se resguardar de ações praticadas por terceiros contra si mesmo, mais precisamente resguardando sua esfera íntima e privada.

Trata-se de um direito que possui significativas características de mutabilidade, visto que encontra-se sempre em constantes modificações, levando-se e em conta os aspectos históricos e sociais aos quais esta sujeitos.

Há certa complexidade em determinar o que vem a ser "intimidade", pois para que seja feita uma relevante definição, deve-se levar em conta o lugar, a época, bem como os valores sociais, morais e políticos de cada período.

Diante disto, verifica-se que a intimidade possui um caráter no que tange ao seu conteúdo muito amplo e extremamente variável, pois emprega certa dificuldade para que seja determinado com precisão.

Nesse sentido, interessante são os ensinamentos e definições proferidas por Tércio Sampaio Ferraz (1992, p.529), os quais defende que não há um conceito absoluto que preceitue o direito à intimidade.

A intimidade trata-se, portanto, de um direito de personalidade, que por consequência possui características de irrenunciabilidade, sendo assim nenhum indivíduo pode abrir mão em detrimento de seu direito, devendo assim resguardá-lo no seu mais profundo ímpeto. Pois, a publicidade inevitavelmente supera a intimidade.

2.3.2 GARANTIA CONSTITUCIONAL

O direito à intimidade foi promovido à garantia de ordem constitucional, visando assim à proteção do maior bem que qualquer pessoa pode possuir qual seja, a vida. De modo que objetiva-se pela proteção da vida pessoal de todo e qualquer individuo, que só poderá ser revelada ou divulgada com a sua devida permissão.

O direito à intimidade encontra-se descrito no Art. 5º, X da Constituição Federal:

> Art.5º .....
>
> X- São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação.

Sendo assim, toda vez que alguém tiver sua intimidade extirpada, invadida ou divulgada, terá o devido direito à indenização pelo dano sofrido, tanto no âmbito moral, quanto no material.

O direito à intimidade está entre os direitos humanos de ordem fundamental, positivados na Constituição Federal, denominados de "cláusulas pétreas". E devido a isso, não se admite, de maneira alguma, que este direito sofra qualquer medida extintiva ou modificativa.

2.3.3 INTIMIDADE E A VIDA PRIVADA

Tanto o direito à intimidade, quando o direito à vida privada são tutelados pela Constituição Federal, sendo assim ambos guardam entre si grande vinculação.

Contudo, mesmo que seus conceitos se confundam, possuem características distintas, que podem ser objeto de diferenciação. Tais diferenças residem no fato de que a intimidade reside em um caráter mais interno, ou seja, um círculo mais restrito, diferente do direito à vida.

Para melhor entendimento do tema, faz-se por necessário a citação da obra de Tércio Sampaio Ferraz (1992, p. 449):

> A intimidade é o âmbito do exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance da sua vida privada que, por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer comum). Não há um conceito absoluto de intimidade, embora se possa dizer que o seu atributo básico é o estar só, não exclui o segredo e a autonomia. Nestes termos, é possível identificá-la:

> o diário íntimo, o segredo sob juramento, as próprias convicções, as situações indevassáveis de pudor pessoal, o segredo íntimo cuja mínima publicidade constrange.

Sendo assim, pode-se entender que o direito à intimidade caracteriza-se pela esfera mais íntima de proteção à pessoa, tais como seus pensamentos, seus desejos e suas emoções.

Dizendo respeito ao modo de ser da pessoa, à sua identidade, sendo uma conceituação mais estrita da vida privada. Sendo a esfera mais íntima da pessoa, abrangendo um âmbito mais limitado, ligada a uma acepção estrita, à zona espiritual da pessoa.

Já a vida privada ou a privacidade, caracteriza-se pelo caráter mais amplo do que a intimidade, ou seja, tudo o que não transparece para a esfera pública, sendo as ligações com os indivíduos de caráter mais próximo, entende-se por relações familiares ou pessoas de contato diário.

Ou seja, a privacidade encontra-se resguardada por um caráter de maior abrangência subjetiva, de modo que o individuo estende seus aspectos pessoais para determinado grupo de pessoas, grupo este que se encontra no convívio social da pessoa.

Faz-se de maneira oportuna a exposição do pensamento de Tércio Sampaio Ferraz (1992, p.449) sobre o tema:

> A vida privada pode envolver, pois, situações de opção pessoal (como a escolha do regime de bens no casamento), mas que, em certos momentos, podem requerer a comunicação a terceiros (na aquisição, por exemplo, de um imóvel). Por aí ela difere da intimidade, que não experimenta esta forma de repercussão.

Conclui-se, portanto, que de fato só a própria pessoa pode pelo seu respectivo comportamento estabelecer o âmbito e o limite de sua intimidade, entendendo-se assim pelo seu sentido mais estrito.

Por fim, a vida privada manifesta-se para o exterior, estando mais exposta e regida por regras e costumes de convivência social.

2.4 DIREITO Á INFORMAÇÃO E A INTERNET

Assegurado pela constituição federal, o Direito à informação encontra-se previsto no Art. 5º, inciso XXXIII, onde diz:

> XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

Conforme o exposto acima, vivemos em uma sociedade, onde perdura a máxima de que informação é poder. Deste modo, configura-se que a informação passa a ser um meio de formação de idéia e interpretação de pensamentos e também possibilitando a difusão de notícias e acontecimentos possuindo assim, importância fundamental na sociedade atual.

A problemática reside quando o objeto são os dados pessoais, exigidos pelo Estado para um efetivo controle da máquina estatal, que na maioria das vezes são dados atinentes à vida pessoal dos cidadãos. Com o passar do tempo, foi adotado pelo Estado o sistema de digitalização destes dados pessoais, ou seja, foram todos armazenados nos bancos de dados do governo, o chamado tratamento automatizado da informação pessoal.

Deste modo, a intimidade das pessoas possui maior vulnerabilidade, vez que encontra-se livremente disponível na Internet e em certas mídias sociais.

O direito de informação encontra-se pautado em 03 (três) vertentes básicas, quais são: o Direito de informar, o Direito de ser informado e o Direito de se informar.

O direito de informar consiste na liberdade de transmissão das informações, ou seja, certos meios que tem como finalidade transmitir qualquer tipo de informação.

O direito de se informar possui como escopo o direito que todo e qualquer cidadão possui de receber as informações que pretende.

E por fim, o direito de ser informado surge no momento em que alguém possui um dever de informar, como podemos verificar nos órgãos públicos este respectivo dever.

Em um mundo contemporâneo onde as informações encontram-se basicamente situadas nos meios eletrônicos, o exercício do direito à informação, deve ser realizado por meios de pesquisas eletrônicas na rede, para que isto não configure uma violação da privacidade ou de eventual sigilo que possua a respectiva informação.

Alguns dados como o sigilo fiscal, bancário, telefônico e até mesmo prontuários médicos, possuem caráter sigiloso, devendo assim serem respeitados sob pena de invasão à privacidade e exposição da vida privadas de algumas pessoas.

Conclui-se, portanto, que direito à informação é direito que todo e qualquer cidadão possui, de poder consultar eventuais informações albergadas na Internet, pois na maioria das vezes tais informações possuem caráter publico, haja vista que encontram-se em um meio extremamente difundido e público.

Em suma, todos os cidadãos pertencentes a um Estado democrático de direito, possuem o direito de se informar de eventuais dados necessários pertencentes a outros cidadãos, mas sempre se levando em conta que certos limites devem ser respeitados, para que não ocorra a deturpação deste direito.

3. A INTERNET

3.1 A HISTÓRIA DA INTERNET

O surgimento da internet deu-se a partir de pesquisas militares nos períodos pertencentes à Guerra Fria, em uma época em que qualquer inovação deste caráter poderia ser decisiva para a batalha em que encontravam-se União Soviética e Estados Unidos da América.

Deste modo, o governo dos Estados unidos temia que suas bases militares fossem atacadas e assim, com este ataque, suas informações de caráter extremamente sigiloso poderiam vir à tona. Partindo deste pressuposto, configurou-se a necessidade de se criar um mecanismo que difundisse, espalhasse estas informações, para que não fossem encontradas todas juntas em eventuais ataques militares.

Dessa forma, criou-se uma rede denominada de ARPANET, que funcionava a partir de um sistema de codificação ou de chaveamento, onde as informações transmitidas eram armazenadas em pacotes distintos, podendo ainda ser conectada a redes de outros países.

Na prática, o ataque temido jamais ocorreu, mas tudo isso contribuiu para o surgimento do maior fenômeno midiático no século 20, que conseguiu atingir cerca de 50 milhões de pessoas no mundo.

No Brasil, a internet surgiu a partir do ano de 1987, onde realizou-se uma reunião entre Governo e a empresa EMBRATEL, com o objetivo de criar-se uma rede que possibilitasse a interação entra a comunidade científica e acadêmica do Brasil com outros países, com o fim de compartilhar informações.

No ano de 1988, o Laboratório Nacional de Computação Científica conseguiu se conectar a Universidade de Maryland, de modo que possibilitou-se a troca de mensagens entre estas instituições.

Por fim, no ano de 1955 realizou-se a primeira transmissão de longa distância entre estados brasileiros e após isto, foi liberada a operação comercial no Brasil, permitindo assim ao setor privado o acesso à internet para fins de exploração comercial no Brasil.

Assim sendo, a internet ganhou vida em nosso dia a dia, e cada vez tornando-se mais presente como ferramenta de trabalho, informação, comunicação e entretenimento.

3.2 UMA BREVE ABORDAGEM ACERCA DO FUNCIONAMENTO DA INTERNET

Entender o que é e como funciona a Internet faz-se por imprescindível, para que seja feito qualquer desenvolvimento de um trabalho atinente à proteção jurídica necessária de um direito nesta seara, no caso o direito à intimidade.

A internet não é apenas uma rede de computadores interligados, mas sim uma rede em caráter mundial de computadores, que se comunicam através de protocolos TCP/IP (Transmission Control Protocol / Internet Protocol).

Segundo Marcelo Cardoso Pereira (2006, p.36):

> A internet é uma rede de computadores formada por milhões de outras redes, e tendo em vista que tanto os computadores como as redes comunicam-se obedecendo a determinados protocolos, é necessário por que não dizer obrigatório, que façamos uma aproximação aos protocolos mais importantes que permitem o funcionamento técnico da Rede (TCP/IP, HTTP,WWW,HTML)"

O protocolo TCP/IP consiste basicamente em um programa que fragmenta em partes uma mensagem enviada de um computador para outro, para que possa ser transferida pela Rede até seu destino final. O protocolo TCP então é o responsável de organizar, transportar, fragmentar e supervisionar as informações através da internet e ainda, se algo se perder durante este processo, ele será o encarregado de proceder o reenvio da parte que se perdeu.

Já o protocolo IP, se diferencia do endereço IP, um dos mais conhecidos assuntos na internet, que consiste em toda vez que firmamos um contrato de acesso com a Rede, surge um número que passará a ser o nosso endereço na Rede, o endereço IP, possuindo assim cada máquina seu número de identificação, que jamais será igual a qualquer outro número.

O protocolo IP, por sua vez, possui a função de estabelecer os endereços de origem e de destino de cada uma das partes, pois o protocolo TCP não sabe a qual computador enviar as informações desejadas.

O protocolo HTTP consiste basicamente na transferência de informações entre o usuário e o servidor de internet, e vice-versa. Quando inserimos uma URL (meio de se localizar servidores existentes na internet) em nosso servidor, este se encarrega de enviar o respectivo pedido ao servidor web, solicitando alguma

informação que encontra-se depositada na Rede, que no final resultará na página da web conhecida por todos os usuários da internet.

3.3 ALGUNS SERVIÇOS OFERECIDOS PELA INTERNET

3.3.1 WORLD WIDE WEB (WWW)

O surgimento da World Wide Web, ocorreu em meados do ano de 1992, mais precisamente no mês da janeiro deste mesmo ano, através do chamado FPT anônimo, programa este necessário à web, sendo os navegadores padrões conhecidos por todos atualmente.

A partir deste momento, a WWW encontrava-se disponível para qualquer pessoa acessá-la.

Atualmente, o prenome WWW é de conhecimento público e notório, constituindo-se basicamente na união de dois fatores imprescindíveis, quais sejam: o hipertexto e internet, sendo considerada pelo estudioso Berners-Lee, a ferramenta mais importante de toda a Rede mundial de computadores.

Marcelo Cardoso Pereira (2006, p.56) explica sucintamente o funcionamento básico da internet (web):

> O protocolo HTTP, o qual, já se sabe, trata-se do protocolo de comunicação utilizado no âmbito da web. Assim, o que o navegador foi, com base em um endereço da Internet (um URL, como dito anteriormente), solicitar ao servidor web uma determinada informação, arquivo, enfim, uma pagina web. Gravas ao protocolo HTTP, a solicitação é enviada desde um computador a um determinado servidor web, que, em seguida, e uma vez que seja um endereço URL valido, enviará a informação solicitada até o browser, o qual será responsável de ler as instruções HTML e apresentar na tela do computador a copia da pagina web que fora solicitada inicialmente.

Sendo assim, pode-se afirmar que a web é uma tecnologia que nos permite o acesso a documentos de hipertexto, para que possa ser recuperadas informações nos servidores web.

Deste modo, está devidamente evidenciado que a WWW, com o devido auxílio dos navegadores, permite aos usuários de internet acessar os documentos desejados, conhecidos como páginas na web.

Por fim, cabe ainda ressaltar que há a possibilidade de haver violação ao direito dos usuários, mais especificadamente o direito à intimidade na própria Web, que será objeto de estudo em seguida.

3.4 POR QUE A INTERNET OFERECE PERIGO PARA A INTIMIDADE DE SEUS USUÁRIOS

Atualmente, a internet passou a figurar como um dos principais meios, senão, o principal meio de interação entre pessoas. Alem disso, possui característica de ferramenta essencial em nossas vidas, pois é por meio dela que realizamos buscas do que desejamos, nos relacionamos, trabalhamos, efetuamos pagamentos, ou seja, quase tudo é realizado na seara virtual.

Marcelo Cardoso Pereira (2006, p.164): explica-nos bem os "rastros" e informações que deixamos depositadas na Rede, que pode acarretar para nós inúmeros prejuízos, conforme segue:

> A maioria dos serviços disponíveis na internet, centra-se no modelo cliente/servidor (envio de solicitações e recebimento de respostas). Isso resulta que "mover-se" pela Rede signifique interação. Quando um usuário se conecta à Internet e começa a " locomover-se " por ela, vai deixando muitos " rastros" (dados e informações, de caráter pessoal ou não) por onde passa (paginas web, mailing, list, grupo de NEWS etc.)

Partindo desta premissa, constata-se que não somente o usuário pode consultar dados e informações de seu interesse, mas também, outros internautas também podem ter acesso a seus dados e informações.

