

CRIMES CIBERNÉTICOS: CARACTERÍSTICAS E OBSTÁCULOS À SUA PUNIBILIDADE

Wallace Delfino Xavier

Sandresson Menezes

RESUMO

Este artigo busca analisar as espécies de crimes virtuais, classificados como próprios e impróprios e os sujeitos ativos e passivos destes delitos, fazendo para isso uma explanação desde o contexto histórico do surgimento da internet no Brasil e no mundo, até o desenvolvimento dos crimes virtuais e os avanços das tecnologias utilizadas pelos hackers. Trás ainda uma análise das condições atuais acerca do sistema especializado em investigação dos cibercrimes e da carência de uma legislação específica para estes delitos em nosso ordenamento, apesar da existência de uma tipificação penal sobre o tema, onde foram editadas algumas leis específicas que versam sobre os crimes cibernéticos, de modo a garantir a estes, respaldo jurídico.

Palavras chave: Crimes cibernéticos. Internet. Ausência de legislação específica. Dificuldades de punição.

ABSTRACT

This article aims at analyzing the types of virtual crimes, classified as purely digital crimes and mixed digital crimes, its perpetrators and victims, and, in order to reach this goal, we put into historical context the emergence of internet in Brazil and around the world, the evolution of virtual criminality and the technological advancements employed by hackers. The text also displays current conditions of the special system used to investigate these crimes and highlights the absence of a proper legislation in Brazilian legal system despite the existence of certain criminal dispositions on the matter, since legislators enacted some especial acts on cybercrimes in order to provide a certain legal support to its punishment.

Keywords: Cybercrimes. Internet. Absence of proper legislation. Hardships in punishment.

INTRODUÇÃO

Na era do mundo informatizado, onde o acesso à informação acontece em tempo real e ao passo de um clique no computador, estamos presos e cada vez mais absorvidos e vislumbrados por toda essa tecnologia que se desenvolveu e hoje se tornou a maior forma de comunicação, informação e entretenimento que possuímos.

É à internet que recorremos quando temos pressa e necessidade de localizar rapidamente informações, esclarecimentos de dúvidas, formas de entretenimento e diversão. Nela, as respostas aparecem numa velocidade muito rápida, a qual acompanha a sede de conhecimento e praticidade que buscamos em nossa sociedade atual.

Não restam dúvidas de todos os benefícios que a informática nos proporciona ao longo dos anos, desde a sua criação, até o desenvolvimento de todas as ferramentas que hoje a compõe. Porém, junto com tantos benefícios, a internet também passou a ser alvo das ações de criminosos, conhecidos como piratas virtuais ou "hackers". Estes usuários mal intencionados aproveitam-se da velocidade e dificuldade de identificar o agente causador dos danos para praticar delitos contra outros usuários da rede, confiando no anonimato e na impunidade de suas práticas delituosas.

É notável que um dos fatores para haver tantos criminosos no âmbito virtual é o fato de os mesmos se ampararem na falta de uma legislação específica que trate do tema, com respaldo para punir os envolvidos, e tampouco por meios adequados de provas que possam identificar os autores dos delitos.

Tais ações se dão através desta grande rede e expõem todos os dias milhares de usuários aos perigos que se escondem por trás de tantos benefícios proporcionados pelo ambiente virtual.

Aqui será tratado quais são os tipos de crimes que assolam a internet e a explanação de suas características principais; quem são estes criminosos virtuais e como estes se manifestam, e quais as formas de se proteger para não cair nas armadilhas da rede. Será exposto ainda, como se dá o trabalho de investigação de tais crimes no Brasil e as dificuldades que um cidadão enfrenta ao ser vítima de cibercrime e precisar do apoio de uma polícia especializada neste caso; e qual o atual cenário da legislação brasileira relativa a essa tipificação penal.

Portanto, o presente artigo fará uma explanação sobre tudo que envolva os crimes cibernéticos, desde a contextualização histórica do desenvolvimento da rede, até o detalhamento de suas características e sujeitos ativos e passivos. Explanando sobre as dificuldades de se punir o agente delituoso e as leis específicas que tratam do tema, buscando esclarecer e compreender, assim, este problema que enfrenta a sociedade moderna do século XXI.

1. SURGIMENTO DA INTERNET E SUA CHEGADA AO BRASIL

Assim como a maior parte das tecnologias, o desenvolvimento da internet também se deu para fins militares. Era pleno período de Guerra Fria e os Estados Unidos buscavam uma forma descentralizada de comunicação e armazenamento de dados, que fosse capaz de resguardar tais informações e continuar ativa, mesmo que parte dela fosse bombardeada, por exemplo. Com isso, a rede foi desenvolvida em ambientes acadêmicos, mas era financiada por um órgão militar especificamente desenvolvido pra esse fim, no ano de 1958, a Advanced Research Projects Agency (ARPA), a qual estava vinculada ao Departamento de Defesa dos Estados Unidos.

A primeira demonstração da ARPANET, a qual pode ser considerada a pioneira desta nova forma de comunicação, ocorreu em 5 de agosto de 1968, tendo porém, sua conectividade restrita a poucos hosts. Com o passar do tempo, mais universidades passaram a se conectar à internet, como a Universidade de Harvard, localizada em Cambridge, Massachusetts, dentre tantas outras. Na década de 80, passou a ser adotado o TCP/IP, o protocolo utilizado atualmente na internet como tecnologia padrão para a comunicação. Como conceitua Fabrício Rosa:

[...] a Internet é um conjunto de redes de computadores interligados pelo mundo inteiro, que têm em comum um conjunto de protocolos e serviços, possuindo a peculiaridade de funcionar pelo sistema de troca de pacotes, ou seja, as mensagens dividem-se em pacotes e cada pacote pode seguir uma rota distinta para chegar ao mesmo ponto. A Internet funciona graças aos protocolos ou sistemas de intercomunicação de programas, cujos protocolos mais importantes são o TCP (protocolo de controle de transferência) e o IP (Protocolo Internet), permitindo, assim, a utilização da Internet por computadores funcionando com qualquer Sistema Operacional: DOS, Windows, UNIX, MAC etc... (2002, p. 33).

