

CRIMES CIBERNÉTICOS: O DESAFIO DO DIREITO PENAL NA ERA DIGITAL

Diego Luís Dantas Guimarães¹
Sandresson de Menezes Lopes²

RESUMO

O presente artigo discutirá e analisará uma das consequências da criação da internet: os crimes cibernéticos. Este novo fenômeno, surge em meio a uma sociedade extremamente vinculada a comunicação virtual e seu modo de vida interligado aos computadores. Será exposto o início desta marcante inovação, sua trajetória, suas classificações, e principalmente, sua forma de utilização, pois, devido ao mal uso da internet o número dos crimes virtuais vem aumentando, provocando a necessidade de se criar uma legislação própria que combatesse de forma específica tais crimes, pois até o ano de 2012, a falta de tipificação penal causava prejuízos graves a nossa sociedade.

PALAVRAS CHAVE: Crimes virtuais. Legislação. Ciberespaço.

CYBERCRIMES: THE CHALLENGE OF CRIMINAL LAW IN THE DIGITAL AGE

ABSTRACT

This current scientific paper will discuss and analyse one of the consequences of the creation of the internet: the cybercrimes. This new phenomenon comes among a society extremely tied to virtual communication and with a way of life connected with computers. Will be exposed the beginning of this remarkable innovation, its history, its classifications, and especially its method of use, because the misuse of the internet is what is increasing the number of cybercrimes and this was the main reason for the need of creating its own legislation that would combat such crimes specifically, because until the year of 2012, the lack of penal classification was causing serious damage to our society.

KEYWORDS: Cybercrime. Legislation. Cyberspace.

¹ Acadêmico do Curso de Direito- UNI-RN – 8º período (N) "B" - 2014- Email: diegoluis1@gmail.com

² Professor Orientador do Curso de Direito – UNI-RN E-mail: sandresson1@hotmail.com

1 INTRODUÇÃO

A discussão sobre os crimes virtuais se mostra importante, observando a evolução tecnológica e em especial a internet, tornando-se um mecanismo rápido e eficaz de informação, modificando assim, a realidade do homem. De forma significativa esta modernização abrangeu-se também sobre o Direito, e obviamente interferiu no campo do Direito Penal.

No contexto dessa revolução tecnológica é possível auferir que o nosso Código Penal apresenta dificuldades de tipificação para crimes que vão além do plano físico. Atualmente, não é necessário ir às ruas para se cometer um crime, o mundo virtual chegou, e com ele consequências também negativas.

Esse novo mundo trouxe para o Direito Penal novos traços criminológicos, apresentando a internet como um meio de execução de crime, afligindo a comunidade jurídica e repercutindo na criação de leis, como a nova lei 12.737/2012, conhecida como Lei Carolina Dieckman.

Neste artigo abordamos a tríplice relação do Direito Penal, Internet e os crimes virtuais, apresentando as deficiências legislativas e as dificuldades de punição dos infratores devido ao baixo aparato tecnológico das nossas autoridades.

Para esclarecer o assunto, foi de extrema importância tecer comentários sobre o aumento da utilização da internet em nossa sociedade, apresentando conceitos doutrinários envolvendo o mundo digital.

Através de citações doutrinárias e pesquisas em diversos sites de referência, conceituamos e definimos através de uma visão jurídica, os crimes digitais. Seguindo na mesma linha de pesquisa, foi feita a classificação dos crimes de acordo com a conduta do agente e também com a doutrina que versa sobre o assunto.

Ultrapassada a primeira etapa do artigo, com enfoque na teoria e embasamento doutrinário, trouxemos a temática para a realidade do Brasil e sua relação com os crimes virtuais. Como se apresenta a legislação nacional em relação aos crimes digitais e quais as leis que versam sobre o assunto foram tópicos também abordados.

Posteriormente foi tratado das problemáticas que usualmente dificultam a persecução criminal, como exemplo a dificuldade em se determinar a autoria dos

crimes virtuais, a produção de prova, a competência em razão do lugar e a legislação insuficiente.

Concluimos assim nosso artigo, enaltecendo que o tema requer medidas e leis mais rígidas, pois o avanço tecnológico cresce de uma maneira que o nosso Código Penal, devido a toda burocracia legislativa, não apresenta paridade de armas para acompanhar. O tema não recebe a atenção que é devida, ficando claro através da escassez de discussão doutrinária. Esse último fator, foi sem dúvidas, o estímulo para realização do trabalho.

2 DO AUMENTO DE UTILIZAÇÃO DA INTERNET PELA SOCIEDADE

Com o objetivo de interligar computadores para transferência de dados, apenas no fim dos anos 60, criada pela ARPANET, surgiu a internet. Todavia, numa modalidade muito precária. A forma utilizada nos dias de hoje, apenas iniciou no ano de 1990, através do Word Wide Web (Rede de Alcance Mundial). Sua primeira forma de utilização foi através da indústria bélica, como forma de busca de métodos de técnicas de espionagem.

O que era de acesso restrito a quem tivesse profundo conhecimento de computadores passou a ser utilizado por outras pessoas que não detinham tanto entendimento. Desta forma, a Internet que era vinculada a pesquisadores e fanáticos por computadores, se popularizou entre os mais distintos tipos de pessoas, sendo utilizadas pelas famílias e presente de forma massiva em muitos lares.

Segundo Zanellato (2002, p.01), “A Internet é um suporte (ou meio) que permite trocar correspondências, arquivos, ideias, comunicar em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos”.

Trazendo para nossa realidade, o Brasil ainda sofre com o problema da inclusão digital, aqueles que tem acesso a essa tecnologia de informação, são chamados de incluídos digitalmente. Devido a uma prática de financiamento para compra de computadores, a partir de 2009, segundo dados da Pesquisa Nacional por Amostra de Domicílios (PNAD 2011), divulgados pelo Instituto Brasileiro de Geografia e Estatística (IBGE), foi possível constatar que a proporção de usuários da internet, passou de 20,9% para 46,5%. Apesar do crescimento, o Brasil ainda

figura como um país de poucos incluídos digitalmente, menos de 50% de nossa população, segundo o IBGE.

Contudo, a expressão exclusão digital não está relacionada apenas a quem não possui acesso à internet. Devemos analisar principalmente, os que tem acesso, mas não detém o menor entendimento sobre ela. Uma parcela significativa de quem tem acesso, não enxergam os riscos que podem correr ao criarem uma simples conta de email. Um básico exemplo destes riscos é falta de privacidade. Bem sabemos que uma empresa pode possuir controle em relação ao acesso quando e como quiser. Alguns pensadores afirmam que, quem não está devidamente informados das desvantagens e vantagens que esse mundo digital pode oferecer, pode até ser considerado um excluído digital.

3 CRIMES DIGITAIS - DEFINIÇÃO E CONCEITO

A globalização foi determinante por propagar e alavancar a internet em diversos países, do mesmo modo, além das vantagens trazidas por ela, nos defrontamos com alguns malefícios que cercam nosso dia-a-dia e se tornam cada vez mais presentes em nossa realidade. A internet passa de um simples mecanismo de obtenção de informações gerais e distração, para um meio de se obter o objetivo almejado, seja na aquisição de um bilhete de cinema, compras de algum produto, essa comodidade permitida com a internet possibilitou da mesma forma, o cometimento de crimes virtuais.

