INSTITUTO VALE DO CRICARÉ
FACULDADE VALE DO CRICARÉ
CURSO DE DIREITO

LORENA DE JESUS MELO

CIBERCRIMINALIDADE – OS CRIMES DA ERA DIGITAL

SÃO MATEUS
2019

LORENA DE JESUS MELO

CIBERCRIMINALIDADE – OS CRIMES DA ERA DIGITAL

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade Vale do Cricaré, como requisito parcial para obtenção do grau de Bacharel em Direito.

.

Orientador: Prof.ª Aline Pinheiro Lima Camargo

SÃO MATEUS

2019

LORENA DE JESUS MELO

CIBERCRIMINALIDADE – OS CRIMES DA ERA DIGITAL

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade Vale do Cricaré, como requisito parcial para obtenção do grau de bacharel em Direito.

Aprovado em _____ de _____ de _____.

BANCA EXAMINADORA

_____

PROFª. Aline Pinheiro Lima Camargo
FACULDADE VALE DO CRICARÉ
ORIENTADOR

_____

PROF.
FACULDADE VALE DO CRICARÉ

_____

PROF.
FACULDADE VALE DO CRICARÉ

SÃO MATEUS
2019

A Deus, pois sem ele nada disso seria possível. A minha família, por sempre me apoiar e torcer por mim.

AGRADECIMENTOS

A minha orientadora Aline, por todo o suporte dado durante a elaboração do trabalho.

Aos meus pais, por sempre me incentivarem e dizer que sou capaz. A minha filha, por ser minha companhia durante as madrugadas enquanto eu elaborava essa pesquisa.

Aos meus professores, todos, sem exceção, pois com todo o amor e carinho compartilharam seu conhecimento comigo.

Ao Vinícius, por todo o apoio e auxílio nas minhas idas a biblioteca, sempre me ajudando nas escolhas das doutrinas.

Às minhas amigas, Aline, Genyf, Larissa e Thainara, que acompanharam a minha trajetória desde o início e comemoram comigo essa vitória.

O conhecimento amplia a vida. Conhecer é viver uma ignorância que a realidade impede desfrutar.

Carlos Bernardo Gonzáles Pecotche

RESUMO

A sociedade vive uma evolução constante, e o Direito deve acompanhar essa evolução. Novos mecanismos surgem a todo instante, novas formas de cometer crimes também. Com o surgimento da *internet* e suas facilidades, não seria surpresa que surgissem crimes praticados no ambiente virtual. Logo, viu-se a necessidade do direito acompanhar à nova realidade tecnológica da sociedade. O presente trabalho tem por objetivo analisar o surgimento e a evolução da internet, citando os primeiros crimes de que se tem conhecimento e como ela afeta o dia a dia da sociedade. Cibercrimes e cibercriminosos serão definidos, além de classificar os principais crimes virtuais e os meios utilizados para a pratica de tais delitos. E por fim, será analisado as dificuldades encontradas no ordenamento jurídico para a identificação dos criminosos, e como a legislação nacional e internacional é aplicada nos cibercrimes.

Palavras-chave: Internet. Cibercrimes. Cibercriminosos.

ABSTRACT

Society is constantly evolving, and law must accompany this evolution. New mechanisms are emerging all the time, new ways of committing crimes as well. With the emergence of the Internet and its facilities, it would come as no surprise that crimes in the virtual environment would emerge. Thus, there was the need for law to accompany the new technological reality of society. This paper aims to analyze the emergence and evolution of the Internet, citing the first known crimes and how it affects the daily lives of society. Cybercrimes and cybercriminals will be defined, in addition to classifying the main cyber crimes and the means used to commit such offenses. Finally, we will analyze the difficulties encountered in the legal system for identifying criminals, and how national and international law is applied to cybercrimes.

Keywords: Internnet. Cybercrime. Cybercriminals.

LISTA DE FIGURAS

LISTA DE SIGLAS

WWW	*Word Wide Web*
IRC	*Internet Relay Chat*
JPEG	*Joint Photographics Experts Group*
MP3	*MPEG Layer 3*
CIA	*Central Inteligence Agency*
NASA	*National Aeronautics and Space Administration*
SET	*Secure Electronic Transaction*
ART.	Artigo
IP	*Internet Protocol*

SUMÁRIO

1 INTRODUÇÃO

A internet trouxe consigo a facilidade da comunicação, interação social e praticidade para o dia a dia. A rede é utilizada em diversos campos da sociedade, na educação, no comercio, na política, na ciência e nas demais áreas.

No entanto, com a agilidade e rapidez com que informações são compartilhadas, houve uma grande dificuldade em acompanhar e ter controle das ações realizadas pelos usuários, uma vez que a internet permite o anonimato.

Diante desse mecanismo, diversos crimes surgiram, já que os usuários acreditavam que suas identidades estavam protegidas. E é diante dessa realidade que a abordagem desse tema torna-se importante, pois será discutido até que ponto a legislação brasileira está preparada para lidar com os crimes do mundo virtual.

No primeiro capítulo será abordado como surgiu a *internet* e como foi sua evolução, além de tratar de como ela tornou-se tão essencial para as pessoas. A porcentagem atual de usuários da rede e o surgimento da *World Wide Web*, conhecido como WWW, também será analisado.

A definição de crimes virtuais e cibercriminoso será tratada no segundo capítulo, com definições de alguns autores, como Marcelo Crespo e Ivette Ferreira. A ideia de que somente *hackers* comentem cibercrimes será desfeita nesse mesmo capítulo.

O terceiro capitulo trás os meios de ataques usados por esses criminosos, tanto para a instalação de um vírus, quanto para clonagem de um cartão de crédito. Veremos que com a evolução da *internet*, os usuários descobriram diversas ferramentas para praticar delitos na web. A *Deep Web* é comentada como uma porta a mais para o anonimato, permitindo que crimes como lavagem de dinheiro – utilizando moeda virtual-, terrorismo, tráfico de drogas e a pornografia sejam praticados com ainda mais facilidade.

No último capítulo serão abordados os principais crimes da era digital e como são punidos no “mundo real”. Serão vistos os meios de provas cabíveis, a utilização da criptografia no combate a alguns desses crimes e como a legislação brasileira e a legislação internacional lida com esses delitos. Ainda será comentado a respeito da Convenção de Budapeste, e qual a competência especifica nessas circunstâncias.

1.1 ASPECTOS HISTÓRICOS DA INTERNET

Desde o início da história da humanidade, o ser humano busca criar ferramentas e tecnologias para facilitar o seu dia a dia e executar tarefas, buscando sempre rapidez e agilidade. Diante da segunda guerra mundial e a revolução industrial, o mundo passou por uma grande modificação, a modernidade trazida com esses eventos fez com que a forma de viver e conviver no planeta fossem alterados. Foi proporcionado assim maior interação do homem com a máquina.

Com toda essa evolução, no final do século XX surge a *internet*. A palavra tem como significado “rede internacional”. Seu uso inicialmente era para internalizar as informações em caso de guerras militares e para estudar as relações do homem com as máquinas. Contudo, seu uso era extremamente limitado, e só foi a partir da década de 1990 que a *internet* passou a ser uma ferramenta pública e de fator indispensável para a sociedade. Essa década marca a utilização dessa ferramenta não só por usuários ligados à área de pesquisa, mas agora também pessoas naturais e jurídicas.

Diante disso a sociedade caminhou em direção a uma geração totalmente dependente da informática, substituindo diversos atos do cotidiano pelos sistemas informatizados. Com a rapidez e praticidade com que a *internet* realiza determinadas funções o ser humano cada vez mais prefere as ferramentas virtuais. Sobre isso Maciel Colli posiciona-se:

> [...] O uso da internet possibilitou a superação da dificuldade ocasionada pela distância territorial e pela limitação comunicativa entre pessoas em locais distantes. A voz e o papel foram desbancados do ranking instrumental de intercâmbio de mensagens. O texto exibido na tela de computadores, produtos de linguagem binária interpretada e transmutada pelas plataformas dos computadores, elimina a distância e o tempo. [...] (COLLI, 2010, p.39.)

A internet é um sistema operacional de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina para qualquer outra máquina conectada à rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento.

Com a popularização desse serviço e o aumento de dados, muitos deles pessoais, circulando na rede, ficando a disposição de milhares de usuários que

utilizam a *internet*, faz com que outros usuários utilizem de tais dados de forma maliciosa.

A partir de 1980, ouve a propagação de diversos crimes ocorridos virtualmente, invasão de sistemas, pirataria, pedofilia, transmissão de vírus, são exemplos. Conforme essas práticas foram se tornando comuns, viu-se a necessidade de cuidados com a segurança virtual e com isso ser necessário a intervenção do Estado para regulamentar tais condutas.

Nos anos seguintes começou uma verdadeira revolução tecnológica, o que acarretou um ciclo de mudanças em toda estrutura da *internet*. O cibercrime também iniciou uma nova fase, já que a criptografia utilizada para proteger dados do mundo virtual, tornou-se objeto de atenção de cibercriminosos.

O conceito de crimes informáticos só ganhou conceitos mais específicos algumas anos depois. Damásio de Jesus e José Antônio Milagre explicam que a doutrina ainda diverge sobre qual seria o primeiro crime informático da história, dividindo-se entre dois acontecimentos de duas universidades norte americanas, em que estudantes invadiram o sistema de dados computadorizados das instituições, uma em 1964 e a outra em 1978.

O termo “cibercrime” surgiu no final da década de 90, no momento em que a *internet* se dissipava nos países da América do Norte. Após um encontro em Lyon, na França, um grupo se formou para estudar os problemas da criminalidade surgidos e disseminados via *internet*.

