UNIVERSIDADE TUIUTI DO PARANÁ

CRISTIANO AUGUSTO GUIMARÃES OLIVEIRA

DIREITO PENAL E CRIMES CIBERNÉTICOS

CURITIBA

2017

CRISTIANO AUGUSTO GUIMARÃES OLIVEIRA

DIREITO PENAL E CRIMES CIBERNÉTICOS

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade de Ciências Jurídicas da Universidade Tuiuti do Paraná como requisito parcial para a obtenção do título de Bacharel.

Orientador: Prof. Dr. Rafael Torres

CURITIBA

2017

TERMO DE APROVAÇÃO

CRISTIANO AUGUSTO GUIMARÃES OLIVEIRA

DIREITO PENAL E CRIMES CIBERNÉTICOS

Este trabalho de Conclusão de Curso foi apresentado à Coordenação do curso de Direito da Universidade Tuiuti do Paraná – UTP, para que seja julgado e aprovado para a obtenção do título de Bacharel em Direito.

Curitiba_____de_____2017

_____

Prof. Dr. PhD Eduardo de Oliveira Leite

Coordenador do Núcleo de Monografias

BANCA EXAMINADORA

_____

Prof. Dr. Rafael Lima Torres

Orientador

Universidade Tuiuti do Paraná – UTP

_____

Professor (a) Examinador (a)

Universidade Tuiutido Paraná - UTP

_____

Professor (a) Examinador (a)

Universidade Tuiuti do Paraná - UTP

AGRADECIMENTOS

Meus mais sinceros agradecimentos à minha mãe, a qual sempre esteve e está comigo durante a caminhada nesta vida que não se mostra fácil, mas que se soubermos apreciar encontramos momentos de deleite, por sua prestatividade, sempre dando apoio, sendo uma mãe amiga, que sabe o momento de exigir, mas também sabe o momento de dar carinho, por seus conselhos de vida, que são como uma inspiração para mim, por sua destreza em lidar com os problemas do dia a dia e me ensinar a enfrenta-los.

Agradeço também à minha querida e amada avó, a qual me incentivou desde o primeiro momento ao ingresso na faculdade, dando palavras de apoio, contribuindo financeiramente no pagamento de mensalidades, me proferindo também palavras de vitória, das quais me recordo plenamente, para que um dia essa conquista fosse possível, pelo seu esmero para comigo, deixo a ela meu mais sincero agradecimento.

Também agradeço ao meu bom Deus, por ter me dado forças para conseguir concluir esta caminhada, a qual não foi nada fácil, mas que sempre esteve comigo, mesmo nos momentos em que pensei que iria desistir ou fraquejar, mas me sustentando em suas mãos, me mostrou que na minha fraqueza eu sou forte.

Gostaria também de agradecer aos meus familiares, que me apoiaram também, tanto emocionalmente quanto financeiramente, gostaria de agradecê-los a todos pois sua ajuda foi de grande valia sem dúvida alguma.

Agradeço também a todos os amigos que fiz durante o período desse curso, e que não foram poucos diga-se de passagem, os mesmos me fizeram sorrir, me fizeram ter ânimo nos momentos tristes e de alguma forma contribuíram para que eu aqui chegasse.

Deixo também agradecimento a todos os professores em especial ao professor Rafael Torres por me orientar neste presente trabalho e que a mim ministraram aula durante estes anos à fio, sem o conhecimento destes não seria possível a compreensão das ciências jurídicas de forma tão eficaz, desta forma deixo o meu agradecimento especial a todos estes.

Por final, mas não menos importante, agradeço à Universidade Tuiuti do Paraná – UTP a qual me acolheu para que eu cursasse e me graduasse em sua instituição de ensino.

Dito isto, deixo por assim escrito o meu muito obrigado da forma mais sincera possível a todos estes do fundo de meu coração.

Dedico este trabalho à minha querida mãe, Wilma Sueli, a qual durante estes anos à fio vem me incentivando nos estudos de forma incansável, com o intuito de me fazer galgar passos inimagináveis, dedico também à minha falecida avó, a qual sonhava em ver-me formado desde o primeiro dia que iniciei o curso de Direito. Deixo a elas e à Deus o meu agradecimento verdadeiro.