Os crimes digitais são fruto do processo evolutivo e sem acompanhamento da internet, pois ao alcance que cresciam os mecanismos de difusão e transferência de dados pela rede, era de suma importância a utilização de um modo protetivo visando à segurança dos utilizadores. São ações de modificação de dados, invasões a sistemas informáticos, espionagem, disseminação da pornografia infantil, estelionato, entre outros.

Várias empresas do ramo digital passaram a produzir softwares para combater esses vírus que objetivam a captura de dados. Porém, a eficiência desses programas, conhecidos como Antivírus, não consegue eliminar completamente a execução danosa da prática delituosa.

Na atualidade, os crimes cibernéticos vêm requerendo atenção, pois conforme as estatísticas do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT-BR) o número de fraudes na internet cresceu 6.513% no País entre 2004 e 2009.

[...] É a conduta atente 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; 2. o 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. 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 software e hardware, para perpetrá-los; 4. a expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. ROSA (2002, P. 53-54)

Sergio Marcos Roque (2007, p. 25), define crime de informática como: “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”.

Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas. (RAMALHO TERCEIRO, a.6, n.58)

Apesar de diferentes posicionamentos para tipificação do crime, o meio não irá mudar, sendo o computador o objeto e a internet o meio de execução deste crime.

4 CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Devido à extensa dimensão do ciberespaço e a falta de barreiras, característica da internet, é necessário trabalho árduo e dedicação para analisar práticas criminosas que se propagam em número crescente na rede. Como a tecnologia avança com rapidez, logo os crimes virtuais também, a tarefa de constatar e classificá-los tem sido algo complexo, e a visão dos estudiosos tenta acompanhar os largos passos realizados pela tecnologia e com isso mudam junto com o passar dos anos.

Segundo Greco Filho (2000,p.56) deve-se adotar a seguinte divisão:

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

Podemos também classificar esses crimes entre próprios e impróprios. Os impróprios são os crimes já conhecidos e já praticados independente da rede, porém que o criminoso utilizou o meio da informática para praticá-lo. Este sendo quase sempre punido de acordo com a legislação comum. Segue análise de alguns crimes mais comuns da nova era digital e outros que passaram a ser realizados por meio da rede. Já os próprios, só podem ser praticados através da informática. Sendo esses típicos crimes do mundo virtual, partindo do pressuposto que existem única e exclusivamente em razão da informática (Carla Rodrigues, 2003, p.10).

4.1 INVASÃO DE PRIVACIDADE

Segundo o dicionário Aurélio a privacidade é definida como “Intimidade pessoal ou de grupo definido de pessoas”. Pode-se dizer que o direito à privacidade é o direito de manter para si informações pessoais.

“Sobre o direito à intimidade, lembremos da lição de Robert Alexy ao mencionar, em sua obra Teoria dos Direitos Fundamentais, a teoria das Esferas, pela qual é possível separar três esferas com decrescente intensidade de proteção, quais sejam: a esfera mais interna (âmbito último intangível da liberdade humana), caracterizando-se por ser o âmbito mais íntimo, a esfera íntima intangível e conforme interpretação do Tribunal Constitucional alemão, o âmbito núcleo absolutamente protegido da organização da vida privada, compreendendo os assuntos mais secretos que não devem chegar ao conhecimento dos outros devido à sua natureza extremamente reservada; a esfera privada ampla, que abarca o âmbito privado na medida em que não pertença à esfera mais interna, incluindo assuntos que o indivíduo leva ao conhecimento de outra pessoa de sua confiança, ficando excluído o resto da comunidade; e a esfera social, que engloba tudo o que não for incluído na esfera privada ampla, ou seja todas as matérias relacionadas com as notícias que a pessoa deseja excluir do conhecimento de terceiros”. (MARQUES, 2008)

Logo, é possível concluir que como MARQUES (2008) ensina, privacidade nada mais é do que aquilo “... que preserva-nos do conhecimento alheio, reservando-nos a nossa própria vivência”.

Entretanto, com a internet e a constante circulação de informação na rede, onde as pessoas passaram a divulgar uma significativa quantidade de informações por meio de cadastros em sites ou até redes sociais, o acesso não autorizado também conhecido como invasão ou “hacking” vem sendo facilitado e se tornando cada dia mais frequente. Esse tipo de conduta onde o agente acessa de forma indevida um sistema informático seja para satisfação própria, curiosidade ou superação de uma habilidade; ao ter acesso a informações pessoais da vítima e sigilosas, pode-se manipular, defraudar ou sabotar dados, sendo assim interpretado como um ilícito chave para prática de outros ilícitos.

4.2 ESTELIONATO

O estelionato ocorre quando o agente induz a vítima a um erro, para assim obter vantagem para si ou para um terceiro. O estelionato eletrônico que vem crescendo de forma significativa nos últimos anos não é diferente, a diferença é que o autor utiliza a internet como meio de operação. Um exemplo comum de estelionato eletrônico é através de e-mails falsos, nos quais muitas vezes as vítimas são induzidas a fornecer suas informações pessoais em sites que elas acreditam ser

verdadeiros, e através desses sites falsos o infrator toma conhecimento de dados importantes da vítima como dados bancários, por exemplo.

Pela definição de Feliciano (2001, p. 75), “a conduta consiste em o sujeito ativo empregar o meio informático para induzir ou manter a vítima em erro, obtendo com isso a vantagem ilícita para si ou para outrem”

Ainda, o Art. 171 descreve o crime de estelionato como: “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”.

Nesse sentido, Rosa (2007) corrobora que:

“Não resta dúvida de que a Internet é um meio novo de execuções de crimes ‘velhos’, contidos no Código Penal; entretanto, esses crimes não são considerados ‘crimes de informática’. Estelionato é sempre estelionato, praticado com assistência do computador com ou sem ela [...]” (Rosa, 2007, p.73).

4.3 FRAUDE VIRTUAL

A fraude virtual acontece quando o criminoso realiza uma invasão, alteração, pagamento ou qualquer outra modificação em um sistema de processamento de dados através de sites espiões por meio da internet, induzindo assim o usuário a fornecer informações sigilosas, tanto pessoais como financeira sem que ele tenha conhecimento do que está fazendo. Muitas vezes através de páginas suspeitas na qual o usuário é encaminhado para uma página fraudulenta ou através de mídias sociais.

Esse tipo de fraude pode ser praticado por um terceiro que se encontra no local a ser fraudado, sendo neste caso de origem interna. Ou o fraudador pode não possuir vínculo com o local que está fraudando, nesse caso sendo de origem externa.

Consoante Eduardo Valadares de Brito apud Carla Rodrigues (2003, 32), habitualmente ocorrem:

“[...]quando o indivíduo ao comprar, vender ou investir via Internet é enganado de alguma forma. O vendedor pode descrever produtos ou serviços de maneira enganosa ou pode, ainda, receber o

pedido e o dinheiro, mas não entregar o bem o qual estava obrigado”.

O CERT-BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), se define Fraude Eletrônica como:

“A fraude eletrônica consiste em uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, esse tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.”

Um dado importante obtido ainda pelo CERT-BR no ano de 2011 é sobre a alarmante quantidade de fraudes no Brasil como pode ser analisado no gráfico:

Ilustração 01 – Gráfico



Fonte: CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Incidentes reportados ao CERT.br – Janeiro a Dezembro de 2011. Disponível em: <<http://www.cert.br/stats/incidentes/2011-jan-dec/fraude.html>>. Acesso em: 08/10/2014

As fraudes virtuais vem sendo cada dia mais comuns e aumentando seu número de forma exponencial com o passar dos anos, é o que observamos na área de furto mediante fraude (art. 155 do Código Penal), representada pela captura de dados da conta bancária do usuário, através da instalação de um programa em um

equipamento com acesso à internet, após recebimento de um e-mail falso, também conhecido como phishing. Segundo relatório de 2012 da empresa de segurança virtual Norton Symantec, os brasileiros perdem uma média de R\$ 16 bilhões por ano em fraudes cibernéticas ou em consequências provocadas por ela como gasto com consertos de máquinas por exemplo.

