Uni-ANHANGUERA CENTRO UNIVERSITÁRIO DE GOIÁS
CURSO DE DIREITO

CRIMES VIRTUAIS FRENTE A FALTA DE LEGISLAÇÃO E EDUCAÇÃO DIGITAL

PATRÍCIA ALVES MACEDO

GOIÂNIA
OUTUBRO/2015

PATRÍCIA ALVES MACEDO

CRIMES VIRTUAIS FRENTE A FALTA DE LEGISLAÇÃO E EDUCAÇÃO DIGITAL

Trabalho de Conclusão de Curso apresentado ao Centro Universitário de Goiás – Uni-ANHANGUERA, sob orientação da Professora Drª. Renata Guilard, como requisito parcial para obtenção do bacharelado em Direito.

GOIÂNIA
OUTUBRO/2015

TERMO DE APROVAÇÃO

PATRÍCIA ALVES MACEDO

CRIMES VIRTUAIS

Trabalho de Conclusão de Curso apresentado à banca examinadora como requisito parcial para obtenção de Bacharelado em Direito do Centro Universitário de Goiás – Uni-ANHANGUERA, defendido e aprovado em _____ de _____ de _____ pela Banca Examinadora constituída por:

_____

Profª Ms. Renata Guilard de Oliveira Castro

_____

Profª Drª / Ms. Karla Beatriz Nascimento Pires

_____

Prof.ª Dr.ª / Ms.

Aos meus pais, por tudo.

AGRADECIMENTOS

A Deus por ter me dado forças para não desistir dessa batalha e que esteve comigo até o final.
Aos meus pais por todo esforço, amor e compreensão, em especial a minha mãe, guerreira que sempre esteve ao meu lado me incentivando e impulsionando. Devo tudo o que sou a você.
Agradeço também a todos que direta ou indiretamente fizeram parte dessa jornada e estiveram ao meu lado desde o começo, deixo aqui o meu muito obrigada.

RESUMO

Disserta-se sobre o surgimento da internet que consigo trouxe grandes avanços na sociedade e cada dia mais interfere de forma efetiva na vida de seus usuários. Através desse avanço, criminosos começaram a praticar novos e antigos crimes através da internet e o poder judiciário se viu despreparado para agir coibindo tais delitos, pois as evoluções tecnológicas estão sempre um passo à frente do sistema legislativo e judiciário. Pretendeu-se mostrar o grande número de crimes possíveis através da internet e como se evitar os mesmos utilizando medidas educativas e conscientização dos usuários e também formas de combater ações criminosas. Constatou-se que para se ter segurança na internet deverá haver educação digital, campanhas concisas no sentido de prevenção e coibição e é claro, legislação específica para tipificar penalmente os crimes virtuais próprios e atualização das leis vigentes para tratar dos crimes impróprios.

Palavras-chave: Internet**.** Cibercrimes. Tipificação Penal.

SUMÁRIO

INTRODUÇÃO

O Surgimento da internet trouxe consigo grandes avanços na sociedade, melhorias, inovações, facilidade de acesso, porém os criminosos se aproveitaram dessa simplicidade de troca de informações para praticar antigos e novos crimes através da internet, agindo de forma oculta uma vez que se acreditava na dificuldade de se descobrir quem é quem na internet.

Tendo em vista as mudanças que vêm ocorrendo no mundo, em especial as que impulsionam o crescimento da internet de modo geral e que paralelamente com os benefícios trazem brechas para o cometimento de práticas ilícitas, as pessoas estão sendo desrespeitadas, enganadas e lesadas, se sentindo cada vez mais desprotegidas.

O interesse pelo estudo do tema surgiu através do crescente número de pessoas que aderem diariamente ao uso da internet e acabam sendo vítimas de crimes cometidos através da mesma, assim como a falta de segurança virtual e necessidade de punição desses criminosos e ao mesmo tempo a conscientização dos usuários para que eles mesmos evitem tais práticas criminosas.

É de suma importância a conscientização dos usuários para se ter uma conduta digital adequada, tendo como resultado a não incidência de práticas lesivas, através do uso correto das principais correntes de comunicação. Devem ser alertados também sobre os cuidados a serem tomados com a divulgação de quaisquer informações pessoais.

Neste trabalho busca-se abordar a temática de crimes virtuais em face a falta de legislação especifica, bem como a falta de educação digital. Também será analisado leis recentes que abordam o assunto e que estabelecem princípios, garantias, direitos e deveres para o uso da internet no Brasil e também aquelas que trouxeram alterações ao Código Penal Brasileiro.

O presente trabalho mostra que através da Constituição Federal e do Código Penal Brasileiro os direitos violados têm amparo legal e com o advento de legislações específicas e a

educação digital, os crimes virtuais serão coibidos e se for o caso punidos.

Será utilizado a princípio o método histórico para se analisar onde tudo começou, o surgimento e evolução da internet, também será utilizada a pesquisa bibliográfica com o intuito de se ampliar o conhecimento do assunto especifico.

Também serão utilizadas as leis que tratam exclusivamente o assunto em pauta, como a Lei nº 12.965 que prevê resguardar os direitos do indivíduo no ambiente virtual e a Lei nº 12.737/12 que tipifica alguns crimes virtuais, assim como os pontos importantes na legislação que devem ser mudados, como por exemplo, a criação de campanhas de conscientização e um maior empenho das autoridades policiais na aplicação das leis existentes.

Por fim, serão abordadas as medidas necessárias para o combate aos crimes virtuais, com o intuito de se restabelecer a segurança digital.

1 A EVOLUÇÃO DA INTERNET

Não há como questionar a disseminação e a evolução da internet, visto que nos últimos anos vem ganhando mais pessoas e atingindo todas as classes sociais. Atualmente todos têm fácil acesso à internet, acesso esse que antes era feito através de *lan-house*, que é um estabelecimento comercial aonde principalmente crianças e adolescentes iam apara acessar a internet, porém esse tipo de estabelecimento caiu em desuso. Hoje é bem mais barato ter um computador em casa.

1.1 O surgimento da Internet

A internet surgiu por volta da década de 60, a partir de um projeto de uma agência do Departamento de Defesa norte-americano que visava à elaboração de um sistema de telecomunicações que fosse seguro o bastante, para que se ocorresse um possível ataque nuclear russo as informações mais importantes permanecessem em sigilo. E graças a essa preocupação foram criadas as primeiras redes locais, nesse sentido Paesani, (2012, p.10), aponta que "a solução aventada foi a criação de pequenas redes locais (LAN), posicionadas nos lugares estratégicos do país e coligadas por meio de redes de telecomunicação geográfica (WAN)".

Porém o auge da internet não aconteceu nesse mesmo momento, veio ocorrer anos mais tarde quando decidiram registrar o Protocolo de Controle da Transmissão/Protocolo Internet, nesse sentido Paesani, (2012, p.10) dá a definição desse protocolo: "trata-se de um código que consente aos diversos *networks* incompatíveis por programas e sistemas comunicarem-se entre si".

Houve um elemento de grande importância como dispõe Paesani (2012, p.11):

> O mais importante elemento, detonador dessa verdadeira explosão, que permitiu à internet se transformar num instrumento de comunicação de massa, foi o *world Wide Web* (ou WWW, ou ainda W3, ou simplesmente Web), a rede mundial. O WWW

> nasceu no de 1989 no Laboratório Europeu de Física de altas energias, com sede em Genebra, sob o comando de T. Berners-Lee e R. Cailliau.

Como visto a internet passou por um longo processo de crescimento antes de chegar ao atual estado que se encontra, atrás de todo esse crescimento visto hoje há uma longa história de transformação. Hoje ela é vista como uma forma rápida e fácil de obter tudo o que almeja.

Pedemonte, 1966 (apud PAESANI, 2012, p.10) afirma que:

> Hoje, a Internet é vista como um meio de comunicação que interliga dezenas de milhões de computadores no mundo inteiro e permite o acesso a uma quantidade de informações praticamente inesgotáveis, anulando toda a distância de lugar e tempo. O mais recente relatório da ONU reconhece que a tecnologia da informação abre uma via rápida para o crescimento baseado no conhecimento, como ocorreu com as exportações de *software* da Índia, os serviços de informática da Irlanda e o processamento de dados do Caribe Oriental.

Não há sombra de dúvidas que a Internet encontra-se em alta em todo o mundo, através dela os usuários conseguem se comunicar de forma rápida e eficaz quebrando as barreiras da distância que antes separavam os indivíduos, porém o alcance da internet ainda não é bem dividida e parte da população ainda nos dias de hoje não tem acesso a tal recurso.

Nesse sentido Paesani (2012, p.11) diz:

> O Sul da Ásia, onde vive 23% da população mundial, abriga menos de 1% dos usuários da Internet. No Brasil, o custo mensal equivale a um quarto do salário-mínimo. Nos países desenvolvidos, o acesso aos provedores é muito barato, quando não gratuito.