A partir daí, com o desenvolvimento e aperfeiçoamento da internet, a mesma foi expandindo-se pelo mundo e sua chegada ao Brasil foi inevitável. Através da BitNet (Because It's Time Network), uma rede de universidades fundada em 1981 e que interligava a Universidade da Cidade De Nova York (CUNY) à Universidade Yale, em Connecticut, àquela que se tornaria a maior ferramenta de comunicação da sociedade, alçava vôos maiores e iniciava seu processo de globalização.

Em princípio a internet no Brasil era restrita aos setores acadêmicos e científicos. Apenas as universidades tinham acesso a essa nova fonte de informação e conhecimento. O Laboratório Nacional de Computação Científica (LNCC), a Fundação de Amparo à Ciência e Pesquisa do Estado de São Paulo (FAPESP) e a Universidade Federal do Rio de Janeiro (UFRJ) foram as primeiras instituições do Brasil a ter acesso a essa tecnologia entre os anos de 1987 a 1989, através da BitNet. Nesse período surgiu, com o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), a Rede Nacional de Pesquisa (RNP), com o objetivo de implantar uma rede com infraestrutura e abrangência nacional para os serviços de internet, a qual foi capaz de fornecer durante a década de 90, acesso à internet a cerca de 600 instituições, desta forma, sendo utilizada por volta de 65 mil usuários no país.

Contudo, apenas em 1995 ela começou a ser acessível à população em geral e não mais apenas um privilégio das universidades e iniciativa privada, como vinha acontecendo. A Internet ganhou novas finalidades como estudos científicos e didáticos, além de possibilitar a comunicação entre os usuários e dessa forma diminuir as fronteiras das relações interpessoais. Com ela foi descoberta uma nova forma de expandir conhecimento, gerar informações em tempo real e garantir a todos os usuários esse novo leque de descobertas sem a necessidade de sair de dentro de casa. Tornou-se um verdadeiro instrumento de comunicação de massa. O advento do uso da banda larga propiciou a fundição da internet no cotidiano de um número considerável e crescente de cidadãos, visto que a mesma possibilitou o aumento da velocidade de transmissão de dados, e consequentemente dando a seus usuários a possibilidade de realizarem um maior número de tarefas em um período menor de tempo enquanto navegavam, seja para baixar músicas, filmes, entre outros.

Hoje a informática é vital para a sociedade, como demonstra Marcelo Xavier de Freitas Crespo:

(...) Os sistemas marítimos, aeronáuticos e espaciais, bem como a medicina, dependem em grande parte de sistemas informáticos modernos. As redes informáticas se constituíram como nervos da sociedade, que cada vez mais depende dos computadores e das intranets (redes internas de cada corporação).

Com isso, apesar de toda sua importância, esta ferramenta virtual tornou-se perigosa pois passou a ser vista por criminosos como uma via livre para a prática de determinados e inúmeros delitos, os quais puseram em risco e expõe todos os internautas que navegavam na rede. Tais crimes serão melhor explicitados a seguir.

2. O QUE SÃO CRIMES CIBERNÉTICOS

O advento da Internet proporcionou um enorme avanço no que compete à velocidade de informação e disseminação em tempo real da mesma, além de garantir uma facilidade de acesso a tudo àquilo que deseje ver, o internauta, à distância de apenas um clique. Tornando-se deste modo, a principal ferramenta utilizada pelas pessoas em todo o mundo, quando o objetivo é buscar entretenimento, educação e informação. Porém junto com todos esses benefícios que a rede mundial de computadores nos oferece, vem também uma série de problemas que se proliferam no ciberespaço e atingem pessoas físicas e jurídicas.

Os Crimes Cibernéticos ou Crimes Digitais como são mais conhecidos, já começaram a existir desde que a Internet passou a ser utilizada, numa escala baixa à época, quando a rede ainda se desenvolvia, e numa quantidade crescente com o passar dos anos, haja vista a maior abrangência da internet para a população.

Crimes digitais, como esclarece Marcelo Xavier de Freitas Crespo:

(...) importam nas menções às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificação de dados, infrações a direitos de autor, incitação ao ódio e discriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros.

Os crimes cibernéticos são praticados todos os dias e os sujeitos do delito se escondem atrás do computador e desta forma, confiando no anonimato, os praticam das mais variadas maneiras.

A internet é comparada por muitos a uma terra sem lei, onde qualquer pessoa com um computador pode fazer uso de fotos, vídeos, áudios, dentre outras formas de mídia, relativas a qualquer outra pessoa e espalha-las para inúmeros usuários em questão de segundos. Toda essa velocidade e facilidade de difusão de materiais acabam por dificultar muito a punição dos sujeitos ativos dos crimes de informática e tornam bem mais complexo o trabalho da polícia especializada, tema este, que será abordado posteriormente. Antes disso é importante esclarecer quem são esses sujeitos e como agem e praticam seus crimes no ambiente virtual.

2.1 Sujeitos dos crimes cibernéticos

Antes de classificar os sujeitos dos crimes cibernéticos, é necessário explicar as duas diferentes formas destes delitos. Os crimes virtuais podem ser próprios ou impróprios. Nos crimes virtuais impróprios, o sujeito do delito pode ser qualquer pessoa, não sendo necessário para praticar tal ação, ter um conhecimento específico sobre informática, apesar de utilizar-se deste meio, diferente dos crimes considerados próprios, onde tais criminosos para provocá-los, precisam sim fazer uso e possuir um nível elevado de conhecimento de informática e manipulação de computadores. Tais sujeitos ativos são popularmente conhecidos e generalizados como hackers, porém há diversas outras denominações, para cada sujeito responsável por um tipo de crime específico, os quais serão diferenciados a partir de agora.