Seja em *noteboks*, *tablets* ou celulares, a frequência com que as pessoas se matem conectadas nesses aparelhos aumentou a cada dia. Muito se cometa sobre dependência digital a nível global, segundo o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic) publicado em agosto de 2019, que o número de brasileiros que utilizam a *internet* continua subindo, atualmente 70% da população tem acesso a rede. E ao longo desses últimos quatro anos, o uso da *internet* vem se expandindo principalmente através das redes móveis.

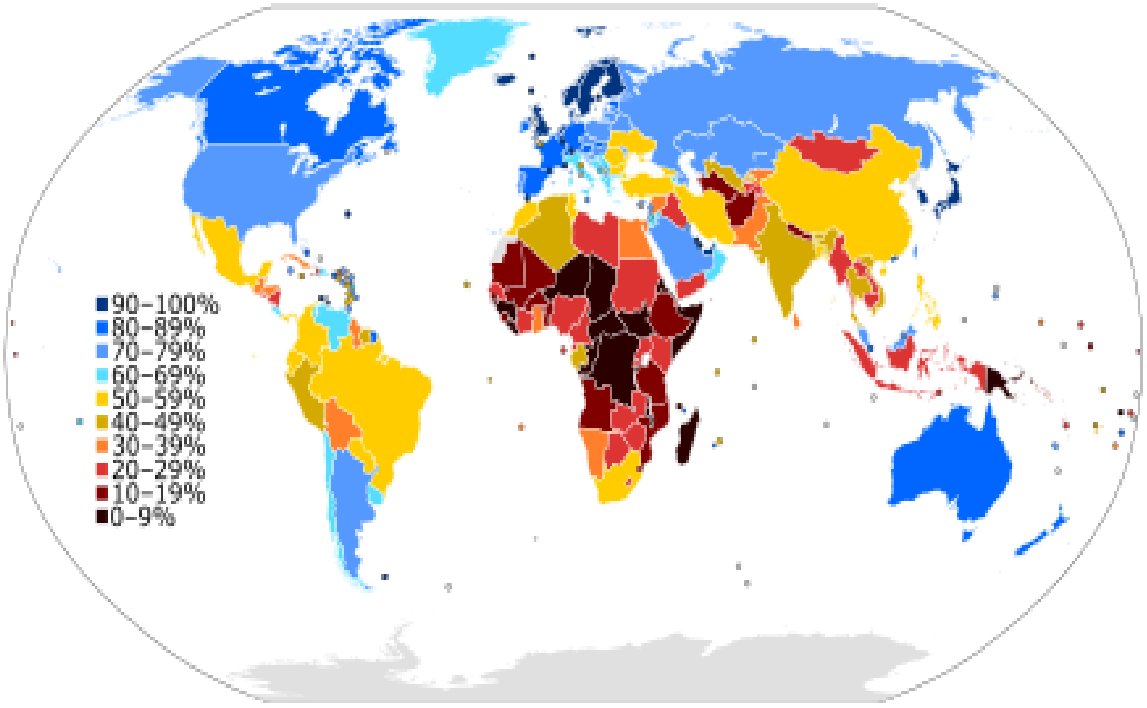

Figura 1: Porcentagem de usuários da internet em relação a população total do país. Disponível em < [*http://wikipedia.moesalih.com/Internet*](http://wikipedia.moesalih.com/Internet)*>*

Devido ao largo espectro de sua abrangência, além de atrair usuários domésticos, a *internet* também atrai um grande número de organizações comerciais conhecedoras das estimativas relativas a suas popularização e capacidade de produzir lucros.

O grande aumento de usuários é fruto, particularmente. Da mudança de conteúdo dentro da rede e também do surgimento de uma interface amigável, e a convergência de computadores e telecomunicações, conhecida por telemática, fruto das inovações do campo tecnológico, culminaram na melhoria da tecnologia de vídeo e de transmissão de dados.

1.2 “WORLD WIDE WEB”

Conhecida também como WWW, a *Word Wide Web* deixou a face da *internet* mais “acessível” e interessante. Ela é a principal responsável por sua popularização; conciliada ao desenvolvimento dos navegadores, ofereceu aos usuários aquilo que mais apreciavam: a utilização da imagem, som e movimento, em vez da melancolia do texto puro.

Tecnicamente seria um sistema de distribuição de hipermídia, e esta, por sua vez, nada mais seria do que um concepção. Com certeza, tal definição é muito confusa e sem clareza. Para melhor conceituar WWW devemos entender o sentido de hipertexto.

O hipertexto foi uma ideia introduzida nos anos 70 pelo visionário Ted Nelson, pesquisador do Instituto Tecnológico de Massachusetts. Seu princípio era, e até hoje é, muito simples. Um documento hipertexto possui palavras que, umas vez selecionadas, direcionam o usuário para outro documento, relacionado aqueles vocábulos. A ideia de Nelson era conectar toda a informação mundial em um sistema gigante de hipertexto, fazendo sua relação dentro de uma base de dados única.

Em poucas palavras, a WWW é um conjunto de padrões e tecnologia que possibilitam a utilização da *internet* por meio dos programas navegadores, que por sua vez tiram todas as vantagens desse conjunto de padrões e tecnologias pela utilização do hipertexto e suas relações com a multimídia, como som e imagem, proporcionando ao usuário maior facilidade na sua utilização, e também obtenção de melhores resultados.

2 CRIMES VIRTUAIS

Da mesma forma como a pratica de crimes comuns vão se aperfeiçoando com o passar do tempo, os crimes virtuais também sofrem mutações com o decorrer do avanço tecnológico que fazem com que suas práticas fiquem mais fáceis. Com mais de 4 bilhões de usuários da rede, fica cada vez mais complicado fazer a identificação dos agentes que comentem crimes na *internet*.

Figura 2: Páginas da internet denunciadas no Brasil. Disponível em < *https://joserosafilho.wordpress.com/2014/03/27/o-que-phishing-e-engenharia-social-ou-como-escapar-de-golpes-na-internet/>*

Apesar de os primeiros relatos de crimes utilizando como meio o computador, foram datados nas décadas de 1960, não há um fato ou data especifica que caracterize o surgimento do primeiro vírus, que foi uma das primeiras modalidades de crimes praticados na internet.

Inclusive, a divergência doutrinária sobre qual seria o primeiro delito. Para uns foi o ocorrido no Instituto de Tecnologia de Massachusetts nos Estados Unidos, cometido por um estudante em 1964. Já para outros, foi na Universidade de Oxford, onde um de seus alunos teria roubado através do computador, informações sobre uma das provas.

Os crimes virtuais podem ter como definição ações destrutivas a sistemas, modificação e interceptação de dados, incitação ao ódio ou descriminação, transferência ilegal de dados, pedofilia, pirataria, terrorismo e dentre outros.
Crespo descreve que:

> [...] As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para os delitos de informática, abuso de computador, fraude informática, em fim, os conceitos ainda não abarcam todos os crimes ligados a tecnologia, e, portanto, deve-se ficar atento quando se conceitua determinado crime tendo em vista que existem muitas situações complexas no ambiente virtual. [...] (CRESPO, 2011)

O conceito de crimes virtuais é recente quando se comparado aos de crimes tradicionais estudados há muito tempo. Krone (2015) definiu crimes virtuais como delitos que vão desde atividades criminosas contra dados até as infrações de conteúdo e *copyright*. Porém para Geese-Zeviar (1998), a definição é mais complexa, e inclui atividades como o acesso não autorizado, a fraude, pornografia infantil e o assédio na internet. E para Ivette Senise Ferrreira crimes cibernéticos são:

> [...] Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial. [...] (FERREIRA, 2005)

Maria Helena Junqueira Reis, em seu livro, *Computer Crimes*, (1997, p.25) ensina “crime informático ou *computer crime* é qualquer conduta ilegal, não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados”.

A verdade é que tal definição não é fácil. Nos Estados Unidos da América e na Inglaterra, o termo informática é desconhecido. Nesses países, o direito de informática é chamado de *computer law* ou de *legal aspects of computers* ou ainda, de *software*

law. Só nos casos de crimes propriamente informáticos, é que os denominam de *computer crimes.*

2.1 OS SISTEMAS OPERACIONAIS

Os Crimes praticados na *internet* necessitam de um complexo sistema de informática. Esse sistema deriva da combinação de três componentes, imprescindíveis para que o computador funcione: *hardware* (os equipamentos), *software* (os sistemas operacionais, linguagens e aplicativos*)* e o *peopleware* (os usuários).

Os *software* são os programas que serão executados no computador, e sua definição legal encontra-se no artigo 1º da Lei n.9.609/1998:

> [...] Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada contida em suporte físico de qualquer natureza, de emprego necessário em maquinas automáticas de tratamento da informação, dispositivo, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para faze-los funcionar de modo e para fins determinados. [...]

2.2 O CIBERCRIMINOSO

Conforme o código penal, são elementos do crime a conduta típica, antijurídica e culpável. E o agente que pratica tais condutas será processado, julgado e punido. O mesmo ocorre com quem pratica esses atos virtualmente.

O cibercriminoso já foi visto por muitos como uma pessoa jovem, já que a *internet* é algo recente. Já outros veem aquela pessoa que possui conhecimento informático mais avançado como um criminoso em potencial.

As pessoas responsáveis pelas práticas desses crimes podem ser tanto aquelas com o conhecimento técnico mais aprofundado, como os *Hackers*, ou qualquer outro usuário da rede que através das suas condutas, comentem crimes contra outros usuários.

2.3 OS HACKERS

Os ataques cibernéticos, praticados pelos *hackers*, iniciaram-se nos Estados Unidos da América e alçaram outros países, inclusive o Brasil. O *hacker* é considerado o intruso do mundo virtual, a invasão dos sistemas por essas pessoas, geralmente deve-se a um mero desejo de demonstração de sua perícia em informática e a curiosidade. Normalmente, não possui um fim ilícito especifico. Porém, sua conduta em si já é considerada ilícita.

