Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

RAFAEL KISUKURI HERNANDES

CRIMES VIRTUAIS

Assis/SP

2014

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

RAFAEL KISUKURI HERNANDES

CRIMES VIRTUAIS

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação.

Orientador: Fábio Alonso Pinha

Área de Concentração: Direito Penal

Assis/SP

2014

FICHA CATALOGRÁFICA

HERNANDES, Rafael Kisukuri.

CRIMES VIRTUAIS/Rafael Kisukuri Hernandes. Fundação Educacional do Município de Assis – FEMA – Assis, 2014.

34 p.

Orientador: Fábio Alonso Pinha

Trabalho de Conclusão de Curso – Instituto Municipal de Ensino Superior de Assis – IMESA.

1. Crimes Virtuais. 2.Internet. 3. Justiça.

CDD: 340

Biblioteca da FEMA.

RAFAEL KISUKURI HERNANDES

CRIMES VIRTUAIS

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação analisado pela seguinte comissão examinadora:

Orientador: Fábio Alonso Pinha

Analisador (a): _____

Assis/SP

2014

RESUMO

Objetiva-se neste trabalho fazer uma avaliação das motivações e receios de pessoas vítimas de práticas criminais. Sabe-se que, principalmente nas redes sociais, há muito abuso, por meio de ofensas, a membros de determinado grupo. Por outro lado tem se observado que poucos encontram disposição à demanda judicial. Preferem amargar-se a entrar na justiça. Isto é em si um problema sério, pois acaba reforçando sentimento de impunidade. Assim pretendemos saber quais são as razões alegadas pelas vítimas que evitam entrar na justiça. Quando entra na justiça geralmente é em decorrência de situações graves, de profunda ofensa pessoal.

Palavras-chave:

Crimes virtuais; Internet; Justiça

ABSTRACT

The objective of this work is to make an evaluation of the motivations and fears of victims of criminal practices. It is known that, especially in social networks, there is much abuse through injuries of members of particular group. On the other hand it has been observed that few are available to the lawsuit. Prefer to embitter than get in the justice. This in itself is a serious problem, because it ends up reinforcing sense of impunity. So we want to know what are the reasons alleged by the victims who avoid entering the justice. When you enter the justice is usually a result of serious, deep personal offense.

Keywords:

Cybercrime; Internet; Justice

SUMÁRIO

Introdução

Com a grande frequência do uso da internet pela população brasileira e mundial, possibilitou a prática de vários crimes tendo a necessidade da ciência jurídica nacional e internacional se evoluir para o mundo virtual. Com o surgimento de crimes na internet surgiu uma nova modalidade de crimes chamada de Crimes Virtuais.

1-História

Pela evolução histórica do computador e da internet, vemos como foi lenta a criação da primeira maquina que pode ser chamado de computador e da primeira rede de internet, que foi usado com o intuito de comunicação entre as pessoas e para guerras. Nesse capítulo pretendo contar como foi a evolução do computador e da internet com o passar do tempo, até o que conhecemos atualmente e também sobre os primeiros crimes virtuais no universo do computador e da internet.

1.1-História do computador

O computador surgiu em meados entre 1937 e 1940 com ideias sobre algoritmos, sendo idealizados por Alan Turing e John Von Neumann, sendo criado uma máquina para calcular, além de cálculos matemáticos, o processamento lógico de informações.

De 1945 a 1950 foram fabricados os primeiros computadores, enquanto que eram construídas as últimas máquinas que são conhecidas como grandes calculadoras, outras máquinas construídas neste período podem ser consideradas os primeiros computadores.

De 1951 a 1958, o computador passa a ser comercializado em maior quantidade. Esta época é marcada pelo surgimento dos primeiros computadores para uso civil e pelo uso de grandes computadores militares.

De 1959 a 1962, é caracterizada pelo aparecimento dos computadores baseados nos transistores inventado no “Bell Laboratories”.

A partir da década de setenta, a indústria da informática começa a não mais depender das verbas militares para seu desenvolvimento.

Com inovações como o "time-sharing" e a tecnologia de redes que tornavam o computador disponível para uso de todos, surgiu à ideia de construção de mini computadores. Os primeiros micro computadores foram comercializados e vendidos sob forma de "kit", construído a partir do circuito integrado. Finalmente, com a criação da linguagem Basic e o aparecimento dos microcomputadores Apple 1 e 2, estava se iniciando a revolução da microinformática, hoje representada por empresas poderosas como a Apple e a Microsoft.

1.2-História da Internet

A internet surgiu a partir da conhecida "Guerra Fria", que foi uma briga intelectual entre os Estados Unidos e União Soviética.

Em 1957, a Rússia lançou para o espaço exterior à Terra o primeiro satélite artificial, que ficava em volta da Terra e em cada 90 minutos e emitia sinais rádio.

Como a criação do satélite o Presidente dos USA criou em 1957, a ARPA (Advanced Reasearch Project Agency) com o objetivo principal da ARPA era o desenvolvimento de programas respeitantes aos satélites e ao espaço, mas com a criação da NASA (National Aeronautics & Space Administration) em 1958, perdeu sua finalidade.

Em 1961 a Universidade da Califórnia (UCLA) em Santa Bárbara, herdou da Força Aérea um super computador que permitir à ARPA orientar a sua investigação para a área da Informática.

Com isso a ARPA foi orientada, a construir redes de comunicação de dados para a comunicação rápida entre as equipes de investigadores, sendo necessária a construção de uma rede (NET).

Em 1965 Licklider se desligou da ARPA, mas a sua orientação foi continuada pelo seu sucessor Robert Taylor. Dispondo de um orçamento de 19 milhões de dólares, Taylor iniciou o financiamento da primeira rede de computadores.

A primeira rede de computadores foi construída entre a Universidade da Califórnia em Los Angeles, o Stanford Research Institute (SRI), a Universidade de Utah e a Universidade da Califórnia em Santa Bárbara. Em 1969 “nascia” a ARPANET, que utilizava a rede telefônica normal através do sistema de aluguel de circuitos.

Em Julho de 1977, Vinton Cerf e Robert Kahn realizaram uma demonstração do protocolo TCP/IP utilizando três redes: a ARPANET, a RPNET e a STATNET, considerando com isso uma demonstração que nasceu a Internet.

Em 1990, o Departamento de Defesa dos Estados Unidos da América desmembrou a ARPANET que foi substituída pela rede da NSF, rebatizada NSFNET que se popularizou, em todo o mundo, com a denominação Internet. Para expansão da utilização da Internet foi decisiva a criação WWW (World Wide Web) criada por dois engenheiros do CERN (Centre Européen por la Recherche Nucléaire).