A internet não é a única fonte de transmissão de dados, existem várias outras formas de se utilizar tal equipamento.

Nesse sentido Paesani (2012, p.12) dispõe:

> [...] a Internet é apenas uma das vastas possibilidades da transmissão de dados via banda larga (nome técnico para cabo, que até agora era usado apenas para a TV por assinatura). As operadoras já estão planejando sistemas de comunicação de dados financeiros, para atrair empresas a um mercado que antes significava apenas entretenimento. Segundo técnicos do setor, o cabo pode permitir até mesmo a medição de gás e luz dos imóveis.

O número de casas conectadas a internet chegou a 32,3 milhões em 2014 e "pela primeira vez, 50% do total de casas estão conectadas, aponta pesquisa realizada pelo Centro de Estudos sobre as tecnologias da informação e da comunicação (cetic.br)". (GOMES, 2015)

O avanço da internet tem proporcionado um mundo de mudanças, de quebra de

paradigmas. Porém é válido lembrar que quando a sociedade muda, o Direito deve mudar também, infelizmente essa mudança se dá de forma lenta e não se faz eficaz para as respostas que os cidadãos precisam e esperam.

1.2 Internet: O Estado e o Direito

Para se entender a conexão de Estado, Direito e Internet, primeiro deve-se entender o que é Internet. A princípio há uma certa dificuldade de se assimilar o que vem a ser Internet e isso se explica pelo fato de não haver uma definição especifica, podendo ser interpretada e vista de formas diferentes por cada pessoa.

Nas palavras de Paesani (2012, p.12):

> [...] Sob o ponto de vista técnico, a Internet é uma imensa rede que liga elevado número de computadores em todo o planeta. As ligações surgem de várias maneiras: redes telefônicas, cabos e satélites. Sua difusão é levemente semelhante à da rede telefônica. Existe, entretanto, uma radical diferença entre uma rede de computadores e uma rede telefônica: cada computador pode conter e fornecer, a pedido do usuário, uma infinidade de informações que dificilmente seriam obtidas por meio de telefonemas.

A partir do momento em que o computador através da Internet começou a ser uma forma rápida de acesso a informações, seja pela navegação nas redes sociais ou pelo pagamento de contas *online*, começou a surgir uma nova modalidade de crime, os chamados *cybercrimes*, que segue a mesma linha dos crimes já conhecidos no mundo real e com isso as pessoas se viram em uma situação inesperada, as autoridades foram pegas de surpresa quando se viram em uma área repleta de falhas e brechas jurídicas.

Nesse sentido Borruso, 1978 (apud PAESANI, 2012, p.13) dispõe:

> O computador entrou no mundo do direito despertando os atrasos, as cautelas, a perplexidade e as desconfianças que circundam os novos fenômenos. Podem ser evidenciadas duas reações típicas dos juristas: a *desconfiança*, característica do mundo fechado do Direito, quando confronta com as inovações tecnológicas, e a *defesa* – típica do Direito, que se fecha e procura expelir o elemento perturbador para neutralizar as forças invasoras.

A cada dia que passa a Internet ganha mais espaço chegando cada vez mais longe e abrangendo um grande número de pessoas. Essa inovação deve ser vista como uma evolução não só informática, mas também como uma revolução de pessoas, na medida em que os indivíduos encontram uma nova culturalidade.

Paesani (2012, p.16) expõe de uma forma muito interessante:

> [...] a nova realidade estatal deve ser interpretada no contexto dos valores da civilização contemporânea, na qual os processos de comunicação ou de informação ganham crescente terreno como consequência das conquistas tecnológicas que informam a cultura cibernética. E conclui que não se trata de substituição da "era do capitalismo" pela "era da informação", mas de uma evolução do capitalismo, que desloca seu eixo, em que a informática dá significado e forma ao capital em razão de sua aplicação, prevalecendo a informação sobre a posse dos bens e produção.

O Estado deve estar sempre a serviço das mudanças corriqueiras, ou seja deve caminhar lado a lado às inovações, não deixando existir brechas ou falhas no sistema visando assim a segurança das pessoas, nesse sentido Paesani (2012, p. 16) ressalta: "[...] poderemos afirmar que o Estado deve estar cada vez mais a serviço da inteligência, como instrumento atuante em função da informação técnica que nosso tempo exige de maneira inexorável".

1.3 Liberdade de acesso e proteção do usuário

A liberdade de acesso e à forma da comunicação encontra embasamento na nossa Constituição Federal, que diz: "Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição".

Dessa forma se faz necessário relembrar que é livre o acesso a informação, devendo ser respeitado o limite que a lei impõe. E por isso não há como esse direito não ser protegido, ficando a cargo das autoridades responsáveis.

Nesse sentido Paesani (2012, p.17) diz:

> Analisando os princípios constitucionais dos principais países e a atual evolução da informação, parece procedente a afirmação de que a liberdade de acesso à rede requer, no mínimo, no plano dos princípios, uma simples tomada de consciência, da qual nenhum constitucionalista pode omitir-se.

Apesar de todo esse avanço na Internet algumas pessoas se sentem inseguras em fazer compras pela internet e outros tipos de transações pelo fato de não se sentirem seguras para passar seus dados pessoais a terceiros. Esse é um dos motivos que deve ser adotada uma política de maior segurança na rede, de maneira a proteger o usuário-comprador e fazer com que esses tipos de serviços tomem uma proporção ainda maior.

Paesani (2012, p.18) frisa que:

> O Brasil conta com mais de 41 milhões de internautas e previsões de movimentar mais de US$ 100 Bilhões no comércio eletrônico futuramente. Entretanto, muitos consumidores têm medo de comprar por esse meio, especialmente de colocar seu número de cartão de crédito na rede mundial. Em consequência desse justificado receio, o maior desafio dos fornecedores de produtos e serviços é justamente conquistar e reter o consumidor e estabelecer com ele, de fato, um relacionamento, uma parceria, e investir numa política de confiança.

Podestá (2000, p.160) nesse sentido diz que:

> A violação da privacidade no âmbito da Internet geralmente ocorre quando informações pessoais do usuário ou a publicidade de sua vida intima passa a ser do conhecimento de pessoas não autorizadas (normalmente um hacker ou "micreiro") que após incessantes e contínuas tentativas acaba "descobrindo" a senha ou chave de acesso que possibilita aquela invasão.

É de suma importância a regulamentação de leis especificas que venham a controlar o acesso à rede e punir aqueles que que usam de recursos para invadir a privacidade alheia, visando prejudicar ou obter vantagem para sim. Existem vários projetos de Lei tramitando no congresso e algumas já aprovadas como por exemplo o Marco Civil da Internet (Lei 12.965/2014) e a Lei 12.737/2012, que ficou conhecida como Lei Carolina Dieckmann, que promoveu alterações no Código Penal Brasileiro.

Nesse sentido, Lima (2011, p.2) diz:

> Com a difusão da tecnologia informática, tornando-se uma presença constante na maioria das relações sociais, o Direito deve cuidar de reconhecer valores penalmente relevantes, criando normas protetoras a fim de estabelecer a segurança dessas relações. Também é dever do Direito Penal a proteção de bens jurídicos tradicionalmente reconhecidos e lesionados com o uso da tecnologia informática, bem como a proteção de outros valores jurídicos recentes havidos com o advento e a proliferação dos computadores.

Há grandes dificuldade quando se trata da temática proteção penal no âmbito da informática, pois não há ainda uma base concreta nas leis que trate desse assunto e por ser relativamente novo o tema essas barreiras aparecem, mas já está mais do que a na hora de se encontrar maneiras eficazes de controle dos crimes virtuais e por consequência a garantia da privacidade e da intimidade. Para isso deve ser delimitado o sentido em que se dará a proteção penal no âmbito informático.

Nesse sentido Lima (2011, p.3) diz:

> Essencial deve ser determinar qual o bem jurídico a ser penalmente tutelado nesta área, indagando, ainda, se há na estrutura constitucional a possibilidade de amparo pelo Direito Penal. Sempre considerando o que já foi afirmado, de que tal ramo do Direito deve somente agir na preservação dos bens mais relevantes e imprescindíveis

> das relações sociais, sempre dentro dos limites da intervenção mínima.

Como já havia sido dito antes, o Direito deve agir de forma eficaz, mas sem ultrapassar os parâmetros legais e dessa forma será alcançada com êxito a verdadeira solução para a problemática Internet e os crimes virtuais que a cercam.

1.4 Hackers X Crackers

Muito se fala em *Hackers*, quando as pessoas vão se referir a alguém que sabe tudo sobre computador e internet, que usam esse conhecimento para boas e más ações, elas usam a palavra *Hacker*, porém eles não são necessariamente aqueles indivíduos que lesam pessoas e equipamentos, eles na verdade utilizam de seu conhecimento para alertar pessoas sobre as falhas do sistema, por exemplo.