2.1.1 Sujeito Ativo

a) Hackers

É o nome dado aos chamados "piratas" de computador. Pode ser considerado um hacker qualquer pessoa que tenha um amplo conhecimento sobre computadores e pratique invasões, porém sem alterar nem danificar nada. Apesar de serem taxados de criminosos, nem todos os hackers buscam o prejuízo alheio. Alguns invadem computadores justamente

para alertar os donos do perigo a qual a máquina pode estar submetida e como proceder para frear as chances de invasões. Muitos são contratados por empresas para testar seus sistemas de seguranças e desenvolver novos mecanismos de proteção. Esses exemplos são conhecidos como "hackers do bem". Contudo, mesmo sem causar danos ou prejuízos, os hackers do bem também praticam crimes, ao passo que invadem sistemas de computadores alheios.

b) Crackers

Esses são os verdadeiros vilões da internet. Praticam invasões de sites apenas com o intuito de destruí-los e ver a sua repercussão na mídia. Em muitos casos são ladrões buscando brechas para roubar dinheiro e informações confidenciais no ciberespaço. Os crackers quebram sistemas de seguranças e os invadem. Sentem prazer em vandalizar e muitas vezes "picham" os sites com conteúdos preconceituosos e ofensivos. Eles ainda podem ser classificados de acordo com suas áreas de atuação ou seus níveis de conhecimento.

c) Carders

São estelionatários. Roubam senhas de cartões de crédito e utilizam-nas para fazer compras e dívidas no nome da vítima. Agem invadindo os computadores das administradoras dos cartões de crédito para subtrair os números dos mesmos. Em muitos casos praticam essas ações junto com os crackers, onde estes realizam a invasão do computador e subtração dos números e os carders realizam as compras. Exige-se muito cuidado para não serem pegos, pois precisam criar uma conta pirata, um IP falso e nunca conectarem-se através de suas linhas telefônicas, de modo que não possam ser localizados.

d) Lammers

Imaturos e despreparados, consideram-se verdadeiros hackers, quando na verdade não passam de aspirantes a invasores. Acham-se experts, apesar de não possuírem nenhuma experiência em cometer invasões e roubos. Acabam por serem "chacotas" no mundo dos crimes cibernéticos, sendo insultados e depreciados pelos hackers profissionais.

e) Wannabes

Semelhantes aos Lammers também não são muito capazes de praticar grandes ações no mundo dos crimes virtuais, apesar disso, são mais conscientes do que sabem e conseguem mais êxito por terem noção dos limites de seus conhecimentos e até aonde podem ir às suas ações criminosas.

f) Phreakers

São os especialistas em telefonia. Agem interceptando ligações e fazendo escutas telefônicas. Porém não se limitam a ouvir conversas alheias, os phreakers também fazem ligações gratuitas, fato que se dá, pois os mesmos utilizam computadores para confundir as operadoras de telefone, de modo que esta não consiga identificar de onde vem à origem da ligação, fazendo com que outra pessoa que possui conta da respectiva operadora acabe pagando a conta da ligação em seu lugar.

g) White e Black Hats

Nada mais é do que outra forma de denominar e diferenciar os "bons" dos "maus" hackers. Chamados de Chapéus Pretos e Brancos, em tradução literal, os mesmos são diferenciados dos que praticam o bem e os que praticam ações delitivas. Geralmente, as expressões tem sido relacionadas à otimização de buscas, ou seja, manipulações fraudulentas de aspectos de uma página na internet de modo a aumentar sua visibilidade em sites de busca, o que inclusive configura concorrência desleal, como dispõe o art. 195, III, da Lei n.9.279/96: "comete crime de concorrência desleal quem: ... III - emprega meio fraudulento, para desviar, em proveito próprio ou alheio, clientela de outrem".

h) Outros Sujeitos

É relevante lembrar que nem todos os criminosos virtuais precisam ter vasto conhecimento de informática, podendo qualquer pessoa que saiba usar de modo básico computador e internet, cometer crimes cibernéticos. Assim ocorrem crimes contra a honra (injúria, calúnia e difamação); pedofilia (ao serem repassados conteúdos pornográficos envolvendo crianças e adolescentes); dentre outros exemplos.

2.1.2 - Sujeito Passivo

O sujeito passivo é aquele que se torna vítima destas modalidades de crimes, sendo passíveis destes, qualquer pessoa que navegue pela internet. Pois ao entrar nesta grande rede, todos estão vulneráveis a ataques dos piratas, que buscam obter nossas informações confidenciais, assim como invadir nossa privacidade e causar prejuízos, sejam eles financeiros, de exposição da intimidade, de danos à honra e moral, entre tantas outras formas de atingir os terceiros.

3. CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

3.1 Crimes digitais próprios

a) Acesso não autorizado

É conhecido como a "invasão" ou "hacking". Tal conduta pode-se dar apenas pelo prazer de superar desafios técnicos de segurança; por vontade de invadir a privacidade alheia, tendo acesso a informações sigilosas, ou ainda pela intenção de manipular, defraudar e sabotar dados. Com isso, nota-se que o acesso não autorizado a computador alheio é apenas o ilícito básico para a prática de tantos outros possíveis.

As técnicas utilizadas para a obtenção do acesso não autorizado surgiram na década de 1980, onde se baseavam basicamente na descoberta de senhas. Em seguida vieram às linhas telefônicas a serem alvos de acesso não autorizados.