1.3-Primeiros Crimes Virtuais

O aparecimento dos primeiros casos de crimes virtuais ocorreu na década de 1960, que nada mais eram que delitos onde o infrator manipulava, sabotava, espionava ou exercia uso abusivo de computadores e sistemas. A partir de 1980, houve um aumento das ações criminosas, que passaram a refletir em, por exemplo, manipulações de caixas bancários, abusos de telecomunicação, pirataria de programa e pornografia infantil.

2-Conceitos e Definições

Nesse capitulo, devemos antes de falar dos crimes praticados com o uso do computador e da internet, fazermos conceitos e definições do tema que vamos tratar em todo o trabalho. Tais doutrinadores usam tais palavras e sentidos para uma mesma definição ou conceito, sendo o mais importante o significado e compreensão.

2.1-Crimes na Informática

Crime informático ou crime digital são termos utilizados para se referir a tudo que envolve um computador ou uma rede de computadores, sendo utilizada como uma ferramenta, uma base de ataque ou como meio para que ocorra um crime.

Embora os termos crimes na informática ou crimes eletrônicos seja mais apropriadamente utilizados para descrever condutas criminais que façam o uso de computadores ou de uma rede de computadores, esses termos também são utilizados para descrever crimes comuns, tais como fraudes, roubo, chantagem, falsificação e apropriação indébita, na qual computadores ou rede de computadores são usados para facilitar as atividades ilícitas.

Segundo Guimarães e Furlan Neto, Crime Informático significa: "qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados". Essa categoria de crime apresenta algumas características, dentre elas: transnacionalidade – pois não está restrita apenas a uma região do globo - universalidade – trata-se de um fenômeno de massa e não de elite - e ubiquidade – ou seja, está presente nos setores privados e públicos.

2.2-Crimes na Internet

Os crimes que ocorrem no mundo virtual são resultado de um processo evolutivo e despreparado da internet, pois, à medida que avançava os métodos de propagação e transferência de dados pela rede, esquecia-se de atribuir um método protetivo voltado à segurança dos usuários.

A cada dia devido o processo de globalização a internet além dos conhecimentos, notícias e culturas que nos é fornecido, propiciou o surgimento de crimes que atualmente vem ocasionando prejuízos a diversos usuários de todo o mundo.

Portanto crimes na internet são atividades, ou seja, condutas praticadas com o uso da internet para cometer algo que seja proibido, afetando de forma patrimonial ou moral alguém ou uma instituição.

2.3-Definição dos Crimes Virtuais

Crime virtual é qualquer ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão em que um computador conectado à rede mundial de computadores, com a internet, sendo usado como instrumento ou objeto para um delito.

Podemos categorizar tais crimes em dois tipos básicos: crimes cometidos utilizando o computador como ferramenta para cometer a infração e aqueles que o crime é cometido contra o computador em si, o objeto é danificado ou prejudicado de alguma forma.

Portanto crimes virtuais podem ser definidos como toda atividade ilegal que envolva o uso da infra-estrutura tecnológica da informática, incluindo acesso ilegal (acesso não autorizado), interceptação ilegal (por meio de uso de técnicas de transmissão não públicas de dados de computador, para, de ou fora do sistema de computadores), obstrução de dados (danos a dados de computador, deteriorização dos dados, alteração ou supressão da dados de computador), interferência nos sistemas (interferência nos sistemas de computadores quanto a entrada de dados, transmissão, apagamentos, deteriorização, alteração ou supressão de dados de computador), uso indevido de equipamentos, falsificação de IPs e fraude eletrônica.

3-Classificação dos Crimes Virtuais

Os crimes virtuais podem ser classificados de várias formas e modos, mas basicamente podemos distinguir os crimes virtuais em Crimes Próprios e Crimes Impróprios. Portanto nesse capítulo pretendo destacar sobre as classificações existentes em se tratando de crimes cometidos no mundo virtual.

3.1-Crimes Próprios

Os crimes virtuais próprios são aqueles em que o sujeito se utiliza do computador o sistema informático da vítima, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime nessa categoria de crimes está não só a invasão de dados não autorizados mais toda a interferência em dados informatizados, ou seja, que atinjam

diretamente o software ou hardware do computador e só podem ser concretizados pelo comutador ou contra ele e seus periféricos.

Para Damásio de Jesus:

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

Portanto, os crimes próprios são aqueles cometidos por meio do computador e da internet, onde o crime se consome no próprio meio virtual, como por exemplo, os crimes contra a honra como difamação, calúnia e injúria.

3.2-Crimes Impróprios

Os crimes virtuais impróprios são aqueles feitos com a utilização do computador, ou seja, por meio dele que é utilizada como instrumento para realização de condutas ilícitas que atinge todo o bem jurídico já tutelado. Com isso Damásio de Jesus descreve

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

Portanto os crimes impróprios são aqueles cometidos por meio do computador e da internet, onde o crime se consome no meio virtual, mas que produz um resultado que afeta o mundo físico, como por exemplo, os crimes que atingem o patrimônio da vítima, como o clone de cartões de crédito, invasão e furtos em contas bancárias etc.

4-Jurisdição, Competência e Territorialidade

Sempre existe a dúvida tanto do estudante de direito, bem como das pessoas, de onde será julgado tal crime virtual ou de onde será considerado o lugar do resultado do crime. Para que podemos explicar essas dúvidas, existem as teorias que o Brasil adotou e as competências em relação à Justiça federal e estadual. Nesse capítulo, portanto, pretendo explicar como será a jurisdição, a competência e da territorialidade dos crimes virtuais.

4.1-Teorias que o Brasil adotou

O local do crime é onde ocorreu a ação ou omissão ou quando se deveria produzir o resultado, sendo o Brasil adotado a teoria da ubiquidade. O Brasil adotou também a teoria do resultado (competência onde se consumou a infração penal), que descreve, quando o fato criminoso começou no Brasil e terminou em outro país a competência será do lugar onde tiver sido praticado o ultimo ato de execução no Brasil.

4.2-Competência da Justiça Federal

Para que o delito cometido por meio da internet seja julgado pela Justiça Federal é necessário que se amolde em umas das hipóteses descritas no art. 109, IV e V, da CF/88:

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

É de competência da Justiça Federal julgar os crimes eletrônicos quando forem praticados contra entes da Administração Federal. Quando os crimes cometidos através da internet e ultrapassam as fronteiras nacionais, a competência para julgar pertence à justiça Federal.