Há de se ressaltar ainda, que há outro fator que evidencia o caráter de vulnerabilidade da Internet facilitando assim os atentados e o furto de informações e dados pessoais confidenciais, são os chamados bugs, que acabam por facilitar o acesso de pessoas de má-fé a dados pessoais de terceiros para fins delitivos.

Deste modo, os usuários da Rede são alvos fáceis de manipulações e de furtos praticados contra seus dados pessoais para utilização em fins ilícitos, passíveis ainda de discriminações seja de ordem social, cultural ou religiosa, de modo que fica muito difícil impedir que tais ataques sejam realizados.

Dessa forma, todo e qualquer usuário que se conecte a Internet, mediante computador privativo, se transformará em uma potencial vítima de abusos no que tange a sua intimidade.

4. OS CIBERCRIMES

4.1 CONCEITO

Cibercrime é o nome dado à prática que consiste no fim de fraudar a segurança de computadores, bem como a exposição de seus dados pessoais e também a invasão de redes empresariais e governamentais.

Mais precisamente, conceitua-se assim os delitos oriundos dos meios informáticos, Ricardo M. Mata Y Martin (2011, p.21/25) dizendo que :

> Crimes de computador, deve ser toda ação dolosa que provoca um prejuízo a pessoas ou entidades, utilizando-se para sua consumação, dispositivos habitualmente empregados nas atividades de informática, devendo sempre estes comportamentos estarem ligados a práticas antijurídicas , não éticas e desautorizadas , cometidos por intermédio da automação de dados.

Interessante também é a conceituação dada por Marco Aurélio Rodrigues da Costa (2012, *on-line*) ao afirmar que crimes de virtuais são:

> "É a conduta que atenta contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar. Isto posto, depreende-se que o crime de informática é todo aquele procedimento que atenta contra os dados, que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão. Assim, o crime de informática pressupõe dois elementos indissolúveis :

> contra os dados que estejam preparados às operações do computador e , também , através do computador, utilizando-se de software e hardware , para penetrá-los. Conclui-se que aquele que ateia fogo em sala que estiverem computadores com dados, com o objetivo de destruí-los, do mesmo modo, aquele que utilizando-se de computador, emana ordem a outros equipamentos, e causa, por exemplo, a morte de alguém. Estará cometendo homicídio e não crime de informática."

Por fim, faz-se por necessário a transcrição dos pensamentos proferidos por Fernando Peres (2012, p.98):

> Em um sentido amplo todos eles se referem ao ato pelo qual um ou mais computadores são utilizados como meio da realização de um crime. Seja qual for o resultado final do crime, o computador, incluindo suas variações, assim como aparelhos eletrônicos como, por exemplo, o telefone celular se transformam em ferramentas para a criação, desenvolvimento ou efetivação de um crime. De acordo com Guimarães e Furlaneto Neto (2003, p. 69) Crime Informático significa:
>
> Qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados. Essa categoria de crime apresenta algumas características, dentre elas: transnacionalidade – pois não está restrita apenas a uma região do globo – universalidade – trata-se de um fenômeno de massa e não de elite – e ubiquidade – ou seja, está presente nos setores privados e públicos.
>
> O Crime cibernético pode levar a produção de danos tanto pessoais quanto materiais. Os danos pessoais podem ocorrer, por exemplo, no envio de mensagens eletrônicas (e-mails) com conteúdo que afete a liberdade individual, enquanto que um dano material pode ser causado por um agente mal intencionado que rouba as senhas de acesso de um sistema de serviço bancário pela Internet (internet banking), causando danos financeiros ao realizar transações financeiras ilícitas.

Considerando assim, os elementos acima transcritos, constatamos que crimes de computador, ou popularmente conhecidos como cibercrimes, são condutas de natureza omissiva ou comissiva, típica, antijurídica e culpável, em que se utiliza do intermédio de um sistema de informática, atrelado a um computador, facilitando-se assim sua execução e consumação . Tendo como objetivo final causar prejuízos a terceiros, ainda que o autor do fato típico não seja beneficiado por sua respectiva conduta, e que a potencial vítima sofra ou não, direta ou indiretamente, os efeitos desta invasão.

4.2. ORIGEM E EVOLUÇÃO DOS CIBERCRIMES

Com a criação desta gigantesca rede tecnológica citada a pouco e com a generalização dos meios informáticos, a partir da década de 1970 houve em consequência da criação deste chamado "mundo virtual" uma consequente incidência de delitos/crimes na seara digital, haja vista que os criminosos migraram do espaço físico, para este novo espaço virtual a fim do cometimento de crimes.

Faz-se de extrema relevância reproduzir a analise histórica da origem e evolução destes cibercrimes trazida por Marcelo Xavier de Freitas Crespo (2011, p.32):

> A sociedade de informação não surgiu repentinamente. Adveio de um longo processo de desenvolvimento, que, entendemos, num sentido amplíssimo pode ter o inicio vinculado à própria Revolução Industrial. Esta consistiu em um conjunto de mudanças tecnológicas com significativo reflexo na cadeia produtiva, seja em nível econômico, seja em nível social. Iniciada na Inglaterra ainda em meados do século XVIII expandiu-se pelo mundo a partir do século XX.
>
> O impacto da Revolução Industrial se verificou pela substituição da força humana pelas máquinas, tendo a era agrícola perdido espaço, impondo-se novas relações entre o capital e o trabalho, estabelecendo novas relações entre as nações. "Disso também se deu a disseminação do uso da eletricidade, bem como o desenvolvimento da física e da química, o que foi providencial para o surgimento dos computadores" (grifo nosso).

Deste modo, verifica-se que na referida parte histórica supracitada, houve a substituição da mão de obra humana, pela mão de obra oriunda de máquinas, e mais tarde ocorrendo ainda a substituição da atividade intelectual humana também pelos meios tecnológicos. Sendo assim, acarretando no surgimento de ilícitos que migraram para estes meios informáticos.

Seguindo tal raciocínio, Rovira Del Canto (2002, p.32/33) discorre algumas linhas, dividindo-as em partes históricas acerca do surgimento e da implementação dos computadores juntamente com a prática de ilícitos virtuais da seguinte forma:

> a) década de 50. Os computadores passaram a ser empregados na indústria, e que em pouco tempo, já se tinha noticias de ações ilícitas praticadas com o uso dos computadores.
>
> b) década de 60. Com o processamento massivo de dados pessoais em bancos eletrônicos de dados, alguns países passaram a ter alguma

> preocupação com o armazenamento, transmissão e conexão de dados pessoais.
>
> c) década de 70. Época de rebeldia juvenil em meio a ideais Orwellianas (teoria do Grande Irmão). Nessa época, houve generalização do uso dos computadores e sistemas informáticos nas atividades comerciais e empresariais, bem como a implantação de redes abertas que, logo, foram alvo de acesso ilegal (ou hacking)
>
> d) década de 80. Com a expansão dos computadores ao uso pessoal, surgiu e disseminou-se a pirataria de programas informáticos. O aparecimento dos caixas eletrônicos (ATMs ou Automatic Teller Machines) foi alvo da fraude dos cartões magnéticos.
>
> e) década de 90. Aqui temos o auge da convergência entre informática e telecomunicações, a generalização e extensão dos computadores, internet e serviços eletrônicos a quase todas as áreas da vida... Isso fez com que o uso passasse a ser feito não só por particulares, empresários, administrações, mas também por grupos racistas, neonazistas, criminosos econômicos e organizações criminosas, de tal forma que a tecnologia informática começa a integrar não só a vida em geral, mas o crime em geral. A sociedade atribui mais importância aos bens imateriais (depósitos em dinheiro, propriedade intelectuais, segredos comerciais) que não só adquirem outro valor, mas transformam-se em fator de poder.

Sendo assim, tal desenvolvimento culminou com a criação da denominada Sociedade da Informação, conferindo maior importância aos bens imateriais, de modo que a informação passou de apenas ter um valor econômico, passando assim a simbolizar forma de poder.

E ainda, por consequência lógica, os sistemas de defesas passaram cada vez mais a depender da informática, o que gera grande manipulação de informações, quase sempre utilizadas para o fim de cometimento de ilícitos, por intermédio de computadores.

4.3 MODALIDADE E CLASSIFICAÇÃO DOS CIBERCRIMES

São varias as classificações utilizadas por doutrinadores da área no que tange aos crimes virtuais, sendo que uma delas confecciona a divisão entre estes delitos, sendo os crimes virtuais próprios e os crimes virtuais impróprios.

Deste modo, faz-se por necessário a classificação dada por Marcelo Xavier de Freitas Crespo (2011, p.63/64):

> Assim, entendemos que a melhor classificação, porque mais objetiva e passível de enquadrar as condutas ilícitas mais modernas é aquela adotada por Ferreira e também por Grecco, assim representada: a) condutas perpetradas contra um sistema informático; b) condutas perpetradas contra outros bens jurídicos.
>
> As condutas praticadas contra um sistema informático ou dadas são o que se pode chamar de delito de risco informático, ao passo que as demais podem ser denominadas delitos vinculados à informática.
>
> Nesse sentido, podemos dizer que todas as condutas praticadas contra bens jurídicos informáticos (sistema, dados) são delitos de risco informático ou próprios. Ao passo que aquelas outras condutas que se dirigirem contras bens jurídicos tradicionais (não relativos à tecnologia) são crimes digitais impróprios.
>
> Assim, parece-nos que a divisão em meios eletrônicos como objeto protegido (bem jurídico) e meios eletrônicos como meio/instrumento de se lesionar outros bens é a melhor das classificações, por ser mais ampla e permitir melhor discorrermos acerca das práticas.(grifo nosso)

Há ainda outra classificação, porém de menor importância e pouco defendida pelos doutrinadores da área, é a chamada classificação tripartida, editada por Aldemário Araújo Castro, conforme segue (2005, p.56) :

> a) Os crimes de informática puros, onde o agente objetiva atingir o computador, o sistema de informática ou os dados e as informações neles utilizadas; b) os crimes de informática mistos, onde o agente não visa o sistema de informática e seus componentes, mas a informática é instrumento indispensável para a consumação da ação criminosa e c) os crimes de informática comuns, onde o agente não visa o sistema de informática e seus componentes, mas usa a informática como instrumento (não essencial, pois poderia ser qualquer outro meio) de realização da ação.

Estas são algumas das várias classificações dadas aos crimes virtuais, sendo que aqui foram transcritas as mais relevantes e de maior abrangência doutrinária. Verifica-se que os cibercrimes possuem característica própria de mutabilidade, de modo que o ordenamento jurídico se vê impossibilitado de acompanhar eventuais mudanças no que tange a estas práticas delituosas, e a passos lentos novas tipificações vão surgindo, enquanto que a incidência destes delitos aumenta gradativamente de maneira inversamente proporcional à sua tipificação.

4.3.1 CRIMES VIRTUAIS PRÓPRIOS

Há de se ressaltar que os delitos virtuais próprios atingem bens jurídicos como os sistemas de informática ou de telecomunicações ou ainda os sistemas de dados.

Sendo os delitos que possuem tanto sua execução quanto sua consumação ocorridas nos próprios meios informáticos onde o bem jurídico tutelado é a informática.

Os delitos de informática denominados de próprios são crimes pelos quais só podem ser praticados única e exclusivamente por intermédio da informática, ou seja, só existem em razão da informática. Em razão disto, são estes os delitos que mais causam problemas aos usuários uma vez que em sua grande maioria não possuem qualquer tipificação penal que o considere como um crime.

A seguir serão transcritos os principais crimes virtuais próprios, que possuem maior abrangência doutrinária e que configuram a ampla maioria das práticas criminosas por intermédio dos meios informáticos.

4.3.1.1 ACESSO NÃO AUTORIZADO

Marcelo Xavier de Freitas Crespo (2011, p.69) define o "acesso não autorizado" como:

> O acesso não autorizado é também conhecido como " invasão " ou ainda , hacking (condutas praticadas pelos conhecidos hackers). A conduta de acessar de forma indevida um sistema informático pode se dar por varias razoes como pelo mero gosto por superar desafios técnicos de segurança, pela vontade de invadir a privacidade alheia tendo acesso a informações sigilosas, ou, ainda, por se ter a intenção de manipular, fraudar ou ainda sabotar dados. O acesso não autorizado, é, portanto, o ilícito básico para a pratica de outros tantos possíveis.
>
> Importante salientar que, quanto ao acesso, pode-se falar em diferentes níveis. Assim, alguém pode ter acesso apenas à leitura, à escrita, à execução ou, ainda, a todas as formas anteriores. Tudo depende da autorização de acesso, que é o que confere legitimidade à disponibilidade dos arquivos em um sistema.

> As técnica mais atuais de acesso não autorizado abarcam o modo indireto e até mesmo passivo, e que a própria vitima atua ao visitar paginas simuladas ou por meio do *web spoofing*,o que se dá pelo manejo dos protocolos IP (Protocolo de internet) e HTTP (Protocolo sobre transferência de hipertexto, enganando o usuário , que se dirige a uma página sem que saiba do perigo em acessá-lo.

A doutrina afirma que este modalidade ilícita de acesso não autorizado é uma das práticas delituosas mais frequentes ocorridas no âmbito informático. Entretanto, verifica-se que esta prática é vista mais como um meio e não como o fim do delito, haja vista que o crime seria de perigo uma vez que o mero acesso não traria grandes prejuízos a vitima, mas que através deste acesso o desdobramento poderia ser muito grande, como a disponibilização de informações sigilosas resultando assim em um enorme leque de crimes que podem advir desta violação ao acesso de informações pessoais, sendo possíveis ilícitos civis, administrativos e até penais.

Há de se ressaltar que a Lei nº 12.737/12, inovando na ordem legislativa vigente, passou a tipificar o acesso não autorizado à dispositivo alheio como um ilícito penal, de forma que se o sujeito invadir dispositivo alheio, violando algum tipo de sistema de segurança que aquele computador possua, tal conduta será tipificada como crime.

De forma que deve o agente violar algum tipo de dispositivo de segurança, sem o consentimento da vítima, e só assim estará configurada a tipificação criminal desta prática delituosa, trazida por esta legislação.

Conforme é trazido pelo Art. 154 –A da Lei nº 12.737-12 :

> 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."

E assim, verifica-se que para a incidência do agente no referido tipo penal, faz-se por imprescindível violação de dispositivo de segurança, sem o conhecimento da potencial vítima.