Nesse sentido Cassanti (2014, p.2), diz:

> Apesar do termo *hacker* sempre aparecer associado a roubo de dados e invasão de sistemas, no entendimento de especialistas em computação, os verdadeiros criminosos são designados como *crackers*. A palavra deriva do verbo inglês "to crack", que significa quebrar. Entre as ações, estão a prática de quebra de sistemas de segurança, códigos de criptografia e senhas de acesso a redes, de forma ilegal e com a intenção de invadir e sabotar para fins criminosos.

Mas existem aqueles que gostam de bagunçar a vida das pessoas e se realizam com o mal causado a terceiros, esses são os *crakers*. Deve-se saber a diferença básica entre um e outro para que assim os usuários saibam com mais clareza quais são os seus problemas e quem os causou.

Ambos são especialistas quando o assunto é computador, ficam boa parte do dia obtendo conhecimentos sobre sistemas, computadores e afins. A forma mais rápida de se diferenciar um do outro é entender como cada um utiliza tal conhecimento.

Cassanti (2014, p.2), define o termo *hacker* como sendo:

> O termo hacker, por sua vez, serve para designar um programador com amplo conhecimento sobre sistemas, mas sem a intenção de causar danos. Inclusive, a habilidade para lidar com sistemas e programações, muitas vezes, é aplicada pela própria polícia em investigações ou até mesmo no desenvolvimento de softwares com o intuito de limar brechas de segurança, criar novas funcionalidades ou adaptar as antigas.

Tendo em vista o exposto, fica evidente que há grandes diferenças entre esses dois

termos e que são diariamente usados de forma equivocada. Existem ainda outros termos que definem outras habilidades dos crackers que serão mostradas adiante.

2 CIBERCRIME

Cibercrime é o nome dado às práticas ilegais cometidas através do uso da internet, utilizando o computador ou outro equipamento como meio com o objetivo de lesar pessoas.

2.1 Bem jurídico e Cibercrimes

O mais moderno conceito de bem jurídico surgiu em 1834, quando foi publicado o pensamento de Birnbaum, um estudo sobre a tutela e a honra, que trouxe uma nova perspectiva ao Direito Penal, pois introduziu a ideia de bem, abandonando o antigo conceito relacionado ao direito subjetivo (CRESPO, 2011, p.52).

Nos dizeres de Lima (2011, p.1):

> O Direito contempla os comportamentos dos homens nas relações que estes mantêm entre si ou com as coisas. O trabalho do jurista consiste em configurar juridicamente estas relações, isto é, as objetivar em normas jurídicas, como faz o legislador, ou confrontar as condutas com as normas jurídicas, como faz o juiz. Esse é o círculo de conversão entre a realidade do mundo e a hiper-realidade das estruturas jurídicas como modelos de comportamento.

O bem jurídico é um dos fundamentos do Direito Penal e ele surge da relação em que os indivíduos criam entre si. Nesse sentido, Lima (2011, p.2) conceitua "bem jurídico designa tudo aquilo com que possa se satisfazer uma necessidade humana e que possa ter o valor reconhecido para o Direito".

No Direito Penal nota-se que o bem jurídico é mais comprimido, uma vez que só é responsável por tratar de assuntos onde exista lei anterior que defina o ato como proibido, obedecendo assim o princípio da reserva legal, que só será passível de sanção aqueles atos descritos como ilícitos e que independe de valores pessoais.

Nesse sentido Lima (2011, p.2) diz:

> A obediência ao princípio da reserva legal é premissa inafastável para a capitulação dos atos lesivos ou prejudiciais aos cidadãos. Somente pode se falar em do cometimento de um crime em caso de a conduta realizada restar descrita em lei como um delito. Cabe lembrar que nem todo comportamento reprovável do ponto de vista ético constituirá crime, sempre dependerá de norma penal a ser elaborada pelos legisladores que devem examinar e considerar os bens jurídicos mais importantes a serem protegidos pelo Direito, através da criação de figuras delitivas.

Através do avanço tecnológico e consequentemente dos crimes virtuais, várias mudanças acontecerem na sociedade, porém deve haver mudanças também no Direito Penal, como a observância da extensão do tratamento dos bens jurídicos.

Segundo Crespo (2011, p.56):

> Ao considerarmos as condutas ilícitas por meio da informática, verificamos a possibilidade de lesão a outros bens jurídicos. Assim, pode-se falar em condutas dirigidas a atingir não só aqueles valores que já gozam de proteção jurídica, como a vida, a integridade física, o patrimônio, a fé pública, mas, também as informações armazenadas (dados), a segurança dos sistemas de redes informáticas ou de telecomunicações.

Os crimes virtuais surgem através da não obediência às normas estipuladas, que geralmente se dão por sujeitos que já praticam atos ilegais no mundo físico e aproveitam da facilidade encontrada na internet para cometê-los também no mundo virtual.

Lima (2011, p.7) diz:

> Os também chamados crimes de computador surgiram nas últimas décadas do século XX, em meados dos anos 70, acompanhando o incremento do uso de computadores, sendo assim considerados as condutas delituosas efetivas mediante o uso de um computador conectado ou não a uma rede, restando aí incluídas a manipulação de dados de instituições financeiras, a cópia ilegal de programas de computador, a revelação de segredo de informação computadorizada (como a recente divulgação pela internet da declaração de imposto de renda do ex-presidente da República).

Há muitas definições para crimes de informática, porém uma das mais claras é a de Martin (apud, LIMA, 2012, p.10) que diz:

> A conceituação do chamado ‘crime informático’, expressão que prefere por sua simplicidade e por, no seu entender, melhor corresponder com o termo inglês *computer crimes*, deve ser toda ação dolosa que provoca um prejuízo a pessoas ou entidades, utilizando-se, para sua consumação, dispositivos habitualmente empregados nas atividades de informática”.

Como visto, crime de computador são quaisquer crimes cometidos por intermédio da máquina, ou seja, são aqueles velhos crimes já conhecidos e alguns outros que só surgiram a partir do advento da internet, como por exemplo, o *cyberbullyng.*

Nos dizeres de Lima (2011, p.11):

> Em verdade, os crimes de computador são, na maior parte das vezes, os crimes comuns cometidos com o auxílio de um computado, podendo os crimes de furto, apropriação indébita, estelionato ou dano, serem cometidos por esse meio com consideráveis prejuízos patrimoniais. Entretanto, há algo além de uma nova ferramenta, de um novo meio, de um novo *modus operandi* para o cometimento de crimes: estamos também diante de novas condutas não tipificadas.

No caso do vírus do computador a ação ilegal é cometida há mais de um computador ao mesmo tempo e por isso é mais difícil de se punir alguém por esses atos. Quando o indivíduo se esconde atrás do computador e ainda vai além se camuflando em meio a programas maliciosos, é muito complexa a solução do delito.

Nesse sentido Lima (2011, p.12) diz:

> [...] evidencia-se que ações delituosas podem ser praticadas contra o funcionamento de um ou mais computadores, sem que exista uma figura típica para tal conduta, exemplificando aqui com a disseminação do *'vírus de computador'*, que tem, quase sempre, como objetivo único a destruição de programas e dados de uma máquina ou rede, podendo tomar contornos colossais justamente pelo uso dos correios eletrônicos e pelo uso da internet.

Os vírus estão escondidos onde as pessoas menos imaginam, eles podem estar em um e-mail que você recebe de um amigo, amigo esse que clicou em um ícone e foi disseminando o vírus para toda a sua rede de contatos, pode estar nos mais variados sites acessados diariamente, ou seja, ninguém está livre desses invasores.

Lima (2011, p.12) fala sobre a dificuldade de vencer tais barreiras:

> Difícil é vencer essa barreira, definindo de um lado o que seriam os crimes novos, merecedores de uma nova tipificação, colocando de um outro lado a reforma das figuras penais atualmente existentes, incluindo nestas eventuais qualificadoras e agravantes decorrentes do uso da informática.

Nota-se que há uma certa dificuldade em se diferenciar crimes novos e crimes antigos, e essa dificuldade se dá pois precisa-se saber qual é qual para que se possa tomar às medidas necessárias, para a adequação do nosso ordenamento jurídico, que diga-se de passagem é bastante obsoleto, criando uma nova tipificação ou reformando as leis existentes.

Nesse sentido Lima (2011, p.12) aponta uma definição:

> De acordo com a definição elaborada por um grupo de peritos convidados pela OCED (Organização para a Cooperação Econômica e Desenvolvimento da Organização das Nações Unidas - ONU) para Paris, em maio de 1983, o termo *crimes de computador*

> se define como qualquer comportamento antijurídico, não ético ou não autorizado, relacionado com o processamento automático de dados e/ou transmissões de dados.

Por fim nota-se que mais complexo que a conceituação de crimes virtuais, é a dificuldade em se criar leis especificas para conter esse surto de delitos, sabe-se que há ainda uma confusão em se distinguir o delito que adveio da internet e os que só mudaram a roupagem para usufruir das brechas existentes.