4.4 PORNOGRAFIA INFANTIL

A pornografia infantil é caracterizada pela comercialização de fotografias pornográficas ou eróticas com crianças e adolescentes envolvidas. Se o praticante tem o objetivo de comercializar as fotografias ou expô-las ao público já pode ser considerado que o crime foi concretizado, mesmo que o público ainda não tenha tido acesso ao material. Para ocorrer punição basta divulgação do material e a existência de uma possibilidade de alguém ter acesso a ele. O elemento subjetivo deste tipo penal é o dolo.

Comentando sobre pornografia em sua generalidade, é importante ser comentando o art. 234 do Código Penal, o qual versa:

Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno:

Pena – detenção, de 6 (seis) meses a 2 (dois) anos, ou multa.

Parágrafo único. Incorre na mesma pena quem:

I – vende, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo;

II – realiza, em lugar público ou acessível ao público, representação teatral, ou exibição cinematográfica de caráter obsceno, ou qualquer outro espetáculo, que tenha o mesmo caráter;

III – realiza, em lugar público ou acessível ao público, ou pelo rádio, audição ou recitação de caráter obsceno.

Segundo balanço da Polícia Federal e dados divulgados pela ONG Safernet Brasil (entidade que monitora crimes e violações dos direitos humanos na internet) o número de prisões decorrentes de pornografia infantil na web aumentou significativamente entre 2012 e 2013, chegando a mais do que dobrar. Ainda segundo a Safernet o Brasil ocupa um ranking de 4º lugar dentre países que exploram esse mercado, movimentando bilhões anualmente.

De acordo com o Estatuto da Criança e do Adolescente, Lei 8.069/9062, são estabelecidas penalidades mais específicas para o criminoso que pratica pornografia infantil, como:

Art. 240 – Produzir ou dirigir representação teatral, televisiva ou película cinematográfica, utilizando-se de criança ou adolescente em cena de sexo explícito ou pornográfica:

Pena – reclusão de 1 (um) a 4 (quatro) anos, e multa. Parágrafo único. Incorre na mesma pena que, nas condições referidas neste artigo, contracenar com criança ou adolescente.

Art. 241 – Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão de 1 (um) a 4 (quatro) anos.

Segue crime tipificado no Estatuto da Criança e do Adolescente:

ESTATUTO DA CRIANÇA E DO ADOLESCENTE – Art. 241 – Inserção de cenas de sexo explícito em rede de computadores (Internet) – Crime caracterizado – Prova pericial necessária para apuração da autoria. “Crime de computador”; publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores atribuída a menores – Tipicidade – Prova pericial necessária à demonstração da autoria – Habeas Corpus deferido em parte.

O tipo cogitado – na modalidade de “publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente” – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma normal aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.

Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta incriminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da Lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.

Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta incriminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da Lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.

A norma que tipifica esse crime previsto no presente artigo é percebida como norma aberta, e o Supremo Federal considera sua aplicação também para crimes cometidos por meio da internet, o crime precisa apenas que tenha havido divulgação para ser considerado consumado independente do meio pelo qual foi feita a publicação.

Porém a grande dificuldade na identificação do autor das condutas citadas é que muitas vezes a quebra de sigilo torna-se necessária, visto que é preciso o rastreamento da origem do agente e após localização, análise das provas eletrônicas por uma perícia técnica rigorosa para que sejam aceitas nos processos.

4.5 CRIMES CONTRA A PROPRIEDADE INTELECTUAL

A definição de propriedade na linguagem jurídica é a condição em que se encontra a coisa, que pertence, em caráter próprio e exclusivo a determinada pessoa. É, assim, a pertinência exclusiva da coisa atribuída à pessoa.

Já a Propriedade Intelectual é definida pela Organização Mundial da Propriedade Intelectual – OMPI – tal como disposta no artigo 2º, inciso VIII, da Convenção de Estocolmo de 1967, como “a soma dos direitos relativos às obras literárias, artísticas e científicas, às interpretações dos artistas intérpretes e às execuções dos artistas executantes, aos fonogramas e às emissões de radiodifusão, às invenções em todos os domínios da atividade humana, às descobertas científicas, aos desenhos e modelos industriais, às marcas industriais, comerciais e de serviço, bem como às firmas comerciais e denominações comerciais, à proteção contra a concorrência desleal e todos os outros direitos inerentes à atividade intelectual nos domínios industrial, científico, literário e artístico.”

De acordo com LICKS (p. 608) “Todavia, no plano jurídico, é necessária a clara ideia da definição de propriedade intelectual, como a de um capítulo do Direito, extensamente submetido a regimes internacionais diversos, compreendendo as disciplinas tradicionalmente definidas como propriedade industrial, os direitos do autor e conexos e outros direitos sobre bens imateriais de vários gêneros”.

O direito industrial fica responsável por regular as criações estéticas utilizadas para satisfação de necessidades humanas imediatas, sendo voltada para área empresarial, popularmente conhecido como patentes (invenção, modelo de utilidade, modelo industrial e desenho industrial) e marcas (de Indústria, de comércio, de serviço ou sinal de propaganda). Em contrapartida o direito do autor aplica-se à regulação das relações jurídicas decorrentes da criação intelectual e é utilizado nas áreas que possuem obras intelectuais no campo da literatura, das ciências e das artes.

Com a globalização e a internet, fica cada vez mais fácil o acesso a informações e propriedades intelectuais espalhadas no mundo inteiro, devido a amplitude já ressaltada do ciberespaço, a rapidez com que as informações circulam e a ausência e dificuldade de fiscalização, que acabam facilitando para que os materiais disponibilizados sejam copiados e utilizados de forma ilegal sem que o proprietário tenha como exigir seus direitos como criador ou sequer tenha conhecimento do que está acontecendo. Para manter a integridade da obra criada os bens jurídicos tutelados na propriedade intelectual são de natureza imaterial, a partir daí é que são decorridas relações jurídicas para defender a personalidade do titular de direitos individuais, ou seja, o proprietário.

O Art. 184 do Código Penal versa:

Art. 184 - Violar direitos de autor e os que lhe são conexos:

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

§ 1º - Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:

Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 2º - Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.

§ 3º - Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:

Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto.

Art. 186 - Procede-se mediante:

I – queixa, nos crimes previstos no caput do art. 184;

II – ação penal pública incondicionada, nos crimes previstos nos §§ 1º e 2º do art. 184;

III – ação penal pública incondicionada, nos crimes cometidos em desfavor de entidades de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo Poder Público;

IV – ação penal pública condicionada à representação, nos crimes previstos no § 3º do art. 184.

Em suma, a propriedade intelectual deve ser protegida e ser dado seu devido valor.