4.3.1.2 OBTENÇÃO E TRANSFERÊNCIA ILEGAL DE DADOS

Outro método também utilizado com o fim de garantir a prática de crimes de informática é a "obtenção e transferência ilegal de dados", conforme conceitua Marcelo Xavier de Freitas Crespo (2011, p.70):

> O acesso a dados de um sistema informático pode se dar por muitas maneiras. Atualmente, uma forma muito simples de obtê-los é por meio dos spywares, termo genérico para disseminar arquivos espiões. Um spyware nada mais é que o programa que rastreia informações do usuário contidas em seu computador, como, por exemplo, os sites que costuma visitar.
>
> Há spywares, que funcionam espionando as praticas do usuário, inclusive quanto a atividades confidenciais ou protegidas pela intimidade. Ainda, se essa pratica não é a mais deletéria por causar danos aos usuários, já que se considerar as discussões sobre a legalidade desse recurso como pratica comercial infringente a intimidade e até mesmo a questão da invasão da privacidade que se impõe às pessoas.
>
> Na mitologia fala-se em cavalo de troia, estes *spywares* possuem os cavalos de troia, que são a versão mais moderna dessa fraude. Sendo programas que aparentam terem utilidade, mas que trazem escondidos em

> si alguma espécie de *malware* invasivo que possibilita o cometimento de atividades prejudiciais aos usuários de um computadores, inclusive pela coleta e envio d dados privados.

Havendo ainda os chamados keyloggers, que são programas que memorizam e gravam as teclas digitadas no teclado da vítima. De modo que possibilitam a obtenção ilícita de senhas de contas bancárias e acesos a diversos sistemas pessoas da vítima.

Tendo em vista ainda, que atualmente grande parte das informações pessoais são guardadas e devidamente armazenadas em nossos computadores, há de se tomar muito cuidado com o que é armazenado em nossos sistemas, uma vez que a todo momento estamos sujeitos a termos nossa privacidade e intimidade violada, e muitas vezes só descobrimos isso após a efetiva ocorrência do dano.

4.3.1.3 DANO INFORMÁTICO

O denominado dano informático advém da prática de disseminação ou contaminação de máquinas de computadores pelos conhecidos vírus.

O dano informático é também conhecido no meio virtual pela "sabotagem virtual", sendo a destruição, inutilização ou ainda a deterioração de um sistema operacional alheio.

Segundo o pensamento formulado por Luiz Guilherme Porto (2011, p.98), dano informático é:

> Consiste na destruição de dados ou programas de computadores, principalmente, através dos chamados vírus num sistema ou rede de computadores. É também conhecida como terrorismo ou vandalismo informático, sendo usualmente praticado pelos denominados: hackers.

Faz-se por necessário também a conceituação construída por Guilherme de Souza Nucci (2011), ao dizer que:

> Atualmente, pode-se falar em crime de dano,quando cometido sabotagem informática por vírus, desde que o vírus inserido no computador alheio, por qualquer meio, afete seu funcionamento de modo relevante ou destrua algum de seus programas. Não basta a mera confusão nos arquivos ou lentidão no seu funcionamento.

A real problemática acerca da tipificação penal do crime de dano informático se faz justamente pela ausência de qualquer tipificação deste delito em nosso Código Penal, haja vista que nosso ordenamento apenas tipifica o crime de dano em relação a coisas em seu aspecto material, ou seja, o dano informático afeta na maioria dos casos a coisa imaterial (dados informáticos), e nosso ordenamento não prevê proteção jurídica quanto as coisas imateriais, como no caso os sistemas de informática e dados informáticos ora havidos como prejudicados.

Não resta nenhuma dúvida que o crime de dano é perfeitamente possível contra coisas materiais, quando cometido contra o próprio computador físico, uma impressora, seu monitor, etc... . Pois, são todas coisas materiais, sendo assim perfeitamente enquadrados como objetos do crime de dano sendo alcançados pelo referido tipo penal.

O Art. 163 do código penal apenas distribuiu sua tutela jurídica, tendo em vista a “coisa móvel” propriamente dita deste modo, entendem majoritariamente que a coisa, dados, não é tida como coisa de caráter móvel, sendo assim não pode fazer parte do tipo penal do referido artigo. Tendo em vista ainda a proibição da *analogia in malam partem* em sede de direito penal. Ou seja, não se pode ampliar a aplicação da lei se a própria lei não previu a tipificação de eventual conduta.

Sendo assim, não é possível considerar fato típico dano a eventuais dados informáticos, pois em havendo a referida conduta não haveria a destruição de nenhuma coisa móvel, haja vista que dados informáticos não são considerados coisas e em assim entendendo, não seria possível a aplicação do referido tipo penal.

Por fim, conclui-se que o direito penal brasileiro não possui em seu ordenamento jurídico qualquer tipificação penal acerca do crime de dano informático, conforme entendimento de Rita de Cássia Lopes da Silva (2003, p.51):

> O direito brasileiro não tem em sua legislação penal matéria atinente ao dano causado por meio de sistema de informática, deste modo três são os pontos de destaque : a necessidade de cuidado no tentar adaptar as leis existentes aos delitos que tenham sido praticados por intermédio do computador; a existência de casos, cujo uso do computador poderia ser circunstancia de aumento de pena ; e outros casos que vislumbram situações novas, nascendo a necessidade de se criar um tipo novo.

Levando-se ao inevitável confronto das correntes tratadas acima, verifica-se a existência de grande divergência acerca da aplicação e tipificação do dano informático no Brasil, surgindo assim três correntes que esgotam o referido tema. A primeira diz que o crime de dano encontra-se tipificado no Art. 163 do Código Penal, deste modo podendo ser tipificado não só crimes contra coisas materiais, mas também contra coisas imateriais, que é o caso do dano informático. O segundo entendimento diz que é de extrema necessidade a criação de um tipo penal novo, tratando-se assim especificadamente do dano informático.

E por fim, a última corrente, e a qual me filio, defende uma adaptação ao tipo do Art. 163 do Código Penal admitindo, portanto, que dados informáticos ou sistemas informáticos também são “coisas” e em assim entendendo, agindo de forma legalmente amparada pela interpretação extensiva da norma, ou seja, buscando o real sentido e significado do texto legal qual seja a proteção de todo e qualquer dano patrimonial.

Não se está, pois, acrescentando um novo conteúdo à lei, mas apenas ampliando o significado da palavra “coisa”, que por razões temporais (Código Penal concluído no ano de 1940) era impossível de ser previsto pelo legislador, mas certamente estava contida esta sua intenção de ampla proteção na referida norma.

Diante de todo o exposto acima, verifica-se a clara e evidente defasagem de nosso Código Penal em relação ao conceito de “coisa” no que tange a tipificação do crime de dano. Haja vista, que conforme esmiuçado acima, “coisa” para o crime de dano consiste no bem corpóreo, que somente pode ser danificado mediante uma ação física razão pela qual, se encontra a impossibilidade de tipificação do crime de dano virtual no referido artigo.

Contudo, não podemos nos ater às conceituações arcaicas e bastante defasadas pela ação do tempo, e assim, serão trazidos a seguir os pensamentos de Dickson Cirilo Andrade Netto Filho (2012, on-line), que nos elucida com bastante maestria como deve ser feita a devida adaptação do Art. 163 do Código Penal para a possibilidade legal de punição dos crimes de dano digital informático:

> Seguindo nesta linha de pensamento, é conveniente expor que, majoritariamente, o objeto do crime de dano visa à coisa móvel ou imóvel, sendo por obvio uma coisa corpórea no sentido realístico, pois somente essa pode ser danificada por ação física. Logo, para o dano virtual bastaria o ataque ou destruição de arquivos; informações; dados ou até um vírus que acarrete a quebra do corpo físico de um computador, mesmo que não tenham valor econômico, pois, o mesmo pode ter um significado ao seu detentor. Quanto ao dado que possua valor econômico é inquestionável atribuí-lo, quando lesado, a figura do dano virtual.
>
> É até compreensível tratarem a punibilidade desta forma, pois o artigo 163 do CP é voltado a bens patrimoniais, corpóreos, passíveis de serem danificados fisicamente, permissa vênia aos autores supracitados, ainda que o dado ou informação não seja bem corpóreo físico, apresenta status de um bem "corpóreo", mas virtual, formado por vários bytes que são, fazendo uma analogia, os átomos que integram um corpo físico, no caso, um arquivo. Desta feita, quanto à punibilidade, deverá incorrer mediante averiguação do animus nocendi, porém, outro empecilho vem à tona, não há tipificação para "dano digital", desta forma, indaga-se: seria considerado fato atípico, pois tal circunstância afrontaria o princípio da legalidade, disposto no art.1º do CP, "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal"?
>
> Assim, resta cogitar, apenas uma legislação específica terá subsídio suficiente para elucidar tamanho imbróglio ante a inexistência de uma lei que caracterize o dano digital, qual seja, o nosso Código Penal.
>
> Sob este panorama, a legislação alienígena revela-se mais preparada que a nossa, inclusive, afastando a concepção, data vênia, anacrônica de nossos doutrinadores, que ainda enxergam o crime de dano apenas sob o aspecto físico, portanto, alheio a esta linha de pensamento, temos a lei federal nº 18 – U.S.C./1030 dos Estados Unidos prevendo três situações punitivas ao crime de dano praticado através de vírus de computador face os Sistemas de computadores, assim, a primeira punindo o agente que dolosamente, transmite programação, informação, código ou comando, tendo, como resultado, dano a computador protegido (utilizado por instituição financeira - Banco); na segunda, temos a situação de punibilidade do agente que acessar computadores protegidos e culposamente causar danos, no caso, considera-se apenas a negligência; a terceira situação pune o agente que intencionalmente acessar computadores protegidos, sem autorização e causar dano.
>
> O crime virtual, in casu, o crime contra o patrimônio é uma problemática atual e que deve ser vista com cuidado por nossos legiferantes, a omissão legal é algo temeroso, pois ainda que aleguem que nosso Código Penal de 1940 possui feição vanguardista, *concessa vênia,* há uma diferença ainda que tênue entre os crimes praticados no ambiente virtual dos praticados no ambiente real.

> Algo bastante preocupante, pois ao tempo em que o criminoso virtual avança, se aperfeiçoa, descobre novas técnicas vis, nossa legislação permanece estagnada, não é uma questão de preciosismo, de positivismo, mas de uma realidade que urge por uma norma que tanto caracterize as condutas como as puna.

Diante de todo o que foi trazido acerca da tipificação do crime de dano digital, como já bastante explanado e esmiuçado acima, há uma nítida e preocupante defasagem no que se refere ao Código Penal brasileiro acerca da tipificação dos crimes de danos praticados na seara digital. Em decorrência disto, encontra-se ainda certa resistência em adequar o crime de dano digital ao Art. 163 do Código Penal, pelas razoes acima trazidas. Entretanto, para o fim de se tentar ao menos evitar tamanha impunidade alcançada nos meios digitais, faz-se por imprescindível utilizar-se de interpretações extensivas e analógicas para o fim de se conseguir a responsabilização dos agentes criminosos que provocam danos pelos meios digitais, sem que se firam, contudo, os princípios da legalidade e da proibição da *analogia in malam partem"* preconizados por nosso ordenamento jurídico, que serão objeto de estudo mais ao fim do presente trabalho.

4.3.1.4 DOS VÍRUS E SUA PROPAGAÇÃO.

Em um primeiro momento, faz-se por necessário transcrever a conceituação trazida por Marcelo Xavier de Freitas Crespo (2011, p.74/75), acerca dos bastante conhecidos vírus:

> Tal como os vírus que atacam os seres humanos, os vírus de informática podem variar quanto ao seu grau de destruição, podendo trazer ao usuário de um computador no uso do sistema (lentidão, incapacidade de acessar arquivos, dentre outros) bem como a total perda de dados e corrupção de arquivos.
>
> Em suma, vírus nada mais são que programas como outros tantos. Sua peculiaridade está no fato de que, enquanto normalmente os programas visam um aumento na produtividade no ambiente de trabalho, o vírus intentará atravancá-lo, destruí-lo, dificultar-lhe o funcionamento.
>
> O fato é que cada vez mais os vírus são criados e disseminados. Um programa malicioso desses, ao ser instalado no computador de alguém, pode proporcionar danos seriíssimos ao sistema. Basta diz

> quer que todo o conteúdo de um disco rígido pode se perder, o que significaria anos de trabalho e pesquisa que se vão num piscar de olhos.

No que tange à prática de disseminação de vírus, atualmente não há previsão expressa no código penal brasileiro, para que este tipo de crime seja tipificado como conduta ilícita.

Deste modo, entende-se que eventual disseminação de vírus, com o fim de causar danos à propriedade alheia, deveria ser enquadrado no tipo penal do Art. 163 do Código de Penal, haja vista que o referido vírus sempre irá causar algum tipo de destruição ou inutilização de um sistema de computador, como dados pessoais ou ainda arquivos de pesquisas, resultando assim em um dano ao usuário.

Entende-se ainda, que os vírus atingem bens jurídicos corpóreos, uma vez que pode vir a causar dano ao equipamento alheio, vez que além de causar a destruição de dados salvos no computador, pode ainda inutilizar a máquina, causando assim prejuízos de cunho material, e não só afetando bens imateriais.

Mesmo que os vírus apenas afetem os bens incorpóreos, tais como programas, arquivos e dados, devem também tais condutas ser enquadradas na modalidade do Art. 163 do Código Penal, uma vez que o referido dano aos bens imateriais, sempre resultarão em danos a bens materiais, pois a vítima sempre terá prejuízos com a prática destas condutas, seja um prejuízo material propriamente dito, ou imaterial.

Em conseqüência disto, há atualmente um Projeto de Lei de nº 5.074/2013, de autoria do Deputado Major Fábio (DEM-PB), que tipifica criminalmente a propagação e distribuição de vírus de computador. Sendo que eventuais condutas que visam espalhar vírus para computadores alheios, serão punidas com pena de reclusão de um a três anos sem o prejuízo do pagamento de multa.

Sendo assim, não mais se pode ignorar um comportamento que vise espalhar ou disseminar vírus pela rede virtual.

4.3.1.5 EMBARAÇAMENTO AO FUNCIONAMENTO DE SISTEMAS

É a prática conhecida pela interferência em sistemas alheios, e conforme nos ensina Marcelo Xavier de Freitas Crespo (2011,p.81), geralmente esta prática se dá pelos chamados ataques de DoS (Denial of Service ou, no vernáculo, denegação de serviço), conforme segue :

> Em um ataque DoS, computadores são utilizados para tirar de operação um serviço ou outros computadores conectados à internet. Exemplos desse tipo de operação é a geração de grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utiliza-lo; geração de grande tráfico de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador dessa rede fique indisponível ; ou retirada de serviços importantes de um provedor do ar, impossibilitando o acesso dos usuários às suas caixas de correio no servidor de e-mail ou servidor web.
>
> Uma das formas de DoS é solicitar dados ou informações de um servidor e este não aceitá-los posteriormente, de modo que se provoca inúmeras tentativas de envio até saturar-se a capacidade do equipamento , que deixa de funcionar.
>
> Outra forma de se causar uma denegação de serviço é enviar e-mails com endereços de IP falsos, de modo que, quando os servidores tentam responder, não vão conseguir, bloqueando-se paulatinamente as conexões até atingir-se o limite do servidor. Geralmente, para se causar um ataque DoS é preciso ter acesso ao sistema, portanto é comum conviver com a figura do acesso não autorizado. (grifo nosso)

Estes ataques podem ocasionar a retirada de grandes sites do ar, o que consequentemente ocasionaria prejuízos numerosos para o proprietário dos sites afetados. E assim, resultando em sérios prejuízos de caráter material, logo cabendo responsabilização tanto penal quanto civil destas condutas, culminando em eventuais ressarcimentos dos prejuízos causados.