2.2 Classificação das condutas danosas

Existem vários tipos de condutas ilegais na internet, condutas que já existiam no mundo físico e que só mudaram o meio de execução e outras que surgiram através da internet, tais condutas são classificadas como: crimes digitais próprios e crimes digitais impróprios.

A melhor classificação é aquela considerada mais clara e objetiva, facilitando o enquadramento de condutas ilícitas, que é: (a) condutas perpetradas contra um sistema informático; (b) condutas perpetradas contra outros bens jurídicos (CRESPO, 2011, p.63).

Nota-se que a tipificação das condutas varia de acordo com o bem jurídico ofendido, podendo os crimes virtuais lesar o próprio sistema e também a terceiros utilizando a internet como meio de execução.

2.2.1 Crimes digitais próprios

Crimes digitais próprios são aqueles que atingem os sistemas informatizados, cujo bem jurídico protegido é a informática. Dentre eles temos:

Acesso não autorizado - que é conhecido também como "invasão". E nada mais é que o uso indevido de sistema informático. Os motivos que levam alguém a praticar tal conduta são muitos, como por exemplo a curiosidade de se invadir a privacidade alheia por mera curiosidade ou para fraudar dados. (CRESPO, 2011, p.64)

Importante se faz ressaltar que foi sancionada a lei nº 12.737/12 (que será abordada mais a fundo no capitulo 3) e que recentemente entrou em vigor, trazendo tipificação aos delitos de invasão de dispositivo informático etc., e acrescentando os artigos 154-A e 154-B ao Código Penal, como pode ser visto:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou

> tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos".

Obtenção e transferência ilegal de dados - é o acesso também sem autorização a dados de terceiros e ainda com o agravante da transferência ilegal dos mesmos.

A principal forma de se ter acesso a esses dados de forma ilegal é a utilização de programas automáticos de computador como o *spyware* (termo genérico que significa arquivos espiões) programas que recolhem tudo o que o usuário faz na internet, assim como o que tem armazenado em seu computador.

Vírus e sua disseminação - estão incluídos dentro dos *malwares*, é que o termo utilizado para se referir a um conjunto de programas maliciosos.

Crespo (2011, p.74) define vírus como sendo:

> [...] Segmentos de códigos de computação que se anexam a programas ou sistemas de modo a se propagar pelas máquinas e contaminar outros sistemas em contato com esta, através de e-mails remetidos automaticamente e até mesmo por transmissão de dados maliciosos por outros métodos.

Assim como uma enfermidade que acomete um ser humano, o vírus pode afetar diversas partes de um sistema informático e em vários níveis, podendo simplesmente deixar o sistema mais lentou ou até mesmo causar a perda total de dados armazenados.

Divulgação ou utilização indevida de informações - se dá através do *spam*, que "é a correspondência virtual não solicitada pelo usuário de um computador e que é remetida em massa, portanto, para um número enorme de pessoas". (CRESPO, 2011, p.78)

Para se caracterizar algo como *spam* precisa existir alguns elementos específicos, como o não consentimento, que é a não autorização de recebimento de algo e também o grande número de destinatários, ou seja, quando vários usuários recebem ofertas de uma determinada loja que nunca fizeram o cadastro para recebimento de tais informações, pode ser considerado divulgação indevida de informações.

Importante se faz mencionar uma medida que a Austrália tomou para coibir o spam propagado pelo celular. Pinheiro (2012, p.95) diz:

> Na Austrália, já há o Spam Act de 2003 que trata a respeito, contudo transgredido por companhia de telefonia norte-americana ao enviar campanhas de famosíssimo reality show de ídolos cantores, em janeiro de 2009, além de outras duas companhias da própria Austrália que utilizaram de maneira equivocada este tipo de publicidade.

Nota-se que diversos países já estão empenhados na coibição de condutas ilícitas, apesar de se saber que é muito difícil manter as leis atualizadas na mesma velocidade em que as coisas acontecem na internet.

Interceptação ilegal de dados - nada mais é do que alguém sem autorização judicial realizar interceptação telefônica, telemática ou informática, ou seja, de forma ilegal.

Encontramos na Constituição Federal preceitos para que não seja violada as comunicações em geral, porém essa inviolabilidade não é absoluta, uma vez que existem casos em que é autorizado, mediante autorização judicial, tal violação para fins de investigação criminal ou instrução processual penal.

2.2.2 Crimes digitais impróprios

Crimes digitais impróprios são aqueles que já possuem tipificação, ou seja, são conhecidos por todos e que atingem bens que já são abraçados pelo ordenamento jurídico brasileiro. Eles se dão por várias formas e a internet é apenas mais uma.

Nos dizeres de Crespo (2011, p.88):

> Ocorre que alguns desses ilícitos ganham impressionante repercussão justamente por serem praticados por meio de ações envolvendo os meios tecnológicos. São exemplos os crimes contra a honra, os crimes de ameaça, falsidade ideológica e até mesmo o estelionato. Apesar disso, nada mais são do que os antigos crimes tipificados sob outra forma de cometimento (...)

Os principais crimes digitais impróprios são:

A) Ameaça: É crime intimidar, amedrontar alguém mediante a promessa de causar-lhe mal injusto e grave. A lei brasileira, no art. 147 do Código Penal, busca proteger a liberdade da pessoa no que toca à paz de espírito, ao sossego, ao sentimento de segurança. O mal prometido precisa ser injusto e grave.
B) Participação em suicídio. Embora no Brasil o suicídio não seja criminalmente punido, quem ajuda, instiga (reforça a ideia) ou induz (dá a ideia) outra pessoa a se matar responde por crime.
C) Incitação e apologia ao crime. Os arts. 286 e 287 do Código Penal mandam punir aqueles que incitam a prática de crimes, isto é, estimulam outras pessoas a praticar a infração penal.

É muito comum vermos a incitação e apologia em jogos de futebol e também é visto

com grande frequência por intermeio das redes sociais, onde uma pessoa reúne conhecidos em um determinado grupo e lá falam abertamente sobre práticas ilegais e instruem indivíduos para que façam o mesmo.

D) Falsidade ideológica. Celebridades e famosos em geral usam a internet e as redes sociais cada vez mais. Isso também faz crescer os perfis falsos, conhecidos por *"fakes",* que são pessoas que se passam por outras.
E) Violação de direitos autorais, uso indevido de marcas e pirataria de *software*. Aqui é encontrado a pirataria, que é o ato de copiar ou vender produto não autorizado pelo detentor dos direitos.
F) Pornografia infantil. É o uso indevido de imagens, filmagens e o registro de cenas de sexo explícito envolvendo crianças e adolescentes.

Ultimamente o *facebook* (rede social famosa por aproximar as pessoas) é um dos meios mais utilizados para a propagação da pornografia infantil e também aliciamento de menores.

G) Crimes contra a honra. Estão previstos nos arts. 138, 139 e 140 do Código Penal e são bastante comuns no ambiente virtual.

2.3 Crimes virtuais nas redes sociais

As redes sociais surgiram com o intuito de facilitar a comunicação entre as pessoas, e hoje reúne um grande número de usuários. O Brasil é o 5º país com o maior número de conexões à internet, ou seja, o brasileiro utiliza cada vez mais a internet e consequentemente as redes sociais.

Cassanti (2014, p.29) afirma:

> O brasileiro está cada vez mais conectado. Uma pesquisa feita no segundo semestre de 2012 pelo Ibope NetRatings apontou 83,4 milhões de brasileiros com acesso à internet, tendo este número pulado para 102 milhões em abril de 2013 segundo a empresa de audiência on-line Navegg. As conexões em domicílios e no trabalho foram as principais responsáveis pela expansão dos internautas.

A partir do momento em que uma pessoa passa a fazer parte desse mundo virtual, a tendência é que ela mude seus hábitos, assim passa a deixar de se comunicar pessoalmente e adere a comunicação a distância, encontra antigos amigos e acaba também fazendo novos, ai

nasce o perigo. Existem pessoas mal-intencionadas que utilizam perfis *fakes* para tirar proveito de outras, se aproximam facilmente através de um simples convite de amizade. E além disso os criminosos virtuais utilizam uma linguagem diferente que aproxima os menores deles e assim conseguem persuadi-los a fazer o que os mesmos desejam, como por exemplo: marcarem encontros ou mesmo mandar fotos e vídeos íntimos.

A pornografia infantil ou pedofilia é um dos crimes que mais vemos quando ligamos a televisão e grande parte dos aliciadores de menores utilizam o *facebook* para o cometimento desses delitos. Infelizmente o crescimento de adeptos a essa rede social que em tese seria uma das novidades mais bem-vindas no mundo, traz também grande facilidade aos criminosos virtuais.

Nesse sentido Cassanti (2014, p.29) fala:

> Quando o assunto é Facebook, o Brasil é o que mais ganhou novos usuários ativos mensais – quase 30 milhões – de 1º de janeiro a 31 de dezembro de 2012, de acordo com estudo divulgado pelo **SocialBakers** (grifo do autor), plataforma que monitora o uso das redes sociais mundialmente.