“Hoje os ‘lobos’ mudaram os meios, mas não as práticas”

Lélio Braga Calhau

RESUMO

Com o advento da era digital, o ser humano buscou adaptar-se para melhor usufruir deste tipo de tecnologia, sendo gerado um novo ambiente no qual grande parte da população mundial moderna se utiliza todos os dias, com o advento da internet e do computador deu-se início ao acesso direto aos ambientes virtuais. Com esses recursos, infelizmente há indivíduos que se utilizam para a prática de atos ilícitos nestes ambientes, assim como no mundo real o Direito existe para manter a prática do justo e do correto e manter um padrão de convivência entre os seres humanos, punindo assim aqueles que ousam cometer atos criminosos. O cenário atual não poderia ser pior, o ser humano tem visto atos criminosos sendo praticados virtualmente de forma espantosa e em larga escala, tamanha é a ousadia destes criminosos. Isto é algo extremamente preocupante, pois mesmo sendo praticado em um ambiente virtual, esse tipo de crime tem impacto diretamente na vida real, tanto da vítima quanto de terceiros. Desta forma, faz-se necessária uma tutela por parte do Direito para o combate deste tipo de crime de forma eficaz.

A presente monografia possui como intuito abordar a temática de como ocorre um crime virtual, a forma que este é praticado, suas principais características, e principalmente a ótica do Direito Penal e da legislação tanto nacional quanto internacional em se tratando da tipificação e da punibilidade deste tipo de crime, com a análise da legislação e a aplicação direta da mesma , as dificuldades para ocorrer a eficaz punição do autor do crime, sendo também utilizados termosvirtuais para uma eficaz compreensão por parte do leitor de como ambiente virtual funciona.

Palavras Chave: Direito Penal, Crimes Cibernéticos, Tecnologia, Ambiente Virtual, Internet, Legislação

ABSTRACT

With the advent of the digital era, the human being looked to adpt himself to enjoy this type of technology, being generated a new environment wich most part of the modern population uses everyday, with the advent of the internet and the computer it started the direct access to virtual environments. With these resources unfortunately there are individuals who are using it to the practice of unlawful acts on these environments, as in the real world, the law exists to keep the practice of the fair and the correct and keep a pattern of coexistence between human beings, punishing then, those who dare to commit criminal acts. The current scenario couldn't be worse, the human being have seen criminal acts being practiced virtually in a terrible way and in large scale such is the audacity of the criminals, this is something extremely worrying, because even though its practiced in a virtual environment, this type of crime has direct impact both of the victim and of third parties.So it is necessary a guardianship by the law to fight this type of crime in an effective way.

The present monograph aims to addres the issue of how virtual crime occurs, the form it is practiced, it's main characteristics, and mainly, the view of Criminal Law, national and internacional legislation, in relation to the criminalization and punishability of this type of crime, with the analysis of the legislation and the direct aplication of it. The difficulties of effective punishment of the perpetrator of the crime and virtual terms are also used for an effective understanding on the part of the reader of how the virtual environment works.

Keywords: Criminal Law, Cyber Crimes, Tecnology, Virtual Environment, Internet, Legislation.

SUMÁRIO

INTRODUÇÃO

Na contemporaneidade em que o ser humano vive é evidente que as tecnologias avançaram muito, nos últimos tempos as pessoas estão cada dia mais interligadas umas com as outras ao redor do planeta, através dos dispositivos tecnológicos. A internet nunca foi tão necessária e a utilização de dispositivos tecnológicos, tais como smartphones, computadores, notebooks, tablets, dentre muitos outros se tornou fundamental, assim como o acesso constante à rede mundial de computadores, popularmente conhecida como internet.