“A partir do momento em que a tecnologia passou a permitir a reprodução em série de produtos a serem comercializados. Além da propriedade sobre o produto, a economia passou a reconhecer direitos exclusivos sobre a idéia de produção ou, mais precisamente, sobre a idéia de que permite a reprodução de um produto. A estes direitos, que resultam sempre numa espécie de qualquer exclusividade de reprodução de um produto (ou serviço) dá-se o nome de propriedade intelectual”. (BARBOSA; ARRUDA; 1990, p.10)

Logo, o direito de propriedade intelectual pode ser considerado um conjunto de privilégios, aferidos por lei, ao criador de determinada obra intelectual, para garantir que ele se beneficie do resultado de sua criação.

4.6 DANO INFORMÁTICO

Este crime está previsto no nosso Código Penal em seu art. 163: Destruir, inutilizar ou deteriorar coisa alheia: Pena – detenção, de um a seis meses, ou multa.

Através deste trecho citado, o legislador determinou na elaboração desse artigo a proteção contra danos efetuados a “coisas”, sendo estas tangíveis, logo, não foi levado em consideração a conduta do dano informático. Pois, esse não é considerado algo material quando nos referimos a dano de dados que estavam disponíveis em pen-drives, hard disks, ou qualquer outro meio de armazenamento, pois se não houve deterioração do equipamento de forma física e sim apenas dos dados, eles não são considerados tangíveis.

Sabe-se que levando em consideração o princípio da legalidade, é proibida a utilização de analogia no Direito Penal em situações que prejudique o agente da conduta, logo, não se poderia usar esse artigo citado como forma de julgar um crime de dano informático visto que algo intangível não pode ser considerado algo material. Logo o agente seria punido de acordo com a legislação existente.

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

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio.

Parágrafo único. Nas mesmas penas incorre quem apaga, altera ou suprime os dados eletrônicos alheios sem autorização ou em desacordo com aquela fornecida pelo legítimo titular.

Nessa nova redação coisas tangíveis de intangíveis são claramente diferenciadas e podem ser julgadas de acordo com o presente artigo, resolvendo assim a lacuna jurídica existente na legislação nesse sentido e dando punição própria a quem comete danos informáticos.

4.7 ESPIONAGEM ELETRÔNICA

Segundo Sun Tzu cita em seu livro A Arte da Guerra, a espionagem consiste na prática de obter informações de caráter sigiloso relativas a governo ou organizações, sem a autorização desses, para obter vantagem de algum modo, seja militar, política, econômica, científica, tecnológica ou social.

Como a tecnologia vem se tornando cada vez mais essencial não só para levar praticidade vida pessoal das pessoas, mas também para as organizações, as empresas vêm se tornando cada vez mais dependentes dos mais variados tipos de softwares e disponibilizando nas redes cada vez mais informações importantes e estratégicas nos servidores organizacionais. Dessa forma, apesar do investimento em segurança existir, abre espaço para o que conhecemos como espionagem eletrônica.

Existem diversos tipos de espionagem eletrônica, Dra. Patricia Peck Pinheiro, advogada especialista em Direito Digital, ressalta que a mais comum é chamada de Sigint (signals intelligence) que se originou na interceptação, decodificação, tradução e análise de mensagens por uma terceira pessoas além do emissor e do destinatário pretendido. Isso pode ser causado por alguém externo a empresa que busca informações, como concorrentes, ou por alguém interno da empresa, um próprio funcionário por algum motivo pessoal.

Não há um tipo penal próprio para determinar o crime de espionagem eletrônica, porém a conduta está tipificada no Código Penal de acordo com os art. 154 e 184 – crime de violação de segredo profissional e crime de violação de direito autoral:

Art.154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena – detenção, de três meses a um ano, ou multa.

Art.184 - Violar direitos de autor e os que lhe são conexos: pena de detenção, de três meses a um ano, ou multa.

O funcionário que cometer tal crime, poderá ter rescisão de contrato por justa causa, visto o que versa o art. 482, “g” da CLT/45:

Art. 482 - Constituem justa causa para rescisão do contrato de trabalho pelo empregador:

g) violação de segredo da empresa.

As organizações precisam priorizar o investimento em segurança no ambiente de trabalho e buscar monitorar tudo que ocorre na empresa, visto que no caso do autor ser interno, ele irá possuir legítimo acesso e deletar qualquer rastro que possa provar que a ação foi cometida.

4.8 CRIMES CONTRA A HONRA

A honra é formada por um conjunto de traços pessoais do indivíduo, sendo essas a junção das qualidades físicas, morais e intelectuais, que o faz digno e respeitado no meio social em que vive e influencia diretamente na sua autoestima. A concepção de honra é construída e modelada por cada um ao longo da vida perante as pessoas que convivem, e se torna um patrimônio possuído por cada um, devendo este ser protegido.

Ter a honra ferida pode acarretar diversas consequências calamitosas no futuro, pois ocorre um estrago de algo que foi construído durante toda sua vida até então, e que definem sua aceitação ou não para convivência em determinado grupo da sociedade. Sendo essas consequências muitas vezes de difícil reparação. Por isso também a necessidade de se preocupar com os crimes contra a honra.

Os crimes contra a honra estão previstos nos artigos 138 ao 141, do Código Penal. Segundo Damásio (2003, p. 201), tais tipos penais visam proteger a honra, que consiste em “conjunto de atributos morais, físicos, intelectuais e demais dotes do cidadão, que o fazem merecedor de apreço no convívio social”.

Segundo Greco (2010, p.400) ao tratar de crimes contra a honra muitos doutrinadores os dividem em duas espécies: a honra objetiva e a honra subjetiva. No primeiro caso, a honra é dita como determinada pela sociedade, onde se encaixa os crimes de calúnia e difamação. Já a segunda se refere a honra atribuída pelo próprio indivíduo a si mesmo, podendo ser citado o crime de injúria.

4.8.1 Calúnia

De acordo com o art. 138 do nosso Código Penal, é definido calúnia como: “Caluniar alguém, imputando-lhe falsamente fato definido como crime”. Nesse crime o infrator imputa à vítima a prática de fato concreto como crime, sabendo que a imputação é falsa, dessa forma, abala sua reputação no meio social.

Nestes termos dispõem segundo o Código Penal:

Art. 138. Caluniar alguém, imputando-lhe falsamente fato definido como crime:

Pena - detenção, de 6 (seis) meses a 2 (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 I do art. 141;

III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

O crime de calúnia é considerado consumado a partir do momento que a informação fica visível a um terceiro, que não seja o autor ou o réu da situação, ou este toma conhecimento do fato.

Como expõe Cezar Roberto Bitencourt em seu livro Tratado de direito penal, a lei estende-se a conduta dos que de qualquer modo divulgam a informação do crime em acordo como §1º, do art. 138, do código penal, “Na mesma pena incorre

quem, sabendo falsa a imputação, a propagar ou divulga”, o que há de mais importante nesta conduta é que sua ação só dependera do dolo direto, pois deve ter conhecimento pleno do caráter ilícito do fato de forma a querer causar dano à vítima.

4.8.2 Injúria

A injúria é ofender a dignidade ou decoro de alguém. Ela atinge a honra subjetiva, ou seja, a honra íntima de cada indivíduo, portanto depende se o sujeito se sentir atingido. Dentre os crimes contra honra pode ser considerada o menos grave. E o código penal subdivide a injúria em três espécies: injúria simples, injúria real e injúria preconceituosa. Como dispõem o código penal:

“Art. 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
 Pena - detenção, de 1 (um) a 6 (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 extorsão 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 3 (três) meses a 1 (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 1 (um) a 3 (três) anos, e multa

No crime de injúria, não é necessário que terceiras pessoas tomem conhecimento para se consumar o crime, pois se considera se a vítima foi ofendida internamente. Na visão de Carla Rodrigues (2003, p. 17): “No crime de injúria, o agente não imputa à vítima a prática de um fato, como na calúnia e na difamação, mas sim uma característica, qualidade, enfim, o conceito que o agente tem sobre a vítima”.