Por ser um ambiente com tamanha aglomeração de usuários foi escolhido como principal vertente para a prática de vários crimes virtuais.

Os pais têm papel fundamental na coibição ou resolução desses delitos, eles precisam acompanhar a rotina dos seus filhos, não só fora de casa, como também dentro. Devem estipular horários para a utilização da internet e saber com quem seu(s) filho(s) conversa(m).

Outra modalidade de crime virtual que também apavora pais e filhos é o *Cyberbullying*, que "é a ação intencional de alguém fazer uso das tecnologias de informação e comunicação (TICs) para hostilizar, denegrir, diminuir a honra ou reprimir consecutivamente uma pessoa". (CASSANTI, 2014, p.25)

O cyberbullying é tão grave que já levou um grande número de pessoas ao suicídio em diversos países.

Se faz necessário salientar que no *cyberbullying* o agressor geralmente está no anonimato, dificultando a percepção da dimensão que o mesmo vai alcançar e assim a vítima se sente mais desprotegida porque não consegue se esquivar de tais atos, já no bullying a identificação do agressor é certa e a vítima acaba encontrando uma solução mais eficaz.

Peck (2012, p.166) elenca o que configura o *cyberbullying*:

- Uso da imagem não autorizada de colega (foto ou vídeo) na Web associando a conteúdo ofensivo ou vexatório, que exponha parte do corpo do mesmo com o

> objetivo de ridicularizá-la (ex: nariz e chamar de narigudo, orelha e chamar de orelha de abano, outros).
> - Associação do nome de pessoa (colega, professor, terceiro) com bichos (por uso de imagem, som, outros efeitos) com o objetivo de expor a pessoa publicamente a constrangimento.
> - Redação de conteúdo dirigido a alguém (seja um colega, um professor, um terceiro) em tom agressivo, de ódio, de ameaça, discriminação, perseguição, falar mal ou denegrir a família da pessoa e do seu contexto social.
> - Incitação à prática de violência de uma ou mais pessoas contra uma pessoa especificamente (basta a menção de detalhes que possam gerar a identificação da vítima, mesmo que não haja citação do nome).

Esse tipo de crime é mais comum entre menores, principalmente adolescentes, que nessa fase se sentem donos da verdade e por mais que sejam alunos dedicados, filhos obedientes podem sim vir a agredir outras pessoas, muitos pais não sabem da rotina dos filhos e por eles aparentarem ser pessoas do bem não procurar saber a fundo como estão. Esse erro dos pais não só traz consequências para os filhos, mas também para eles mesmos, uma vez que a justiça vem decidindo que a responsabilidade no caso desse crime é dos pais.

Cassanti (2014, p.35) exemplifica:

> A justiça do Paraná condenou os pais de duas adolescentes ao pagamento de R$ 15 mil como indenização por danos morais, em razão destas terem colocado no perfil de uma página de relacionamento social da vítima mensagens de cunho pejorativo. Após perder o acesso a seu perfil, pois as infratoras haviam trocado a senha, a vítima não se importou com o fato e só alguns meses depois, alertada por uma professora, descobriu o ocorrido e constatou as ofensas. A vítima procurou então a polícia, que, mediante inquérito policial, chegou à identidade de quem postou as ofensas.

Visto isso, nota-se que é de suma importância os pais terem acesso ao conteúdo que o seus filhos visualizam e postam na internet, assim como faz-se necessário saber quem são as amizades que eles mantem nas redes sociais. Essas medidas não são só importantes para o uso adequando da internet, mas também para se evitar futuras dores de cabeça.

Nesse sentido Peck (2012, p.165) diz:

> Segurança é papel da família! Os pais precisam fazer parte do processo de iniciação de seus filhos no ambiente eletrônico, especialmente quando envolver redes sociais. Assim como se comprar um videogame vão instalá-lo, mostrar como funciona, jogar uma partida juntos, isso também deve ocorrer na web. Hoje, o jovem acaba por acessar sozinho, falta a "assistência" inicial necessária para ensinar a usar do jeito certo e sem riscos.

O sequestro também se dá ultimamente por intermédio das redes sociais. Os criminosos começam a observar a rotina da vítima, através das postagens observam que tipo de casa e carro as mesmas possuem, se viajam com frequência para o exterior, quais lugares

costumam frequentar e assim formam um perfil e se esse for de acordo com o que procuram agem rapidamente e com muita facilidade, pois já tem tudo que precisam sem nem mesmo saírem de casa. Por isso é importantíssimo ter apenas conhecidos nas redes sociais e mesmo assim divulgar apenas o necessário, evitando o acesso indesejado a sua privacidade.

Os perfis falsos fazem parte de qualquer rede social e podem ser descritos como um indivíduo se passando por outro.

Nos dizeres de Cassanti (2014, p.37) é:

> Uma conduta que cresce a cada dia no meio eletrônico, principalmente nas redes sociais, também conhecidos como "fakes" com o uso não autorizado de imagens de terceiros divulgando conteúdos que atacam a honra e a imagem destes.
> Quem cria perfil falso usando a imagem de outra pessoa viola o previsto na Constituição Federal em seu artigo 5º, inciso X, bem como o direito de personalidade previsto pelo Código Civil.

Qualquer pessoa pode cair no golpe do perfil falso, o mais correto a se fazer é não aceitar de forma alguma pessoas desconhecidas em suas redes sociais, priorizando pessoas da família e amigos mais próximos e nunca misturar trabalho com lazer, saber separar uma coisa da outra se faz importante também no mundo virtual.

2.4 Como se proteger de ataques e crimes virtuais

Antes de falarmos sobre as atitudes básicas para se proteger de ataques virtuais, devemos lembrar que na internet nada é 100% claro e confiável, nem tudo que parece é, assim como no mundo real. As pessoas que aderiram as redes sociais, que são quase o total da população brasileira devem se precaver e estarem cientes dos riscos para que possam se defender de uma forma mais eficaz.

Existem muitas pessoas pensando em fazer o mal para o próximo, mas também existem várias querendo proteger a população, "pensando nisso, diversos órgãos governamentais e privados se dedicam a desenvolver um conjunto de ações visando o uso ético, responsável e seguro da internet no Brasil". (CASSANTI, 2014, p.41)

Podemos ver essas ações em propagandas, revistas, artigos e até mesmo na própria internet que é a grande fonte de disseminação de conteúdo da atualidade, através de blogs e sites especializados.

Manter o computador protegido é sem dúvidas uma das alternativas mais simples e eficazes para a proteção do usuário, e para isso devem ser utilizados antivírus e o manter sempre

atualizado, para que nenhum arquivo seja danificado. “Um estudo indica que 16% dos computadores no Brasil não possuem software contra ameaças virtuais instalado, o que os torna mais vulneráveis a invasões de atacantes e a vírus”. (CASSANTI, 2014, p.42)

Apesar de ser um número considerado pequeno, esses computadores que ainda estão desprotegidos afetam indiretamente aqueles que estão, então o recomendável é que todos os usuários tenham instalados em seu computador esses programas que são armas contra o criminoso virtual.

Utilizar sistemas operacionais e demais programas originais e autorizados é mais um ponto de proteção que deve ser observado. (CASSANTI, 2014, p.42)

As vezes em busca de economia o usuário acaba utilizando uma cópia dos produtos que estão no mercado por serem quase sempre gratuitos, só que o barato quase sempre sai caro quando falamos em segurança digital.

A primeira medida de quem acabou de comprar um computador é instalar o antivírus, pois até mesmo quem não tem nenhuma intimidade com a máquina já ouviu falar no antivírus, que é medida de segurança para qualquer computador.

Segundo Cassanti (2014, p.43):

> Um bom antivírus é capaz de identificar e eliminar phishing (que é um golpe eletrônico, que tem por objetivo ter acesso a dados, como por exemplo o CPF e dados bancários), spyware (é o acesso não autorizado as atividades diárias do usuário que ficam armazenadas em seu computador), rootkit (é um arquivo que tem o objetivo se esconder no sistema para que usuários mal intencionados tenham acesso a todos os dados armazenados) e deve ter ainda sistemas para verificar vírus em e-mails, mensageiros e programas (...)

Um detalhe importante e que muita gente desconhece é que a utilização de mais de um antivírus acaba atrapalhando o desempenho do outro. Muitas pessoas ainda acham que ter mais de um antivírus é sinal de uma maior proteção, mas isso não é verdade, não se deve utilizar mais de um programa. Deve-se manter a atualização de todos os aplicativos do computador em dia em nome do bom desempenho.

Por fim, estar atento aos detalhes é uma dica importante. Sempre que for acessar o e-mail, por exemplo, deve-se evitar clicar em links desconhecidos ou suspeitos, nunca forneça dados e senhas em sites não confiáveis que esteja acessando pela primeira vez, sempre faça pesquisas antes de realizar compras em determinados sites, porque muitos são falsos, crie senhas difíceis e anote-a para evitar o esquecimento.