O termo *hackers* surgiu por volta de 1960, e era usado para designar as pessoas que se interessavam em programação de computadores. Após o surgimento e expansão da *internet*, o sentido do termo mudou, passando a identificar os invasores de computadores alheios.

O perigo consiste no fato de poder, o *hacker*, descobrir senhas de cartões de crédito, senhas de acesso as contas bancárias e de quebrar as senhas de proteção dos programas comerciais, tornando possível a denominada pirataria. Dessa forma eles violam o sistema de segurança de empresas, tornando seus arquivos acessíveis a quem desejar. Assim foi feito com o código de segurança de DVDs, que foram violados, permitindo que o filme seja compactado em um formato especial, tornando possível seu compartilhamento pela *internet*.

Resta evidente que os usuários, quando efetuam compras ou realizam ações, fornecendo seus dados, desconhecem o que acontecerá com tais informações. Simplesmente são obrigados a confiar em um sistema de segurança da rede.

3 A CRIATIVIDADE DOS INTRUSOS: MEIOS DE ATAQUE

Diante da grande expansão da *internet*, ganharam relevo, em decorrência do seu grande potencial ofensivo, diversas “pragas cibernéticas”, como os *Trojans*, os *worms* de *internet* - como o “Happy99” - e alguns vírus novos que continuam a atormentar a vida daquele que se propõe a navegar na *Web.* Além desses mecanismos existe a engenharia social e o *phishing.*

3.1 VÍRUS

Um vírus de computador é um programa ou um pedaço de código executável que tem habilidade inigualável para se reproduzir, talvez com mais rapidez do que um vírus biológico (dependendo de sua construção), e frequentemente são difíceis de erradicar pois ao serem descobertos, muitos prejuízos já causaram.

Na definição de um programador, dependendo da quantidade de organismos digital, um vírus é um conjunto que pode infectar um programa, alastrando-se para diversos outros. Para isso, ele contém nesse código, instruções que permitem que o programa realize ações que facilitam a infecção de outros programas.

Estar sempre atento para arquivos ou documentos que lhes são remetidos pela internet, é uma das atitudes preventivas que poderão minimizar a contaminação por vírus. O usuário precisa saber que um pouco de profilaxia é amplamente vantajoso em função das consequências que poderão sobrevir pela falta delas.

3.2 WORMS DE INTERNET E WORMS DE IRC

Os primeiros são programas (“vermes”) que se propagam de um sistema para o outro, automaticamente, através de auto reprodução, sem interferência do usuário infectado. Já os *Worms* de IRC, que são os mesmos vermes, que se alastram por meio de canais de bate-papo chamados de *Internet Relay Chat* (IRC). Como exemplo temos o HAPPY99, MELISSA e o ILOVEYOU.

Merece destaque, em razão do ineditismo até então, e do seu poder destrutivo, o *worm* denominado ILOVEYOU, que no dia 04 de maio de 2000 – confiante de boa

fé dos usuários da *internet,* travestido de Carta de Amor – Infectou mais de 45 milhões de computadores em 24 horas.

Nos Estados Unidos grandes empresas como a Ford, a Microsoft e as repartições estratégicas do Exército e Marinha foram atacadas, bem como a *National Aeronautics and Space Administration* (NASA) e a *Central Inteligence Agency* (CIA). Todas tiveram que ficar com suas maquinas fora do ar para que os técnicos pudessem combatê-lo.

O ILOVEYOU também causou grandes estragos na Ásia, Europa e inclusive o Brasil. Por aqui, além da Companhia Telefônica Vésper, foram contabilizados ataques ao sistema federal e ao portal Globo.com. A vítima recebia uma mensagem com um pedido parar que fosse aberto um arquivo anexo com o nome (*love-letter-for-you.txt*). No momento do duplo clique desencadeava-se o processo.

> [...] O vírus que em cinco horas se [sic] havia espalhado pelo mundo inteiro, só poupou as empresas em que a neurose de segurança está acima de tudo. Na sede da Volkswagen, em Wolfsburg, Alemanha, ele foi detectado antes que pudesse causar qualquer estrago. (...) talvez a solução seja a eterna vigilância, como a que se propôs a Volkswagen alemã. O problema é que ao vigiar as mensagens em busca de vírus os administradores de sistemas podem acabar quebrando a privacidade dos funcionários [...] (Revista Veja, 2000)

Inicialmente o malicioso programa destrói arquivos JPEG (imagem digital) e músicas no formato MP3. Numa segunda fase, de auto reprodução, o vírus atinge os usuários do Outlook (*software* da Microsoft, que gerencia o envio e recebimento de mensagens eletrônicas – utilizado por mais de 70% dos computadores do mundo interiro). O ILOVEYOU lê os endereços de correio e armazenamento no computador infectado e auto encaminha para eles. É justamente ai que reside seu potencial destrutivo. Além de acelerada disseminação, o *worm* chega a sua caixa postal indicando como remetente um parente, um amigo, que nem sabe o que aconteceu. Então, o receptor, confiante – pois a mensagem é de origem conhecida – abre o arquivo e se infecta.

Existem várias outras versões do *worm*, igualmente de aparência amistosa. *Joks* (piada), *mother's day* (dia das mães) e também uma outra, em que o programa se faz passar por antivírus.

3.3 TROJANS

Conhecidos como cavalos-de-troia ou *backdoors*, são programas enviados para um sistema anfitrião, costuma ser associado a um “arquivo bonitinho” com música, desenhos animados, piadinhas – e por trás desse “belo cavalo” (um arquivo executável, normalmente *server.exe*) descarrega no seu sistema diversos arquivos que permitem a conexão do computador infectado com o do invasor, sem a necessidade de qualquer autorização. Dessa forma o *cyberpirata* passa a controlar e monitorar quase todas as atividades do usuário hospedeiro.

> [...] Há diversas meios do Trojans se infiltrar em uma rede ou computador domiciliar: Um método comum é o disquete que contenha o arquivo e seja inserido e carregado por um funcionário da própria rede. Nove entre dez incidentes de segurança reportados, são provenientes de fontes internas, e em consequência, um trojan será deliberadamente carregado no sistema. Também existem diversos casos em que profissionais maliciosos de suporte técnico domiciliar ou de rede, ao serem requisitados para reparos em computadores de seus clientes, acabam instalando dissimuladamente os arquivos executáveis do Trojan que mais tarde lhes darão acesso remoto a essas mesmas maquinas. [...] (CONCERINO, 2005)

Uma das formas mais simples de um computador ser contaminado é via *e-mail*. Um *trojan* pode facilmente ser instalado através da recepção de um e-mail malicioso, quando vier com um programa qualquer anexado ao correio eletrônico.

Existem *trojans* que fornecem meios ao intruso para identificar um *login* e também, quando e onde é mais seguro penetrar sem ser descoberto. Como na rede não há nenhum meio de distinguir o usuário legitimo e o invasor, esse acesso torna-se indetectável. Muitos administradores de rede acreditam que empregando um *software* antivírus, não estará em risco e muitas vezes sofrem decepções, pois em sua quase totalidade os Trojans não são virais, e consequentemente nunca poderiam ser detectados por softwares antivírus. Um trojan pode ser um programa legítimo, não há meios desses *softwares* limparem esta ameaça constante, desde que suas “autorias” sejam protegidas por direitos autorais.

3.4 ENGENHARIA SOCIAL

Os crimes envolvendo a engenharia social são mais comuns do que qualquer outro. Envolvendo 70% dos ataques cibernéticos do mundo, além de outros tipos de ataques usarem ele para prover outros, visto que ele busca o meio mais vulnerável da segurança da informação, que são as pessoas.

Engenharia social é a técnica de enganar pessoas para obter delas, dados ou informações, explorando a curiosidade da pessoa, ao contrário de invadir ou usar técnicas de *hackers* no seus computadores ou na rede utilizada. Há um tempo atrás era comum receber ligações como: “A senhora foi contemplada pelo seu plano de saúde, e poderá realizar consultas gratuitamente em qualquer clínica credenciada, para que o benefício seja ativado a senhora precisa confirmar suas informações pessoais”, ou até mesmo “O senhor acaba de ganhar o concurso do Luciano Hulk”.

E-mails como: “Por favor me ajude, sou da África... estou com R$50,000,00 na minha conta mas estou sendo ameaçada...preciso transferir imediatamente esse dinheiro para uma conta no Brasil, que é para onde estou indo. Se houver interesse, por favor entre em contato no meu endereço... e te passarei mais informações.” Os *e-mails* ou ligações são elaborados de acordo com o momento, ou comportamento continuo da sociedade Diante da crise econômica que o nosso pais encontra-se, não é difícil encontrar alguém que certamente responderia esse e-mail e trocaria informações pessoais.

3.5 PHISHING

Phishing é uma forma de fraude onde um *hackers* tenta fingir ser uma pessoa ou uma organização legitima com o intuito de roubar informações.

A palavra é um neologismo criado a partir do inglês *fishing* (pesca) devido a semelhança entre as duas técnicas, servindo-se de isca para apanhar uma vítima. É um dos golpes mais comuns na web, e os cibercriminosos estão constantemente modificando seus ataques para incluir detalhes que farão os usuários acreditarem que o golpe é real. Em uma tentativa de *phishing*, o cibercriminoso pode enviar uma mensagem suspostamente de um site de vendas pedido que a pessoa confirme ou modifique suas informações de conta clicando em um *link*, a partir desse clique no

link, é instalado o *trojan* (visto anteriormente), onde todas as informações digitadas a partir dali são enviadas para o cibercriminoso.

O mesmo pode ocorrer com e-mail de bancos, o infrator faz o parecer tão real quanto possível, e normalmente vem com solicitações de recadastramento de dados bancários ou alteração de senhas eletrônicas, inventando inúmeros motivos para que você atenda a solicitação.