As técnicas atuais utilizam-se do modo indireto, onde a própria vítima acessa o site pelo manejo dos protocolos IP (protocolo de internet) e HTTP (protocolo sobre a transferência de hipertexto) e dirige-se a uma página sem saber o perigo de acessá-la. O acesso não autorizado já está tipificado em nosso Código Penal, com a lei 12.737/2012 visto sua notável ilicitude e a forma como o mesmo abre portas para a prática de tantos outros crimes mais graves.

b) Obtenção e transferência ilegal de dados

Os dados de um usuário são coletados através de spywares, termo genérico que designa arquivos espiões, o qual se torna uma forma bastante simples de obtenção de tais dados. Os mesmos podem ser utilizados para descobrir, por exemplo, quais os sites que o usuário tem acessado. No caso dos arquivos espiões, estes podem ser encontrados em forma de cookies, propagandas inocentes que acabam por encontrar potenciais clientes baseando-se naquilo que interessa ao usuário do computador. Porém também existem os spywares negativos que coletam dados pessoais e íntimos do usuário.

Os cavalos de Tróia são outro tipo de arquivos espiões, estes aparentam ter utilidade, mas trazem escondidos uma espécie de malware, que causa danos a quem o utiliza, permitindo a coleta e envio de dados privados.

Já os keyloggers são outra espécie de programa, onde os mesmos decoram as teclas digitadas pelo usuário, de forma a facilitar a obtenção de senhas de contas bancárias, cartões de crédito, etc.

Tal tipificação penal também já está em nosso ordenamento e é pertinente, visto que a conduta de obter e transferir dados são uma gravíssima violação à intimidade e privacidade do usuário, pois o mesmo contém informações pessoais e sigilosas, sendo assim amparado pelo artigo 5º da Constituição Federal, em seu inciso X.

c) Dano Informático

"Destruir, inutilizar ou deteriorar coisa alheia: Pena - detenção de 1 (um) a 6 (seis) meses, ou multa".

Este é o art. 163 do Código Penal, que trata sobre o crime de dano. Porém o mesmo não se aplica a dano informático, pois uma das características para que seja configurado o dano é que o mesmo seja causado sobre algum bem material. Portanto, no caso de bens imateriais como os arquivos digitais de um computador, a legislação penal ainda não aplica o art. 163 sobre os eles. Eles poderiam se enquadrar em uma forma de responsabilidade civil ao invés da penal.

d) Dos vírus e sua disseminação

Os vírus são outras espécies de programas que, ao infectar o computador, podem causar lentidão, dificuldades de acessar arquivos na máquina, e possibilitar a um terceiro,

que tenha acesso aos dados confidenciais de um usuário, abra arquivos, acesse contas, exclua programas e espione a intimidade do sujeito passivo.

Com isso observamos que os vírus são aptos a causar danos e desta forma podem ser instrumentos para o crime.

e) Divulgação ou utilização indevida de informações

O UCE (Unsolicited Commercial Email ou Mensagem Comercial Não Solicitada), mais popularmente conhecido como spam, é um dos problemas que mais incomodam o dia a dia dos internautas. Trata-se de uma correspondência virtual, a qual se caracteriza por não ser enviada em consenso com o usuário que a recebe e por ser sempre destinada em grande quantidade para um enorme número de usuários. O primeiro spam via email de que se tem notícia, foi enviado há 25 anos e desde então tem se tornado uma praga no meio virtual. Tornou-se muito mais fácil divulgar sua empresa através deste tipo de mensagem do que por panfletos e outras formas de divulgação. Não é o mais adequado, mas considerando a ausência de uma "educação digital", torna-se cada dia mais corriqueiro tal medida, a qual deve ser evitada.

Apesar disso, não há projetos de lei no Brasil, que procurem incriminar o spam, apenas aplicar multa. Porém há doutrinadores que consideram o spam uma espécie de dano, tipificado no art. 163 do Código Penal. Porém isso só seria admissível se fosse enviado uma quantidade de grandeza excepcional, como nos casos de email bombing, onde são enviadas muitas mensagens, a muitos usuários, dificultando a celeridade das comunicações.

f) Embaraço ao funcionamento de sistemas

Se dá geralmente pelos DoS - Denial of service - ou denegação de serviço, e se trata de uma interferência em sistemas, a qual vem se tornando uma prática bastante comum.

Nesta forma de ataque, computadores são utilizados para atingir o sistema operacional de outro computador conectado a internet, seja através da geração de uma grande sobrecarga no processamento de dados de um computador, fazendo com que o usuário não consiga utilizá-lo; ou causando a retirada de um servidor do ar, o que acaba por impedir ao usuário o acesso a caixas de email e servidor web, por exemplo.

g) Engenharia social e Phishing

A Engenharia social é o ato de persuadir terceiro a fornecer informações sigilosas, sejam elas pessoais ou de empresas, por exemplo. O sujeito ativo da ação delituosa age enganando o terceiro que imagina estar participando de um ato rotineiro, por ter tido sua confiança conquistada pelo delinquente. Seja através do preenchimento de formulários, ou através do cadastramento de determinada instituição, onde o mesmo expõe as informações que o criminoso almejava. Assim sendo, tal prática pode vir a ser a causadora desde crimes de dano, até a violação de direitos autorais.

Já o Phishing ocorre quando uma pessoa envia a outrem uma mensagem eletrônica, onde tenta induzi-lo a fornecer informações como senhas de conta bancária e números de cartões de crédito, ou ainda fazer com que o receptor da mensagem, clique em determinados links, os quais levam a paginas que executam automaticamente arquivos, os quais permitem no futuro que o criminoso acesse tais informações através do computador do usuário. Deve-se tomar muito cuidado, pois geralmente tais crimes, são simulados como se fosse um pedido de órgãos do governo, como a Receita Federal, com o intuito de atrair a atenção da vítima ao golpe.

O phishing é um exemplo claro de estelionato, onde a obtenções de tais informações leva a vantagem econômica por parte do agente ativo do crime, que objetiva induzir o usuário a erro através da engenharia social e das práticas tecnológicas que nos são inerentes hoje em dia. Contudo, o simples fato de enviar mensagens fraudulentas, caso não haja consequências derivadas disso, não representa um crime tipificado em nosso código.

h) Interceptação ilegal de dados

O item é sobre interceptação de dado e não telefônica. São conceitos distintos. A Lei n. 9.296/96 também autoriza a interceptação de dados de sistemas de informática e telemática. O que acaba por criar uma questão de cunho contraditório com a constituição, onde a mesma em seu Art. 5º, inciso XII, afirma que: "É inviolável o sigilo das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo no último caso, por ordem judicial (...)"