Nesse sentido Cassanti (2014, p.45) mostra dados curiosos:

> Um estudo divulgado pela empresa de segurança SplashData criou uma lista das senhas mais fracas utilizadas pelos usuários de computadores. A mais usada é a própria palavra *password* (senha em inglês), seguida por 123456 e 12345678. Logo depois aparecem senhas como abc123 e qwert (a sequência das seis primeiras teclas alfabéticas de qualquer teclado). Na lista ainda é possível encontrar as sequências numéricas 111111, 123123 e o nome de Jesus.

Muitas pessoas utilizam também senhas formadas pela sequência dia, mês e ano de nascimento o que é inegavelmente uma senha fácil de ser descoberta, por isso recomenda-se a utilização de senhas fortes e senhas diferentes para cada serviço.

Ao fazer compras pela internet certifique-se que a loja escolhida é bem vista por outros usuários, ou seja, se os produtos realmente chegam e se são de boa qualidade. Nunca compre em sites que não possuam telefone para contato ou nenhuma outra forma de contato caso necessário.

O mercado de vendas pela internet é o que mais cresce no país. “Em 2011, mais de 24 milhões de brasileiros fizeram compras online. Em 2012, o setor faturou mais de R$ 22,5 bilhões, um aumento de 20% sobre o ano anterior”. (CASSANTI, 2014, p.46)

Muitos são os riscos ao comprar pela internet, um deles é comprar um determinado produto e receber outro bem diferente daquele mostrado na imagem, outro comum é estelionatários roubarem os dados do cartão de crédito quando a vítima finaliza o pagamento. Antes de mais nada confie no seu extinto, se achar que a loja ou o vendedor não é de confiança encerre o mais rápido a compra e procure outras lojas virtuais ou outros meios de compra.

Por fim, como pode-se notar, o que mais ajuda na proteção dos usuários da internet é o uso do bom senso, a pesquisa e o cuidado na hora de fazer transações por intermédio do computador. Vale lembrar que mesmo que o inimigo não seja visível, ele pode trazer bastante complicações a vida da vítima.

3 DIFICULDADE DE IDENTIFICAR O SUJEITO ATIVO

Identificar o sujeito ativo dos crimes virtuais é extremamente complexo, tendo em vista que o mesmo não é visto e teoricamente se camufla em meio a tantos outros usuários da internet, com isso a imputação objetiva do mesmo quase sempre não ocorre, pois existem grandes obstáculos frente a necessidade de punição.

Com isso, a solução mostrada é a divisão desses sujeitos por grupos denominados: *Hackers, Crakers, Carders, Lammers, Wannabes, Phreakers e White e Black hats,* para se chegar a uma definição mais precisa de cada um e com isso saber diferenciar quando cada um está agindo.

3.1 Sujeitos ativos dos delitos

Para quem não conhece a fundo a internet em si, existe apenas um tipo de sujeito ativo que comente crimes virtuais, os *Hackers*, pois é o mais comentado no dia-a-dia, porém não sabe que existem outros sujeitos espalhados pelo mundo virtual e que causam bem mais dor de cabeça.

Os hackers são os curiosos, aqueles que sabem muito sobre computadores e passam horas e horas navegando na internet em busca de novas descobertas. Muitos acham que eles são os vilões, confundindo-os com os chamados *Crakers* que serão apresentados a seguir.

Segundo Crespo (2011, p.94): "A definição dada, por um hacker, a tal palavra é no sentido daquele que invade sistemas em benefício próprio, obtendo dados e informações alheias (documentos, programas, músicas etc.), mas sem danificar nada.

Como visto, os *hackers* são pessoas que utilizam o seu grande conhecimento para obter vantagens para si, porém a grande maioria não usa essa habilidade para danificar sistemas e nem lesar pessoas, mas isso não impede que eles também sejam enquadrados em outras

denominações.

Já os Crackers são os verdadeiros causadores dos prejuízos alheios. Eles são inconsequentes, pensam apenas no benefício próprio e gostam de lesar sites, por exemplo, se sentindo felizes com o prejuízo causado a outros.

Nesse sentido Crespo (2011, p.96) conceitua: "O *cracke*r é aquele que, basicamente, 'quebra' um sistema de segurança, invadindo-o. Fanáticos pelo vandalismo, também adoram 'pichar' páginas da *web* deixando, na maioria das vezes, mensagens de conteúdo ofensivo e racista".

Equivocadamente a expressão usada para se referir a quem ataca sistemas e os danifica é *hacker*, porém como demonstrado a palavra correta a ser usada é *cracker*.

Os *carders* são os bandidos do mundo real que praticam crimes também na internet, são aqueles que roubam e enganam pessoas, tirando proveito de diversas situações na busca de vantagens para si. Eles podem agir em conjunto com outros criminosos, apesar de possuírem conhecimento suficiente para agirem sós.

Nessa linha de raciocínio Crespo (2011, p.96) diz:

> Todavia, os *carders* podem agir em conjunto com os *crackers*. Nessa hipótese os *crackers* é que ficam responsáveis pelas invasões e roubos de números, enquanto os *carders* fazem as compras. De qualquer forma, ambos os criminosos precisam ter elevado conhecimento de informática e um mínimo de inteligência, pois os primeiros têm de conseguir invadir os computadores alheios e os outros, além de preencherem os dados em uma página para fazerem as compras, têm de se certificar de que conseguiram uma "conta pirata" (...)

No mundo digital pode-se agir sozinho, mas o mais comum é formação de grupos para se ter um resultado mais rápido e abrangente.

Os *lammers* se auto intitulam *hackers*, mas de *hackers* não têm nada, pois não tem o conhecimento, nem a experiência de um.

São aqueles que são novos nesse mundo, mas já acham que sabem de tudo. "Podem ser comparados àqueles que fazem uma ou duas aulas de artes marciais e já querem bater em todo mundo. Geralmente são insultados e depreciados pelos *hackers*". (CRESPO, 2011, p.97)

Os *wannabe*s ao contrário dos *lammers* já possuem certo conhecimento na área, mas ainda não estão preparados para agirem da forma que os grandes *hackers* agem. "Diferenciam-se dos *lammers* por terem mais consciência do que são capazes de fazer". (CRESPO, 2011, p.97)

Os phreakers são aqueles que possuem amplo conhecimento em telefonia e utilizam esse conhecimento para fazer ligações gratuitas ou para escutar conversas alheias, por exemplo.

"Os phreakers são notórios não apenas por terem marcado – talvez iniciado – a cultura hacker, mas porque alguns phreakers são, hoje, um tanto famosos. Um exemplo? Steve Jobs, o fundador e diretor-executivo da Apple". (ROHR, 2010)

Como exposto, os *phreakers* são intelectuais que escolherem a área a telefonia para atuarem e muitos são conhecidos e bem sucedidos, diferente daquilo que se imagina.

Os *White e black hats* é mais uma maneira de se referir a *hackers* do bem e *hackers* do mal. "As expressões significam, em tradução livre, 'chapéu branco' e 'chapéu preto', e indicam, respectivamente, os bons e maus, aqueles que fazem o bem e os que praticam ações delitivas". (CRESPO, 2011, p.97/98)

Nota-se que existem vários termos para se referir àqueles que tem grande conhecimento em computador e há realmente certos detalhes que diferenciam uns dos outros, porém a maior diferença é a finalidade da ação, ou seja, ajudar ou lesar pessoas.

3.2 Mudanças na legislação

Como já se sabe a nossa legislação encontra sérias dificuldades em acompanhar os avanços tecnológicos, ou seja, a cada dia surge uma novidade no âmbito digital e o legislador não consegue caminhar junto a tais mudanças e o que acaba acontecendo é que crimes são praticados todos os dias através da internet e infelizmente não são punidos e quando são a lentidão se mostra presente.

Apesar da necessidade da tipificação penal de alguns crimes, deve-se ter em mente que a criação de novas leis precisa ser feita com cautela, pois existem um grande número de leis e que não são colocadas em prática, pois para tudo se cria lei no âmbito penal, sem pensar em outras esferas para resolução do problema.

Nesse sentido Crespo (2011, p.161) diz:

> Em tempos onde tudo se torna alvo de leis incriminadoras é preciso ter bom senso e cuidado ao se pretender criar novos crimes. Todos estão exauridos de verificar a enxurrada de tipos penais em nosso ordenamento sem que tragam efetiva contribuição para o convívio em harmonia, para que haja paz social. Isso se dá pela incriminação indistinta de condutas que, no mais das vezes, deveriam ser objeto de políticas sociais mais cuidadosas e de áreas Civil e Administrativa, deixando no ramo Penal como a *ultima ratio*, sempre tão discutida cientificamente, mas que, na prática, não é observada.

Os crimes impróprios que são aqueles que já são tipificados no ordenamento jurídico não são o foco do interesse, mas sim os crimes próprios que são crimes que surgiram através

da internet e que a nossa legislação ainda não abarca, visto que o Código Penal foi criado antes mesmo do advento da internet. E por essa falta de atualização, tais crimes são praticados diariamente e encontra-se impunes, causando a sensação de que na internet tudo pode ser feito e mesmo aqueles atos ilegais passarão despercebidos.