Figura 3- Exemplo de e-mail de Phishing. Disponível em <https://canaltech.com.br/hacker/O-que-e-Phishing-Scam/ >

3.6 A DEEP WEB

Também conhecida como *deep net* ou *undernet,* é a parte da web que não é indexada pelos mecanismos comuns de busca, como Google, Explore e outros, fincando oculta a maior parte dos usuários, que acabam acessando somente a

superfície. É como se a *deep web* fosse um *iceberg,* no qual só temos acesso a ponta, e as demais camadas ficam submersas.

A *deep web* surgiu em 1996, após Paul Syverson desenvolver um *software* livre de rede aberta e capaz de aguentar analises e ataques dos pacotes de dados trafegados para que não fosse possível identificar a origem do acesso. Assim, para cada nova conexão criada, imediatamente surgirá novos “nós” até que alcance o objetivo. Dessa maneira é criado o anonimato, visto o quando difícil é a identificação do usuário.

Muito usuário consideram difícil, e até mesmo perigoso tentar navegar nas profundezas do iceberg que é *a deep web*. Porém, pra outros que já trafegaram e conheceram os meios de acessa-la, não há dificuldade em manter o anonimato. Esses usuários ficam sem nenhuma identificação e sem o controle governamental enquanto está na rede. E nessa “profundezas” da *internet,* que os exploradores sexuais, pedófilos, organizações criminosas terroristas, assassinos de aluguel e até mesmo tráfico de pessoas, armas e drogas costumam se esconder.

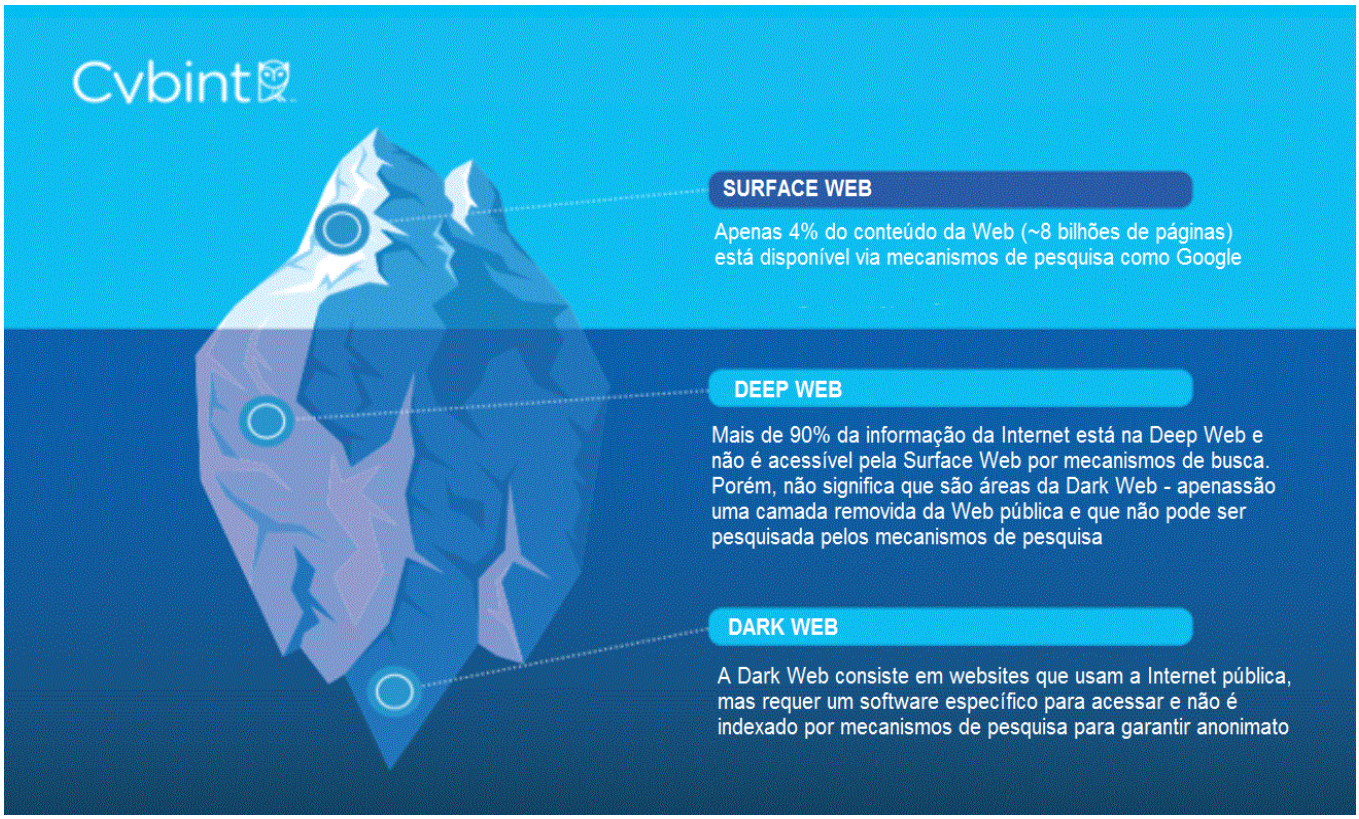

Figura 4 – Deep Web, o iceberg. Disponível em https://www.gta.ufrj.br/ensino/eel878/redes1-2019-1/vf/deepweb/valor.html

Com essa facilidade do anonimato que o usuário encontra ao acessar a *deep web,* logo ela é muito utilizada para arquivar e trocar informações sigilosas que não podem ficar ao acesso de outros usuários. Diante disso, cientistas, jornalistas e militares são exemplos de utilizadores da *deep web* para guardar informações.

Nessa rede ocorrem, diariamente, milhares de compartilhamentos e acessos a conteúdos pornográficos, encomenda de homicídios, compra e venda de armas. Para o pagamento desses serviços, é utilizado uma moeda virtual, um exemplo é a *bitcoin,* permitindo que usuários realizem transações entre si de forma anônima, muitas vezes associadas ao tráfico de drogas. Tal forma de pagamento prejudica a identificação das atividades criminosas, uma vez que tal moeda – *bitcoin* – é mundialmente aceita e não regulamentada, logo não é fiscalizada.

Além dos crimes citados anteriormente, essa moeda facilita ainda mais a lavagem de dinheiro, outro crime ilícito praticado na rede.

4 A INTERNET, OS CRIMES E O DIREITO

Poderíamos dizer que os “crimes” digitais seriam todos aqueles relacionados as informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico.

4.1 OS CRIMES VIRTUAIS

No campo dos crimes virtuais uma vasta gama de infrações penais podem ser cometidas, desde os denominados crimes comuns, até os delitos propriamente de computador, tais como furto de informações confidenciais, o acesso não autorizado a uma conta bancária para a pratica de fraude, crimes de dano, de sabotagem, crimes contra a ordem econômica, criação e inserção de vírus, criação de *sites* de pedofilia e de pornografia infantil, sites incitando o racismo, violações de direitos autorais e usurpação de nomes de domínios.

O “palco” da maior parte desses “crimes” digitais está dentro das facilidades oferecidas pela *internet*. Isso é notório, visto que toda uma comunidade está se desenvolvendo por meio da implementação dessa tecnologia. Além disso, a popularidade da WWW, aliada à possibilidade do anonimato que é dada aos seus usuários, vem fazendo dela um desafio para as autoridades mundiais.

4.1.1 PORNOGRAFIA

Atualmente podemos dividir a pornografia existente na *internet* em três categorias. A primeira categoria é relacionada ao começo da rede, ou seja, usuário interessados em fotografias eróticas de pouca intensidade, e que as tornavam públicas por meio de mensagens nas listas de discussões. Naquele tempo, a rede era utilizada por uma população essencialmente adulta, fazendo com que a publicação dessas fotos não tivesse como finalidade precípua o constrangimento de qualquer pessoa.

Passado esse primeiro momento, com o desenvolvimento tecnológico aliado ao interesse econômico, uma segunda categoria surgiu e começou a se destacar. Nela a tecnologia desenvolvida foi utilizada por empresas baseadas no acesso à pornografia mediante publicações *on-line,* que eram feitas por meio da confecção de páginas eletrônicas disponibilizadas na web. Essas empresas foram responsáveis por inovações no campo da segurança e transações financeiras por meio da *internet,* pois seus serviços só podiam ser acessados depois do pagamento de uma taxa que "destrancava" a porta virtual da página eletrônica, tornando as imagens acessíveis.

A terceira categoria, a mais preocupante, é aquela relacionada à pedofilia e outros matérias obscenos, que variam de rituais macabros a fotos de mutilações. Justamente pelo anonimato e palas técnicas de criptografia, o material pedófilo é disseminado por intermédio de uma comunidade virtual fechada, geralmente sem relação com empresas que cobram pelo serviço. Os integrantes dessa comunidade podem ser chamados de "oportunistas". Aproveitam-se da alta tecnologia para manter oculta a ilicitude de suas transmissões, deixando claro o porquê do grande sucesso da rede nesse contexto, seja devido à facilidade de ocultar, ou ao menos manter anônimo, o ato de capturar o material pornográfico, seja pela habilidade de importação de imagens sem ser rastreado ou deixar "pistas".

A lei 13.718 em seu artigo 218-C, traz que:

> [...] Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena – reclusão de 1 (um) a 5 (cinco) anos, se o fato não constituir crime mais grave. [...]

Todas as condutas descritas são encontradas na *internet*, em *sites* pornográficos. Na rede, encontra-se fotografias eróticas ou pornográficas, envolvendo crianças e adolescentes. É indubitável que tais imagens e ilustrações pornográficas, se enquadrarão, conforme o caso, ou no art. 234 do Código Penal ou no Estatuto da Criança e do Adolescente.

> [...] Art. 234 - Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno:

> Pena - detenção, de seis meses a dois anos, ou multa.
> § 1º. Incorre na mesma pena quem:
> I - vende, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo; [...]