Delitos como racismo e pedofilia cometidos na internet possuem previsão em convenções internacionais de direitos humanos, sendo de competência da justiça federal.

O artigo 7º, II, do Código Penal, serve como parâmetro no caso do autor de crimes virtuais contra a honra, como por exemplo, no caso de publicações em redes sociais de mensagens ou fotos publicadas no exterior:

> Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:
>
> II - os crimes:
>
> a) que, por tratado ou convenção, o Brasil se obrigou a reprimir;

Nesse caso, a aplicação da lei brasileira depende do concurso das seguintes condições:

> a) entrar o agente no território nacional;
>
> b) ser o fato punível também no país em que foi praticado;
>
> c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição;
>
> d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena;
>
> e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.

Em sendo preenchidos esses requisitos, o delito seria julgado no Brasil pela Justiça Federal, sendo competente a Seção Judiciária da capital do Estado onde o acusado por último morou ou, se nunca residiu aqui, será competente a Seção Judiciária do Distrito Federal. Essa regra encontra-se prevista no art. 88 do CPP:

> Art. 88. No processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República.

4.3- Competência da Justiça Estadual

Já os crimes contra particulares praticados na internet, deverão ser investigados nas Justiças Estaduais. É de competência estadual, julgar os crimes contra a honra (calúnia, difamação, injúria) praticados por meio da internet, em páginas eletrônicas internacionais.

5-Crimes Virtuais nos Ramos do Direito

Os crimes virtuais que antes eram encontrados só no mundo do direito penal, hoje se arrasta e cresce no mundo tributário, civil e empresarial, envolvendo com isso todo universo jurídico, sendo doutrinário e jurisprudencial para discutir o assunto. Com isso, nesse capítulo pretendo expor sobre os diversos crimes virtuais que podem ser cometidos no direito tributário, direito civil, direito empresarial e no direito penal.

5.1-Crimes Virtuais no Direito Tributário

Condutas previstas no art. 1º da Lei n.º 8.137/90, podem ser adaptadas no mundo virtual, sendo com isso, ocorridas por meio do computador ou internet, causando um crime virtual também. É o que se passa a demonstrar, senão vejamos:

> Art. 1º. Constitui crime contra a ordem tributária suprimir ou reduzir tributo, ou contribuição social e qualquer acessório, mediante as seguintes condutas:
>
> I - omitir informação, ou prestar declaração falsa às autoridades fazendárias;
>
> II - fraudar a fiscalização tributária, inserindo elementos inexatos, ou omitindo operação de qualquer natureza, em documento ou livro exigido pela lei fiscal;
>
> III - falsificar ou alterar nota fiscal, fatura, duplicata, nota de venda, ou qualquer outro documento relativo à operação tributável;
>
> IV - elaborar, distribuir, fornecer, emitir ou utilizar documento que saiba ou deva saber falso ou inexato;
>
> V - negar ou deixar de fornecer, quando obrigatório, nota fiscal ou documento equivalente, relativa a venda de mercadoria ou prestação de serviço, efetivamente realizada, ou fornecê-la em desacordo com a legislação;
>
> Pena - reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
>
> Parágrafo único. A falta de atendimento da exigência da autoridade, no prazo de 10 (dez) dias, que poderá ser convertido em horas em razão da maior ou menor complexidade da matéria ou da dificuldade quanto ao atendimento da exigência, caracteriza a infração prevista no inciso V.

Portanto se ocorrer umas dessas hipóteses de crime contra a ordem tributária, provocadas por computadores ou internet, está claramente demonstrado um crime virtual no direito tributário.

5.2-Crimes Virtuais no Direito Civil

Desde de janeiro de 2003, o novo Código Civil vem sendo aplicado na resolução de conflitos decorrentes de relações virtuais.

Quando o tema é a invasão da privacidade, o art. 187 do Código Civil é absoluto ao estabelecer que "comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos maus costumes". Em outro momento, o Código Civil enquadra a pessoa ou empresa que envia os conhecidos *spam*, sujeitando-se o agente a processo por danos morais ou financeiros. Com isso, decisão proferida pelo Tribunal de Justiça de Santa Catarina nos autos da Apelação Cível nº 2004.012152-0, DJSC de 19.08.04, pp. 34-35, descreve o seguinte:

> APELAÇÃO CÍVEL – INDENIZAÇÃO POR DANOS MORAIS – PUBLICAÇÃO DE ANÚNCIO EM PÁGINA DE CLASSIFICADOS EM *SITE* DA INTERNET – MENSAGEM OFENSIVA À HONRA, IMAGEM E NOME DO AUTOR DA DEMANDA – NECESSIDADE DE CONTROLE E FISCALIZAÇÃO POR PARTE DO PROVEDOR – DEVER DE INDENIZAR – *QUANTUM* CAPAZ DE COMPENSAR O LESADO E REPRIMIR ATOS SEMELHANTES PELO LESANTE – MAJORAÇÃO – RECURSO DO AUTOR PROVIDO E DA RÉ DESPROVIDO.

Cabe, portanto, no direito civil, buscar uma reparação no dano decorrente dos crimes, praticados no universo virtual (por meio de computadores, tablets, celulares). A finalidade da indenização é amenizar e punir a infração causada pelo autor à vítima.

5.3-Crimes Virtuais no Direito Empresarial

Com o passar do tempo os crimes que aconteciam nas grandes empresas como furtos, roubos de matérias ou de documentos, passaram do mundo físico para o mundo virtual, sendo tão perigoso e danoso quanto o físico. Cada ano que passa as empresas aumentam os investimentos em treinamento e conscientização na área de segurança da informação.

Entre os principais impulsos para este crescimento estão recentes exemplos de ataques sofridos por grandes companhias e empresas, que mostram a vulnerabilidade do sistema virtual.

Atualmente no Brasil e no mundo das empresas, os crimes mais comuns entre elas são a espionagem e furtos de documentos virtuais com a finalidade de copiar ideias e procedimentos. Já outro crime comum nas empresas é entre ela e usuários ou pessoas que querem entrar no sistema alheio com o intuito de bagunçar ou adquirir informações, que terá importância para ela.

Sites, como a maior rede social do mundo, o Facebook, foi vítima de um ataque de hackers que ultrapassou boa parte das defesas instaladas pelo site. O programa encontrado pela equipe do Facebook teria se alocado em computadores dos próprios funcionários da rede. Segundo o Facebook, a companhia não foi a única a sofrer esse tipo de ataque e, por conta disso, a rede social trabalha em conjunto com outras empresas para ampliar os esforços de prevenção. Assim como a rede social, outros gigantes da internet também já foram vítimas de ataques semelhantes, como o Twitter, que já foi alvo de um ataque que pode ter exposto informação pessoal de cerca de 250 mil contas do microblog. Outro caso notório é o da Sony, que em 2011 teve cerca de 70 milhões de usuários afetados por um ataque à rede Playstation Network (PSN).