Com isso, nossa doutrina possui dois posicionamentos acerca da interceptação de dados de informática, um permitindo tal fato e outro o proibindo. Porém como a nossa

constituição é soberana, leva-se em conta o seu posicionamento contra a inviolabilidade de tais dados eletrônicos.

Esclarecida essa questão constitucional, a própria Lei n. 9.296/96 caracteriza como crime, em seu art. 10, o fato de alguém realizar tais tipos de interceptações e tal prática deve ser coibida, ao passo que cada vez mais dependemos do ciberespaço para nos comunicar e não podemos ficar à mercê deste tipo de atitudes ilícitas.

3.2 Crimes digitais impróprios

São aqueles crimes já tipificados em nosso ordenamento jurídico, porém praticados através de um novo meio. O sistema informático. Outra característica destes crimes é a possibilidades de pratica-los sem ter necessariamente um conhecimento avançado do funcionamento de um computador. Qualquer leigo que possua tal aparelho eletrônico e tenha acesso à internet, pode praticá-los. Vejamos os principais tipos:

a) Ameaça

A Lei Brasileira, no art. 147 do Código Penal, prevê o direito à proteção da liberdade dos cidadãos, ao sossego e à paz de espírito. Ações ameaçadoras, através de emails ou redes sociais com frases de mal prometido, os quais sejam injustos e graves, configuram crimes de ameaça.

b) Participação em suicídio

Cometer suicídio não é crime no Brasil, porém qualquer pessoa que instigue, induza ou auxilie outrem, a cometer suicídio, deverá responder por crime. Seja com palavras de incentivo ou fornecendo materiais para que seja cometido o ato. Deste modo aquele que cria sites ou fóruns com dicas para suicídio ou ainda praticam cyberbullying desejando a morte de outra pessoa, pratica participação em suicídio, pois de acordo com o art. 122 do Código Penal, pode induzir a vítima, à prática de tal atitude.

c) Incitação e apologia ao crime

É punível de acordo com os artigos 286 e 287 do Código Penal, aqueles que incitem outros a cometer crimes ou que pratiquem eles mesmos tais apologias a prática de infrações penais. Quem participa de comunidades, que geram preconceitos com outras pessoas e incitação ao uso de drogas, por exemplo, devem ser punidos de acordo com esta tipificação penal.

d) Falsa identidade e falsidade ideológica

Na internet, falsa identidade se dá quando uma pessoa se passa por outra, fazendo uso de sua imagem, perfil ou até mesmo senhas. São conhecidos como perfis "fakes" ou falsos e buscam com isso tirar proveito próprio ou alheio, ou ainda causar dano para a vítima. Já a falsidade ideológica, trata-se de alterar o conteúdo de um documento, ou mentir no mesmo, para retirar um direito de alguém. De acordo com o art. 307 do Código Penal, o crime de falsa identidade é subsidiário, ou seja, só será aplicado caso a falsa identidade não constitua um crime mais grave. Tais perfis devem ser retirados do ar e a vítima tem direito a indenização.

e) Violação de direitos autorais, uso indevido de marcas e pirataria de software

É onde está o verdadeiro uso da pirataria, a qual é a ação de copiar ou vender produtos, não autorizados pelo detentor de seus direitos. Violação de direitos autorais e uso indevido de marcas completam essa categoria de crimes. As pessoas não podem fazer uso de tudo que está na internet. Não é por que está lá, que necessariamente é de uso público e possa ser usado por qualquer um sem citar fonte ou autor. Tal crime vem sendo praticado de maneira desenfreada e às vezes o sujeito ativo nem se dá conta da prática ilegal que está cometendo. Segundo a Associação Antipirataria Cinema e Música (APCM), no ano de 2010, por exemplo, cerca de 38 milhões de CDs e DVDs piratas haviam sido apreendidos em todo o país, e um aumento equivalente a 110,2% no número de condenações, comparado a anos anteriores.

f) Pornografia Infantil

É proibido compartilhar, divulgar, transmitir, adquirir, possuir, imagens ou vídeos de crianças ou adolescentes praticando sexo explícito ou mesmo imagens de nudez desses

jovens. Sentir atração por crianças e adolescente, é conhecido como pedofilia e não se trata de um crime, mas de uma forma de desvio sexual, onde a pessoa poderá ser enquadrada na tipificação penal, no caso de promover de algum modo os verbos mencionados acima. Os principais crimes que envolvem a pornografia infantil estão tipificados no art. 240 e seguintes do Estatuto da Criança e do adolescente.

g) Crimes contra a honra

Estão previstos nos arts. 138, 139 e 140 do Código Penal e estão muito presentes na internet.

Honra de acordo com Crespo: "São as qualidades físicas, morais e intelectuais de uma pessoa, fazendo-a respeitada no meio social e que diz respeito, ainda, à sua autoestima".

Todos possuem direito à proteção de sua honra, pois a mesma revela o seu valor social e suas características mais íntimas, sendo responsáveis por sua aceitação ou rejeição social.

No ciberespaço há muitos exemplos de crimes contra a honra. Todos os dias são visto inúmeros casos de injúria, calúnia e difamação pela internet, além de casos de racismo e preconceito. Pratica calúnia, aquele que atribui um fato criminoso a outro, sabendo ser falsa tal acusação. Já a difamação, trata-se de fato ofensivo à reputação de alguém, desacreditando-a publicamente. Enquanto à injúria não se atribui fato a ninguém, e sim a propagação de ofensas e insultos sem necessidade à vítima. São fatos comuns na rede, pelo conforto e segurança no anonimato e possibilidade de expressar insatisfação e revolta contra outra pessoa, sem precisar se expor e mostrar seu rosto. Pessoas covardes utilizam-se deste crime de forma banal, sem perceberem a gravidade dos atos que praticam e das consequências sentidas por aqueles que enfrentam tais problemas.