No caso de sites que cobrem pelo acesso ao material obsceno o que ofereçam serviço de remessa periódica de fotos pornográficas, através do correio eletrônico, mediante pagamento, aplica-se o parágrafo único, do inciso I, do art.234, do Código Penal.

4.1.2 PIRATARIA DE *SOFTWARE*

A pirataria de software consiste na apropriação e venda de cópias de programas de computador sem a licença do autor, estando regulada no Brasil pela Lei n. 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador e a sua comercialização no país. É possível, atualmente, fazer uma cópia perfeita de um programa de computador em meios de mídia, como em um CD. Feita tal cópia, também há necessidade da replicação de toda embalagem e manuais do programa, objetivando maior autenticidade. A cópia da embalagem e do manual é muito mais cara que a cópia do programa em si.

A web entra nesse contexto como grande alternativa para o barateamento do processo de duplicação, pois por meio dela é possível distribuir sem a necessidade de quaisquer “meios físicos” e embalagens. No Brasil e demais países latino-americanos, para termos um parâmetro dessa realidade, a pirataria é responsável por um rombo de mais de 1,1 bilhão de dólares. A taxa de pirataria é superior a 80% dos programas vendidos, perdendo apenas para os países asiáticos.

Saliento que a rede possibilita a aquisição de uma vasta gama de programas, muito destes chamados de *freeware* e *shareware.* No primeiro o autor ou detentor dos direitos autorais licencia a utilização destes para uso público sem que haja necessidade de pagamento, e no segundo a gratuidade está restrita a um período de experiência.

Podemos dizer que a *internet* é um mecanismo perfeito para a obtenção de programas, sejam estes sofisticados ou simples. Mas como esse “pirata” atuaria na pratica? Tomaria vantagem da *internet* para oferecer cópias ilicitamente, permitindo

que compradores tenha acesso ao programa duplicado mediante provedores diversos. Alguns desses “piratas” seriam até idealistas, distribuindo copias através da *internet* gratuitamente, sem ônus algum, sob o pretexto de que a indústria de programação teria lucros exorbitantes.

É importante enfatizar que os maiores problemas relacionados a pirataria na *internet* residam justamente na facilidade de distribuição proporcionada por ela. Existem, e existirão cada vez mais países-refúgios para “piratas” que desejem distribuir ilegalmente programas, vídeos, filmes, músicas e textos a qualquer indivíduo conectado na rede.

4.1.3 CARTÕES DE CRÉDITO

Da mesma forma que no cotidiano, os pagamentos feitos pela internet podem ser realizados através de vários mecanismos, como a troca de dinheiro, o débito em conta, a utilização de cartões de cartões de crédito e outros. Dentro dela, a maneira mais popular para efetuação de pagamento é o cartão. Atualmente estão sendo desenvolvidos muitos meios visando a constituição e consolidação do “dinheiro eletrônico”, tais como o *e-cash* e os bancos via internet (internet banking), ampliando a capacidade da utilização de moedas pela rede.

No caso das fraudes a cartões de crédito, temos como núcleo da ação a intenção de enganar o titular do cartão para obter informações necessárias para seu débito. Isso, porém, não acontece somente na internet, mas também no mundo real. É simples, quando verificamos que cartões de crédito passe pelas mãos de garçonetes, balconistas, recepcionistas, vendedores etc., sendo perfeitamente possível que algum deles venha anotar as informações necessárias do cartão para praticar algum ato ilícito.

As companhias de cartões, reiteradamente, alertam seus clientes sobre o custo dessas fraudes, um prejuízo dividido por meio do pagamento de taxas de anuidade, de juros e outras despesas. Mas o que difere a internet do mundo real é o esconderijo proporcionado aos fraudadores. A maioria das transações relacionadas aos cartões de crédito ocorre sem a percepção de seu titular. Uma vez preenchida a autorização

de débito pela rede, o titular do cartão não tem nenhum meio de determinar com quem está fazendo negócio.

A partir daí começas os abusos. Recebidas as informações necessárias, os cibercriminosos debitam do cartão sem remeter o bem comprado, e até mesmo debitam dele várias vezes, simplesmente desaparecendo após tais práticas. Podem, eventualmente, processar o pedido de maneira exata, mantendo porem detalhes sobre o cartão de crédito para eventual fraude futura, talvez até vendendo o número do cartão parra quadrilhas organizadas para esse tipo específico de fraude.

O interessante, e o mais comum, é que a fraude quanto ao cartão não se limita ao comerciante. Pelo fato de a internet, até agora, em termos, não ser particularmente segura, é possível que transmissões sejam interceptadas, e o número do cartão, consequentemente, também. A explicação é simples: o provedor a qual o servidor está conectado é o local responsável pelo processamento de todo o correio eletrônico e das páginas eletrônicas. Toda pagina carregada ou transmitida, ou seja, armazena temporariamente dentro do sistema. A partir disso, o administrador do provedor, ou quem tiver acesso a ele, pode facilmente ler o conteúdo dessas páginas, podendo até mudá-lo.

As empresas vem aconselhando, devido a fragilidade dos mecanismos de segurança na *internet*, vêm aconselhando, em alguns casos, seus clientes a não informar detalhes sobre seu cartão por meio da *web*. Parra evitar tais problemas, essas empresas vêm desenvolvendo mecanismos que implementem a segurança, como a tecnologia da criptografia. É possível citar o a utilização de um mecanismo chamado *Secure Electronic Transaction* (SET), sinônimo de “transação eletrônica segura”, que funciona como uma máscara para os dados enviados pela internet, somente o transmissor e o receptor poderão compreender os dados intercambiados pela rede.

4.1.4 AMEAÇA

Através da *internet*, pode, ainda, ser cometido o crime de ameaça. Encontra-se o crime, capitulado no artigo 147, do Código Penal: “Ameaçar alguém, por palavra,

escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave. Pena de detenção de 1 (um) a 6 (seis) meses e multa.”.

. Sua conduta é a de ameaçar alguém, por palavra, escrito, gesto ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave.

Como se trata de um crime formal, seu momento de consumativo ocorre no instante em que a vítima toma conhecimento do mal prenunciado, independente de sentir-se ameaçado ou não. Portanto, é apodítico que o correio eletrônico enviado a vítima, com ameaça do mal injusto e grave, consubstancia o crime de ameaça na modalidade escrita, vinculada através da *internet.* Mesmo a modalidade simbólica pode ser utilizada através da *internet*, já que, com uso de *scanners* e *softwares* gráficos, é possível enviar fotos ou desenhos intimidativos, configurando o crime de ameaça.

4.1.5 CONTRA A HONRA

Os crimes contra a honra são a injuria, a difamação e a calunia, que encontram-se capitulados nos arts. 138, 139 e 140 do Código Penal.

> [...] Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa. [...] Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. [...] Art. 140 - Injuriar alguém, ofendendo lhe a dignidade ou o decoro: Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa. [...]

Tais crimes listados, violentam a honra objetiva e subjetiva da vítima. A honra objetiva é a reputação da vítima, a sua moral perante a sociedade. Por honra subjetiva, entende-se o sentido da pessoa, a respeito da sua conduta moral e intelectual. Essa diferenciação é importante, pois, tanto a calunia, quanto a difamação, atingem a honra objetiva da vítima: a injuria ofende a honra subjetiva da vítima.

Na calúnia, o agente ativo atribui a vítima, a pratica de fato definido como crime. Na difamação, o agente ativo atribui fato ofensivo à reputação da vítima. Na injuria, o agente ativo propala qualidade negativa da vítima, em relação aos seus atributos morais, intelectuais ou mesmo, físicos.

É obvio que tais infrações penais podem ser cometidas através da *internet.* Na internet, os crimes contra a honra são muito frequentes, principalmente nas redes sociais. As pessoas excedem-se nos comentários e acabam atingindo a reputação alheia, e nesses casos, os autores estarão sujeitos as consequências criminais e civis.

Em qualquer caso de injuria, calunia ou difamação que possa provocar a responsabilidade civil ou penal para o ofensor, a vítima precisará comprovar os fatos. Como em qualquer ação judicial, é necessário provas para gerar a condenação. Nos casos ocorridos na internet, na maior parte das vezes, a prova é simples e fácil, que é possível gravar o texto, salvar a imagem, o vídeo ou som que represente o ato, podendo ser feito diretamente pela vítima ou pro outra pessoa que tenha conhecimento do fato.

4.1.6 CYBERBULLYING

O Cyberbullying é a pratica do *bullying,* atos de violência física ou psicológica que ocorrem de maneira intencional e repetida, como intimidação, exposição vexatória, humilhação, perseguição e difamação pelo meio virtual, através de celulares, *tablets* e computadores, utilizando de redes sociais, *e-mails* e aplicativo de mensagens. Cassanti define o cyberbullying como:

> [...] A ação intencional de alguém fazer uso das tecnologias de informação e comunicação pra hostilizar, denegrir, diminuir a honra ou reprimir consecutivamente uma pessoa. Contrário do tradicional e não menos preocupante bullying, que é presencial, ou seja, as ações do agressor têm lugar certo, no cyberbullying o agressor não consegue presenciar de forma imediata os resultados da sua ação, minimizando um possível arrependimento ou remorso. [...] (CASSANTI, 2014)

A incidência maior desse crime ocorre entre os adolescentes, porém o número de jovens e adultos que praticam esse ato criminoso veem aumentando consideravelmente.

Podem ser considerados como cyberbullying ações como divulgação de fotografias intimas, exposição de fotografias ou montagens constrangedoras, críticas a aparência, à opinião e ao comportamento. O autor geralmente utiliza de perfis falsos (*fakes*), pois acreditam estar totalmente protegidos no anonimato, e ocorre no mundo virtual pelo fato de não ter que encarar a vítima pessoalmente.