4.3.1.6 ENGENHARIA SOCIAL OU *PHISING*

Para melhor elucidação da referida prática delituosa, faz-se por necessário a conceituação proferida por Marcelo Xavier de Freitas Crespo (2011, p.82):

> O que se denominou recentemente engenharia social há muitos anos já se chama ardil ou artifício fraudulento para o Direito Penal. Entende-se como engenharia social todo método capaz de mascarar a realidade para explorar ou enganar a confiança de uma pessoa detentora de dados importantes a que se quer ter acesso. É o artifício intelectual para acessar informações sigilosas e que, portanto, não utiliza necessariamente tecnologia, mas sim qualquer meio de comunicação. Deste modo, a engenharia social é arma para que se consigam informações sigilosas importantes, mas o faz sempre mediante artifício ou ardil, de forma sub-reptícia.
>
> Importante frisar que tanto a prática de *spamming* quanto a engenharia social são utilizadas em conjunto com tecnologias criminosas desenvolvidas por agentes mal-intencionados, levando, pois, a um cunho criminoso. A engenharia social por si só, no mais das vezes, vai levar à configuração de um estelionato. Entretanto, quando somada à invasão de computador alheio e prejuízo à maquina pode configurar os mais diversos crimes, desde dano até violação de direitos autorais.

O termo *phishing*, deriva do vocábulo "to fish", que traduzido para o vernáculo, significa pescar.

O *modus operandi* da conduta citada consiste, na intenção de enganar as vítimas, de modo que lhe são enviadas mensagens ou até mesmo e-mails, e ao passo que elas efetuem cliques ou até mesmo baixem tais conteúdos, tudo o que possuem gravados em seus computadores serão automaticamente passados para o criminoso, tais como senhas de cartões bancários e informações sigilosas que pertence ao caráter intimo destas vítimas.

Marcelo Crespo (2011, p.83), nos elucida de forma bastante clara, como se dá o funcionamento desta prática, conforme segue:

> A identidade usada nessas mensagens comumente é de órgãos do governo como a Receita Federal ou o Banco central, ou ainda bancos e empresas de cartão de crédito. Essas mensagens trazem links que direcionam para sites falsos, normalmente muito parecidos com os sites verdadeiros, onde existem formulários que a vítima deve preencher com as informações solicitadas. O conteúdo preenchido no formulário é enviado ao criminoso, que se vale das informações em prejuízo da vítima. Outra modalidade recente consiste em informar que foi tomado empréstimo com o número do CPF do usuário e que seu nome irá para a lista de proteção de crédito caso a pessoa não efetue o pagamento ; o usuário é rígido

> para o site do banco ou imprime boleto e os paga. O golpe então encontra-se finalizado.

No Brasil, são utilizados não apenas o nome de entidades famosas para a propagação de falsas mensagens, com o intuito de se apoderar de informações sigilosas alheias, mas também são utilizados diversos tipos de assuntos, com o mesmo objetivo, qual seja de despertar a curiosidade da potencial vítima fazendo assim com que ela efetue o clique ou que baixa a mensagem enviada, e assim fornece involuntariamente suas informações para os criminosos.

São mensagens que possuem caráter pornográfico em seu conteúdo, convites para participar de programas de televisão ou ainda anunciando que a vítima é ganhadora de algo, deste modo inconsequentemente se interessa e ao passo de que baixe a mensagem, suas informações serão todas passadas para o estelionatário.

4.3.1.7 INTERCEPTAÇÃO ILEGAL DE DADOS

A Constituição Federal autoriza a violação ou interceptação das comunicações em geral, somente mediante ordem judicial devidamente fundamentada e devendo-se demonstrar a necessidade de se efetuar tal medida naquele momento, sempre para fins de investigação policial.

Deste modo, a Lei nº 9.296/96 regulamenta as interceptações telefônicas, de modo que será objetivo de sanção criminal o sujeito que realiza tais interceptações sem qualquer autorização judicial ou em caráter de desconformidade com o que preceitua a lei em tela.

Conforme encontra-se descrito no texto da lei supra citada :

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
>
> Pena: reclusão, de dois a quatro anos, e multa.

Deste modo, a referida lei coíbe a interceptação de dados de informática, resultando assim em uma tipificação penal caso eventual prática criminosa venha a ser praticada.

4.3.2 CRIMES VIRTUAIS IMPRÓPRIOS

Os cibercrimes denominados de impróprios consistem nos delitos que podem vir a serem praticados de qualquer forma ou mediante qualquer meio, contudo, o agente se utiliza do meio informático para a prática do delito mesmo que ele tenha a seu dispor vários outros meios, mas o meio por ele escolhido para chegar ao resultado finalístico daquela conduta delituosa for o meio informático.

Os delitos impróprios, quase sempre possuem tipificação da legislação comum mais precisamente no Código Penal, pois são crimes já tipificados em nosso ordenamento, onde o agente apenas se valeu do meio informático para praticá-lo, como por exemplo, crimes de pedofilia, estelionato, ameaça, apologia ao crime, dentre outros que serão a seguir explicitados.

No próximo tópico, serão tratados alguns dos principais crimes virtuais impróprios praticados por intermédio da informática.

4.3.2.1 AMEAÇA

O tipo penal do crime de ameaça tipifica as condutas de intimidar ou amedrontar alguém mediante a promessa de cometimento de um mal grave e injusto, o Código Penal em seu Art. 147 tipifica o delito de ameaça protegendo assim a liberdade e o sentimento de segurança das pessoas.

Por intermédio da informática, mais precisamente da Internet, é perfeitamente possível e até comum atos que carregam em si ameaças de uma pessoa direcionada a outra, tais como o envio de e-mails ofensivos ou ainda a publicação em redes sociais de dizeres ameaçadores sempre direcionados para uma pessoa específica, tais condutas caracterizam o crime de ameaça.

4.3.2.2 PARTICIPAÇÃO EM SUICÍDIO

Esta conduta que culmina em auxílio ao suicídio, foi oportunamente esclarecida por Marcelo Crespo (2011, p.88), onde se traça com maior preciosismo referida conduta, conforme disposto:

> Embora no Brasil o suicídio não seja criminalmente punido, quem ajuda, instiga (refoca a idéia) ou induz (dá a idéia) outra pessoa a se matar responde por crime. Assim, importa responsabilidade penal participar em suicido de alguém seja de forma moral ou material, isto é, seja com gestos e dizeres ou emprestando as ferramentas necessárias para a prática do delito. No Brasil, esta modalidade é mais comum de se verificar nas próprias redes sociais, onde pessoas criam fóruns de como tirar a própria vida ou até mesmo concedendo dicas via Internet, o que é mais comum do que se pensa.

Em tempos do chamado Cyberbullying, onde pessoas constantemente proferem ofensas graves contra outra pessoa, tais dizeres podem ecoar como instigação ou até induzimento à pratica do suicídio das vítimas destas perseguições, conforme previsto no Art. 122 do Código Penal.

4.3.2.3 INCITAÇÃO E APOLOGIA AO CRIME

Referidas condutas, encontram-se amparadas legalmente nos Arts. 286 e 287 do Código Penal, que trazem em suas palavras os dizeres que deverão ser punidas as pessoas que incitam a pratica de crimes, estimulando assim outras pessoas a praticarem determinadas infrações penais.

No âmbito virtual, é muito comum a ocorrência destes crimes uma vez que existem inúmeras páginas e comunidades em redes sociais que defendem e fazem apologia à condutas criminosas, e pessoas que aderem a estas comunidades, paginas e grupos de discussões, podem responder por tais ilícitos.

Portanto, participar de grupos ou páginas que estimulam o preconceito, apóiam agressões, entre outras coisas, poderão ser responsabilizadas por estes crimes.

4.3.2.4 FALSA IDENTIDADE E FALSIDADE IDEOLÓGICA

A lei penal brasileira tipifica vários crimes oriundos da falsa identidade, contudo, os mais comuns e que mais são praticados por intermédio da informática são a falsidade ideológica e a falsa identidade.

O delito de falsa identidade é aquele onde o agente se faz passar por uma pessoa que efetivamente ele não é, utilizando-se de dados pessoas desta pessoa, em proveito próprio com o fim lhe de causar dano. Sendo assim, a falsa identidade nada mais é do que o agente fingir ser quem não é. No crime de falsa identidade somente será o agente punido se a pessoa que ele se baseia realmente exista, ou seja, se aquela identidade falsa pro ele criada for de uma pessoa que efetivamente exista, se for de uma pessoa que não existe ou algum personagem, não será o sujeito punido.

Agora, quanto ao crime de falsidade ideológica, há diferenças, uma vez que neste tipo de delito o agente insere dados falsos ou omite algo que não poderia ter sido omitido em relação a si mesmo, com o objetivo de obter vantagens para si ou para terceiros.

O crime de falsa identidade encontra-se tipificado no Art. 307 do Código Penal, contudo, é um delito de caráter subsidiário, ou seja, só será o agente por ele punido se não tiver praticado crime mais grave.

Por fim, Marcelo Crespo (2011, p.88/89), nos traz ainda os sujeitos que se passam por pessoas conhecidas como celebridades e famosos, e se utilizam da Internet para a criação destes perfis falsos em redes sociais, o que é extremamente comum nos dias de hoje. Sendo assim, a vítima destes criminosos possui direito a pleitear indenizações em caso de comprovados prejuízos sofridos, e ainda podem requerer que tais perfis sejam retirados do ar imediatamente, para o fim de cessar tais abusos e prejuízos.

4.3.2.5 VIOLAÇÃO DE DIREITOS AUTORAIS

Conforme nos ensina Marcelo Crespo (2011, p.89), esta modalidade de delito virtual pode ainda abarcar o uso indevido de marcas e pirataria de softwares:

> Aqui é que se encontra a pirataria, que é o ato de copiar ou vender produto não autorizado pelo detentor dos direitos. Não só pirataria, mas também o uso de marcas e documentos encontrados com o auxílio da Internet pode configurar crime. A nossa lei protege a propriedade intelectual, que se subdivide em dois grandes ramos : a propriedade industrial (refere-se as patentes , desenhos industriais, marcas e nomes de domínio) e os direitos autorais (referentes aos softwares, bancos de dados, documentos técnicos). Não é o simples fato e algo estar disponível na internet que signifique que possa ser usado por qualquer pessoa sem a devida citação da fonte, do autor. Assim, é crime violar direitos de autor de programa de computador, bem como a venda, aquisição exposição à venda, o deposito ou a ocultação, para fins de comercio, de original ou cópia de programa de computador, resultando estas condutas em violação de direito autoral.

Conforme encontra-se disposto na Lei nº 9.609/98, no que tange as violações que não são relativas a software a tipificação das condutas delituosas são punidas com base no Art. 184 do Código Penal, e violações que objetivam a propriedade industrial são punidas pela Lei nº 9.279/96.

4.3.2.6 PORNOGRAFIA INFANTIL

Em prima face, faz-se por necessário transcorrer a passagem muito bem explicitada acerca das diferenças entre pornografia infantil e pedofilia, trazidas por Marcelo Crespo (2011, p.90), conforme segue:

> Primeiramente é preciso deixar claro uma coisa. Muita gente, até mesmo pessoas com formação técnica, cometem o equivoco de denominar "pedofilia" os crimes de divulgação e armazenamento de imagens com conteúdo de pornografia infantil. Também é comum chamar a relação sexual de maiores com menores de idade de "pedofilia". Tecnicamente, pedofilia refere-se a um transtorno da preferência sexual, uma parafilía (um transtorno sexual recorrente), não havendo um crime no Brasil com esta denominação. Ocorre que a lei brasileira pune diversas situações envolvendo a exposição da sexualidade infantil em fotos, imagens e filmagens, trazendo nestes meios crianças ou adolescentes. Também é

> crime transmitir, publicar, distribuir, adquirir, possuir e armazenar vídeos e fotos que contenham situações pornográficas envolvendo crianças e adolescentes, conforme os arts. 240 do Estatuto da Criança e do Adolescente.

Sendo assim, crianças e adolescente possuem proteção tanto no referido Estatuto quanto no Código Penal em seu Art. 217-A, dentre outros tipos penais, tais como a exploração da prostituição e tráfico de pessoas. Assim sendo, qualquer conduta que se valha do meio informático para propagar qualquer tipo de documento com caráter pornográfico envolvendo crianças e adolescentes estará tipificado como uma conduta criminosa.

4.3.2.7 CRIMES CONTRA A HONRA

Os delitos direcionados a ofender a honra de terceiros consistem em deturpar as qualidades físicas, morais e intelectuais de uma pessoa. Sendo assim, a honra merece sua devida proteção quanto a eventuais ofensas, uma vez que se objetiva a proteção da autoestima e o valor social da pessoa, e por consequência possui devida tipificação penal nos Arts. 138,139 e 140 do Código Penal.

São tipos penais que protegem a honra em seu todo, abarcando assim os delitos de calúnia, difamação e injúria que ocasionam lesões à honra das pessoas.

No delito de calúnia, consiste basicamente em atribuir a uma pessoa uma conduta criminosa que ela não praticou, mas o sujeito imputa a ela tal conduta delituosa sabendo que esta conduta é falsa, ou seja, sabendo que a pessoa não praticou o crime a ela imputado. Nos meios informáticos, é bastante comum a referida prática, vez que vários agentes se utilizam deste meio espalhando e-mails caluniosos e ainda com a publicação em redes sociais acerca da atribuição de uma conduta criminosa a outra pessoa acusando-a, como por exemplo, de desvio de verbas públicas sem que se tenha prova sofre tal fato, o que por si só configura o tipo penal de calúnia.

No crime de difamação ocorre a atribuição de fato ofensivo à reputação de uma pessoa, seja este fato verdadeiro ou não, e em sede de redes sociais tal prática é bastante usual, no qual pessoas difamam outras com dizeres pejorativos como o envio de e-mails aos demais usuários da rede dizendo, por exemplo, que tal pessoa é dependente de entorpecentes ou também difamando-as no que tange à sua vida sexual, espalhando boatos que prejudicam a honra destas pessoas.

Por fim, no crime de injúria ocorre a violação da chamada honra subjetiva, ou seja, atribuindo-se qualidades negativas no que tange ao aspecto físico, moral ou intelectual de cada pessoa. Praticando assim ofensas gratuitas e totalmente desnecessárias com intuito de prejudicar aquela pessoa perante seu ambiente social, com o único intuito de lhe prejudicar.

Bastante comum também é a incidência nos meios informáticos de praticas delituosas referentes aos crimes contra a raça humana, uma vez que existem inúmeras comunidades e sites que pregam a discriminação e também a aversão a certas raças e credos, modo pelo qual seus participantes poderão ser responsabilizados por estes delitos, com base na Lei nº 7.716/89 e demais artigos do Código Penal.