Mudanças deverão ocorrer, porém com cautela. “Nesse sentido, alterações no Código Penal devem ser feitas com muito cuidado e precisão, já que se está lidando com o mais enérgico diploma que pode interferir na liberdade dos cidadãos”. (CRESPO, 2011, p.162)

Ainda que falte muito para se ter controle dos crimes que acontecem na internet e consequentemente punição, há uma preocupação em relação a isso, pois existem projetos de lei referentes ao tema e algumas leis já entraram em vigor.

3.2.1 Leis 12.737/12 “Carolina Dieckmann”

A lei 12.737/12 surgiu após a atriz Carolina Dieckmann ter fotos intimas copiadas de seu computador sem a permissão da mesma e que foram divulgadas na internet. Isso gerou bastante burburinho por se tratar de pessoa pública, mas antes disso acontecer com a citada atriz, havia acontecido outras tantas vezes, só que infelizmente por ter acontecido com pessoas “comuns” não despertou tanto interesse.

Após o ocorrido foi elaborado um projeto de lei (PL 35/12) que deu origem a referida lei que foi sancionada em 03 de dezembro de 2012 e passou a vigorar no dia 02 de abril de 2013. Trouxe alterações ao Código Penal, tipificando condutas cometidas através da internet, tais como: invasão de dispositivo informático alheio, falsificação de documento particular e interrupção ou perturbação de serviço telegráfico.

Segundo Cassanti (2014, p.90/91), os principais pontos dessa alteração são:

> Passa a ser crime o simples ato de interromper (os conhecidos DDoS) os serviços de utilidade pública em mídias disponíveis na internet. Mas atenção: se sua empresa for atacada você deve provar que o serviço prestado é de utilidade pública.
> Os cartões de crédito e débito passam a ser um documento particular. Ações como roubo, adulteração ou falsificação passam a ser regidas por lei existente.
> O simples fato de invadir um dispositivo e obter informações privadas, com ou sem intenção de utilizá-las de forma ilícita, passa a ser crime também. Assim, senhas, documentos sigilosos, conversas particulares e correspondências, se forem encontrados de posse de terceiros, sem autorização, já são indicados como crime, independente de serem ou não utilizados para algo ilícito.
> Desenvolver e distribuir softwares de grampo, escutas ou controle remoto para fins ilícitos também passam a ser considerados crime.

Essa lei gerou e gera até hoje (até mesmo por ser recente) vários comentários e críticas,

um exemplo é em relação a pena que é leve demais, visto que crimes virtuais são crimes que merecem uma maior atenção por trazer junto com eles uma série de condutas danosas graves, quem a pratica não sofrerá perda de liberdade, pois no Brasil penas de até 4 anos de reclusão para crime sem violência é transformada é restrição de direitos.

As penas cominadas aos crimes virtuais provavelmente não fazem com que o estimulo que os criminosos virtuais têm de praticar ilícitos diminua, porém apesar de precisar ainda de ajustes, como textos mais claros e definições mais precisas, essa nova lei mostra a preocupação em se acompanhar o avanço da tecnologia.

3.2.2 O Marco Civil da Internet (12.965/14)

O Projeto de Lei nº 2.126/2011 deu origem a lei 12.965/14, conhecida como o Marco Civil da internet, que veio de uma maneira geral ratificar as garantias constitucionais, com natureza programática, ou seja, estabelecem caminhos para se chegar a finalidade, sendo assim não tipifica condutas criminosas e por isso não tem efetividade real no combate aos crimes virtuais, diferenciando-se assim da chamada Lei "Carolina Dieckmann".

Segundo Cassanti (2014, p.91/92), os direitos e garantias estabelecidos pelo Marco Civil são:

> Remoção de conteúdo: Segundo o Marco Civil, os provedores de conexão à internet não serão civilmente responsáveis por danos relacionados ao conteúdo gerado por terceiros (essas empresas não responderão na Justiça pelo conteúdo publicado por seus usuários. Isso só acontecerá, após ordem judicial, a empresa não tome as providências para tornar o conteúdo indisponível.
> Dados pessoais: O Marco Civil assegura ao internauta o direito ao sigilo de suas comunicações via internet (salvo por ordem judicial); informações claras e completas dos contratos de prestação de serviço; não fornecimento a terceiros de seus registros (...)
> Neutralidade da rede: Este item propõe que o responsável pela transmissão do conteúdo deve tratar de forma igual quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino. É a chamada neutralidade da rede.

Como visto, essa lei como é chamada por muitos como "Constituição da Internet", veio para proteger os interesses dos usuários e não para tipificar condutas criminosas. Não podemos dizer que essa lei não foi importante para assegurar a liberdade expressão e neutralidade na rede e proporcionar que a internet continue avançando a cada dia mais, porém as leis mais importantes para a população brasileira são aquelas que os protegem de forma mais efetiva, fazendo com que não tenham medo de embarcar nessas novas tecnologias. Os brasileiros já se encontram presos dentro de casa por conta do alto índice de criminalidade e

não podem se sentir ainda mais quando o assunto é internet, que é fonte de praticidade, economia de tempo e lazer sem precisar sair de casa e se aventurar por esse mundo repleto de maldades.

3.2.3 Decreto Federal 7.962/13

Esse Decreto Federal que entrou em vigor no dia 14/05/2013, veio com o objetivo de dar suporte ao Código de Defesa do Consumidor, suprindo lacunas relacionadas ao processo de compra e venda pela internet.

Essas novas regras vieram para ajudar os consumidores virtuais, que realmente são muito lesados ao fazerem compras pela internet, pelo fato de existirem inúmeras lojas fantasmas, que vendem e não entregam os produtos, que entregam produtos com defeito ou diferentes daqueles mostrados na imagem e não querem efetuar trocas e muito menos devolução da quantia paga. Diante dessa dificuldade os compradores virtuais se vêm lesados e tem grande dificuldade para descobrirem onde procurar ajuda para resolução de seus problemas.

Passaram a vigorar através do novo decreto as seguintes mudanças:

Os sites deverão disponibilizar o nome da empresa e número do CNPJ, ou do CPF (no caso da venda ser feita por pessoa física), e também o endereço físico e eletrônico, que deverá ser feito da forma mais clara possível, evitando assim que o consumidor tenha dificuldade de identificar o vendedor.

Deverá ser usado todos os meios de comunicação vendedor X comprador, como por exemplo, chat, e-mail e telefone. E alertar os consumidores de forma clara sobre o seu direito de arrependimento da compra, que ressalta-se ser de 07 dias.

As novidades recaem sobre as novas normas para ofertas em sites de compras coletivas. Esses sites deverão agora informar o número mínimo de compradores para que a oferta seja válida, o prazo para utilização das ofertas e endereços e outros dados para facilitação da localização. (CASSANTI, 2014, p.94)

Esse decreto se faz muito importante para coibir as práticas ilegais na internet, diariamente pessoas são lesadas através de sites não confiáveis, através de compras em redes sociais e demais meios de venda na internet.

Recentemente veio a público o caso da modelo goiana apelidada de “Barbie do crime”, que utilizava as redes sociais para criar perfis falsos de vendas de produtos importados. Ela vendia os produtos, porém não os entregavam e com isso centenas de pessoas espalhadas por todo o Brasil foram lesadas, o prejuízo até o momento calculado é de mais de R$ 50.000,00

(cinquenta mil reais).

Diante disso, esse novo decreto se faz necessário para ajudar na luta contra a criminalidade virtual, com todas essas mudanças esses crimes serão pouco a pouco evitados.

3.3 Como combater o crime digital?

O crescente aumento dos crimes virtuais leva a seguinte reflexão: "Quais são as medidas necessárias para se combater tais crimes?"

A mudança na legislação, o uso consciente da internet, campanhas preventivas para alertar a população sobre os riscos na internet, são algumas medidas que se concretizadas farão com que aos poucos haja a coibição desses delitos.

Segundo Peck (2012, p.340) "A primeira medida efetiva de combate ao crime digital tem a ver com a capacidade de prova de autoria, bem como a definição de uma regra clara para a guarda dos dados e *logs* de acesso à Internet ou a caixa postal de e-mail para toda empresa que disponibilizar este tipo de serviço, pago ou gratuito".

Através da identidade digital obrigatória seria mais fácil a identificação do sujeito ativo e com isso a punição, porém não existe lei que torne a identidade digital obrigatória.

Através do IP (número de protocolo único) é possível a identificação do computador usado para determinado ato, porém os criminosos são perspicazes e não utilizam computadores pessoas para prática de contravenções e sim utilizam computadores públicos, como os encontrados em *lan houses* (estabelecimento que possuem vários computadores e que qualquer pessoa pode acessar o que quiser, mediante pagamento). Já existem estados que possuem Lei para Lanhouse, como Alagoas, Amapá, Amazonas, Bahia, Ceará etc, leis essas que obrigam esses estabelecimentos a manterem cadastro de seus clientes. Infelizmente no estado de Goiás não existe nenhuma lei nesse sentido.