O Brasil tem ocupado posições de destaque nos rankings de ataques cibernéticos. Nos últimos anos o país alcançou a terceira colocação no ranking dos países com o maior número de empresas atacadas por hackers do mundo, de acordo com um relatório feito pela RSA. O país foi responsável por 5% do volume global, ao lado de Austrália, Índia e Canadá, enquanto Estados Unidos e Reino Unido lideraram a lista, respectivamente. Além disso, a RSA ainda indicou que entre os principais países hospedeiros dos chamados phishers, o Brasil fica em quarto lugar, com 4% dos ataques hospedados. O ataque de phishing é hoje a principal maneira utilizada por hackers para invasão de dados corporativos e pessoais.

Ainda em relação aos crimes virtuais no direito empresarial, de acordo com o artigo 195 da Lei n. 9.279 /96, o fato de usar logomarca de empresa sem autorização do titular, no todo ou em parte, ou imitá-la de modo que possa induzir à confusão, se caracteriza crime contra a propriedade industrial.

5.4- Crimes Virtuais no Direito Penal

Toda conduta ilícita praticada no mundo virtual, que atingem direitos e princípios previstos em lei, é passível de punição de acordo com o código penal, como crimes contra a honra (injúria, calúnia e difamação), furtos, extorsão, ameaças, violação de direitos autorais, pedofilia, estelionato, fraudes com cartão de crédito, desvio de dinheiro de contas bancárias. A lista de crimes cometidos por meio eletrônico é muito extensa e sua prática tem aumentado rapidamente com a universalização da internet, passando as fronteiras entre os países.

Atualmente e diariamente, o Judiciário vem coibindo a sensação de impunidade que reina no ambiente virtual combatendo a criminalidade cibernética com a aplicação do Código Penal.

As condutas ilícitas que acontecem no mundo dos crimes virtuais, já estão sendo aplicadas as leis vigentes, como no caso do nosso código penal brasileiro, como veremos a seguir no capítulo 6.1.

6-Crimes Virtuais e Normas Vigentes

Crimes que acontecem por meio de computadores, tablets, smartphone, entre outros aparelhos que acessa a internet podem cometer crimes, sendo com isso aplicado regras e normas que já tipificam a conduta. Com o desenvolvimento tecnológico, o mundo jurídico se evolui também, passando a ter regras e legislações. Nesse capítulo pretendo destacar sobre as leis que podem ser aplicadas nos crimes virtuais, sobre o marco civil da internet e sobre a Lei nº 12.737 conhecida como Lei Carolina Dieckmann.

6.1-Disposição Legal Aplicável

Como existe uma ausência de uma legislação específica que pune os crimes eletrônicos, os tribunais brasileiros estão enfrentando e punindo internautas, crakers e hackers que utilizam a rede de computadores como instrumento para a prática de crimes. Grande parte dos magistrados e advogados considera que a maioria dos delitos cometidos eletronicamente já está tipificados no Código Penal brasileiro por caracterizar crimes comuns praticados por meio da internet. Já os outros faltariam o enquadramento jurídico que abrangeria as transgressões que só existem no mundo virtual, como a distribuição de vírus eletrônico.

Os crimes que podem ser tipificados no código penal se acontecerem no mundo virtual pode ser no caso de insulto a honra de alguém (calúnia artigo 138 CP), espalhar boatos eletrônicos sobre pessoas (difamação artigo 139 CP), insultar pessoas considerando suas características ou utilizar apelidos grosseiros (injúria artigo 140 CP), ameaçar alguém (ameaça artigo 147 CP), utilizar dados da conta bancária de outrem para desvio ou saque de dinheiro (furto artigo 155 CP), comentar, em chats, e-mails e outros, de forma negativa, sobre raças, religiões e etnias (preconceito ou discriminação artigo 20 da Lei n. 7.716 /89), enviar, trocar fotos de crianças nuas (pedofilia artigo 247 da Lei n. 8.069 /90, o Estatuto da Criança e do Adolescente - ECA).

6.2-Marco Civil da Internet

O Marco Civil da internet foi criado para regulamentar a internet, sendo estabelecido regras e conceitos de rede. Após várias audiências públicas em todo o Brasil e o recebimento de sugestões por meio de vários sites e rede social, o Marco Civil da internet foi sancionado pela presidente Dilma Rousself em 23 de abril de 2014, sendo considerado por especialistas, um texto pioneiro no mundo ao estabelecer regras, direitos e deveres no meio virtual brasileiro.

O Marco Civil da internet está descrito na Lei nº 12.695, de 23 abril de 2014 e está dividido em capítulo, seção e subseção.

O capítulo um estabelece conceitos, princípios, direitos, deveres para o uso da internet no Brasil, bem como o respeito à liberdade pessoal e de comercio, levando em consideração os usos e costumes.

O capítulo dois estabelece direitos e garantias dos usuários, como garantias e direitos que o usuário tem sobre sua vida pessoal e profissional, e também o direito de saber sobre as políticas e termos de uso dos sites, provedores e redes sociais.

O capítulo três descreve sobre a provisão de conexão e de aplicações de internet, sendo divididos pela seção um, dois, três e quatro, sendo que a seção dois se subdivide por subseção um, dois e três. A seção um, descreve sobre a neutralidade da rede, ou seja, sobre a responsabilidade do responsável pela transmissão, comunicação e roteamento de dados. A seção dois descreve sobre a proteção aos registros, aos dados pessoais e às comunicações privadas, ou seja, os registros de conexão, os dados pessoais e às comunicações privadas devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. A seção três descreve sobre a responsabilidade por danos decorrentes de conteúdo gerado por terceiros, ou seja, descreve sobre a responsabilidade dos provedores em relação a conteúdos criados e publicado por usuários, sendo somente punido se após a ordem judicial o provedor não tomar nem uma providência para tornar indisponível o conteúdo. Já a seção quatro descreve sobre a requisição judicial de registros, ou seja, descreve a possibilidade de alguém, vítima de algum fato ilícito para uso cível ou penal, requerer ao juiz para que o responsável pela rede que aconteceu o fato, o fornecimento dos registros de conexão ou de registro de acesso a aplicação de internet.

O capítulo quatro descreve sobre a atuação do poder público, ou seja, constitui diretrizes para a atuação da União, Estados, Distrito Federal e Municípios no desenvolvimento da internet no Brasil.