4.8.3 Difamação

O crime de Difamação é realizado na internet de formas variadas, pode ser através de e-mails destinados as pessoas diversas além da vítima, imputando à

esta, algum acontecimento que ofenda sua honra objetiva, ou até divulgando em redes sociais as mesmas ofensas. É disposto no código penal como:

Art. 139. Difamar alguém, imputando-lhe fato ofensivo à sua reputação:

Pena - detenção, de 3 (três) meses a 1 (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.

Nesta prática criminosa, a pessoa Jurídica não pode ser sujeito passivo, visto que no art. 139 do CP a norma é dirigida à pessoa humana, porém, quando o crime for praticado por meio da imprensa, pode-se aplicar a Lei nº 5.250/67 – Lei de Imprensa.

Nesse crime a lei não faz exigência que a atribuição seja falsa, é necessário apenas que tenha havido a perpetuação de algo que ofenda a reputação do agente diante da sociedade. No ambiente virtual, o crime se concretiza no momento que outros usuários façam leitura de um ato ofensivo publicado em redes sociais por exemplo. Assim, no seu livro, Cezar Roberto Bitencourt (2012, p 364) relata:

“Determinado segmento doutrinário tem sustentado que não se justifica punir alguém porque repetiu o que todo mundo sabe e todo mundo diz, pois está caracterizada sua notoriedade. Segundo Tourinho Filho, 'se o fato ofensivo à honra é notório, não pode o pretense ofendido pretender defender o que ele já perdeu, e cuja perda caiu no domínio público, ingressando no rol dos fatos notórios. No entanto, não nos convence esse entendimento, por algumas razões que procuraremos sintetizar. Em primeiro lugar, quando o Código Penal proíbe a exceção da verdade para o crime de difamação, está englobando a exceção da notoriedade; em segundo lugar, a notoriedade é inócua, pois é irrelevante que o fato difamatório imputado seja falso ou verdadeiro; em terceiro lugar, ninguém tem o direito de vilipendiar ninguém.”

Logo, é necessária à punição de qualquer tipo de desconstrução de honra objetiva do sujeito, mesmo que se trate de fatos verídicos, não é permitido que a honra seja desconstruída por outra pessoa.

5 BRASIL E CRIMES CIBERNÉTICOS

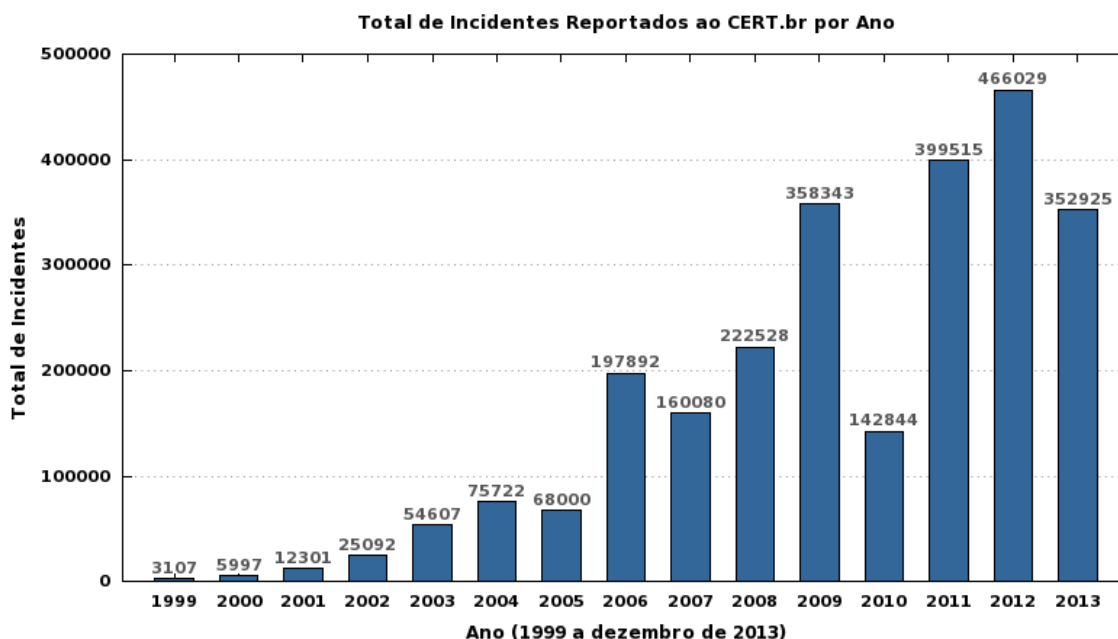
O Brasil vem gradativamente buscando o combate à criminalidade virtual. Um dos exemplos é o surgimento de centros de investigação especializados na

prevenção e combate das infrações cometidas através de meios virtuais, como as Delegacias Especializadas de Repressão a Crimes contra Informática e Fraudes eletrônicas. A Unidade de Perícia Informática da Polícia Federal, SEPFIN (Serviço de Perícia em Informática), é um dos exemplos no âmbito federal.

Não obstante, motivado pela criminalidade virtual crescente e a insurgente necessidade de buscar meios alternativos de combate, surgiram em nosso país iniciativas particulares, especializadas no acompanhamento de denúncias de infrações que firam os direitos humanos pelo mundo digital. Como um exemplo deste tipo de organização, é apresentada a SaferNet Brasil, associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial.

Porém, apesar de possuímos um mercado economicamente estratégico, estamos imersos na rota das fraudes virtuais e ataques cibernéticos. Nos últimos anos, os dados não foram favoráveis ao apresentarem um número alarmante de crimes digitais relacionados ao roubo de senhas bancárias, números de cartões de crédito e furtos de dados pessoais. A avaliação de fraude da RSA Anti-Fraud Command Center (AFCC), setor de segurança da EMC² Corporation, empresa de referência internacional no segmento de proteção digital, constatou que estamos no quarto lugar, em um ranking de 5 componentes, se tratando de atentados digitais a corporações – uma posição péssima para um Estado que busca atrair investimentos internacionais.

Ilustração 02 - Gráfico



Fonte: CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Incidentes Reportados ao CERT.br. Disponível em: < <http://www.cert.br/stats/incidentes/>>. Acesso em: 18 out. 2014.

6 LEGISLAÇÃO NACIONAL EM RELAÇÃO AOS CRIMES VIRTUAIS

Quando tratamos da situação da tipificação dos crimes digitais em nosso ordenamento jurídico, somos conduzidos a pensar em fragilidade total, todavia, o que poucos sabem é que a legislação vigente consegue abarcar mais de 90% das infrações cometidas no meio virtual.

Respalhando tal afirmativa, foi elaborado um quadro expositivo para apresentar as modalidades de atos cometidos por meio da internet e que já possuem tipificação legal:

Calúnia.	Art. 138 do Código Penal
Difamação	Art. 139 do C.P.
Injúria	Art. 140 do C.P.
Ameaça	Art. 147 do C.P.
Furto	Art. 155 do C.P.
Dano	Art. 163 do C.P.