Concluindo parte deste estudo acima trazido, faz-se por necessário a transcrição das ideias de Marcelo Crespo (2011, p.92/93), acerca dos principais ataques praticados pelos conhecidos hackers no meio digital:

> a) Uso indevido de senha (pode configurar falsa identidade, falsidade ideológica ou até mesmo estelionato)
>
> b) Vazamento de informações (pode configurar violação de sigilo e concorrência desleal)
>
> c) copia ilegal de dados, desvio de clientes (pode configurar concorrência desleal)
>
> d) uso não autorizado da marca (que pode configurar crime de violação de marcas, patentes ou desenhos industriais)
>
> e) mau uso do e-mail corporativo (que pode levar à corresponsabilização por ilícitos praticados pelo funcionário)
>
> f) pirataria e download de softwares não homologados e download de músicas, imagens ou vídeos.
>
> g) falhas de segurança podem permitir que hackers modifiquem arquivos de modo a permitir que se obtenha acesso a contas de outras pessoas e efetuar transações fraudulentas, como compras e transferências de dinheiro

h) Contaminação por vírus ou trojans (possivelmente crimes de dano).

Os delitos acima trazidos consubstanciam grande parte das condutas criminosas realizadas por criminosos por intermédio dos meios informáticos. Crimes estes, que possuem a devida tipificação penal em nosso ordenamento jurídico penal, mas são praticados por intermédio dos sistemas de informática, ou seja, estes criminosos se utilizam de meios tecnológicos para o fim de disseminação de suas condutas delituosas.

4.4 ELEMENTOS DO TIPO

4.4.1 SUBJETIVO E NORMATIVO

O elemento subjetivo do tipo consiste basicamente na intenção e na vontade do agente causador do mal injusto, ou seja, é necessário que seja feita uma análise psicológica no agente ofensor a fim de constatar a real intenção e a vontade ao momento da prática do delito, em outras palavras, para que seja verificado se o sujeito tinha a real intenção de cometer determinado crime, caracterizando-se pelo dolo.

Já o elemento normativo do tipo baseia-se na exigência de um juízo de valoração, isto é, dependem de uma interpretação, ou seja, uma busca do real significado da norma que não se encontra nela explícito, mas sim devendo ocorrer uma interpretação a fim de se extrair o real significado de determinada expressão. A exemplo disto temos a expressão “mulher honesta” que se trata de um elemento normativo, pois o que seria a mulher honesta que o código antigo queria conceituar? Logo, temos uma expressão que necessita de uma interpretação para o fim de se obter a sua real e correta interpretação.

Conforme nos leciona Zaffaroni (2003, p.447), elementos normativos são

> “Elementos para cuja compreensão se faz necessário socorrer a uma valoração ética ou jurídica.”

Já para Cezar Roberto Bitencourt (2011, p.205), elementos normativos:

> São aqueles para cuja compreensão ‘e insuficiente desenvolver uma atividade meramente cognitiva, devendo-se realizar uma atividade valorativa. São circunstancias que não se limitam a descrever o natural, mas implicam um juízo de valor. São exemplos característicos de elementos normativos expressões tais como “ indevidamente” (arts. 151; 162; 316;317), “sem justa causa” (arts. 153;154;244) “ sem permissão legal” (art. 292); “ coisa alheia” (arts. 155;157) etc.

Posto isso, a seguir serão transcorridos os delitos anteriormente tratados, com o fim de explicitá-los e trazer seus elementos subjetivos e normativos de seus tipos penais.

4.4.1.1 ACESSO NÃO AUTORIZADO

O elemento subjetivo deste delito consiste no dolo, na intenção do usuário de acessar dados, e-mails e informações sigilosas da vítima que são de caráter íntimo e que não deveriam ser acessados por ninguém. O violador possui a intenção e a vontade de obter para si lucro no sentido do furto de informações bancárias, ou ainda causando sérios prejuízos para a vítima uma vez que pode vir a apagar todo o conteúdo de seu computador ou mesmo furtar informações confidenciais utilizando-as para o fim de prejudicar a vítima.

O acesso não autorizado passou a ser tipificado como um delito criminal com o advento da Lei nº 12.737/2012 em seu Art.154-A, conforme segue:

> 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.

Contudo, para que o delito venha a ser tipificado é necessário que se tenha a violação de um dispositivo de segurança, ou seja, neste crime o elemento

normativo do tipo consiste em violar qualquer dispositivo de segurança. Sendo assim, se o agente invade um computador alheio sem que seja violado nenhum dispositivo de segurança, não poderá ser enquadrado neste artigo, uma vez que o próprio artigo traz como elemento normativo do tipo a necessidade de violação de um dispositivo de segurança, qualquer que seja ele, para o fim de configuração do delito em tela.

4.4.1.2 OBTENÇÃO E TRANSFERÊNCIA ILEGAL DE DADOS

O elemento subjetivo deste delito consiste na vontade única e exclusiva de obter para si ou para outrem a transferência ilegal de dados da vítima com intuito de auferir vantagens patrimoniais ou extrapatrimoniais.

O referido delito não se encontra tipificado em nosso ordenamento jurídico penal, todavia, devemos nos socorrer de legislações internacionais para que seja suprida tal lacuna sendo assim, tendo como base a Convenção de Budapeste em seu Art. 6º tipifica o delito de obtenção e transferência ilegal de dados uma vez que coíbe o uso abuso de dispositivos, ou seja, utilizar os chamados *malwares* para que se obtenham dados pessoais de outros usuários, conforme segue:

> Art.6º - Uso Abusivo de Dispositivos
>
> 1. Cada parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer como infrações penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegitimamente:
>
> a) A produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de:
>
> i. Um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para permitir prática de uma das infrações definidas em conformidade com os artigos 2º e 5º.
>
> ii. Uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam aceder a todo, ou a parte de um sistema informático.

Posto isso, conclui-se que para que haja a tipificação do delito acima tratado, faz-se por necessário o elemento normativo da inserção de uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam o

agente obter dados e transferi-los para o seu domínio e assim causando sérios prejuízos para o usuário da rede.

Como trazido acima, esta prática é muito comum mediante a utilização dos *malwares* que são tipos de vírus que são inseridos nos computadores das vítimas disfarçados e assim enganando-as ao ponto delas mesmas, ao passo de um clique, transferir todos os seus dados pessoais para o agente criminoso em potencial.

4.4.1.3 DANO INFORMÁTICO

O crime de dano informático possui como elemento subjetivo o dolo, a vontade livre e consciente de destruir ou apagar dados ou programas de computadores através da propagação ou disseminação de vírus num sistema ou em uma rede de computadores, sendo usualmente praticados pelos denominados *hackers.*

O delito de dano informático não possui uma tipificação específica, uma vez que o Art. 163 do Código Penal tutela apenas o dano em relação às coisas materiais e o dano informático é entendido como coisa imaterial, logo não encontra-se protegido por este dispositivo sendo que ainda, é proibida a analogia *in malam partem* no Direito Penal pátrio. Entretanto, há correntes que norteiam-se em entendimentos contrários ao acima exposto, e possibilitam a tipificação do dano informático no Art. 163 do Código Penal, uma vez que entendem que este tipo penal também abrange coisas imateriais, sendo assim considerando-se para tanto a tipificação do dano informático.

O elemento normativo do crime de dano informático consiste na destruição de coisa alheia, conforme dito no Art. 163 do Código Penal quando especifica: Destruir, inutilizar ou deteriorar coisa alheia.

Sendo assim, para que se configura o delito de dano basta que o sujeito tenha a intenção inequívoca de destruir, inutilizar ou deteriorar coisa alheia, coisa de outra pessoa no caso, da própria vítima do delito.

4.4.1.4 DOS VÍRUS E SUA PROPAGAÇÃO

O elemento subjetivo desta conduta consiste basicamente no dolo de dissemina/propagar vírus por toda uma rede de computadores, com a vontade inequívoca de causar sérios prejuízos advindos dos danos causados por esta conduta.

Em nosso ordenamento jurídico não há ainda uma tipificação criminal para o sujeito que dissemina ou propaga vírus com o fim de prejudicar terceiros, todavia, há doutrinadores que defendem a tipificação deste delito no crime de dano como já foi objeto de estudo acima, contudo, há correntes contrárias e que defendem a impossibilidade de utilizar-se do tipo penal do crime de dano para punir crimes de internet uma vez que se proíbe a analogia *in malam partem,* o que nos traz uma clara e evidente necessidade de se criar um tipo penal para o referido delito e até para os crimes de internet em seu todo.

Sendo partidário da corrente que admite a tipificação dos crimes virtuais no tipo penal do crime de dano, subsidiariamente, quando não houver legislação que trate destes crimes, defendemos que a disseminação e propagação de vírus pela rede devem sim ser coibidas, mediante tipificação das condutas dos *hackers* no crime de dano, responsabilizando-os pelo Art. 163 do Código Penal.

Não podemos deixar de trazer a tipificação dada pela legislação eleitoral em seu Art. 72, II, Lei nº 9.504/1997, a respeito da disseminação e propagação de vírus:

> Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:
> 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;

O referido artigo tipifica o desenvolvimento ou a introdução de vírus em um sistema informático eleitoral, trazendo assim a expressão "introduzir ou desenvolver comando" que em outras palavras é o termo técnico de vírus, logo o

elemento normativo desta conduta norteia-se na introdução ou desenvolvimento de vírus e a sua disseminação em rede.

4.4.1.5 EMBARAÇAMENTO AO FUNCIONAMENTO DE SISTEMAS

O elemento subjetivo desta conduta consiste no dolo e na vontade inequívoca do agente ofensor em atrapalhar, embaraçar e derrubar o funcionamento de sistemas alheios, ou seja, o sujeito tem a intenção, a vontade de derrubar um sistema alheio causando ao usuário inúmeros prejuízos advindos desta prática muito comum.

Em nosso ordenamento jurídico penal ainda não se tem uma tipificação criminal para este tipo de delito sendo assim, devemos nos socorrer da Convenção de Budapeste, em seu Art. 5º, conforme segue:

> Art. 5º - Interferência em sistemas
>
> Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer como infração penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos.

Sendo assim, entende parte da doutrina já citada neste trabalho que em decorrência da ausência de legislação que trate destes delitos, subsidiariamente, há entendimentos que autorizam a tipificação destas condutas como um delito de dano previsto no Art. 163 do Código Penal isto é, se estas práticas efetivamente causarem danos aos usuários o agente causador será imputado pela prática de dano.

4.4.1.6 ENGENHARIA SOCIAL OU *PHISHING*

O elemento subjetivo do delito de *phishing* ou popularmente conhecido como engenharia social norteia-se no dolo e na vontade inequívoca de enganar

mediante artifício fraudulento e/ou ardil, com o fim de obter informações sigilosas. Simplificando, consiste na prática do agente utilizar-se de armadilhas e assim induzindo o usuário a divulgar suas informações de caráter sigiloso, sem que tenha consciência de que se está passando todas as suas informações para o aproveitador.

A engenharia social passou a ser conhecida em nosso Direito Penal como ardil ou artifício fraudulento sendo assim, para que se configura este delito é necessário a presença dos elementos normativos "fraude, artifício ou ardil" + "vantagem indevida" + “prejuízo alheio" e com isso teremos a tipificação do delito de estelionato, conforme segue :

> 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 um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

Posto isso, se o agente espalha na rede mensagens fraudulentas e ainda utiliza-se de fraude, artifício ou ardil obtendo para si ou para outrem vantagem indevida ou causando prejuízo alheio, será responsabilizado pelo caput do Art. 171 do Código Penal.

4.4.1.7 INTERCEPTAÇÃO ILEGAL DE DADOS

O elemento subjetivo do delito de interceptação ilegal de dados consiste basicamente no dolo e na vontade inequívoca de interceptar ligações telefônicas e também a interceptação de comunicação em sistemas de informática e telemática.

A Constituição Federal elegeu como direito fundamental de todo e qualquer cidadão, a inviolabilidade das comunicações em seu todo, conforme trazido em seu Art. 5º, XII:

> 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.

Temos ainda a Lei nº 9.296/96 que trata das interceptações de comunicações em sistemas de informática e telemática, conforme segue:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Posto isso, será enquadrado no Art. 10 da referida lei o sujeito que utilizar-se destas interceptações de dados sem qualquer autorização judicial.

4.4.1.8 AMEAÇA

Trata-se em sua essência de crime doloso e assim sendo, para a configuração do delito exige-se a vontade de ameaçar com a injusta intenção de intimidar e amedrontar, pois, a mera bravata, ou seja, o mero palavreado não configura o delito, sendo portanto necessário que a vítima sinta-se ameaça e altere o seu comportamento costumeiro, em virtude do constrangimento ilegal sofrido.

O delito de ameaça encontra-se tipificado em nosso Código Penal em seu Art. 147, conforme segue:

> Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:
>
> Pena - detenção, de um a seis meses, ou multa.

Conforme nos traz Marcelo Crespo (2011, p.88), acerca do crime de ameaça virtual:

> O mal prometido precisa ser injusto (isto é, que a vítima não está obrigada a suportar) e grave (que possa produzir prejuízo relevante, como a morte, por exemplo). Pode a ameaça ser direta ou indireta, explicita ou implícita. Por exemplo, enviar e-mails ou publicar em redes sociais dizeres como "vou te pegar, vou te matar", configuram crime de ameaça.

Sendo assim, constata-se que para a consumação do delito de ameaça faz-se por necessário a presença do elemento normativo do "mal injusto e grave", ou seja, é necessário que cause efetivamente a vitima a promessa de um mal injusto e grave.

4.4.1.9 PARTICIPAÇÃO EM SUICÍDIO

O elemento subjetivo do crime de participação em suicido é o dolo, seja o genérico ou o dolo específico. O dolo genérico está na vontade livre e consciente de induzir, instigar ou auxiliar alguém a se suicidar, conforme previsto no caput do Art. 122 do Código Penal. E o dolo específico residiria na intenção de que a vitima viesse a se matar.

O delito de participação em suicídio encontra-se previsto no Art. 122 do Código Penal, conforme segue:

> Induzimento, instigação ou auxílio a suicídio
>
> Art. 122 - Induzir ou instigar alguém a suicidar-se ou prestar-lhe auxílio para que o faça:

A participação em suicídio pode se dar por mero induzimento, instigação ou até mesmo o auxílio propriamente dito. Nas duas primeiras formas acima tratadas, tanto induzir quanto instigar trata-se de uma participação moral do sujeito onde será criada ou reforçada a ideia na cabeça da vítima para que esta tire sua própria vida, já na ultima hipótese o sujeito presta auxilio material, ou seja, contribuir materialmente para o resultado finalístico do suicídio concedendo à vitima meios para que ela tire sua vida, como emprestando armas de fogo ou outros meios necessários.