O capítulo cinco descreve sobre as disposições finais sobre o tema, ou seja, descreve sobre a liberdade de escolha do usuário na utilização de programa de computador, sobre a defesa de interesses e dos direitos estabelecidos nesta lei entre outras coisas.

6.3- LEI Nº 12.737/2012 (Lei Carolina Dieckmann)

Sancionada pela presidente Dilma Rousseff em três de dezembro de 2012 a Lei nº 12.737 conhecida como Lei Carolina Dieckmann, alterou o código penal brasileiro, fazendo que ocorra a tipificação dos delitos cometidos no mundo virtual (informático e da internet).

O artigo 154-A tipifica a conduta no caso do sujeito que invade computador alheio, ou seja, de terceiros, conectado a rede de computadores ou não com a finalidade de obter, adulterar ou destruir dados sem a devida autorização que tem que ser expressa ou tácita do titular (dono) do respectivo computador. A pena para quem cometer esse ato ilícito é de detenção de 3 (três) meses a 1 (um) ano, e multa.

Esse crime trata-se de um crime comum, ou seja, pode ser praticado por qualquer pessoa. O objetivo do legislador do crime de invasão de dispositivo informático é a inviolabilidade da intimidade e da vida privada que consiste na proteção e guarda dos dados e informações armazenadas no dispositivo informático da vítima.

Nesse crime prevê duas formas de se praticar, que seria na conduta (invadir) o dispositivo informático, sendo o crime praticado de forma vinculada ou (instalar) vulnerabilidades, sendo o crime praticado de forma livre, ou seja, pode ser cometido por qualquer meio de execução. Para poder praticar esse crime, o sujeito ativo tem que ter o dolo, ou seja, uma vontade de invadir dispositivo informático alheio, com violação indevida de mecanismo de segurança ou instalar vulnerabilidades, tornando-o desprotegido o dispositivo e fazendo com que fiquem mais fáceis as violações.

A pena é aumentada de um sexto a um terço, se no caso do crime resultar de prejuízo econômico para a vitima. E se da invasão do dispositivo informático resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, ou o controle remoto não autorizado do dispositivo invadido a pena será de reclusão de 6 (seis) meses a 2 (dois) anos e multa. No caso do §3º, é aumentado a pena de dois terços se haver a divulgação, comércio ou transmissão dos dados a terceiros. A pena é ainda aumentada de um terço à metade se o crime for praticado contra a Presidente da República, governadores, prefeitos, Presidente do Supremo Tribunal Federal, Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal, Câmara Municipal ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

A invasão de dispositivo informático é um crime formal, ou seja, de consumação antecipada, que se consome sem a produção do resultado naturalístico. Ocorrendo a adulteração ou destruição dos dados ou das informações da vítima constitui no simples exaurimento do crime. Portanto, esse crime se consome no momento em que o agente invade o dispositivo informático da vítima, mediante a violação indevida de mecanismo de segurança, ou no caso de instalação vulnerabilidades, tornando o dispositivo fácil para violações. Como é um crime instantâneo, sua consumação não se prolonga no tempo.

7-Vitimas dos Crimes Virtuais

Atualmente, todos podem ser vítimas de crimes virtuais, como pessoas comuns da sociedade (Pessoa Física), empresas (Pessoa Jurídica) e países (Estados e todas as pessoas envolvidas), sendo que ninguém está imune cem por cento contra ataques virtuais, pois a cada dia é criado um programa (vírus) capaz de invadir ou violar um sistema, como em computadores e outros aparelhos que podem ser acessados e invadidos. Nesse capítulo pretendo mostrar quem podem ser as vítimas dos crimes virtuais e quais crimes que podem acontecer com elas.

7.1-Estado

O Estado vai ser sempre vítima do crime virtual quando envolver ele, ou seja, pode ser vitima pelo motivo tributário (sonegação fiscal, por exemplo), ofensa a políticos (invadir rede social do político ou invadir página de partido, por exemplo) ou quando ocorre a invasão do sistema virtual do governo (invade site da república ou diário oficial do poder executivo, por exemplo) entre outras coisas.

É exemplo de crimes virtuais contra o Estado, o que ocorreu no dia 22 de junho de 2013, quando hackers invadiram a página oficial do governo do Brasil na internet, fazendo com que todo o conteúdo do site ficasse indisponível, ou seja, quando alguém tentasse entrar no site, não dava para visualizar nada. O fato ocorrido foi assumido pelo grupo Anonymous no facebook, servindo de justificativa, um apoio aos protestos que ocorriam no país em 2013.

Esse mesmo grupo de hackers (Anonymous) ainda invadiu outros sites oficiais como o portal da Polícia Militar de Minas Gerais, email do governador do estado de São Paulo em 2014 entre outros.

7.2-Pessoas Físicas

As pessoas físicas, vítimas de crimes virtuais são aquelas pessoas comuns da sociedade brasileira, ou seja, são aquelas pessoas que não fazem parte do Estado e não são pessoas jurídicas, sendo vítimas de crimes financeiros (conta bancária saqueada por hackers, compras realizadas por conta em sites, por exemplo) e crimes contra a honra (difamação, calúnia, injúria praticada na internet, por exemplo).

Atualmente vemos pessoas sendo processadas tanto na justiça comum, como no juizado especial (JECrim) por causa de crimes cometidos no mundo virtual, como nas redes sócias, quando por motivo pessoal uma pessoa atinge a moral da outra na internet, fazendo com que o efeito produzido pelo crime se torne ainda pior, pois muitas pessoas veem o fato e com isso o crime se consumir.

7.3-Pessoas Jurídicas

As pessoas jurídicas, vítimas de crimes virtuais são aquelas que possuem direitos e obrigações, sendo com isso atribuído personalidade jurídica, podendo ser pessoa jurídica de direito público (são entes da administração pública) ou pessoa jurídica de direito privado (como por exemplo, as associações, as sociedades, as fundações, as organizações religiosas, os partidos políticos e as empresas individuais de responsabilidade limitada, ou seja, as pessoas jurídicas de direito privado são instituídas por iniciativa de particulares).

Os crimes comuns que geralmente acontecem contra as pessoas jurídicas são furtos, roubos de materiais ou documentos por meio virtual, sempre com a finalidade de copiar ideias, procedimentos ou de adquirir informações sigilosas. Atualmente grandes empresas possuem suas centrais de anti hackers e também para investigar se sua marca, logo, produto

estão sendo usados por terceiros sem a autorização (produtos piratas, marcas e logo estampados em objetos, como por exemplo).