O crime de racismo é previsto na lei n. 7.716/89 e refere-se à prática, indução ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. Aqueles que proíbem acessos a lugares públicos, que negam vagas de emprego, por alguma das características descritas acima, pratica crime de racismo, o qual é inafiançável, imprescritível e sujeito a reclusão, de acordo com o art. 50, inciso XLII da Constituição Federal.

4. DIFICULDADES DE PUNIÇÃO DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos são mais complexos de serem desvendados, vistos que os criminosos podem com uma imensa facilidade, se desfazer das provas do crime. Com apenas um "click" é possível excluir informações fundamentais para a punição dos infratores digitais.

Ao passo que a sociedade avança e a internet e todo o meio digital se desenvolve, novos mecanismos para cometer cibercrimes também vão sendo aperfeiçoados. São pessoas que dedicam todo o seu tempo e seu vasto conhecimento de informática para criar novas formas de garantir acesso à intimidade alheia, no que tange ao campo virtual, e com isso aproveitar as brechas e a insegurança a que estamos diariamente submetidos pela internet, para se infiltrar nos nossos dados eletrônicos e obter informações de nossa vida virtual e também dados da mesma, fora dela.

A investigação de tais crimes divide-se em duas fases: A fase técnica e a fase sequencial. A primeira é a fase inicial onde é localizado o computador do criminoso e qual o meio pelo qual o mesmo fez uso para cometer o crime, como emails, websites, etc.

A segunda fase corresponde à fase de campo, da investigação policial propriamente dita, onde são realizadas diligências ao local onde se encontra o "hacker" para então efetuar sua prisão.

Uma das principais formas de identificar um criminoso virtual se dá através do endereço de IP que cada computador possui. Uma espécie de Registro Geral que torna cada máquina diferente da outra, podendo ter sua localização rastreada e descobertas todas as suas atividades.

Um problema neste caso é que o computador não é uma pessoa, com isso não se pode precisar se quem cometeu tal crime foi o verdadeiro dono do endereço do IP, portanto, a identificação de um IP, como ofensor, não é prova de autoria do crime.

Outro fato muito importante que acaba por prejudicar na investigação e punição dos crimes cibernéticos é o fato da ausência de profissionais capacitados para exercerem tais ações de segurança e punição. Nosso país ainda sofre com a falta de legislação específica para punir tais crimes e precisa que os peritos criminais estejam sempre atualizados para

suprir da melhor forma possível a ausência de um apoio mais específico do nosso Código Penal.

Os operadores do Direito, também precisam estar atualizados e as faculdades precisam implantar eventos relacionados ao tema para buscar desenvolver nos estudantes a consciência da necessidade que a sociedade tem hoje em dia de profissionais capacitados que possam combater com eficácia estes delitos. Os meios acadêmicos, o próprio Poder Judiciário, e também as entidades de classe devem ser alvo dessa capacitação técnica.

E ainda que estejam tecnologicamente atualizados, segundo Gustavo Testa Corrêa, os operadores devem sempre se lembrar de que:

"Os operadores jurídicos deverão utilizar o bom senso para dirimir questões jurídicas relacionadas à Internet, procurando sempre relacionar a parte técnica com o ordenamento jurídico em exercício. São as análises simples e lógicas que possibilitarão um eficaz entendimento das questões cotidianas de nossos tribunais, sendo, principalmente, os bancos acadêmicos os futuros responsáveis pela construção deste, já que é neles que existe uma verdadeira interdisciplinaridade, essencial para a resolução dessas novas questões." (CORRÊA, 2000, p. 107).

São poucas as delegacias especializadas em crimes digitais no nosso país, enquanto a demanda de usuários só se multiplica, atualmente apenas 16 estados da nossa federação possuem uma DRCI (Delegacia de Repressão aos Crimes Informáticos) que se dedica exclusivamente a solucionar crimes dessa espécie. São muitas pessoas praticando crimes na internet e ainda mais pessoas sendo vítimas desses crimes. Falta além de delegacias especializadas, compartilhamento de informações e recursos humanos e financeiros. Falta interação entre organismos públicos e empresas de antivírus, as quais poderiam fornecer mais relatórios sobre as novas atividades dos cibercriminosos. Assim, elas poderiam contribuir para uma maior compreensão sobre o modo de agir dessas quadrilhas especializadas em crimes na Internet.

Resumindo, carece estrutura para o combate ao cibercrime no Brasil. E esta é uma realidade que precisa ser mudada. Não pode ser permitido que estes piratas da internet continuem levando o ciberespaço como uma terra sem lei, onde confiam no fato de que sairão impunes dos graves delitos que cometem pela fragilidade na assistência a esses casos específicos.

5. LEGISLAÇÃO PUNITIVA NO BRASIL

Como observado, o número de casos de crimes virtuais cresce a cada dia, e pouco tem sido feito em nosso país para frear o avanço desta criminalidade no ambiente virtual. Não existe uma legislação específica em nosso ordenamento jurídico para punir tais crimes, porém existem algumas normas que regulam o tema e desta forma regem a forma de proceder perante tais crimes.

Boa parte do que é praticado criminalmente na internet, acaba sendo julgado e enquadrados em crimes que já estão tipificados em nosso ordenamento, variando apenas o meio em que o mesmo se deu, no caso, a rede mundial de computadores. Deste modo, apesar de ser uma legislação específica de crimes virtuais, a grande maioria dele, acaba se encaixando nessa leva de crimes comuns, o que termina por generalizar a ocorrência e em determinados casos, gerar uma punição inadequada, seja por torná-la mais branda ou mais pesada que o necessário.

A seguir, uma explanação da legislação vigente em nosso país com relação aos crimes cibernéticos, demonstrando as áreas em que são aplicadas e onde a legislação brasileira carece de desenvolvimento adequado para lidar com todos os casos de crimes virtuais.