Apropriação indébita	Art. 168 do C.P.
Estelionato	Art. 171 do C.P.
Violação ao direito autoral	Art. 184 do C.P.
Pedofilia	Art. 247 da Lei 8.069/90 (Estatuto da Criança e do Adolescente)
Crime contra a propriedade industrial	Art. 183 e segs. da Lei 9.279/96
Interceptação de comunicações de informática	Art. 10 da Lei 9.296/96
Interceptação de E-mail Comercial ou Pessoal	Art. 10 da Lei 9.296/96
Crimes contra software -“Pirataria”	Art. 12 da Lei 9.609/98

A problemática existente quanto a punibilidade dos referidos atos quando cometidos pela internet é a identificação dos autores, pois a existência de provas que configurem o crime e a caracterização desta modalidade praticada em meio virtual em nossa lei, é precária.

Contudo, através das Leis 12.737/2012 e 12.735/2012, temos a tipificação penal específica sobre crimes digitais próprios, aqueles praticados contra informações, dados ou sistema de informação, ao contrário dos crimes virtuais impróprios, quando os sistemas são utilizados apenas como meio para se praticar a infração.

6.1 LEI CAROLINA DIECKMAN E LEI AZEREDO

A Lei 12.737/2012, externada como “Lei Carolina Dieckmann”, tipifica os crimes digitais cometidos no Brasil, punindo todo tipo de violação das estruturas de segurança da internet para obtenção de informações privadas ou comerciais. Ganhou esse nome extraoficial, pois na época em que tramitava na câmara, a respectiva atriz teve fotos publicadas devido a uma invasão em seu computador.

A criação desta lei visa punir qualquer invasão a computadores, tablets, smartphones, entre outros, conectados ou não à internet.

As punições determinadas vão até dois anos, sendo importante verificar dois adendos: quando as informações retiradas do sistema são divulgadas e, caso uma das vítimas seja uma figura política do Brasil, ocorre assim aumento de pena.

A entrada em vigor da lei gerou uma grande repercussão para este tema, principalmente pela exposição de uma figura pública. Contudo, existem lacunas como exemplo: que serão considerados crimes apenas os atos praticados em aparelhos protegidos por senhas.

Foi definido também que o crime se configura quando o proprietário não autoriza o acesso ao aparelho ou quando o infrator instala programas ilícitos para obter vantagens. A pena será de três meses a um ano de reclusão, além de multa.

A Lei 12.735/2012, intitulada como Lei Azeredo, entrou em vigor na mesma data da Lei Carolina Dieckman, porém conseguiu ter aprovada pouca coisa do seu projeto original. Primeiramente sinalizando que as Polícias Judiciárias por intermédio de regulamentação deverão se preparar para combater os crimes digitais e que nos casos de discriminação pela internet, o juiz poderá solicitar a retirada de conteúdo discriminatório não somente de rádio, tv ou internet, mas de qualquer meio possível.

É notório que as penas são baixas, permitindo o enquadramento destas condutas nos crimes de menor potencial ofensivo, não se integrando com a segurança das vítimas. Uma espionagem empresarial pode gerar uma concorrência desleal, assim como um acesso ilícito a certos dados, pode ser mais prejudicial que um furto comum.

Essas duas leis não conseguiram exaurir todos os tipos penais, muitos crimes ainda estão sem previsão legal e cada vez mais a sociedade está conectada.

6.2 DOS PROJETOS DE LEI

Apesar das novas leis terem sido consideradas uma evolução no certame dos crimes digitais, a diversidade de crimes existentes e principalmente, o rápido avanço tecnológico provocam uma maior tipificação em nosso ordenamento jurídico. Segue abaixo alguns dos principais projetos de leis desta temática, com comentários:

PL nº 21, de 2013, que modificou o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar o crime de bullying virtual praticado pela internet ou por mensagens de celular, do Senador Clésio Andrade.

Este Projeto não chegou a ser apreciado por qualquer Comissão. Além do mais, segundo a avaliação da comissão, “Todavia, julgamos que tais condutas não têm dignidade penal. É excessivo o uso do direito penal para lidar com esse tipo de conflito social. Portanto, julgamos que essa proposta, assim como a constante do Projeto de Código, não merecem seguir adiante.”

PL nº 101, de 2011, que altera o Código Penal para criminalizar a criação de identidade ou perfil falsos na internet e outras condutas equiparadas, de autoria do Senador Ciro Nogueira. O Projeto não chegou a ser apreciado por qualquer Comissão, mas estas condutas estão atendidas nos crimes de fraude informática (art. 170) e de falsa identidade (art. 268).

PL nº 386, de 2011, que altera o Código Penal, para prever como modalidade qualificada do crime de difamação o ato de divulgação não autorizada de imagens ou vídeos por meio eletrônico que contenha cena de sexo ou qualquer forma de exposição de sua intimidade, conhecido como sexting, de autoria do Senador Blairo Maggi. O Projeto não chegou a ser apreciado por qualquer Comissão.

PL nº 427, de 2011, que altera o Código Penal para prever o crime de atentado contra a segurança de meio ou serviço de comunicação informatizado, de autoria do Senador Jorge Viana. O Projeto não chegou a ser apreciado por qualquer Comissão.

PL nº 481, de 2011, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para dispor sobre os crimes de constrangimento e de ameaça praticados por meio das redes sociais presentes na rede mundial de computadores – Internet, de autoria do Senador Eduardo Amorim. O Projeto foi sensível a questão da calúnia, injúria ou difamação praticadas pela Internet e previu causa de aumento de pena, dado o efeito multiplicador proporcionado pelo meio cibernético.

PL nº 484, de 2011, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para dispor sobre os crimes de calúnia, difamação e injúria praticados na rede mundial de computadores – Internet, de autoria do Senador Eduardo Amorim. A proposta foi incorporada ao substitutivo oferecido pela CCT ao PLS nº 481, de 2011.

PL nº 567, de 2011, que estabelece causa de aumento de pena para os crimes contra a honra praticados por meio da Internet e prevê prazo mínimo de dois anos para o armazenamento dos dados pelo provedor da conexão, de autoria do Senador Blairo Maggi. Segundo o relatório do Senador Pedro Tarkes, estas regulações sobre a guarda de logs vão além da matéria penal e que devem ser feitas pelo órgão regulador desse setor.

(ANCHISES,2013,Artigo Virtual)

6.3 MARCO CIVIL DA INTERNET

Aprovada este ano, a lei n.12.965/14, conhecida como “Marco Civil da Internet”, tem origem ao longo de muitos debates e participações sociais. Como forma de diminuir a insegurança jurídica, esta lei introduziu algumas regras que protegem direitos de quem usa e impõem deveres às empresas.

Em síntese, os temas principais abordados pelo Marco Civil são: as normas para a responsabilização de provedores de aplicações de internet por conteúdo

gerado por terceiros; a imparcialidade da rede e as disposições a respeito da coleta, utilização e guarda de registros dos usuários de internet.

O primeiro tema versa sobre a liberdade de expressão. Segundo os dispositivos da nova lei, os provedores de internet, somente por ordem judicial específica, devem retirar os conteúdos postados por terceiros. Existem duas exceções à esta regra: a exibição não autorizada de nudez e cenas íntimas de sexo (conhecidas também como revenge porn), o provedor poderá ser responsabilizado se não retirar o conteúdo após a notificação das partes; e quando ocorrer a utilização indevida de direitos autorais, o provedor deverá retirar após o pedido dos usuários.