Na seara digital, o referido delito tem ocorrido com certa frequência tendo em vista a prática do conhecido ciberbullying, onde são proferidas ofensas intermináveis contra uma determina pessoa até que chega ao ponto dela não mais aguentar tamanha humilhação, e acaba por tirar sua própria vida. E estas meras ofensas podem ser tipificadas como induzimento ou instigação ao suicídio.

Sem contar ainda, usuários que criam determinadas páginas e até mesmo algumas redes sociais que incentivam a prática do suicídio, concedendo dicas para que o mesmo seja realizado, qualquer destas condutas ou que se assemelhe à ela serão todas tipificadas no Art.122 do Código Penal.

4.4.1.10 INCITAÇÃO E APOLOGIA AO CRIME

O elemento subjetivo do delito de incitação ao crime é o dolo, vontade de se concretizar os elementos objetivos do tipo.

O delito de incitação ao crime encontra-se previsto no Art. 286 do Código Penal, conforme segue:

> Incitação ao crime
> Art. 286 - Incitar, publicamente, a prática de crime:
> Pena - detenção, de 3 (três) a 6 (seis) meses, ou multa.

O elemento normativo neste caso norteia-se na condição do crime ser cometido em público, ou seja, cometido perante um número indeterminado de pessoas. A incitação no caso deve ser para que se pratique um crime determinado e previsto em nosso ordenamento jurídico.

No meio digital, este crime ocorre com certa frequência em meio às redes sociais onde um número indeterminado de pessoas são incitadas a praticarem delitos como preconceito racial, discriminação, dentre outros.

Faz-se por necessário explicitar a diferença entre incitação e apologia, vez que incitação consiste em um crime que ainda não aconteceu enquanto que apologia se faz de um crime que já se consumou ou de seu autor.

Temos ainda, o crime de apologia de crime ou criminoso que encontra-se previsto no Art. 287 do Código Penal, conforme segue:

> Apologia de crime ou criminoso
>
> Art. 287 - Fazer, publicamente, apologia de fato criminoso ou de autor de crime:
>
> Pena - detenção, de 3 (três) a 6 (seis) meses, ou multa.

O elemento subjetivo aqui também consiste no dolo, na vontade inequívoca de se fazer apologia, apoiar e divulgar o seu apoio publicamente a favor de um crime cometido ou de seu autor.

Aqui o delito também deve ser cometido em público, ou seja, a apologia ao crime ou ao seu autor deve ocorrer publicamente aos olhos de um número indeterminado de pessoas.

Nos meios digitais, a apologia de crime ou criminoso ocorre nos casos em que usuários aderem a certas comunidades e/ou grupos de discussões na internet que defendem o preconceito racial, estimulam a prática de agressões físicas e verbais, consumo de drogas e outros ilícitos, condutas das quais serão todos responsabilizados pelo delito do Art. 287 do Código Penal.

4.4.1.11 FALSA IDENTIDADE

O crime de falsa identidade encontra-se criminalmente tipificado no Código Penal em seu Art. 307:

> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
>
> Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

O elemento subjetivo desta conduta é o dolo, ou seja, a vontade inequívoca do sujeito atribuir para si ou para outrem falsa identidade, mas também

faz-se por imprescindível a presença de outro elemento subjetivo, qual seja o fim de obtenção de vantagem para si ou para outrem ou ainda com o fim de causar dano a outrem. Neste caso, o sujeito finge ser quem não é utilizando-se até de dados ou até mesmo a senha de outra pessoa na rede virtual.

Posto isso, será transcrita uma passagem da obra de Ney Moura Teles (2012, p.79), acerca da falsa identidade:

> Identidade é o conjunto dos elementos que individualizam a pessoa. Nome, idade, estado civil, profissão, sexo, cor, condição social, filiação, nacionalidade, personalidade, atributos morais, físicos etc. Cada pessoa tem uma identidade própria, que a distingue dos demais seres humanos.
>
> Realiza o tipo quem, ao se relacionar com outra pessoa, apresenta-se com identidade diversa da própria, seja quando atribui a si mesmo a identidade de outra pessoa determinada, seja quando se atribui identidade de pessoa imaginária. Também quando apresenta outra pessoa com outra identidade, de terceiro ou de pessoa inexistente. Realiza-se o crime pelas mais diversas formas de execução, como afirmando, verbalmente, nome diverso do que tem, profissão que não possui, nacionalidade outra etc. Também quando entrega cartão de visita no qual se vê a informação de que é médico, quando nem faculdade tenha frequentado.
>
> A ocultação da própria identidade, por omissão do agente em desfazer o equívoco que outra pessoa tenha cometido acerca de seu nome ou outra qualidade que o individualize, não realiza o tipo, posto que aí nenhuma conduta positiva foi por ele realizada.
>
> A atribuição da falsa identidade deve ser realizada por meio idôneo, de modo a enganar as pessoas em face das quais é praticada a conduta. A falsidade grosseira é atípica.

No meio digital é muito comum a ocorrência desta prática delituosa, uma vez que o sujeito finge ser uma pessoa que não é, ou seja, o sujeito cria um perfil falso em uma determinada rede social com o intuito exclusivo de causar prejuízos para um outro usuário, se passando por ele e fingindo ser ele, deste modo o criador deste falso perfil será imputado pelo Art. 307 do Código Penal.

4.4.1.12 VIOLAÇÃO DE DIREITOS AUTORAIS

O elemento subjetivo do referido delito consiste no dolo, ou seja, na vontade livre e consciente de o sujeito violar direito autoral de outrem, realizando qualquer uma das figuras trazidas pelo caput do Art. 184 do Código Penal. Agora,

tendo em vista as figuras qualificadas trazidas pelos §§ (1º ao 3º), para que se configurem estas modalidades é necessário que o agente atue “com o intuito de lucro direito ou indireto".

O crime de violação de direitos autorais encontra-se transcrito no Art. 184 do Código Penal, conforme segue:

> Violação de direito autoral
>
> 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.

Tendo como norte os §§ 1º, 2º e 3º do Art. 184, para que se configure o referido delito é necessário que se proceda a uma análise do elemento normativo trazido nas formas qualificadas deste crime, qual seja, "sem autorização expressa", ou seja, para que se efetive o crime é necessário que o sujeito lesado não tenha concedido nenhum tipo de autorização ao violador de direitos autorais, caso contrário não haverá crime e o fato será atípico.

4.4.1.13 PORNOGRAFIA INFANTIL

O crime de pornografia infantil encontra-se embasamento legal no Estatuto da Criança e do Adolescente em seu Art. 240, conforme segue:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
>
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
>
> § 1o Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
>
> § 2o Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
>
> I – no exercício de cargo ou função pública ou a pretexto de exercê-la;
>
> II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
>
> III – prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento.

E ainda, o mesmo Estatuto nos traz o Art. 241-A que será transcrito a seguir:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
>
> § 1o Nas mesmas penas incorre quem:
>
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
>
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
>
> § 2o As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

Os artigos acima expostos se preocuparam em tratar da pornografia infantil, combatendo-a. Deixando para o Código Penal o combate à violência sexual decorrente de atos distintos da pornografia.

No que tange o Art. 240 do referido Estatuto, o elemento subjetivo do tipo consiste no dolo e na vontade livre e consciente do agente produzir ou realizar qualquer conduta que tenha como objeto cenas de sexo explícito ou pornográfico envolvendo criança ou adolescente, mesmo que o sujeito não tenha a intenção de obter lucro com esta conduta será ele responsabilizado pelo caput do Art. 240 do Estatuto da Criança e do Adolescente.

Para que tenha o sujeito sua conduta enquadrada no Art. 240 do referido Estatuo, faz-se por necessário a presença do elemento normativo “criança” que para o Estatuto seria pessoa de até 12(doze) anos incompletos e “adolescente” seria qualquer pessoa com idades entre 12 (doze) e 18 (dezoito) anos. E no caso do Art. 240 do Código Penal, via de regra, será sempre punido o agente produtor, ou seja, aquele que produz o conteúdo ilícito.

Já o Art. 241-A optou por tipificar as condutas dos criminosos que se utilizam dos meios informáticos para a divulgação, transmissão ou publicação de imagens contendo cenas de sexo explicito ou pornográficas que envolvam crianças ou adolescentes e, por consequência, será punido o agente divulgador, ou seja, mesmo não tendo ele produzido o conteúdo ilícito e nem o tenha vendido, ele estará sempre divulgando o material de algum modo para que outras pessoas possam tomar conhecimento, o que por si só configura a sua responsabilidade penal.

Agora, nas figuras qualificadas do Art. 241-A, o elemento normativo necessário para que seja o sujeito imputado pelo delito do referido artigo é a “notificação prévia”, ou seja, se o sujeito fora notificado previamente e quedou-se inerte, ou seja, pouco se importou em continuar com a referida prática ilícita, deste modo será imputado pelo delito em tela.

Posto isso, será transcrito o entendimento do Superior Tribunal de Justiça e da Suprema Corte, acerca dos delitos acima tratados:

> O envio de fotos pornográficas de menores pela Internet (e-mail) é crime. A questão foi definida pelo Superior Tribunal de Justiça (STJ) durante

> julgamento de um recurso especial do Ministério Público contra decisão da Justiça fluminense que entendera ser crime apenas a publicação e não apenas a mera divulgação de imagens de sexo explícito de menores.
>
> Corrobora com esse entendimento o ministro do Supremo Tribunal Federal Joaquim ao Barbosa:
>
> "EMENTA: HABEAS CORPUS. TRANCAMENTO DE AÇÃO PENAL. DIVULGAÇÃO DE FOTOGRAFIAS CONTENDO CENAS DE SEXO ENVOLVENDO CRIANÇA OU ADOLESCENTE. TIPICIDADE, EM TESE, DO CRIME DO ART. 241 DO ECA, NA SUA REDAÇÃO ORIGINAL, MESMO QUANDO A DIVULGAÇÃO DAS FOTOS ERÓTICAS FOI FEITA POR MEIO DA INTERNET. HABEAS CORPUS PARCIALMENTE CONHECIDO E, NA PARTE CONHECIDA, DENEGADO. - Não se conhece, em habeas corpus, de causa de pedir não apreciada pelo Superior Tribunal de Justiça, sob pena de supressão de instância. - O trancamento da ação penal, por ausência de justa causa, via habeas corpus, apesar de perfeitamente possível, é tido como medida de caráter excepcional, não se aplicando quando há indícios de autoria e materialidade de fato criminoso. Precedentes. - Não resta dúvida de que a internet é um veículo de comunicação apto a tornar público o conteúdo pedófilo das fotos encontradas, o que já é suficiente para demonstrar a tipicidade da conduta. Ademais, a denúncia foi clara ao demonstrar que qualquer pessoa que acessasse o servidor de arquivos criado pelo paciente teria à disposição o material. (HC 84561, JOAQUIM BARBOSA, STF)"

Por fim, conclui-se que o crime de pornografia infantil tutelado pelo Estatuto da Criança e do Adolescente, praticado por intermédio dos meios informáticos, consiste basicamente na prática de disseminação de fotos, vídeos ou qualquer que seja o material atinente à criança ou adolescente cujo conteúdo seja pornográfico e impróprio para idades reduzidas.

4.4.1.14 CRIMES CONTRA A HONRA

Os crimes contra a honra se subdividem em calúnia, difamação e injúria, todos eles tutelados pelo Código Penal em seus Arts. 138, 139 e 140, conforme trazido a seguir:

> Calúnia
>
> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
>
> Pena - detenção, de seis meses a dois anos, e multa.
>
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
>
> § 2º - É punível a calúnia contra os mortos.

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

O Art. 138 do Código Penal nos traz o crime de calúnia e seu elemento subjetivo norteia-se no dolo eventual ou direto, ou seja, a vontade inequívoca de imputar falsamente fato definido como crime a terceira pessoa, sendo assim o caluniador tem o real objetivo de atribuir a prática de um crime a um sujeito que efetivamente não o cometeu.

O elemento normativo deste crime é a falsidade da imputação, ou seja, para que se configura o crime acima narrado é necessário que o sujeito impute um crime a uma pessoa que efetivamente não o praticou.

Nos meios informáticos é bastante comum a incidência de delitos contra a honra, mas em se tratando de calúnia ocorre corriqueiramente em *chats* ou

grupos de redes sociais, na internet onde indivíduos fazem acusações e acabam por imputar a prática de crimes contra pessoas que não cometeram nenhum crime, a exemplo disso temos casos bastante comuns onde usuários acusam outros, por exemplo, de terem desviado verbas públicas ou ainda atribuindo ao sujeito a conduta de traficante de drogas e/ou consumidor de drogas sendo assim, se estas acusações forem inverídicas haverá o crime de calúnia contra quem as proferiu.

O delito tipificado no Art. 139 do Código Penal é a difamação e o elemento subjetivo do injusto é o dolo, direto ou eventual, ou seja, a vontade livre e consciente de ofender a pessoa (*animus difamandi)* sendo assim, se o sujeito apenas possuía a intenção de fazer uma piada (*animus jocandi*) ou qualquer outro meio que não seja a intenção de ofender, não será configurado o crime. Além do mais, a mera exaltação ou emoção em uma acalorada discussão, seja nos meios informáticos ou não, não haverá o ilícito.

Já para que se consume o crime de difamação, é necessário que o usuário do meio informático atribua fato ofensivo à reputação de alguém, desacreditando-a publicamente. Nos meios informáticos é também bastante comum a referida prática nos casos em que usuários em ambiente de redes sociais acabam por difamar outras pessoas, como atribuindo a elas o uso de drogas, a prostituição, dentre outras condutas.

E por fim, o Art. 140 tipifica o crime de injúria e seu elemento subjetivo também é o dolo (*animus injuriandi*), vontade livre e consciente de injuriar, ofender e deturpar a honra de outra pessoa.

Para que se configure o crime de injúria é necessário a atribuição de características negativas sobre as qualidades físicas, morais ou intelectuais de cada ser humano, o injuriador irá falar mal, ofender, insultar sem a mínima necessidade. Nos meios informáticos também se faz bastante comum a prática de ofensas que caracterizam o crime de injuria como, por exemplo, em redes sociais ou até em páginas de *blogs* na internet usuários cometem injúria ao atribuir as demais pessoas xingamentos como : gordo(a), imbecil, idiota, dentre outros, e o referido palavreado já caracteriza o crime de injúria.

4.5 UMA BREVE ANÁLISE CRÍTICA ACERCA DA LEI Nº 12.737/12

O dia 03 de dezembro do ano de 2012 entrou para o marco do sistema legislativo na busca de sua tentativa de criminalizar os chamados crimes virtuais próprios (aqueles que somente podem ser praticados por intermédio de um computador), com o advento da Lei nº 12.737.

Pois, ao se fazer uma breve análise de todo o panorama social que o país enfrenta, constata-se uma clara e evidente deficiência no que tange à criminalização dos crimes praticados pelos meios informáticos e assim, tornando-se de extrema necessidade o aprimoramento da legislação penal informática. Posto isso, com a publicação da referida lei passou-se a tutelar direitos de qualquer dos usuários pertencentes à rede de computadores que for lesado por meio de ataques cibernéticos como foi o caso da atriz brasileira Carolina Dieckmann, ao qual deu nome a esta lei.