8-Direito Comparado

O direito, culturas, expressões, costumes entre outras coisas, foram incorporadas no Brasil e com isso não podemos deixar de destacar as normas e regras de outros países, que já possuem uma legislação ou regulação sobre crimes virtuais. Portanto, nesse capítulo pretendo explicar como são regulados os crimes virtuais nos países, como Estados Unidos, França e Suécia.

8.1-Estados Unidos

Nos Estados unidos foi implantado o sistema federalismo, que possibilita aos estados criarem suas próprias normas, ou seja, fazendo com que cada estado crie seu modelo de legislação para combater os crimes virtuais. Os EUA tem como método o sistema “Common Law”, que tem como base e fundamento os procedentes judiciais, que são decisões que vinculam todas as demais posteriores que tenham a conduta ou fato parecidos ou idênticos. O sistema “Common Law” tem a capacidade de criar direitos e obrigações a partir de decisões judiciais que sirva de procedentes, mas se no caso o tribunal decidir de forma controvérsia, essa decisão pode-se abrir um novo procedente.

No Brasil o sistema “Common Law” dos EUA é parecido com as súmulas vinculantes, mas tem diferença, como a sumula vinculante tem que ter origem do Supremo Tribunal Federal, sendo votada e aprovada por pelo menos dois terços do plenário, fazendo que se torne um entendimento obrigatório, no qual todos os juízes e tribunais terão que seguir.

Nos EUA as condutas podem ser incriminadas de acordo com o código penal norte-americano ou através de decisões judicial (sistema “Common Law”) como já explicado.

Nos EUA existem as leis federais e as estatuais que tipificaram os crimes virtuais, como a Lei de Proteção aos Sistemas Computacionais (Federal Computer System Protection Act of - 1981), que tipifica a conduta com o uso de computadores como objeto de praticar fraudes,

furtos, apropriação indébita e como a lei (Eletronic Funds Transfer Act - 1982)que regulamenta as transferências eletrônicas de fundos e fazendo com que se tornasse fato típico (crime) as fraudes informáticas que não tinham relações interpessoais.

8.2- França

Na França usa-se um sistema inquisitorial em relação ao poder de apurar crimes em geral, pois o juiz pratica certo grau de supervisão ou controle nas atividades da policia, participando com isso das investigações dos crimes virtuais também.

Atualmente a França não possui legislação específica sobre crimes virtuais, mas o Código Penal da França em 1988 acrescentou na Lei nº88-19 um capitulo importante, sobre atentados contra o sistema informático. A Lei nº88-19 do Código Penal Frances descrevia sobre o acesso fraudulento a sistema de elaboração de dados, sobre a sabotagem na informática, sobre a destruição de dados, sobre a falsificação de documentos informatizados e sobre o uso de documentos falsos retromencionados.

A Lei nº88-19 foi revogada em 1995 sendo substituída pelos artigos 323-1 a 323-7 que passou a descrever melhor os crimes virtuais. A partir dessa nova legislação a França passou a punir com mais rigidez e os casos mais específicos de crimes virtuais em suas variáveis situações.

8.3-Suécia

Na Suécia o sistema penal é conhecido como adversarial, pois o juiz não administra de forma ativa o processo, porque nesse sistema o processo é administrado pelas partes, apresentando elas o conteúdo fático e de direito da lide, ficando o juiz na relação processual, com a finalidade de decidir a lide com base no que foi apresentado pelas partes.

Portanto na Suécia em se tratando de crimes virtuais, a vítima não será autora no processo e sim como litisconsorte ativo facultativo, sendo o promotor o autor da ação penal e o juiz com o simples fato de julgar conforme as provas produzidas e demonstradas em juízo.

9-Crimes Virtuais e Redes Sociais

Atualmente vemos muitos crimes sendo planejados ou consumidos na internet, em especial nas redes sociais, e com isso pretendo focar e explicar nesse capítulo sobre a responsabilidade civil e penal nas redes sociais, e também mostrar as jurisprudências que demonstram esses casos.

9.1- Da Responsabilidade Civil nas Redes Sociais

Em se tratando da responsabilidade civil decorrente de crimes virtuais cometidos nas redes sociais, devemos saber o que é e como funciona essa responsabilidade no mundo jurídico. Responsabilidade Civil é quando á a obrigação de reparar o dano que uma pessoa física ou jurídica, grupo ou entidade, causou a alguém.

No direito brasileiro em se tratando da responsabilidade civil, existe duas teorias (Teoria Subjetiva e a Teoria Objetiva). Na Teoria Subjetiva o dano só é indenizável quando o agente agiu com dolo, ou seja, com vontade de causar um dano para a vítima, podendo com isso, ser indenizável. Já na Teoria Objetiva todo dano será indenizável, ou seja, se alguém mesmo sem agir com dolo causou um prejuízo moral ou material a alguma pessoa, será possível de se cobrar uma indenização.

No direito civil se prevê como fundamental para a responsabilidade civil, o princípio da responsabilidade subjetiva, descrita nos artigos 186 e 951 do Código Civil brasileiro, que prevê que a conduta será passível de indenização se o agente causador do dano agir com culpa ou dolo stricto sensu.

Mesmo com a teoria subjetiva, é passível de indenização se atingir um direito de alguém, como o direito da personalidade, direito da intimidade, direito à honra, direito da imagem e o direito da intimidade. Acontece isso muito nas redes sociais, como por exemplo, quando alguém compartilha foto com montagens vexatórias de alguém conhecido no Facebook.

O marco civil da internet prevê o respeito desses direitos, já descritos na constituição federal de 1988, como o direito da personalidade, direito da intimidade, direito à honra, direito da imagem e o direito da intimidade, sendo punidos, se infringidos na internet e por meio de computadores.

As pessoas que violarem direitos de alguém além de serem punidos na área penal podem ser punidas também na área civil. As Redes sociais e sites também podem ser punidos se ajudar, criar ou reproduzir conteúdo que afeta direitos referentes a alguém, sendo punida também se mesmo com ordem judicial não tirar conteúdo produzido por terceiros.

9.2- Da Responsabilidade Penal nas Redes Sociais

Na esfera penal, em se tratando da responsabilidade penal nas redes sociais, o crime que mais acontece, são os crimes contra a honra, ou seja, que afeta a vitima de forma moral e as vezes até material. Os crimes contra a honra é a Calúnia, Difamação e Injúria, que vamos esclarecer um por um e como acontece nas redes sociais, como no facebook.