Os perfis e *e-mails* falsos das redes sociais, utilizados com a intenção se manterem “protegidos”, podem facilmente serem identificados através do seu IP. O IP é pode ser revelado através de uma investigação policial autorizada pelo poder judiciário.

O cyberbullying é passível de punição por meio do Código Penal, quando configura os crimes contra a honra (calunia, injuria e difamação). A punição pode chegar até 4 (quatro) anos de reclusão. Na esfera civil, os criminosos podem ser condenados ao pagamento de indenização por dano moral. No caso de menor de idade, o responsável responde pelos crimes.

4.1.7 LAVAGEM ELETRONICA DE DINHEIRO

O tráfico de dinheiro é um dos maiores exemplos de crime organizado. A produção, distribuição e a venda podem até ser complexas, mas não são comparáveis ao processamento do dinheiro ganho com essa atividade parra ser utilizado por esses criminosos.

Essas divisar ilegais entram pela *internet* ou por outra rede de contas e companhias e empresas, e em seguida, são transferidas rapidamente para outras contas, e assim sucessivamente. Enquanto o dinheiro obtido pelo traficante da esquina é considerado “sujo”, ele é posteriormente legitimado por uma complexa serie de transações bancárias, dentro de uma rede eletrônica, até que chegue, aparentemente “limpo”, as mãos do chefe. A “lavagem” de dinheiro é feita por meio de um complicado mecanismo de transações em cadeia, que dificultam em muito seu rastreamento. O dinheiro acaba misturado com fundos de investimento legítimos, que à primeira vista são completamente legais.

A lavagem está baseada em uma cadeia de rápidas transações envolvendo mais do que a mera movimentação para fora do pais, para fora do controle jurisdicional, tornando o seu rastreamento e controle quase impossível. Esse dinheiro deveria ser tributado e confiscado, por ser resultado de atividades imorais e ilegais. O governo deveria. Por intermédio de suas instituições, rastrear e processar os responsáveis por tal lavagem. Porém, trata-se de um tarefa muito difícil. Para que

esses criminosos sejam processados é necessária a explicação de todas as transações que representam a rápida transferência de fundos legais em juízo.

O envolvimento de computadores e redes nessas lavagem de dinheiro acarreta o aparecimento de características únicas dentro desse processo. Primeiro porque um criminoso pode usar computadores para gravar, carregar e até estabelecer um controle da complexa rede de transações que envolvem tais atividades. Quanto mais “enrolada” fica essa rede, mais difícil identificá-la, entendê-la e explica-la, mas, por outro lado fica também difícil para o criminoso controla-la e utilizá-la. A utilização de poderosos computadores e programas para o entendimento dessa cadeia complexa de relações supera, muitas vezes, a compreensão do homem.

Na Era da Informação, a tecnologia digital está intimamente relacionada com tal situação. Os bancos, por exemplo, transferem dinheiro de suas contas por meio de arquivos digitais. A transmissão é feita pela utilização de um formato criptografado internacionalmente, irreconhecível por terceiros. É exatamente ai que resido o maior perigo.

Primeiramente devido ao fato de os próprios criminosos utilizarem esses sistema de segurança para ocultar suas transações ilegais, Segundo, todo o sistema de segurança pode ser quebrado. Organizações criminosas pode obter acesso a sistema bancários contratando *hackers* profissionais no assunto, ou, até mesmo, torturando, sequestrando ou forçando funcionários e administradores do sistema do banco a lhes dar acesso. A Lei nº 9.613, de 3 de março de 1998 discorre que:

> [...] Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente de infração penal. Pena: reclusão de 3 (três) a 10 (dez) anos. [...]

O rápido crescimento da *internet*, aliado ao fato de ela oferecer cada vez mais oportunidades para a aquisição de bens de consumo. Evidenciam a potencialidade de materialização de tais crimes, o que culmina na necessidade de implementação da sua segurança.

4.1.8 CONTRA O CONSUMIDOR

Nos dias atuais o comercio eletrônico é uma realidade. Os fornecedores ampliam, cada vez mais, a publicidade e a comercialização de seus produtos e serviços através da *internet*, podendo, em certos casos, suas condutas tipificarem infrações penais, previstas no código do consumidor. Tais condutas, violadoras da lei, vinculadas através da internet, constituem-se, como define, com muita propriedade, Erenberg em seu livro Publicidade Patológica na Internet à Luz da Legislação brasileira, em publicidade patológica. Ele divide a publicidade patológica em publicidade enganosa, publicidade intrinsecamente abusiva e publicidade extrinsecamente abusiva:

> [...] A publicidade enganosa é aquela que oferece produtos ou serviços inexistentes ou que oferece produtos ou serviços, mediante informações falsas ou omissão de informações relevantes sobre eles. De igual modo, constitui publicidade enganosa, a oferta de produtos, por preços que não serão praticados. A publicidade intrinsecamente abusiva é aquela em que a publicidade vem mascarada como noticia ou informação. Nesses casos, a publicidade apresenta-se com semelhança editorial, gráfica e visual a um texto informativo sobre determinado assunto. Também constitui publicidade intrinsecamente abusiva, a omissão de dados do fornecedor, a exploração de situações desfavoráveis ao consumidor e a publicidade contraria à moral, os bons costumes a à lei. Já a publicidade extrinsecamente abusiva, é a que impõe mensagem publicitaria na tela do usuário, sem que tenha ele, procurado por ela. Outra forma de publicidade extrinsecamente abusiva, é a de obstrução da saída do usuário de um determinado *site.* [...]. (ERENBERG, 2003)

O art. 37 do Código de defesa do consumidor traz que:

> [...] É enganosa qualquer modalidade de informação ou comunicação de caráter publicitário, inteira ou parcialmente falsa, ou, por qualquer outro modo, mesmo por omissão, capaz de induzir em erro o consumidor a respeito da natureza, características, qualidade, quantidade, propriedades, origem, preço e quaisquer outros dados sobre produtos e serviços. É abusiva, dentre outras a publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, se aproveite da deficiência de julgamento e experiência da criança, desrespeita valores ambientais, ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança. [...]

O Código de Defesa do Consumidor, em seu art. 37, preconiza ser proibida toda publicidade enganosa e abusiva. É enganosa, qualquer modalidade de informação ou comunicação de caráter publicitário, inteira ou parcialmente falsa ou por qualquer outro modo, mesmo por omissão, capaz de induzir em erro o consumidor a respeito da natureza, características, qualidade, quantidade, propriedades, origem,

preço e quaisquer outros dados sobre o produtos e serviços. É abusiva. A publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, se aproveite da deficiência de julgamento e experiência da criança, desrespeite valores ambientais ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança.

4.2 O DIREITO

A facilidade que a *internet* oferece para a pratica crimes, deixou os juristas completamente assarapantados. É evidente que no combate aos crimes virtuais a justiça utiliza o Código Penal, pois, a grande maioria de infrações penais cometidas na *internet*, pode ser capitulada nas condutas criminosas prevista em tal código. Sobre isso Gabriel Cesar Zaccaria de Inellas comenta:

> [...] Como promotor de justiça criminal que sou, sei que infelizmente, os criminosos são mais rápidos que os legisladores. Isso acontece em todo o mundo e o Brasil não é exceção. Ainda mais, em se tratando de Internet, que passou a ser largamente utilizada em nosso pais há pouco tempo e que possui peculiaridades que outros meios de comunicação não tem. [...] (DE INELLAS,2009)

O professor Túlio Lima Viana, em seu trabalho apresentado perante a Faculdade de Direito da Universidade Federal de Minas Gerais, em Belo Horizonte, no ano de 1999, intitulado dos crimes por computador, ensina que “Nosso objetivo aqui será, principalmente, o de despertar nos operadores do direito o interesse pelo estudo interdisciplinar da ciência jurídica e da informática, como forma de coibir os crimes cometidos com o auxílio de computadores. Tais crimes apresentam-se de várias formas destacando-se dentre eles a violação dos direitos autorais sobre softwares, o furto de tempo e de dano causado pelos famosos vírus do computador”.

A lei é, e sempre será, essencial para a prevenção e punição dos crimes, sejam estes dentro do mundo material ou digital A lei visa determinar a conduta humana dentro de determinados princípios, possibilitando a pacificação social. É por meio dela que o imoral e as atividades destruidoras podem ser prevenidos, gerando um Estado onde os integrantes dessa sociedade possam atuar. Se não houvesse limites, seria difícil assegurar que alguém não invadisse a esfera pessoal de outrem.

Atualmente, tirando as raras exceções, existem leis, tanto no Brasil como em outros países, suficientes para coibir crimes praticados com o auxílio do computador. Porém, serão criados “crimes” cada vez menos “óbvios”, e as leis existentes não preencherão tais lacunas de maneira eficaz. A maioria dos crimes digitais encontram-se tipificadas em nossa legislação. O furto de componentes de computador não deixa de ser furto. A lavagem de dinheiro não deixa de ser crime. Ameaça é ameaça. Sejam esses crimes cometidos por meio da internet, ou de outros mecanismos tradicionais, são crimes previstos na lei. O problema está em outros pontos. No surgimento de crimes complexos, novos, específicos, como o cyberbullying, cujo controle passa a ser necessário.

Além disso o anonimato oferecido pela *internet* faz com que as incidências de provas seja mínima.

4.2.1 A OBTEÇÃO DE PROVAS

O Código Civil, no art. 225 traz que a utilização de provas eletrônicas não é proibida.

> [...] As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão. [...]

O usuário ao utilizar a rede mundial de computadores recebe uma identificação virtual conhecida como IP (*internet protocol*). O IP é o principal protocolo de interação da *internet*, e é responsável por direcionar os pacotes de dados que trafegam na *web*.