O segundo ponto diz respeito à neutralidade da rede, sendo essencial para garantia da internet que utilizamos, assegurando que não ocorra uma monopolização de poder na mão dos detentores da infraestrutura, o que possibilitaria uma redução na inovação nas pontas da rede. Com um poder maior, as empresas de telefonia e TV à cabo, donas dos cabos, poderiam, por exemplo, estabelecer taxas para empreendedores que quisessem oferecer conteúdos ou serviços através da Internet, aumentando o custo de entrada no mercado.

Por fim, trata-se da coleta e tratamento de dados pessoais, ferramenta direta das empresas que atuam no mercado de marketing digital, por exemplo. A lei 12.965/2014 estabelece que o usuário deverá sempre ser informado sobre o objetivo e utilização dos dados que foram coletados.

Não foi fácil aprovar o Marco Civil, nem muito menos consolida a melhor solução para os problemas que foram elencados. Para os segmentos de comunicação e marketing, a lei aponta o norte a ser seguido, o que, pelo menos em termos de previsão, é uma evolução.

7 PROBLEMÁTICAS NA SEARA DOS CRIMES CIBERNÉTICOS

Para um completo entendimento deste assunto, é de fundamental importância se analisar as dificuldades enfrentadas para a investigação e punibilidade dos agentes. Trataremos a seguir das principais problemáticas que envolvem o mundo digital

7.1 AUTORIA

Uma das atividades mais complexas realizadas pelos agentes policiais está relacionada com a identificação dos autores que praticam crimes no mundo virtual e vale informar que tal obstáculo é encontrado não só pelo nosso país, como também a nível internacional.

“O único método realmente seguro de atribuição de autoria em crimes informáticos é o que se funda no exame da atuação do responsável penal, quando este se tenha valido de elementos corporais para obter acesso a redes ou computadores. Há mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. As formas mais comuns são a análise do fundo do olho do usuário ou a leitura eletrônica de impressão digital, ou, ainda, a análise da voz do usuário”. ARAS (2001)

Os agentes destas práticas delituosas já são reconhecidos pela comunidade digital internacional por seus conhecimentos específicos voltados ao crime. São várias as denominações, como expostos a seguir:

7.1.1 Cracker

No universo digital existem as denominações hacker e cracker que devem ser distinguidas, pois são sujeitos que trabalham em lados contrários.

O Cracker é um expert em informática, que direciona seus conhecimentos para a prática de crimes e obtenção de informações em benefício próprio. Acrescenta Crespo (2011, p. 170) que o cracker “é aquele que “quebra” um sistema de segurança, invadindo-o”.

O hacker, denominação que significa “pirata”, é um expert em informática, que invade um sistema, mas que não pratica infrações ilícitas, ao contrário, utiliza seu conhecimento para identificar falhas e até mesmo melhorias no sistema de segurança.

7.1.2 Carder

São especialistas na modalidade de estelionato. Utilizam seus conhecimentos e buscam falhas nos sistemas de segurança das administradoras de cartão de crédito para obter seus dados e assim revende-los.

7.1.3 Phreaker

São experts em alteração no sistema de telefonia. Utilizam seus conhecimentos para obter ligações gratuitas e realizar escutas telefônicas clandestinas.

7.2 O PROBLEMA DA COMPETÊNCIA EM RAZÃO DO LUGAR

É de amplo conhecimento que é possível se conectar no mundo todo por meio da internet, sendo necessário apenas um computador e um provedor de internet. Devido a essa internacionalização da rede, surge um grande problema para os juristas ao se trabalhar com o aspecto de territorialidade e jurisdição na internet.

Excelente pensamento por Celso Valin (1978) apud Vladimir Aras (2002), na Internet não existem fronteiras e, portanto, algo que nela esteja publicado estará em todo o mundo. Como será possível determinar o juízo responsável para analisar um caso referente a um crime ocorrido no sistema virtual?

Segundo Carla Rodrigues (2003, p. 107), a determinação da competência será de acordo com o artigo 70, do Código de processo Penal, que versa o seguinte: “A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução”.

Em sua visão, Vladimir Aras (2002), se posiciona através da aplicação por equiparação da Lei n. 5.250/1967 conhecida com Lei de Imprensa, que por meio do artigo 42, considera competente para o processo e julgamento o foro do local onde for impresso o jornal.

Artigo 42: Lugar do delito, para a determinação da competência territorial, será aquele em que for impresso o jornal ou periódico, e do local do estúdio do permissionário ou concessionário do serviço de radiodifusão, bem como o da administração principal da agência noticiosa.

Partindo deste posicionamento, o provedor de acesso à Internet teria tratamento equipado à empresa jornalística. Deste modo, seriam resolvidos os conflitos de competência que eventualmente surgiriam.

Seria considerado como local do crime aquele onde estiver hospedado o site com conteúdo ilícito, para efeito de competência.

É notório que existe uma grande variedade de soluções para a instauração de competência. O que não se pode deixar de lado é a busca do resultado final do processo, o julgamento e punição do infrator.

7.3 PRODUÇÃO DE PROVAS

A obtenção de provas destinadas aos crimes praticados por meio virtual vem enfrentando sérios obstáculos e desestimulando as vítimas a ingressarem com ações à justiça.

Os tipos variados de crimes vem atingindo grande parte dos usuários da internet. Uso da imagem sem permissão, utilização de informações particulares em páginas falsas, crimes de invasão de privacidade, entre tantos outros.

As provas comprobatórias destinadas aos delitos virtuais são obtidas por meios de investigação pericial, e essa é uma das dificuldades, pois além do necessário conhecimento específico para realização desta perícia, muitas vezes as próprias vítimas tornam suas provas ilícitas, devido a ansiedade em apresentação na justiça, desrespeitando o devido processo legal e tornando assim as provas ilícitas.

A responsabilização pelo crime deverá ser manifestada e, a pena correta aplicada ao infrator, quando houver convicção da autoria e da realização do delito. O objetivo da prova é possibilitar o conhecimento do juiz para sanar a problemática sobre a autoria e a conduta criminosa, e não somente isso, fornecer todos elementos, da mesma forma que todos os fatos relevantes que influenciem na decisão do magistrado.

Tratando sobre as provas ilícitas, Alexandre de Moraes versa:

“Saliente-se que a doutrina constitucional passou a atenuar a vedação das provas ilícitas, visando corrigir distorções a que a rigidez da exclusão poderia levar em casos de excepcional gravidade. Esta atenuação prevê, com base no Princípio da Proporcionalidade, hipóteses em que as provas ilícitas, em caráter excepcional e em casos extremamente graves, poderão ser utilizadas, pois nenhuma liberdade pública é absoluta, havendo possibilidade, em casos delicados, em que se percebe que o direito tutelado é mais importante que o direito à intimidade, segredo, liberdade de comunicação, por exemplo, de permitir-se sua utilização.” (MORAES, 2010, p.112-113).

O órgão capacitado e responsável para atribuição de integridade, validade jurídica e autenticidade as provas documentais eletrônicas no nosso país é o Instituto Nacional de Tecnologia. Todavia, não são todas as provas eletrônicas admitidas pelo nosso Direito Penal como documento com validade jurídica, pois não é uma fonte muito confiável de constituição de provas, segundo doutrinadores.