5.1 Estatuto da Criança e do Adolescente

Um dos avanços de nossa legislação contra os crimes cibernéticos se deu com a edição da Lei 11.829/2008 que alterou os artigos 240 e 241 da Lei 8.069/90, mais conhecida como ECA. Antes disto, não havia uma especificação quando aos crimes de pedofilia praticados na internet. A referida edição trouxe grandes benefícios para a proteção contra o crime da pedofilia, aumentando a pena que antes era de dois a seis anos para quatro a oito anos, para quem produzisse, reproduzisse, possuísse ou compartilhasse qualquer conteúdo erótico de crianças e adolescentes.

Além disso, houve mudança dos seguintes artigos:

241-A, que prevê punição para quem divulgar imagens que contenham sexo explícito ou pornografia infantil por meio de sistema de informática ou telemático;

241-B, que prevê punição para quem armazenar imagens que contenham sexo explícito ou pornografia infantil;

241-C, que prevê punição para quem realiza montagens ou modificações, simulando a participação de crianças e adolescentes em cenas que contenham sexo explícito ou pornografia; e, finalmente, o art.

241-D, que prevê a punição para quem alicia, assedia ou constrange criança ou adolescente para a prática de ato libidinoso.

5.2 Lei Carolina Dieckmann

Outra Lei sancionada no Brasil é a Lei 12.737/2012, também conhecida como a lei Carolina Dieckmann. Esta pode ser considerada um dos maiores avanços da nossa legislação contra os crimes digitais. Tem esse nome, devido a toda a repercussão do vazamento de fotos íntimas que estavam no computador da atriz e teve sua vida pessoal invadida pela ação dos criminosos, ao tempo que tramitava este projeto de lei na Câmara dos Deputados.

Com ela, invadir dispositivo alheio, conectado ou não a rede de computadores, mediante violação de segurança com o fim de obter informações sem autorização passou a ser crime, com pena de detenção de três meses a um ano e multa.

Obter de forma ilícita informações em que causem prejuízos econômicos passou também a ser crime, com aumento da pena de detenção de três meses a um ano e quatro meses.

Obter conteúdo de comunicações privadas de forma não autorizada aumenta a pena de detenção de seis meses a dois anos e multa.

A divulgação e comercialização de conteúdo roubado de dispositivo informático também passam a ser crime, com pena de reclusão de oito meses a três anos e quatro meses.

Quando o usuário não autoriza o acesso ao aparelho ou quando o criminoso “instala vulnerabilidades para obter vantagem ilícita”, com pena de detenção de três meses a um ano e multa.

Também há a previsão da pena de reclusão de seis meses a dois anos e multa para quem obtiver dados “de comunicações eletrônicas privadas, segredos comerciais ou

industriais, informações sigilosas assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido”. A pena será majorada de um a dois terços se o crime for cometido contra autoridades do Executivo, Legislativo ou Judiciário. E também se houver divulgação, comercialização ou transmissão a terceiros dos dados obtidos.

5.3 Marco civil da Internet

Aprovado em abril de 2014, a Lei 12.965/14, mais conhecida como o Marco Civil da Internet, pode ser considerado a Constituição para a internet no Brasil, servindo de bases para a tipificação de todos os crimes virtuais. As principais características dele são a Neutralidade da rede, a privacidade online e a responsabilidade civil aos usuários e provedores por conteúdo veiculado. Este foi um recente grande avanço para a tipificação dos cibercrimes. O Marco Civil começou a ser elaborado em 2009, pelo ministério da justiça, em colaboração com o Centro de Tecnologia e Sociedade, da Fundação Getúlio Vargas, bem como com a participação direta da sociedade civil, comunidade empresarial e representantes das áreas técnicas e acadêmicas, por meio de colaboração online direta e aberta.

Após extenso debate público, o projeto foi encaminhado ao Congresso Nacional em 2011, como o PL 2126/2011, tendo o deputado Alessandro Molon como seu relator no ano seguinte. Durante o período da relatoria, foram realizadas sete audiências públicas, que contaram com a participação de representantes de 60 instituições dos mais diversos setores, como empreendedores, acadêmicos, operadoras telefônicas, ativistas, órgãos do governo, artistas e empresas de tecnologia, entre outros.

O Marco Civil ainda foi colocado em debate no portal e-Democracia da Câmara dos Deputados, onde o texto teve 45 mil visitas, 2.215 comentários e 374 propostas. Foi a primeira vez na Câmara dos Deputados que um relatório utilizou sugestões utilizadas pela internet, até mesmo via Twitter.

Por tudo isso, a lei não é apenas um marco da internet, mas também do processo legislativo brasileiro, por todo o debate realizado antes e durante a tramitação no Congresso Nacional. Apesar disso, o Marco Civil tem a desvantagem de não prever punição para crimes cometidos através da internet, tornando-se insuficiente nesse sentido. Além de não

poder acionar provedores internacionais, já que esta lei só vale no território nacional. Portanto se alguém adicionar uma foto de outro sem autorização em uma rede social de provedor internacional e esta pessoa solicitar a retirada da foto, a justiça brasileira através do Marco Civil não pode punir empresas internacionais.

5.4 Mais exemplos de leis específicas para cibercrimes

Apesar do destaque dado às referidas leis acima, elas não são as únicas que compõem nosso Código Penal. Temos também em nosso ordenamento jurídicos outras legislações específicas:

A Lei 9.609/1998, a qual garante a proteção da propriedade intelectual do programa de computador.

A Lei 9.983/2000, o qual tipifica os crimes relativos a acessos indevidos aos sistemas operacionais informáticos da Administração Pública.

A Lei 9.296/1996, que se refere a interceptação ilegal de comunicações.

A Lei 12.034/2009, que traça uma linha de direitos e deveres dentro da rede mundial de computadores, durante o período das campanhas eleitorais.