O IP é fornecido ao usuário por meio de um provedor de acesso, que disponibiliza data, hora e fuso horário do sistema. Todos esses elementos não essenciais para a verificação do sigilo de dados. É por meio do provedor de acesso à *internet* que após a determinação judicial é possível verificar o sigilo de dados informáticos que associe o endereço de IP disponibilizado ao usuário na data e hora que ocorreu delito ao seu endereço físico.

Existem diversas dificuldades de investigação nos crimes praticados na *internet,* o advogado Daniel Alla Burg especialista em crimes virtuais em uma entrevista à revista jurídica Conjur (Consultor Jurídico) diz:

> [...] A internet facilita a impunidade, uma vez que a investigação é mais complicada e, muitas vezes, quando é identificado o autor, já ocorreu a prescrição. Isso sem contar na questão de fronteira: o crime pode ser cometido por alguém que está em outro país, com leis completamente diferentes. A fronteira acaba motivando também, de certa forma, a impunidade. E aqui, infelizmente, não tem muito o que fazer. Porque não tem como criar lei obrigando o cidadão da Estônia a vir para o Brasil no prazo. [...] (BURG, entrevista à revista Conjur, em 2017.)

A utilização do IP não é a melhor forma de rastrear um cibercriminoso, porém a única forma de controlar o aumento da criminalidade virtual é o Direito, pois tem como objetivo punir as condutas ilícitas e deter o caráter imperativo por meio de leis.

4.2.2 CRIPTOGRAFIA E LEGISLAÇÃO

Para os governos a criptografia é algo que dificulta a tarefa de detectar e rastrear criminosos quando enviam comunicações sigilosas. Antes do advento da *internet,* as atividades que envolviam criminosos em países diferentes, como o tráfico de drogas, exigiam o cruzamento de fronteiras, o que criava provas.

> [...] Os governos temem que os terroristas possam agir à solta, que os traficantes de drogas façam seus negócios livremente. Que malfeitores de todos os tipos planejem crimes e lavem dinheiro sujo na rede [...] Enquanto os governos são impotentes para detê-los ou vigiá-los. [...] É concebível que os terroristas possam atacar um banco ou uma instalação do governo de um lugar seguro em um país estrangeiro, fora do alcance da lei, e provocar o caios de longe. [...] (DYSON, Esther. 1998)

Nos Estados Unidos, um pais líder em tecnologia, no qual o Brasil muitas vezes se espelha para tomar suas decisões em relação a determinado uso da tecnologia, a criptografia é considerada arma, constando na lisa de munições e no Regulamento Internacional de Vendas de Armas.

Atualmente, o ordenamento jurídico do Brasil comporta normas, técnicas e procedimentos com escopo de instituir um sistema de certificação digital baseado em chaves públicas. O decreto n. 3.587, de 5 de setembro de 2000, que instituía a

Infraestrutura de Chaves Públicas do Poder Executivo Federal (ICP-Gov), estabelece normas básicas para a implantação do uso da criptografia de chaves públicas pela Administração Pública federal, com o intuito de conferir segurança às comunicações eletrônicas entre os entes administrativos, prevendo ainda uma futura e progressiva substituição dos documentos físicos por meios eletrônicos.

Sem a criptografia, o que as pessoas enviam por computador é algo equivalente a um cartão postal, uma mensagem aberta para ser vista por muitos enquanto em trânsito. Com a criptografia as pessoas podem colocar tanto mensagens como dinheiro em envelopes eletrônicos, assegurando que o conhecimento do que está sendo enviado não possa ser acessado por qualquer outra pessoa.

Por que precisamos da criptografia na grande rede? Por vários motivos, dentre eles;

- tornar original uma mensagem enviada por *e-mail*, mediante assinatura digital;
- tornar documentos pessoais inacessíveis e, assim, privados.
- verificar a fonte provedora de um arquivo que está sendo copiado; em outras palavras, tornar o *download* mais seguro;
- proteger transações financeiras;
- habilitar o fluxo de caixa digital na *internet*;
- proteger a propriedade intelectual;
- evitar opiniões ilegais e puni-las;
- proteger a identidade e privacidade de todos;

A criptografia é uma necessidade do crescimento e desenvolvimento da rede. Por meio dela será possível alcançar um ambiente mais seguro. Como em qualquer sociedade existem criminosos impunes devido à ineficiência das autoridades estatais. É impossível o poder estatal ter o controle de toda a sociedade, sobretudo da internet, onde a grandiosidade, o anonimato e a velocidade são realidades incontestáveis.

4.2.3 LEGISLAÇÃO APLICÁVEL

Atualmente podemos dizer que a legislação atual do Brasil por si só, abrange uma grande parte do crimes praticados na *internet*. Mesmo que não haja uma

exemplificação, os artigos do Código Penal tipificam as mesmas condutas, e logo podemos aplicá-las analogicamente ao caso concreto.

Diante disso, viu-se uma grande necessidade da criação de Leis especificas para garantir maior eficácia do judiciário no combate aos crimes cibernéticos. Assim, duas leis que tratam sobre os crimes da *internet* foram sancionadas em 2012, modificado o Código Penal e instituindo penas para crimes específicos da era digital.

A primeira delas é a Lei 12.737 de 2012, a lei dos Crimes Cibernéticos, conhecida como Lei Carolina Dieckmann. Ganhou esse nome pois durante sua criação ocorreu o incidente com a atriz, que teve seu computador invadido, e suas fotos intimas foram divulgadas. A lei tipifica atos como invadir computadores (*hacking*), violar dados de usuários, interrupção ou perturbação de serviço telegráfico, telefônico ou informático, roubar senhas e divulgar informações privadas (fotos, mensagens e etc.). Além disso, tipifica condutas que até então não eram tratadas como crime.

Apesar de ter ganhado espaço na mídia devido o caso com a Carolina, o texto já era discutido pelo sistema judiciário e financeiro diante do volumoso número de golpes e roubos de senhas pela internet.

Os parágrafos 1º e 2º do art. 154- A da Lei Lei 12.737 de 2012 diz que:

> [...] Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. [...]

Como é possível notar, a lei prevê que a invasão ao dispositivo como o intuito de adulterar, obter ou destruir dados, é infração penal com pena de 3 (três) meses a 1 (um) ano, porém não traz por exemplo os casos de bisbilhotagem, em que o autor tem por intuito apenas acessar dados para o proveito próprio ou para chantagear a vítima, e como consequência, distribuir esses arquivos roubados. Então, se o autor não violar nenhum dispositivo de segurança, não haverá crime.

> [...] Eu tenho um medo muito grande no processo de criação de leis. Vejo ainda que leis que tratam de áreas específicas como a tecnologia, acabam recebendo muita influência de empresas que possuem algum tipo de interesse. E grandes provedores de internet no Brasil, possuem representantes de relações governamentais, que visam impedir que algumas leis sejam aprovadas junto ao Congresso. Agora, na hora de se criarem leis técnicas, apesar de muitas colaborações que recebem, acabam criando previsões que não são inúteis ou são impossíveis de ser realizadas. Como por exemplo, a Lei Carolina Dieckmann, que possui artigos tão específicos, que muitos crimes podem não ser enquadrar. [...] Quando se trata de questão criminal, temos que ser pontuais, não podemos fazer analogias e interpretações em desfavor do réu. [...] (PERES. Entrevista dada a Isadora Marina. 2017)

Foi sancionada em 2014, a lei 12.965, conhecida como o Marco Civil da I*nternet,* que visa regulamentar o uso da rede por meio de princípios, garantias, direitos e deveres para os usuários. Ele protege os dados pessoais e a privacidade dos usuários. Dessa forma somente mediante ordem judicial poderá haver a quebra de dados e informações particulares que existem na redes sociais ou em sites.

O projeto surgiu com a resistência à Lei de Azeredo (12.735/2012), como uma proposta do Poder Executivo da Câmera dos Deputados, e foi aprovada em 2014. É conduzida a partir de princípios como o da reserva jurisdicional, da neutralidade, da responsabilidade dos provedores e entre outros. O Art. 2º da Lei 12.965 de 2014, discorre que:

> [...] A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I - o reconhecimento da escala mundial da rede;
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III - a pluralidade e a diversidade;
> IV - a abertura e a colaboração;
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI - a finalidade social da rede. [...].

Uma das grandes inovações dessa lei é a possibilidade de retirada de conteúdo do ar. Antes de sua entrada em vigor, não havia nenhuma regra clara sobre este procedimento. A partir da Lei do Marco Civil da *Internet,* a retirada de conteúdo só é feita mediante ordem judicial, com exceção dos casos de pornografia de vingança. As vítimas de violação de intimidade podem solicitar a retirada de conteúdo, de forma direta, aos sites ou serviços que possuam esse conteúdo.

Ambas as Leis foram de extrema importância para impor obrigações e responsabilidade civil aos provedores e usuários.

4.2.4 LEGISLAÇÃO INTERNACIONAL APLICÁVEL

O Concelho da Europa em 2001 aprovou a convenção de Budapeste também conhecida como Convenção do Cibercrime. Tratando de crimes praticados pela *internet*, a convenção é uma referência legislativa mundial, sendo assinada por 43 países e ratificada por 21 nações signatárias. Diferente dos Estados Unidos, França, Japão, Espanha e Canadá por exemplo, o Brasil não assinou o tratado.

> [...] Os Estados membros do Conselho da Europa e os seguintes Estados signatários. [...]Reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada no combate à cibercriminalidade, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias da informação; Acreditando que uma luta efetiva contra a cibercriminalidade requer uma cooperação internacional em matéria penal acrescida, rápida e eficaz; [...] (Convenção de Budapeste, 2001).

Na convenção foi determinado procedimentos de investigação que obrigava fornecedores de serviços informáticos a conservar imediatamente os dados de tráfego, e deverão comunicar às autoridades investigadoras dados informativos que fossem necessários pra identificar o cibercriminoso. Além de tipificar os cibercrimes como; infrações de sistema; os crimes que envolvem pedofília; infrações relacionadas aos crimes com computadores; e também tipificar violações de direitos autorais.