A propósito, foi oportunamente este caso da atriz Carolina Dieckmann, que desprendeu velocidade à tramitação e a publicação da referida lei. A atriz teve suas fotos copiadas de seu computador e por não ter cedido às chantagens dos chamados *hackers,* teve suas fotos nuas todas publicadas na rede de computadores, expondo-a totalmente e extirpando por completo a sua intimidade. Sendo assim, gerando ampla repercussão midiática em torno do referido caso o que acelerou ainda mais a aprovação deste projeto de lei que tipifica condutas criminosas advindas dos meios informáticos.

Criando-se, portanto, o novo tipo penal denominado de Invasão de Dispositivo Informático trazido pelo Art. 154-A do Código Penal, com a referida redação:

> 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."

O verbo do núcleo trazido é invadir, portanto, entrar sem qualquer autorização prévia do proprietário ou possuidor. E o detalhe mais importante trazido pelo referido artigo é a elementar, *mediante violação indevida de mecanismo de segurança*. Ou seja, o sujeito somente será enquadrado neste delito acima trazido no caso de efetivamente violar algum dispositivo alheio de segurança. Posto isso, podemos concluir que se o agente furtar qualquer tipo de dados de um computador alheio que não possua nenhum dispositivo de segurança protegendo-o, não será o criminoso punido pelo referido artigo, pois a elementar do tipo é bastante clara ao dizer, *violação indevida de mecanismo de segurança*, caso não tenha havido a referida violação, não há de se falar em crime e a conduta será atípica.

Sendo assim, conclui-se que todos os usuários devem procurar os mais avançados sistemas de proteção contra os referidos ataques e jamais deixarem suas máquinas sem qualquer dispositivo de segurança instalado, pois, caso ocorra o ataque além dos enormes prejuízos resultantes o agente ofensor não poderá ser enquadrado no Art. 154 do Código Penal uma vez que não violou nenhum dispositivo de segurança.

Além disso, ocorreu certa omissão por parte do legislador ao passo de que o novo tipo penal acima descrito também nos traz o elemento subjetivo necessário para a caracterização do referido crime, qual seja, *com o fim de obter, adulterar ou destruir dados ou informações ou instalar vulnerabilidades para obter vantagem ilícita*. Por isso, se o sujeito tinha a intenção apenas de violar o dispositivo de segurança sem qualquer intenção finalística de obter, adulterar ou destruir dados ou informações, não haverá o crime por ausência clara dos elementos subjetivos do tipo.

Posto isso, ficou clara a intenção do legislador em aplicar o principio da lesividade penal, ou seja, explicitando que não basta apenas a ação para que se configure o delito, mas sim que efetivamente este cause um dano, uma lesão ou uma ameaça a determinado bem jurídico. Entrementes, há pensamentos de que deveria ser previsto como crime de perigo e não como um crime de dano, bastando, portanto, que a mera invasão já fosse passível de punição.

O §1º da referida lei, tem como objetivo a punição dos criadores de programas informáticos que os utilizam de forma maliciosa e com a vontade finalística de promover lesão ou ameaça de lesão a certos bens jurídicos. Entretanto, estes programadores trabalham de forma lícita uma vez que é fruto de seu trabalho a produção de determinados vírus para que se proceda testes de sistemas de segurança. Ademais, também produzem outros tipos de materiais lesivos, contudo, será tipificado como crime quando o sujeito incidir em abuso de seu direito, ou seja, mediante desvio de finalidade utiliza-se de sua profissão devidamente regulamentado para fragilizar e facilitar a invasão de sistemas alheios.

O § 3º desta lei nos traz a figura da invasão qualificada que foi explicitada de forma bastante lúcida por Auriney Brito (2013, *on-line*), conforme segue:

> Se dessas condutas 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, o crime é qualificado e a pena pode chegar a 2 anos de reclusão ou multa.
>
> Um ponto interessante a ser ressaltado na Invasão qualificada, é o controle remoto do dispositivo invadido. É muito comum hoje a prática do Distributed Denial of Service Attack (Ddos Attack) que tem causado prejuízos

> incomensuráveis à empresas que perdem o seu sistema por um tempo após um ataque como esses. O detalhe é que o sistema da empresa não é invadido, mas em razão de uma sobrecarga de acesso dos seus recursos num mesmo momento.
>
> Pouco se noticiou, mas o mês de março de 2013 foi marcado pelo maior ataque cibernético da história, e essa (Ddos) foi a técnica utilizada. Também chamada de Ataque de Amplificação, foi somado à um grande conhecimento de estratégias militares e direcionado à uma empresa que combate spams na rede (Spamhaus), o que acabou por atrapalhar o funcionamento da internet em quase todo o mundo. Tem-se notícia que a "guerra" se deu por motivos de disputa empresarial entre duas grandes empresas do ramo.
>
> Isso ocorre quando um cracker instala o seu programa malicioso e vários computadores de vários usuários, que passam a obedecer aos comandos do seu "líder", tornam-se máquinas "zumbis". Ao seu comando, todos acessam o servidor vítima até que ele esgote sua capacidade de atendimento e trave ou reinicie, causando graves lesões ao seu patrimônio. No ano de 2012, os sites de várias empresas como TAM, GOL, Bancos BRASIL, BRADESCO e outros, foram atacados dessa forma. Muitas não assumem o ataque para não transparecer vulnerabilidade e insegurança aos clientes, mas os prejuízos são milionários.

O referido tipo penal nos traz causas de aumento como no parágrafo segundo, quando houver prejuízo econômico ou ainda quando o crime tiver sido praticado contra autoridades dos Poderes Executivo e Legislativo.

Um problema muito grave que a Lei nº 12.737/2012 não tratou de resolver norteia-se no cerne da questão atinente às penas irrisórias trazidas por esta legislação e também pelo nosso ordenamento jurídico como um todo, uma vez que na maioria dos casos em que o sujeito tiver sua conduta enquadrada nesta lei por conta de um crime informático, será beneficiado pelo rito sumaríssimo do JECRIM (Juizado Especial Criminal), sendo que ao invés do criminoso cumprir a pena restritiva de liberdade em sua integralidade, será ele beneficiado pela aplicação de penas restritivas de direito como, prestações de serviços comunitários ou até com o mero pagamento de cestas básicas vendo-se impunes, conforme nos leciona Rony Vainzof (2013, *on-line*):

> As punições até poderiam ser maiores para evitar que os criminosos tivessem o benefício do juizado especial criminal", pondera em entrevista ao Terra. No juizado especial criminal, dependendo de certos requisitos - como não ter sido condenado anteriormente, ou não ter usado esse juizado durante cinco anos - se a pena maior do crime em questão não ultrapassa dois anos, o réu tem direito de, em vez de cumprir pena, pagar cestas básicas ou prestar serviços à

> comunidade. "Mas não é uma punição, porque não se discute o mérito da ação", explica.

O Art. 60 e seguintes da Lei nº 9.099/1995 nos traz a competência dos Juizados Especiais Criminais, conforme segue:

> Art. 60. O Juizado Especial Criminal, provido por juízes togados ou togados e leigos, tem competência para a conciliação, o julgamento e a execução das infrações penais de menor potencial ofensivo, respeitadas as regras de conexão e continência
>
> Art. 61. Consideram-se infrações penais de menor potencial ofensivo, para os efeitos desta Lei, as contravenções penais e os crimes a que a lei comine pena máxima não superior a 2 (dois) anos, cumulada ou não com multa

Posto isso, verificamos que toda e qualquer infração penal cuja pena máxima não ultrapasse 2 (dois) anos serão inteiramente julgadas e processadas pelo rito sumaríssimo do JECRIM e não serão apreciados pela Justiça Comum. O grande problema da Lei nº 12.737/2012 é justamente a pena máxima de seus crimes que não ultrapassam 02 (dois) anos logo, serão todos apreciados pelo Juizado Especial Criminal o que, por consequência, torna a punição mais branda do que se fosse julgado pela Justiça Comum.

Verificamos, portanto, que há de se adequar e alterar os limites das penas da referida lei, pois de nada adianta todo o desprendimento de esforço para a criação de uma lei se na prática ela não terá praticamente nenhuma efetividade e não estará revestida de caráteres coercitivos ou intimidadores para o criminoso, que continuará a praticar o seus crimes por meio de um sistema informático, sem que tenha contra ele uma pena de caráter mais rigoroso.

Evidente que se o sujeito praticar o crime em sua modalidade qualificada ou com o aumento de pena trazido por esta lei, sua pena máxima será majorada e sairá o delito da competência do JECRIM, mas fora estes casos os delitos desta lei serão todos julgados e processos no Juizado Especial Criminal.

4.6 A INCIDÊNCIA DA ANALOGIA, INTERPRETAÇÃO ANALÓGICA E INTERPRETAÇÃO EXTENSIVA NOS CRIMES VIRTUAIS

Para início de entendimento do referido tema, faz-se por necessário a citação do pensamento de Damásio E. de Jesus (2011, p.46) que traz a devida e correta diferenciação entre analogia e interpretação analógica :

> Às vezes, a própria lei pretende que a ausência de previsão legislativa seja suprida pela analogia, que seus preceitos sejam por ela completados. Em casos tais, cuida-se de interpretação analógica, em que está na vontade da lei a extensão de seu conteúdo aos casos análogos. Na analogia, porém, tratas-se de aplicar o conteúdo de uma lei a casos não pretendidos abranger pela sua vontade. A diferença,pois, entre interpretação analógica e analogia reside na *voluntas legis:* na primeira, pretende a vontade da norma abranger os casos semelhantes por ela regulados; na segunda, ocorre o inverso: não é pretensão da lei aplicar o seu conteúdo aos casos análogos, tanto que silencia a respeito, mas o intérprete assim o faz, suprindo a lacuna.

Portanto, analogia é aplicar uma determina lei em vigor para um caso pontual que ainda não possui lei que o regulamente, e assim não ficando este caso impune ou sem qualquer tipo de sanção, modo pelo qual aplica-se o disposto na lei em vigor para o caso concreto que não possui nada que o tipifique.

Conforme ainda nos exemplifica de forma bastante clara e exata Damásio E. de Jesus (2011, p.50), acerca da correta aplicação da analogia:

> O legislador , através da lei A, regulou o fato B. O julgador precisa decidir o fato C. Procura e não encontra no direito positivo uma lei adequada a esse fato. Percebe, porem, que há pontos de semelhança entre o fato B(regulado) e o fato C (não regulado). Então, através da analogia, aplica ao fato C a lei A.

Já na interpretação analógica, é intenção clara do legislador estender a aplicação da norma por ele trazida, ou seja, o próprio dispositivo determina que seja aplicado analogicamente o preceito sendo que a própria lei menciona os casos que devem ser compreendidos por semelhança. A exemplo desta interpretação analógica, temos o Art. 171, caput, que ao definir estelionato fala em " qualquer outro meio fraudulento", que quer dizer : qualquer meio semelhante ao "artifício" ou "ardil" , deste modo constata-se a própria vontade da lei em abranger casos semelhantes.

Faz-se de maneira basta oportuna a distinção dada por Heleno Fragoso (1985, p.86/87) acerca da analogia e da interpretação extensiva, conforme segue :

> A analogia distingue-se da interpretação, porque constitui um processo de integração da ordem legal, e não meio de esclarecer o conteúdo da norma. Através da analogia aplica-se a lei a hipótese por ela não prevista, invocando-se substancialmente, o chamado argumento a pari ratione. Há aplicação analógica quando a norma se estende a caso não previsto, mas semelhante, em relação ao qual existem as mesmas razões que fundamentam a disposição legal. A analogia distingue-se da interpretação extensiva, porque nesta não falta a vontade da lei, mas tão-somente a expressão verbal que a ela corresponda.
>
> A interpretação extensiva é perfeitamente admissível em relação à lei penal, ao contrário do que afirmavam autores antigos. Nestes casos não falta a disciplina normativa do fato, mas, apenas, uma correta expressão verbal. Há interpretação extensiva quando se aplica o chamado argumento a fortiori, que são casos nos quais a vontade da lei se aplica com maior razão. É a hipótese do argumento a maiori ad minus (o que é válido para o mais, deve necessariamente prevalecer para o menos) e do argumento a minori ad maius (o que é vedado ao menos é necessariamente no mais). Exemplo deste último argumento: se o Código Penal incrimina a bigamia, logicamente também pune o fato de contrair alguém mais de dois casamentos (Manzini).

Já a intepretação extensiva consiste basicamente no processo de extração do real e autêntico significado da norma, ampliando-se assim os seus significados legais, para o fim de se adequar à real finalidade e intenção do texto. Ou seja, tratando-se de mera interpretação da norma com o fim de se obter o correto entendimento da *intentio legis*, portanto ação perfeitamente cabível sem qualquer objeção à sua feitura.

A discussão sobre a aplicação ou não da analogia nos crimes virtuais é um tema bastante discutido por estudiosos da área penal devido sua complexidade e grande divergência, uma vez que devem ser respeitados os princípios da reserva legal e da proibição da analogia *in malam partem*, conforme foram objetos do entendimento da Suprema Corte:

> Em conclusão de julgamento, o Tribunal, por maioria, rejeitou denúncia apresentada contra Deputado Federal, em razão de ter despendido quantia em dinheiro na tentativa de obter, por intermédio de cola eletrônica, a aprovação de sua filha e amigos dela no vestibular de universidade federal, conduta essa tipificada pelo Ministério Público Federal como crime de estelionato (CP, art. 171), e posteriormente alterada para falsidade ideológica (CP, art. 299) — v. Informativos 306, 395 e 448. Entendeu-se que

> o fato narrado não constituiria crime ante a ausência das elementares objetivas do tipo, porquanto, na espécie, a fraude não estaria na veracidade do conteúdo do documento, mas sim na utilização de terceiros na formulação das respostas aos quesitos. Salientou-se, ainda, que, apesar de seu grau de reprovação social, tal conduta não se enquadraria nos tipos penais em vigor, em face do princípio da reserva legal e da proibição de aplicação da analogia in malam partem. Vencidos os Ministros Carlos Britto, Ricardo Lewandowski, Joaquim Barbosa e Marco Aurélio, que recebiam a denúncia. Inq 1145/PB, rel. orig. Min. Maurício Corrêa, rel. p/ o acórdão Min. Gilmar Mendes, 19.12.2006. (Inq-1145)" Informativo STF n. 453/2006.[5]

Posto isso, verifica-se a ausência de normas penais incriminadoras que tornam impunes algumas condutas criminosas, contudo, a analogia tem sido utilizada em alguns delitos pontuais como exemplo, o crime de destruição de dados eletrônicos que tem sido equiparado ao crime de dano ao patrimônio.

Entretanto, há alguns delitos como os já trazidos acima que têm sido objetos de punição por intermédio da analogia, são crimes já trazidos pelo Código Penal praticados por intermédio único e exclusivo dos meios informáticos.