Descrito no artigo 138 do Código Penal, a calúnia consiste na conduta de caluniar alguém, imputando-lhe falsamente fato definido como crime, ou seja, é quando o autor do crime conta a alguém ou a várias pessoas na internet que aquela pessoa cometeu um crime. Se essa pessoa que contou (narrou) na internet que aquela pessoa cometeu um crime, mas não tem provas, ela pode ser punida, com detenção de 6 meses a 2 anos presa e multa. Dos três crimes, é o único que, se você tiver provas, não é condenado.

Descrito no artigo 139 do Código Penal, a difamação consiste na conduta de difamar alguém, imputando-lhe fato ofensivo à sua reputação, ou seja, é quando o autor do crime conta a alguém ou a várias pessoas na internet, afetando sua reputação, como por exemplo, descreve que a mulher trai seu marido com outra mulher ou com outro homem. Mesmo tendo provas, o autor da conduta pode ser punida com detenção de 3 (três) meses a 1 (um) ano, e multa.

Descrito no artigo 140 do Código Penal, a injúria consiste na conduta de injuriar alguém, ofedendo-lhe a dignidade ou o decoro, ou seja, é quando o autor do crime ofende com

ofensas ou xingamentos de forma diretamente a vítima, como por exemplo, quando uma pessoa xinga a outra de burro, retardado ou bicha. A pena para esse crime é detenção 1 a 6 meses ou multa.

Além de serem punidas as penas podem ser motivo de aumento, pois nas redes sociais ainda encontra um agravante, que aumenta as penas em um terço, por ter sido realizada na presença de muitas pessoas, e por meio que facilite a divulgação da calúnia, da difamação ou da injúria.

9.3-Jurisprudências

STJ - RECURSO ESPECIAL : REsp 1175675 RS 2010/0005439-3

CIVIL E PROCESSUAL CIVIL. MENSAGENS OFENSIVAS À HONRA DO AUTORVEICULADAS EM REDE SOCIAL NA INTERNET (ORKUT). MEDIDA LIMINAR QUEDETERMINA AO ADMINISTRADOR DA REDE SOCIAL (GOOGLE) A RETIRADA DASMENSAGENS OFENSIVAS. FORNECIMENTO POR PARTE DO OFENDIDO DAS URLS DASPÁGINAS NAS QUAIS FORAM VEICULADAS AS OFENSAS. DESNECESSIDADE.RESPONSABILIDADE TÉCNICA EXCLUSIVA DE QUEM SE BENEFICIA DA AMPLALIBERDADE DE ACESSO DE SEUS USUÁRIOS.

1. O provedor de internet - administrador de redes sociais -, aindaem sede de liminar, deve retirar informações difamantes a terceirosmanifestadas por seus usuários, independentemente da indicaçãoprecisa, pelo ofendido, das páginas que foram veiculadas as ofensas (URL's).

2. Recurso especial não provido.

STJ - AGRAVO REGIMENTAL NO AGRAVO EM RECURSO ESPECIAL : AgRg no AREsp 12347 RO 2011/0111990-0

AGRAVO REGIMENTAL. AGRAVO EM RECURSO ESPECIAL. AÇÃO CIVIL PÚBLICA. INTERNET. REDES SOCIAIS. RESPONSABILIDADE DO PROVEDOR DE HOSPEDAGEM. PRECEDENTES DA CORTE. DANO MORAL. 100 SALÁRIOS MÍNIMOS. RAZOABILIDADE.

1.- O provedor não responde objetivamente pelo conteúdo inserido pelo usuário em sítio eletrônico, por não se tratar de risco inerente à sua atividade. Está obrigado, no entanto, a retirar imediatamente o conteúdo moralmente ofensivo, sob pena de responder solidariamente com o autor direto do dano.

2.- É possível a intervenção desta Corte para reduzir ou aumentar o valor indenizatório por dano moral apenas nos casos em que o quantum arbitrado pelo acórdão recorrido se mostrar irrisório ou exorbitante, situação que não se faz presente no caso concreto.

9.4-Facebook

De acordo com a reportagem de Mônica Bergamo, colunista do jornal Folha de São Paulo, uma pessoa pode ser condenada, se compartilhar ou curtir comentários ou noticias ofensivas, podendo ter que pagar indenização à pessoa ou às pessoas que se sentir atingidas. Foi dada uma sentença nesse sentido pelo Tribunal de Justiça de São Paulo, onde foi julgado uma causa, onde a lide envolveu um veterinário acusado de negligência no tratamento de uma cadela que seria castrada. A informação de tal negligência, que não foi comprovada, foi compartilhada e curtida na rede social “Facebook”, por duas mulheres que após apurado, foram condenadas a pagar uma indenização de 20 mil reais à vítima.

10-Solução para evitar os Crimes virtuais

Atualmente existem sites, blogs entre outros meios de comunicação, dedicados para explicar como evitar que aconteça um crime virtual contra você, mas devemos lembrar que nem toda proteção é capaz de proteger de um crime virtual específico, por isso que nesse capítulo pretendo demonstrar e explicar como se prevenir de vários crimes virtuais existentes e de como agir após ser vitima de um crime virtual.

10.1-Prevenção

Para se prevenir que aconteça futuros crimes virtuais que envolvam você ou amigos e parentes, basta tomar alguns cuidados técnicos e preventivos.

No caso de crimes virtuais que não afeta a honra, como crimes de estelionato entre outros tipos de fraudes, quanto melhor a prevenção, mais difícil será para o autor desses crimes chegarem ao seu objetivo, que é praticar um furto de dados ou de bens matérias e de até de dinheiro.

Um dos melhores modos para evitar que seu computador pegue vírus ou que seja sujeito a invasões é atualizar sempre os programas que identificam o vírus e eliminam, sendo conhecidos esses programas como “antivírus”. Esses programas que protegem o computador é conhecido como programas “antivírus”, pois como uma vacina de gripe, a finalidade do programa é fazer com que fique imune de qualquer programa invasor e que se no momento que algum programa tentar invadir o computador ou tentar se instalar nele, o programa alertara o usuário e eliminará o programa invasor (o vírus). Para evitar que seu computador pegue vírus, evite de entrar em sites desconhecidos, pois a maioria das pessoas pegam vírus através de sites pouco populares e que possuem a finalidade de conquistar a vítima pelo preço ou pela grande quantidade de arquivos, musicas, filmes, livros entre outras coisas para baixar (download). Evite também entrar em suas redes sociais e outras paginas pessoais em computadores compartilhados, ou seja, aqueles computadores que todo mundo usa, como por exemplo, em lugares que alugam por tempo os computadores para as pessoas usarem.