Atualmente são poucos os países que possuem legislação especifica para crimes virtuais, além da maioria dos crimes virtuais serem cometidos fora dos países no qual reside o criminoso.

A orientação do direito internacional é que primeiramente o autor seja acusado e processado em seu pais, o que na maioria das vezes é impossível, pois a maioria não possui leis específicas que definam a natureza penal do delito. E se o crime atingir outro país o cibercriminoso deverá ser extraditado, de acordo com a forma legal daquele país.

4.2.5 COMPETÊNCIA JURÍDICA

A Lei 12.965 de 2014 estabelece os princípios, garantias, direitos e deveres para o uso da internet no Brasil além de determinar as competências em relação a matéria.

> [...] Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.
> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I - o reconhecimento da escala mundial da rede;
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III - a pluralidade e a diversidade;
> IV - a abertura e a colaboração;
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI - a finalidade social da rede. [...]

Em seu art. 18 parágrafo 3º:

> [...] As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais. [...]

Determinando que os juizados especiais são os responsáveis pelas decisões sobre a ilegalidade ou não dos conteúdos. Isto é aplicado nos casos de ofensa a honra, que serão tratados da mesma forma como os que ocorrem fora do da rede.

A fixação da competência independe do local do provedor de acesso ao mundo virtual, sendo considerado o lugar de consumação do delito. Já nos casos de crimes como violação de privacidade o atos que atinjam bens, interesses ou serviços da União ou de suas empresas autárquicas ou públicas, a competência é da Justiça Federal, assim como os crime previstos em convenções internacionais.

CONCLUSÃO

Conclui-se que é de extrema importância o tema, visto que a tecnologia avança a cada dia, passando por uma grande evolução e expandindo-se cada vez mais. Os crimes mencionados merecem uma atenção especial, uma vez que a *internet* se tornou parte essencial do cotidiano da sociedade, necessitando de normas especificas que regulamentem tais delitos.

No primeiro capitulo nota-se que com o surgimento da internet, e com os primeiros crimes virtuais cometidos, as denominações como cibercrime e cibercriminoso tiveram que ser criadas. E que com o aumento de pessoas conectadas a rede, e a diversidade de crimes que foram surgindo, foi necessário a intervenção do Estado no mundo virtual.

No segundo capitulo é trazido os primeiros crimes virtuais de que se tem notícia. Há também o conceito de crime virtual pelos olhares de alguns autores conceituados. Desconceitua também que cibercriminoso é necessariamente alguém com conhecimento técnico em informática, mas que pode ser qualquer usuário comum que utiliza da *internet* e pratica qualquer uma das condutas tipificadas no Código Penal.

No terceiro capitulo foi abordado o meio que os cibercriminosos utilizam para praticar os seus crimes, seja por vírus, *worms, trojans, phishing,* engenharia social e a *deep web.* A *deep web* é trazida como uma facilidade a mais no cometimento de crimes virtuais, visto que a dificuldade de identificar os agentes é muito mais difícil. Aborda também, a utilização da moeda *bitcoin* no mercado negro e na lavagem de dinheiro eletrônico. Fato este que potencializa a necessidade de regulamentação e fiscalização do Governo.

No quarto capitulo são arrolados os principais crimes cometidos na rede. Desde a pornografia até os crimes cometidos contra o consumidor. Mostrando como há diversos delitos que podem ser praticados através de uma conduta na rede, suas descrições no Código Penal e suas penas. Além de trazer o *cyberbulliyng,* que é o bulliyng praticado no mundo virtual. Além de abordar a dificuldade da produção de provas que facilitem a identificação do agente. Também vemos como podemos tipificar e punir esses criminosos, utilizando o Código Penal e as Leis especificas que já foram criadas.

A fragilidade e instabilidade da *internet* é fato gerador para o aumento dos crimes. É essencial a criação e divulgação de políticas de prevenção contra esses crimes, tanto por parte das empresas quanto do Estado.

E é de extrema necessidade a criação de normas especificas que tratem de forma mais eficaz os atos cometidos no mundo virtual, mesmo que já existam algumas Leis, nota-se que as mesmas ainda não são suficientes.

Por fim, nota-se que o Direito Penal precisa alcançar de forma mais plena as mudanças que a sociedade vem passando frente a evolução tecnológica. O Estado deve oferecer uma restituição da ordem social, para evitar o aumento da criminalidade virtual e ao mesmo tempo acompanhar a evolução da internet.

REFERÊNCIAS

BRASIL. **Lei nº 9.609, de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasil, Brasília, 19 de fevereiro de 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9609.htm#:~:targetText=L9609&targetText=LEI%20N%C2%BA%209.609%20%2C%20DE%2019,Pa%C3%ADs%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias.> Acesso em: 19 de novembro de 2019.

BRASIL. **Lei nº 13.718, de 13.718 de 24 de setembro de 2018**. Tipifica os crimes de importunação sexual e de divulgação de cena de estupro. Diário Oficial da República Federativa do Brasil. Brasil, Brasília, 24 de setembro de 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm#:~:targetText=Praticar%20contra%20algu%C3%A9m%20e%20sem,n%C3%A3o%20constitui%20crime%20mais%20grave.%E2%80%9D> Acesso em: 19 de novembro.

BRASIL. **Lei nº 9.613, de 3 de março de 1998.** Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores. Diário Oficial da República Federativa do Brasil. Brasil, Brasília, 3 de março de 1998. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9613.htm#:~:targetText=LEI%20N%C2%BA%209.613%2C%20DE%203%20DE%20MAR%C3%87O%20DE%201998.&targetText=Disp%C3%B5e%20sobre%20os%20crimes%20de,COAF%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias.> Acesso em: 19 de novembro de 2019.

BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Diário Oficial da República Federativa do Brasil. Brasil, Brasília, 7 de dezembro de 1940. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm> Acesso em: 19 de novembro de 2019.

BRASIL. **Lei n º 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Diário oficial da República Federativa do Brasil. Brasil, Brasília, 10 de janeiro de 2002. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm > Acesso em: 19 de novembro de 2019.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da República Federativa do Brasil. Brasil, Brasília, 30 de novembro de 2012. Disponível em: <

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 20 de novembro de 2019.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da República Federativa do Brasil. Brasil, Brasília, 23 de abril de 2014. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm#:~:targetText=LEI%20N%C2%BA%2012.965%2C%20DE%2023%20DE%20ABRIL%20DE%202014.&targetText=Estabelece%20princ%C3%ADpios%2C%20garantias%2C%20direitos%20e,uso%20da%20Internet%20no%20Brasil.> Acesso em 19 de novembro de 2019.

BRASIL**. Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasil, Brasília, 13 de julho de 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8069.htm> Acesso em: 19 de novembro de 2019.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasil, Brasília, 11 de setembro de 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8078.htm> Acesso em: 20 de novembro de 2019.

CASSANTI, Moises de Oliveira. **Crimes Virtuais, Vitimas Reais.** Rio de Janeiro: Brasport, 2014

COLLI, Maciel. **Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos**. Curitiba: Juruá Editora, 2010, p. 39.

CONCEIÇÃO, Arthur José. **Direito & Internet: Aspectos jurídicos relevantes**, 2 ed. São Paulo: Quartier Latin, 2005.

CONCERINO, Arthur José. **Cybercrimes**. São Paulo: Quartier Latin, 2005. p.161.

Convenção Sobre o Cibercrime. **Convenção de Budapeste** de 23 de novembro de 2001. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf > Acesso em :17 de Novembro de 2019.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 3. Ed. São Paulo. Saraiva, 2007.

ERENBERG, Jean Jacques. **Publicidade patológica na internet à luz da legislação brasileira.** São Paulo. Juarez de Oliveira, 2003**.**

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo. Saraiva, 2011.p.48

BURG, Daniel Alla. **Revista Conjur**, 2017.

DYSON. Esther. **Release 2.0 A Nova Sociedade Digital**. São Paulo. Campus. 1998.

DE INELLAS, Gabriel Cesar Zaccaria. **Crimes na internet**. 2. ed. São Paulo. Juarez de Oliveira, 2009.

FERREIRA, Ivette Senise**. Direito & Internet: Aspectos Jurídicos Relevantes**. 2 ed. São Paulo. Quartier Latin, 2005, p.261.

FILGUEIRAS, Isadora Cavalli de Aguiar; LIMA, Thaís Soldera de. **CIBERCRIME**. Encontro de iniciação cientifica, ETIC 2015, ISSN 21-76-8496

JESUS, Damasio de; MILAGRE, José Antônio. **Manual de Crimes Informáticos**. São Paulo. Saraiva, 2016.

KRONE, Tony. **High Tech Crime Brief.** Australian Institute of Criminology. Canberra, Australia. ISSN 1832-3413. 2005

PERES, Fernando. **Entrevista concedida a Isadora Marina C. de Almeida Pagnozzi**. Curitiba, 1 de novembro de 2017.

REIS, Maria Helena Junqueira. ***Computer Crimes.*** Belo Horizonte.1997, p.25.

Revista Veja, nº1649, ano 33, nº20, de maio de 2000. Editora Abril, p.166.

ROVER, Tadeu, **"Internet facilita crimes e dificulta investigação, estimulando a impunidade".** Disponível em < https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais > Acesso em 17 de novembro de 2019.

VIANA, Túlio Lima. **Dos Crimes por computador.** Universidade Federal de Minas Gerais, Belo Horizonte. 1999, p.4.

ZEVIAR-GEESE, G. **The State of the Law on Cyberjurisdiction and Cybercrime on the Internet**. California Pacific School of Law. Gonzaga Journal of International Law. Volume 1. 1997-1998.