A problemática consiste na ideia preconizada no Ordenamento Jurídico Penal, onde reside a regra de que não se pode utilizar-se da analogia para prejuízo do réu, deste modo o criminoso somente poderá ser processado e devidamente responsabilizado quando praticar uma conduta tida como crime e que esteja expressamente prevista pela lei, o que acaba impondo certos limites à discricionariedade do poder estatal, privilegiando-se assim o principio da reserva legal, conforme nos demonstra Cezar Roberto Bitencourt (2007,p.2)

> O princípio da legalidade ou da reserva legal constitui efetiva limitação ao poder punitivo estatal. Feuerbach, no início do século XIX, consagrou o princípio da reserva legal por meio da fórmula latina nullun crimen, nulla poena sine lege. O princípio da reserva legal é um imperativo que não admite desvios nem exceções e representa uma conquista da consciência jurídica que obedece a exigências de justiça; somente os regimes totalitários o têm negado.

Entretanto, como já dito no estudo realizado, há alguns delitos virtuais que não possuem tipificação penal e estão sendo punidos por intermédio da interpretação extensiva analógica, como por exemplo, o desvio de dinheiro alheio de uma conta corrente valendo-se da internet, em benefício próprio ou de terceiros vem

sendo tipificado como delito de furto, o que o diferencia do furto propriamente dito seria apenas o *modus operandi* desprendido pelo executor.

Sendo assim, verifica-se a possibilidade de se fazer uma interpretação extensiva de determinada norma, a fim de se alcançar uma conduta criminosa. Uma vez que é impossível o Poder Legislativo criar todas as normas necessárias para a correta criminalização de determinadas condutas, deste modo, criam-se normas genéricas, abertas que podem ser ampliadas e utilizadas em condutas que ainda não possuem a sua norma, sem que haja nenhum prejuízo. Deste modo, a interpretação extensiva de determinada norma deve ser relativa, ou seja, respeitando sempre os princípios da legalidade ou reserva legal.

Obviamente que os avanços legislativos caminham em passos lentos enquanto que os avanços tecnológicos são construídos com imensurável rapidez, contudo, isto não é motivo para que os operadores do Direito cruzem seus braços e fiquem inertes em relações às condutas criminosas advindas dos meios informáticos que não possuem leis ou esperam que leis sejam criadas para que façam algo, muito pelo contrário, se no caso concreto haver a possibilidade de se adequar a conduta criminosa a um tipo penal já existente é isto que deve ser feito, e não quedar-se inerte o aplicador do Direito.

Disseminar afirmações alegando que alguém cometeu um fato definido como crime sem que tal afirmação seja plausível, configura-se o delito de calúnia trazido pelo Art. 138 do Código Penal Brasileiro, logo o sujeito que realiza a mesma conduta só que dissemina tal informação por meio da Internet também comete calúnia. O mesmo pode-se afirmar do delito de dano, um sujeito que atira pedras contra uma vidraça responde pelo Art. 183 do Código Penal, do mesmo modo que o sujeito que através de um meio informático, invade um sistema alheio e apaga todos os seus arquivos também pratica um crime de dano.

5. CONCLUSÃO

Como claramente trazido e bastante difundido no presente trabalho, o Direito Penal brasileiro não encontra-se apto a lidar com as mudanças e as novas

realidades trazidas pela era digital, principalmente no que tange aos crimes virtuais por absoluta ausência de tipificação de tais condutas delituosas.

Através do estudo realizado e levando-se em conta que o direito possui como uma de suas principais funções o acompanhamento da evolução da sociedade, verifica-se com extrema necessidade a tipificação destas condutas criminosas praticadas através de meios informáticos, pois a inércia legislativa só faz aumentar ainda mais a sensação de impunidade, gerando assim total insegurança de pessoas de bem, e ainda promovendo a ampla disseminação e o incentivo à prática dos chamados cibercrimes.

Ao contrário do que se vê em outros países que se mostram bastantes avançados no que tange a coibição destas praticas criminosas com o advento de leis pesadas e coercitivas o que, por consequência gera aos agentes criminosos um grande receio ao praticarem seus delitos e ocasionalmente acaba por diminuir acentuadamente a incidência destes crimes virtuais em razão do caráter coercitivo e intimidador das normas penais. No Brasil é justamente o contrário o que se ocorre, destoando-se assim da prática Internacional aplicada na coibição destas práticas criminosas, infelizmente.

Os crimes virtuais demandam um conhecimento específico bastante complexo, vez que envolve questões em pleno desenvolvimento sendo que muitas destas questões sequer são conhecidas por pessoas sem a devida habilidade técnica sobre o referido tema. Há de se ressaltar também, o rápido crescimento dos crimes realizados pelos meios informáticos, os chamados crimes próprios, e esta crescente não deveria passar despercebida aos olhos de nossos legisladores, uma vez que estes crimes possuem um caráter de mutabilidade bastante incidente e que somado a inércia legislativa, dificulta ainda mais a sua devida e necessária tipificação.

O que corrobora ainda mais com o nítido crescimento da prática de crimes virtuais é a conveniência para a sua realização posto, que o agente criminoso não precisa nem ausentar-se de sua residência para a execução do delito, além do mais que muitas das vezes, o conhecimento da autoria delitiva destes crimes fica bastante restrita devido às habilidades utilizadas por estes criminosos, o que ao final novamente resulta em impunidade.

Outro ponto a se destacar tomando como base as lacunas legislativas e a ausência de tipificação de alguns crimes virtuais trazidos neste estudo, seria a aplicação da devida punição destas condutas criminosas por meio da analogia, para que seja possível abranger estes atos não criminalizados ainda, mas que possuem similaridade com alguns crimes já tipificados. Contudo, não é o mais correto o processamento destes crimes pelo uso da analogia, pois é vedada a chamada *" analogia in malam partem",* ou seja, a analogia para o fim de prejudicar o réu, muito embora conforme trazido neste trabalho há doutrinadores que defendem a utilização desta analogia para o fim de diminuir tamanha impunidade e também bastante defendida a utilização das interpretações analógicas e extensivas, para o fim de se diminuir tamanha impunidade nos meios digitais.

Portanto, a ampla maioria dos agentes criminosos responsáveis pela crescente incidência dos chamados cibercrimes (crimes virtuais) não podem ser punidos, tendo como norte o Art. 5º, inciso XXXIX da Constituição Federal que dispõe "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Sendo assim, não havendo um tipo penal incriminador o sujeito não poderá ser processado, o que o incentiva a continuar praticando os seus delitos pelos meios informáticos, contribuindo ainda mais para a gradação da sensação de impunidade oriunda deste meio.

Portanto, devemos ponderar que muitos dos delitos praticados pelos meios informáticos já possuem a devida tipificação legal, ou seja, já são crimes definidos em lei e apenas são cometidos pelos meios informáticos, devido a maior rapidez e facilidade da execução do delito. Deste modo, encontra-se certa facilidade em tipificar e punir os agentes cometedores destes crimes, todavia, há ainda delitos como os que foram amplamente trazidos e esmiuçados no presente trabalho, que necessitam de uma regulamentação urgente e célere para que haja a devida e necessária punição destes infratores. Em alguns casos pontuais, tem-se usado da interpretação analógica, ou seja, estendendo o conteúdo da norma para abranger outras condutas, mas ainda é algo que vem encontrando algumas barreiras no Direito Penal Brasileiro.

6. BIBLIOGRAFIA

ARAÚJO, Luiz Alberto David de. Curso de Direito Constitucional. 13 ed. São Paulo: Editora Saraiva. 2013.

ASCENSÃO. José de Oliveira. Estudos sobre direito da internet e da sociedade da informação: Editora Almedina. 2013.

ANDRADE, Allan Diego Mendes Melo. O direito à intimidade e à vida privada em face das novas tecnologias da informação. Disponível em (http://www.faete.edu.br/revista/ODIREITOAINTIMIDADE_E_%20A_VIDA_PRIVADA_EM_FACEDASNOVASTECNOLOGIASDAINFORMACAO-Allan%20Diego.pdf).

Acessado em 15 de março de 2013.

Analogia aos delitos virtuais com ênfase nos direitos humanos. Disponível em: http://araguaia.ufmt.br/revistapanoramica/index.php/revistapanoramica/article/viewFile/436/119. Acessado em 15 de março de 2013.

A legalidade penal e os meios eletrônicos. Disponível em: http://www.aldemario.adv.br/infojur/conteudo18texto.htm. Acessado em 18 de outubro de 2013.

Arpanet (advanced research projects agency network). Disponível em: http://pt.wikipedia.org/wiki/ARPANET. Acessado em 15 de setembro de 2013.

BITENCOURT, Cezar Roberto. Código Penal comentado. 6 ed. São Paulo: Editora Saraiva. 2011.

BRITO, Auriney. Análise da Lei 12.737./12. Disponível em: http://atualidadesdodireito.com.br/aurineybrito/2013/04/03/analise-da-lei-12-73712-lei-carolina-dieckmann/. Acessado em 20 de outubro de 2013.

BOBBIO, Norberto. A era dos direitos. 4 ed. Rio de Janeiro: Editora Forense. 1992.

BONAVIDES, Paulo. Curso de Direito Constitucional. 28 ed. São Paulo: Editora Malheiros. 2012.

BRASIL, Constituição Federal do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em 18 de outubro de 2013.

BRASIL, Código de Processo Penal Vade Mecum. 13 ed. São Paulo: Editora Saraiva. 2013

BRASIL, Código Penal. Vade Mecum. 13 ed. São Paulo: Editora Saraiva. 2013.

BRASIL, Estatuto da criança e do adolescente. Vade Mecum 13 ed. São Paulo: Editora Saraiva. 2013: Lei federal nº 8069, de 13 de julho de 1990.

CASTRO, Aldemário Araujo. A internet e os tipos penais que reclamam ação criminosa em público. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf. Acessado em 12 de agosto de 2013.

CASTRO, Aldemário Araujo. Manuel de Informática Jurídica e Direito da Informática. 1 ed. São Paulo : Editora Forense. 2005.

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. 1 ed. São Paulo: Editora Saraiva. 2011.

CRESPO, Marcelo Xavier de Freitas. Noções introdutórias aos delitos informáticos. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6325. Acessado em 16 de julho de 2013.

Cibercrime e forense computacional e a validade do documento eletrônico como prova no processo. Disponível em: http://fperes.com/web/blog/2012/01/02. Acessado em 03 de maio de 2013.

CONVENÇÃO, de Budapeste sobre os Cibercrimes de 2001.

COSTA, Marco Aurélio Rodrigues da. Crimes de Informática. Jus Navigandi, Teresina, ano 2, n. 12, 5 maio 1997 . Disponível em <http://jus.com.br/artigos/1826>. Acesso em: 18 out. 2013.

Dos crimes praticados em ambientes virtuais. Disponível em: http://www.conteudojuridico.com.br/artigo-dos-crimes-praticados-em-ambientes-virtuais.38483.html. Acessado em 25 de junho de 2013.

FERRAZ, Tércio Sampaio. Sigilo de dados: direito à privacidade e os limites à função fiscalizadora do Estado. Cadernos de Direito Constitucional e Ciência Política. São Paulo. 1992.

FILHO, Dickson Cirilo Andrade Netto. Crime Virtual: crime contra o patrimônio no âmbito da internet, suas peculiaridades e controvérsias à luz do CP de 1940. Disponível em: http://www.egov.ufsc.br/portal/conteudo/crime-virtual-crime-contra-o-

patrim%C3%B4nio-no-%C3%A2mbito-da-internet-suas-peculiaridades-e-controv. Acessado em 20 de outubro de 2013.

FRAGOSO, Heleno. Lições de Direito Penal. 17 ed. São Paulo : Editora Forense. 2006.

GRECO, Rogério. Curso de Direito Penal Parte Geral. 15 ed. Rio de Janeiro: Editora Impetus. 2013.

JESUS. Damásio De. Direito Penal Parte Geral 30 ed. V-1.Ex.4: Editora Saraiva.2009.

KAMINSKI. Omar. Internet Legal e o Direito na tecnologia da informação. 5 reimpressão: Editora Juruá.2009.

LAKATOS. Eva Maria. Fundamentos da metodologia científica. 4 ed. São Paulo : Editora Atlas. 2001.

MARTIN, Ricardo M. Mata. La propriedade Intelectual En La Era digital. 2 ed. : Editora Actualidad. 2011.

MORAES, Alexandre de. Direitos fundamentais: teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 1 ed. São Paulo.1997.

NOGUEIRA, Sandro D'amato. Crimes de Informática. 1 ed. São Paulo : Editora BH. 2008.

NUCCI, Guilherme de Souza. Manual de Direito Penal. 9 ed: Editora RT. 2013

PARENTE, André. Tramas da rede: novas dimensões filosóficas, estéticas e políticas da comunicação. Porto Alegre: Sulina. 2004.

PEREIRA, Marcelo Cardoso. Direito à intimidade na Internet. 1 ed : Juruá Editora. São Paulo.2006.

PERES, Fernando. Introdução à Ciência da Computação. 2 ed: Editora Cengage Learning. 2012.

PORTO, Luiz Guilherme Moreira. Disponível em: http://www.egov.ufsc.br/portal/conteudo/crime-virtual-crime-contra-o-patrim%C3%B4nio-no-%C3%A2mbito-da-internet-suas-peculiaridades-e-controv. Acessado em 28 de setembro de 2013.

REPÓRTER, Claudio Weber. Fechando o cerco aos criminosos da internet agora o bicho vai pegar. Disponível em: http://claudioweberreporter.blogspot.com.br/2010/08/fechando-o-cerco-aos-criminosos-da.html?zx=9655e983ba2d449f. Acessado em 18 de setembro de 2013.

ROVIRA, Enrique Del Canto – Delincuencia Informática y Fraudes Informáticos, Estúdios de Derecho Penal. 33 ed: Editoria Comares. Granada. 2002.

RONY, Vainzof. Lei Carolina Dieckmann só vale para eletrônicos com sistema de segurança.http://tecnologia.uol.com.br/noticias/redacao/2013/04/24/lei-carolina-dieckmann-so-vale-para-eletronicos-com-sistema-de-seguranca.html. Acessado em 05.08.2013 .

SILVA, Rita de Cássia Lopes. Direito Penal e Sistema Informativo. 1 ed :Editora RT. 2012.

TELES, Ney Moura. Direito Penal. 2 ed. São Paulo: Editora Atlas. 2006.

TELES, Ney Moura. Falsa Identidade. Disponível em: http://www.neymourateles.com.br/direito-penal/wp-content/livros/pdf/volume03/79.pdf. Acessado em 20 de outubro de 2013.

Tipicidade penal dos crimes cometidos na internet. Disponível em: http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10065. Acessado em 19 de agosto de 2013.

ZAFFARORNI, Eugenio Raul. Direito Penal Brasileiro. 4 ed: Editora Revan. Argentina.