Nesta temática, Marco Antônio de Barros realiza apresenta seu posicionamento:

“Com efeito, se a infração penal for praticada por meio da Internet, é necessário identificar a máquina utilizada. Nesse tipo de investigação o objetivo é descobrir o endereço IP (Internet Protocol) do computador dentro de uma rede. E nem sempre isto será suficiente, pois há casos em que um único computador sirva a mais de uma pessoa, sendo então necessário identificar quem realmente o utilizou para a prática delituosa. Na apuração dos chamados crimes digitais, informáticos ou cibernéticos, ou de infrações penais praticadas mediante o uso de microcomputadores, os peritos costumam empregar a técnica “post-mortem”. Ou seja, o sistema é examinado após o desligamento da máquina, situação em que cabe ao perito proceder à duplicação das mídias e à avaliação de evidências armazenadas e/ou recentemente apagadas.” (BARROS, 2011, p. 126).

É possível concluir que os documentos/provas virtuais carecem de segurança jurídica devido ao déficit tecnológico que sofremos, contudo, a sua apresentação deve ser realizada com cuidado e atenção, realizada por profissionais específicos em tal área para que elas não se tornem inválidas, e após essa série de etapas seja instaurado o devido processo legal e a punição aos infratores.

7.4 Legislação Insuficiente

O universo virtual avança de uma forma assustadora, por outro lado, a nossa legislação penal caminha vagarosamente, como é de fácil constatação através das baixas leis específicas contra crimes digitais.

O nosso Código Penal necessita urgentemente de uma reforma, pois não conseguiu acompanhar todas as mudanças e inovações de nossa sociedade, gerando no judiciário uma avalanche processual, o qual, sem uma legislação atual e forte, precisa de forma análoga, recorrer a outros institutos jurídicos para tentar solucionar os casos da melhor forma, ocasionando uma maior lentidão neste poder.

É necessário criar instrumentos legais mutáveis às contínuas inovações tecnológicas, evitando-se, a criação de normas ultrapassadas, condenadas à realidade em que foram feitas, e que, conseqüentemente, não tem os instrumentos necessários ao combate dos delitos virtuais desenvolvidos após a sua edição.

Com a ausência desta medida legislativa, o Brasil seguirá nas mãos de infratores, possuidores dos conhecimentos mais específicos da internet, exigindo mais esforço interpretativo do judiciário para aplicar a punição aos delitos que, até então, seguem sem a correta tipificação em nosso ordenamento.

8 CONCLUSÃO

Com o aumento de usuários no mundo cibernético e com a facilidade ao acesso a internet, o número de crimes digitais vem crescendo cada vez mais, visto que a internet é tida pelos seus usuários como um lugar em que há plena liberdade, para que este possa usufruir dela como bem entender, por isso torna-se necessário a intervenção do Estado, para que ele puna aqueles que ultrapassarem os limites da sua liberdade e adentrem na esfera jurídica alheia. Porém, para que o Estado consiga exercer o seu direito de punir, primeiramente é indispensável que haja meios adequados para tal ação, ou seja, torna-se necessário que esses crimes já se encontrem tipificados na legislação, o que atualmente não acontece.

Por tais razões podemos entender que para ações que apenas utilizam o computador e/ou internet como um instrumento para o cometimento do delito é desnecessária a criação de novos tipos penais, pois estes já se encontram previsto no nosso ordenamento jurídico, porém ainda existem os casos em que não há nenhum tipo de previsão e também não é possível fazer o uso da analogia, nesses casos, é de suma importância que haja uma nova tipificação, para que assim o Estado possa exercer o seu direito de punir, respeitando o princípio da legalidade.

Conclui-se, portanto que é mais que necessário que o ordenamento jurídico faça a devida regulamentação quanto ao uso da internet, para que assim os efeitos da sua má utilização sejam minimizados e o ambiente virtual e o jurídico convivam em equilíbrio.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DOS ANALISTAS DE INTELIGÊNCIA COMPETITIVA. **Glossário de IC**. Disponível em: <<http://www.abraic.org.br/V2/glossario.asp?letra=I>>. Acesso em: 12 ago. 2014.

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 5, n. 51, out. 2001. Disponível em: <<http://jus2.uol.com.br/doutrina/texto.asp?id=2250>>. Acesso em: 12 ago. 2014.

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

BARROS, Marco Antonio. **A busca da verdade no processo penal**. São Paulo: Editora Revista dos Tribunais, 2011, p. 126.

BITENCOURT, Cezar Roberto, **Tratado de direito penal, 2 : parte especial** : 12. ed. rev. e ampl. —São Paulo : Saraiva, 2012, p. 364

BRASIL. Código Penal. Decreto Lei n. 2.848/40. Disponível em: <http://www.dji.com.br/codigos/1940_dl_002848_cp/cp184a186.htm>. Acesso em: 12 ago. 2014.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Disponível em: <<http://www.cert.br>>. Acesso em: 14 set. 2014.

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

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

GRECO, Rogério. **Curso de Direito Penal: parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a honra**. 7a. Edição. Niterói, RJ: Impetus, 2010, pág. 400

JESUS, Damásio Evangelista. **Direito Penal**. 26 ed. São Paulo: Saraiva, 2003. 754 p. v. 1.

LICKS, Otto B. **“O Acordo Sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio”**. In: Guerra Comercial ou Integração

Mundial pelo Comércio? a OMC e o Brasil". Paulo Borba Casella, Aramita de Azevedo Mercadante, coordenadores, São Paulo: LTr.

MARQUES, Andréa Neves Gonzaga. **Direito à intimidade e privacidade**. Jus Vigilantibus, Vitória, Fev 2008. Disponível em: <<http://jusvi.com/artigos/31767>>. Acesso em: 10 out 2014.

MORAES, Alexandre de. **Direito Constitucional**. São Paulo: Editora Atlas, 2010, p.112-113.

OMPI: Disponível em: <http://www.OMPI.org>. Acesso em 26 de set. 2014.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. São Paulo: Saraiva, 2010.

PINHEIRO, Reginaldo César. **Os Cybercrimes na Esfera Jurídica Brasileira**. In: "A priori", INTERNET. Disponível em <<http://www.apriori.com.br/cgi/for/viewtopic.php?p=181>> Acesso em: 14 de set. 2014

ROCHA, Carolina Borges. **A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012**. Jus Navigandi, Teresina, ano 18, n. 3706, 24 ago. 2013. Disponível em: <<http://jus.com.br/artigos/25120>>. Acesso em 19 outubro de 2014

ROSA, Fabrício. **Crimes de informática**. Campinas: Bookseller, 2002.

SEGURANÇA – NOVA LEI DOS CRIMES VIRTUAIS – **Anchises** - Disponível em: <<http://anchisesbr.blogspot.com.br/2013/09/seguranca-nova-lei-dos-crimes.html>>. Acesso em: 19 de set. 2014

VADE MECUM. 11ª Ed. São Paulo. Saraiva, 2011

ZANELATO, Marco Antonio. Condutas Ilícitas na sociedade digital. **Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet**, n. 4, Julho de 2002. p. 173.

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

_____. Presidência da República – Casa Civil – Subchefia para Assuntos Jurídicos – Medida Provisória nº 2.200-1, de 27 de Julho de 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-1.htm>. Acesso em: 12 ago. 2014.

_____. **Cartilha**. Disponível em: <[http:// http://cartilha.cert.br/conceitos/sec8.html](http://http://cartilha.cert.br/conceitos/sec8.html)>. Acesso em: 11 set. 2014.

_____. **Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2011.**
Disponível em: <<http://www.cert.br/stats/incidentes/2011-jan-dec/fraude.html>>.
Acesso em: 28 de setembro. 2014.

_____. Cartilha. Disponível em: <<http://cartilhacert.br/glossario>>. Acesso em: 12 out. 2014.