Uma mudança importantíssima a ser feita é a educação digital não só com crianças e adolescentes, mas também com adultos e principalmente com os próprios formandos e operadores do direito. É espantoso saber que os novos bacharéis em direito não conhecem os crimes digitais, sabem da existência, mas não estão preparados para lidar com isso em seus escritórios de advocacia. Saber lidar com ferramentas tecnológicas e investir em treinamentos na área é um diferencial nos dias atuais.

A educação digital se mostra importante para que as pessoas saibam quais são os ricos que estão correndo quando acessam o navegador da internet, quando navegam pelas redes sociais, quando publicam fotos e informações pessoais nas mesmas, na medida em que

conhecerem a fundo o ambiente em que estão e os possíveis riscos e formas de proteção, o número de crimes cairá, pois essa é umas soluções mais plausíveis a serem tomadas.

Nesse sentido Peck (2012, p.341) diz:

> Somente com campanhas maciças para a população em geral, com treinamento, com adoção de aulas de 'Cidadania e Ética Digital' como disciplina obrigatória na grade de ensino fundamental e médio, de escolas públicas e particulares, poderemos criar o 'usuário mais protegido e também mais ético', combatendo consideravelmente o crime eletrônico em sua raiz, visto que em muitos casos houve certo desconhecimento, desatenção e negligência do usuário como agente facilitador da conduta.

O esclarecimento dos usuários quanto a como e a quem recorrer, também se faz necessário porque a maioria dos usuários não sabem como registrar um boletim de ocorrência quando se trata de crimes virtuais, até mesmo não sabem que apesar do crime ter acontecido por intermédio da internet, devem recorrer a delegacia de polícia, e em alguns estados já existem delegacias especializadas em crimes virtuais.

A lei 12.735/12 determina que órgãos da polícia judiciária deverão criar setores especializados no combate a crimes virtuais. "Alguns estados brasileiros já possuem essas estruturas. Se você foi vítima de um crime virtual, veja se o seu estado possui uma delegacia especializada; caso contrário, você pode e deve registrar a ocorrência na Delegacia de Polícia mais próxima. O que não pode acontecer é você deixar de buscar orientação policial". (CASSANTI, 2014, p.82)

Em Goiás existe uma delegacia especializada em Crimes Virtuais, é a Gerência de Inteligência da Polícia Civil- Setor de Análise (062) 3201-6352 e 3201-6357. Assim, o estado de Goiás se mostra a frente de outros estados na busca de combater os crimes virtuais.

O Brasil encontra-se empenhado no combate aos cibercrimes, apesar de ainda não ter encontrado o caminho mais eficaz, o país está correndo atrás dos prejuízos. Hoje vemos muito em meios televisivos reportagens que mostram o assunto e dessa maneira deixam os usuários atualizados a respeito do que acontece no mundo virtual, hoje já visualizamos criminosos virtuais sendo presos, o que há tempos atrás não se via.

A legislação também está evoluindo, não na mesma velocidade da internet, porém já se deram conta que é preciso medidas contundentes para o combate.

Leis foram criadas para tipificar crimes que se dão através da internet, tais leis ainda não abrangem todos os delitos, porém já nota-se uma movimentação em prol da segurança virtual.

"Novos artigos relacionados à tipificação dos crimes digitais, bem como o aumento de

pena daqueles em que o ambiente computacional é apenas meio de execução do crime (crimes contra a honra, por exemplo), mas em conjunto com uma alteração (atualização) da Lei de Execuções Penais, para que seja repensado o modelo de cumprimento da pena e reintegração deste tipo de criminoso na sociedade". (PECK, 2012, p.341)

Esse é o caminho a ser percorrido na busca do combate aos crimes virtuais, conscientização dos usuários, implementação nas escolas e universidades de matérias especificas de Direito Digital, a atualização de leis existentes e é claro, a tipificação dos crimes cometidos por intermédio da internet que ainda não são susceptíveis de punição.

CONCLUSÃO

Tendo em vista o crescente número de pessoas que aderem diariamente ao uso da internet, mudando seus hábitos, como por exemplo, o pagamento de contas através do site do seu banco, confiando cada vez mais nas ferramentas digitais deixando assim de tomar os cuidados essenciais para a seguridade na rede e por consequência acabam caindo nas armadilhas dos criminosos virtuais, mostra-se cada vez mais necessário a implementação de medidas educativas para o usuário da internet, seja ele estudante, estudante universitário ou até mesmo operador do direito.

Por se ter tantas pessoas usando essa ferramenta precisa-se encontrar formas de se garantir a segurança das mesmas, garantindo assim o direito de navegar com segurança na internet.

É de suma importância a conscientização dos usuários da internet quanto a conduta digital adequada, na busca de coibir as práticas lesivas, com o uso correto das principais correntes de comunicação, entre ela o e-mail, as redes sociais, os cuidados que devem tomar na divulgação de fotos, informações pessoais, como por exemplo, número de telefone, endereço etc.

Para se encontrar medidas necessárias para o combate aos crimes virtuais, devem ser mudados pontos importantes na legislação, criar campanhas de conscientização, bem como um maior empenho do poder judiciário na aplicação das leis existentes.

Igualmente importante, é relembrar que apesar de muitos acharem que os crimes praticados na internet não são passiveis de punição foi visto que o judiciário está cada vez mais empenhado no esclarecimento e punição desses crimes e que existem projetos de lei esperando aprovação e algumas leis já em vigor tipificando alguns dos crimes existentes.

Conclui-se que é de grande valia abordar um tema tão atual e que trouxe grandes mudanças na sociedade, como também revolucionou o judiciário, pois surgiram novos

caminhos para a prática criminosa e consequentemente se tornou necessário novos meios de coibir essas ações.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei 12.737 de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 12 de out. 2015.

_____. Lei 12.965 de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 12 de out. 2015.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. 1. ed. Rio de Janeiro: Brasport, 2014.

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

GOMES, Helton Simões. "**Pela 1ª vez, acesso à internet chega a 50% das casas no Brasil, diz pesquisa",** 2015. Disponível em: http://g1.globo.com/tecnologia/noticia/2015/09/pela-1-vez-acesso-internet-chega-50-das-casas-no-brasil-diz-pesquisa.html. Acesso em: 12 de out.2015.

INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. 2. ed. São Paulo: Juarez de Oliveira, 2009.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. 2. ed. São Paulo: Atlas, 2011.

LUCCA, Newton de; SIMÃO FILHO, Adalberto. **Direito & Internet**, 1. ed. São Paulo: Edipro, 2000.

MPSP, Ministério Público do Estado de São Paulo. "**Nova lei de Crimes Cibernéticos entra em vigor**", 2013. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR.pdf>. Acesso em: 11 de out. 2015.

PAESANI, Liliana Minardi. **Direito e Internet**. 5. ed. São Paulo: Atlas S.A, 2012.

PINHEIRO, Patrícia Peck. **Direito Digital Aplicado**. 1. ed. São Paulo: Intelligence, 2012

RESENDE, Vanessa; MARTINS, Paula. **Modelo é presa suspeita de aplicar golpes em clientes por redes sociais**, 2015. Disponível em: <http://g1.globo.com/goias/noticia/2015/08/modelo-e-presa-suspeita-de-aplicar-golpes-em-clientes-por-redes-sociais.html>. Acesso em: 11 de out.2015

ROHR, Altieres. "**Segurança para o PC**", 2010. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/05/conheca-os-especialistas-em-brincar-com-telefonia-os-phreakers.html>. Acesso em: 11 de out.2015.

UNI-ANHANGUERA, Centro Universitário de Goiás. **Manual de Elaboração de Trabalhos de Conclusão de Curso**, Goiânia, 2014.

DECLARAÇÃO E AUTORIZAÇÃO

Eu, Patrícia Alves Macedo, portador (a) da Carteira de Identidade nº 5549-236 emitida pelo Departamento Geral da Polícia Civil, inscrito (a) no CPF sob nº 039.873.521-24, residente e domiciliada na rua H 83, Qd. 325, Lt.17, telefone (0xx62) 3277-4630 e (0xx62)8472-9142, endereço eletrônico, declaro, para os devidos fins e sob pena da lei, que o Trabalho de Conclusão de Curso: CRIMES VIRTUAIS FRENTE A FALTA DE LEGISLAÇÃO E EDUCAÇÃO DIGITAL**,** é de minha exclusiva autoria. Autorizo o Centro Universitário de Goiás, Uni - ANHANGUERA a disponibilização do texto integral deste trabalho na biblioteca (consulta e divulgação pela Internet), estando vedadas apenas a reprodução parcial ou total, sob pena de ressarcimento dos direitos autorais e penas cominadas na lei.

_____

Patrícia Alves Macedo

Goiânia (GO), ___ de _____ de _____.