Ao comprar um computador novo ou usado, verifique se ele possui configurações de segurança, pois isso é muito importante, pois tudo que você armazena no computador pode estar correndo risco. Os programas como o navegador, o e-mail entre outros é uma das coisas que merece mais atenção, pois eles possuem regulagem e opção de segurança.

É usado muito hoje em dia as senhas para quase tudo que envolva a internet, o computador entre outros aparelhos de tecnologia, e com isso o usuário dessas tecnologias, pode e deve colocar senhas na quilo que achar importante, como senhas de e-mail, de redes sociais, de sites, de contas bancárias entre outras, com a finalidade de proteger e evitar furtos ou violações, como se fosse uma chave do seu cofre. Para a senha se tornar mais difícil de ser descoberta, evite falar para as pessoas a sua senha e nem forneça pistas, como data de

nascimento, endereço entre outras, podendo ser essa senha ter vários caracteres (dígitos) e várias combinações de letras, números e símbolos.

Mais um cuidado e muito importante no caso de clones de documentos e nos crimes contra a honra, é a sua exposição em relação a compartilhamentos de informações pessoais, como o nome, endereço, telefone, e-mail, perfil em rede social entre outras informações pessoais.

10.2-O que deve fazer a vítima de crimes virtuais

Quando você perceber que está ocorrendo um fato estranho com você na internet, como o aparecimento da frase senha incorreta em contas bancarias, em contas de e-mail ou em contas de sites, verifique se você não digitou errado, pois você pode estar sendo vitima de um crime virtual. São crimes virtuais, divulgações de conteúdo que se refere a sua pessoa, como por exemplo, divulgação na internet de frases ou montagens fotográficas que atingem a sua moralidade.

A primeira coisa a fazer em relação a crimes praticados na internet contra a honra (Difamação, Calunia e Injúria), é tentar criar uma prova, para futuramente ser usada judicialmente, com a finalidade de usar como prova que foi vitima de um crime. Essa prova pode ser testemunhal, ou seja, perguntar se as pessoas tiveram ciência do conteúdo, e com isso anotar o nome delas para que sirvam de testemunha do que aconteceu. Outra prova seria o chamado “print” da pagina e do conteúdo que foi praticado o crime, sendo o “print”, em português significa impressão, uma espécie de foto tirada da pagina, site ou e-mail.

Quando o crime virtual for financeiro, ou seja, praticado contra o seu patrimônio, como por exemplo, os crimes de estelionato, roubo de senhas bancárias, clonagem de cartões etc, o mais importante que se deve fazer, é avisar imediatamente a empresa que fornece esses serviços que ocorreu tal fato, sendo que a empresa vai tomar as providências cabíveis a ela. Nesse tipo de crime virtual, as provas que serão usadas será o boletim de ocorrência e provas que a policia vai conseguir obter através de registros dos computadores que entraram no seu computador ou na sua conta para praticar tal ato ilícito, entre outras provas.

Umas das coisas muito importantes, para que você tenha registrado que tal crime virtual aconteceu com você e futuramente buscar uma restituição de seus bens é fazer o boletim de ocorrência (B.O.), na delegacia mais próxima a você. O boletim de ocorrência é um documento utilizado e feito em órgão público, como na Policia civil, Policia Federal, Policia Militares, Bombeiros e da Guarda Municipal com a finalidade de fazer um registro de um crime, ou seja, registrar a noticia de um crime, sendo o seu conteúdo descrito o que ocorreu, relatado pela vítima. Após feito o boletim de ocorrência, a policia abre um inquérito policial com a finalidade de investigar e apurar o crime.

Após o inquérito policial, se achando a pessoa ou grupo que cometeu o crime contra a sua pessoa, será aberto uma possível ação penal, para que o acusado seja julgado e condenado, mas você pode entrar com uma ação civil para buscar a reparação do dano, através de uma indenização, sendo ela podendo ser de danos morais ou de danos materiais.

11-Conclusão

Portanto crime virtual é quando ocorre um fato ilícito, podendo ser tipificado tanto no código civil, penal ou tributário, devendo ser praticado com o uso do computador ou da internet.

Com o avanço da tecnologia, sendo usado tanto para o bem, mas como também para o mal, os crimes virtuais tendem a crescer e com isso mais e mais vítimas de crimes virtuais surgem, sendo que futuramente existirão delegacias e órgãos públicos especiais para investigar os vários tipos de crimes cometidos com o uso do computador e da internet no Brasil e no Mundo.

Como sabemos, a tecnologia está sempre mudando e avançando, sendo os mecanismos para a produção desses crimes virtuais, estarem sempre mudando e se tornando a cada vez mais inteligentes, acabam infringindo e violando os mecanismos de segurança das pessoas, empresas e governos, devendo elas, de forma continua, investir em proteção e segurança da informação e dados, pois a tendência é um dia ter mais crimes virtuais do que físicos, sendo a melhor vítima, aquela que menos se proteger virtualmente.

Referências

CASTRO, Carla Rodrigues Araújo de; **"Crimes de Informática e seus Aspectos Processuais".** Editora Lumen Juris, 2001.

CORRÊA, Gustavo Testa, **"Aspectos Jurídicos da Internet".** Editora: SARAIVA JURIDICO. Ano de Edição: 2010.

GOUVÊA, Sandra; **"O Direito na Era Digital"**. Crimes praticados por meio da Informática. Editora Mauad Ltda. Ano 1997.

INELLAS, Gabriel Cesar Zaccaria de; **"Crimes na Internet**". Editora Juarez de Oliveira. Ano 2009.

LUCCA, Newton de e Adalberto Simão Filho**; "Direito e Internet". Aspectos jurídicos relevantes**. Editora: QUARTIER LATIN. Publicação: 2008.

MATTOS, Alexandre M.; **"Crimes na Internet".** Editora: Espaço Jurídico. ANO DE EDIÇÃO: 2012.

PAULINO, José Alves; "Crimes de Informática". Editora: Projecto Editorial. Ano 2001.

REIS, Maria Helena Junqueira; **"Computer crimes". A criminalidade na era dos computadores**. Editora: Del Rey. Ano: 1997.

ROSA, Fabrízio; **"Crimes de Informática".** Editora: BOOKSELLER. Ano 2006.

SANTOS, Coriolano Aurélio de Almeida Camargo. Comissão dos Crimes de Alta Tecnologia da OAB/SP. **"As múltiplas faces dos crimes eletrônicos e dos fenômenos tecnológicos e seus reflexos no mundo jurídico".** Ano 2009.

VIANNA, Túlio Lima; **"Fundamentos de Direito Penal Informático". Do acesso não autorizado a sistemas computacionais.** Editora Forense. Ano 2003.