Cumprir destacar também o papel que o Código Penal possui frente aos crimes cibernéticos, já que alguns de seus dispositivos tutelam tais condutas, como:

O art. 153, que trata da divulgação, sem justa causa, de informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou bancos de dados da Administração Pública;

O art. 313-A, que trata da inserção de dados falsos em sistemas de informações, alteração ou exclusão indevida de dados corretos nos sistemas informatizados da Administração Pública;

O art. 313-B, que trata da modificação ou alteração não autorizada de sistema de informações ou programas de informática;

O art. 325, que trata da violação do sigilo funcional;

O art. 184, que trata da violação dos direitos autorais; entres outros.

Considerações finais

Do exposto, observa-se que crimes cibernéticos são aqueles que necessitam especificamente do ambiente virtual para serem configurados ou aqueles que apenas utilizaram o meio para cometer crimes, os quais eram possíveis também através de outros meios.

A busca de provas torna-se mais importante do que a própria tipificação de temas como a pedofilia e pornografia, pois de nada adianta verificar a ocorrência de tais delitos, se não formos capazes de identificar de que computador partiu tal ação delituosa e como o agente delituoso executou os atos típicos.

Deve-se propagar a ideia de que os crimes virtuais serão punidos, haja vista que o que motiva o sujeito ativo do crime é a possibilidade de seu anonimato, desta forma intimidando-o e incentivando a polícia a localizá-los. Porém a ausência de profissionais capacitados para estar à frente das investigações destes crimes e a falta de uma legislação específica mais completa, são fatores que preocupam, pois é notável o crescimento do número de criminosos virtuais e as suas habilidades e capacidades de produzir mecanismos cada vez mais inteligentes e invasivos para se infiltrar nos computadores dos cidadãos, através de quaisquer brechas que este dê.

É necessária uma política de prevenção contra os crimes cibernéticos e exigir do Estado uma proteção mais segura contra esses tipos de ataques. Devem ser criados métodos de evitar que estes maus usuários, não consigam acessar dados sigilosos de outros, assim como incentivar a formação e capacitação de novos profissionais, preparados para atuar nessa área.

Também deve ser cobrada uma legislação específica que possa de fato punir de forma mais eficaz, quem pratica tais delitos. Sendo assim, além de uma forma segura de capturar tais criminosos, sirva ainda para coibir novas ações dos mesmos ou de outras pessoas que pensem em praticar estes crimes.

Não é possível que em pleno século XXI, sejamos reféns de uma ferramenta tão útil, que tanto crescimento nos proporciona, mas ao mesmo tempo provoca insegurança e receio de acabar sendo vítimas de crimes tão graves como tantos desses mencionados neste trabalho. Porém em um esforço conjunto de usuários e Estado, podemos minimizar a ação

desses criminosos e assegurar que a internet possa voltar a ser apenas uma fonte de incessável saber e divertimento, como já foi em seus primórdios.

REFERÊNCIAS

A EPIDEMIA via internet. PCWORLD. Disponível em: <<http://www.cin.ufpe.br/~rdma/documentos/revistaPCWORLDseguranca.pdf>>. Acesso em: 18 fev. 2014.

BRASIL. Código Civil (2002). Código Civil Brasileiro. Brasília, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 18 fev. 2014.

BRASIL. Código Penal (1940). Código Penal Brasileiro. Brasília, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 18 fev. 2014.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 24 abr. 2014.

BRASIL. Lei n.º 11.829, de 25 de novembro de 2008. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acesso em: 20 abr. 2014.

BRASIL. Lei n.º 12.034, de 29 setembro de 2009. Altera as Leis nos 9.096, de 19 de setembro de 1995 - Lei dos Partidos Políticos, 9.504, de 30 de setembro de 1997, que estabelece normas para as eleições, e 4.737, de 15 de julho de 1965 - Código Eleitoral. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2007-2010/2009/lei/l12034.htm>. Acesso em: 19 abr. 2014.

BRASIL. Lei n.º 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2011-2014/2012/lei/l12737.htm>. Acesso em: 15 mar. 2014.

BRASIL. Lei n.º 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 19 abr. 2014.

BRASIL. Lei n.º 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 20 abr. 2014.

BRASIL. Lei n.º 9.459, de 13 de maio de 1997. Altera os arts. 1º e 20 da Lei nº 7.716, de 5 de janeiro de 1989, que define os crimes resultantes de preconceito de raça ou de cor, e acrescenta parágrafo ao art. 140 do Decreto-lei nº 2.848, de 7 de dezembro de 1940. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9459.htm>. Acesso em: 17 mar. 2014.

CORRÊA, Gustavo Testa. Aspectos jurídicos da Internet. São Paulo: Saraiva, 2000.

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

FOLHA DE SÃO PAULO. Estudante é responsabilizado por racismo na internet. Disponível em: <<http://www1.folha.uol.com.br/fol/tec/tx033414.htm>>. Acesso em: 21 abr. 2014.

FONTES, Edilson. Segurança da informação: O usuário faz a diferença. São Paulo: Saraiva, 2006.

LUCCA, Newton; SIMÃO FILHO, Adalberto. Direito & Internet: Aspectos Jurídicos Relevantes.v.2. São Paulo: Quartier Latin, 2008.

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

SANTOS, Moisés J. Fraude Eletrônica. 2008. Disponível em: <<http://www.febraban.org.br/Arquivo/Servicos/Eventoscursos/Palestras/CLAIN2008/PalestraSrMoisesJSantos.pdf>>. Acesso em: 21 abr. 2014.

TECMUNDO. 20 Anos de Internet no Brasil: aonde chegamos?. Disponível em: <<http://www.tecmundo.com.br/internet/8949-20-anos-de-internet-no-brasil-aonde-chegamos-.htm>> Acesso em 12 abr. 2014.

WIKIPÉDIA. História da Internet no Brasil. Disponível em: <http://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_Internet_no_Brasil> Acesso 12 abr. 2014.