Os usuários acessam através destes dispositivos os ambientes virtuais, os quais permitem a interação e relação entre as pessoas, para as mais diversas atividades, mas, assim como no mundo real, existem pessoas de má conduta, as quais se aproveitam para cometer crimes neste ambiente virtual. O Direito deve moldar-se para garantir que juntamente com esta nova era digital a lei esteja amparando e regrando todas as condutas que sejam praticadas nestes ambientes, com o intuito de combater de forma eficiente a criminalidade.

O presente trabalho tem por objetivo apresentar e explicar o que são e quais são os principais crimes praticados nos ambientes cibernéticos, discorrendo também sobre a ótica do Direito Penal quanto a prática destes crimes, sendo este embasado em obras de diversos autores, além de contar com pesquisa em sítios da internet, apresentando a forma com que o Direito Penal lida com as condutas criminosas perpetradas no ambiente virtual.

Este trabalho busca sanar dúvidas, tais como: O que é um crime cibernético? Quais são os principais crimes cibernéticos? De que forma o Direito Penal combate esta prática criminosa? A legislação tem punido esta conduta ilícita? Perguntas fundamentais para a compreensão e discernimento acerca do tema,

O primeiro capítulo do presente trabalho apresenta o surgimento do computador e da internet, a forma com que foram criados e os objetivos, o avanço da tecnologia, assim como a criação do ambiente virtual suas características e funções.

O segundo capítulo tem a função de realizar uma apresentação acerca dos crimes cibernéticos, explicar o seu conceito, suas características, o uso dos computadores, sistemas e principalmente da internet, além de demonstrar quais são os principais praticantes desta conduta criminosa neste espaço.

O terceiro capítulo procura explicar quais são as principais formas desta conduta criminosas ser praticada, exemplificando e detalhando, além de apresentar a legislação e como se dá o combate a esta prática ilícita nos termos da lei.

O quarto capítulo busca demonstrar a forma com que o Direito Penal observa este crime, a conduta, a legislação, a criação de novas leis a competência para o julgamento deste crime e a necessidade da intervenção no ciberespaço. O quinto capítulo busca apresentar as formas de defesa e combate do crime virtual por parte dos usuários dos ambientes virtuais com a intenção de prevenir e alertar acerca das ameaças deste crime que podem afetar todos os usuários deste ambiente.

1. ADVENTO DO COMPUTADOR E DA INTERNET

O ser humano evoluiu à medida que o tempo passou, desde os primórdios de sua existência, vem buscando encontrar formas que facilitem a convivência em sociedade, é sabido que para uma melhoria de vida em um grupo a comunicação é de fundamental importância, desta forma em um processo de evolução ocorreram várias evoluções e também inventos o qual levou o ser humano até o alcance da era tecnológica.

Durante o século XX deu-se início à uma era de grandes avanços tecnológicos, formas de comunicação foram aperfeiçoadas, tais como o computador, o qual teve início à sua era no ano de 1943, e criadas, como a internet tendo seu desenvolvimento no ano de 1969, após ser popularizada a internet evoluiu gradativamente e tornou-se indispensável na vida das pessoas, assim como o computador.

O computador atrelado à internet fez com que a evolução tecnológica ultrapassasse os limites e sendo difundida pelo mundo em uma velocidade sem precedentes, fazendo com que a vida das pessoas tivesse seu cotidiano mudado seja nos campos da sociedade seja nas formas de comunicação, tudo isto com o intuito de tornar a vida das pessoas mais fácil tanto na agilidade das comunicações, quanto na facilidade de realizar atividades.

Sendo possível realizar compras de diversos gêneros, realizar transações bancárias, estudar e muitas outras atividades, isto tudo sem ao menos se dirigir a outro local ou sair de casa, devido a praticidade estas ferramentas digitais apresentam ao ser humano imensas oportunidades.

1.1 DA ORIGEM DO COMPUTADOR

O computador se trata de uma máquina tecnológica que facilita diversas atividades humanas, como seu próprio nome cita é um aparelho que computa ou calcula.

Tendo em vista a complexidade de sua construção e a tecnologia que fora empregada para sua criação ser limitada para a época que foi iniciada sua construção, este era muito diferente da forma que nós o conhecemos da forma que é hoje em dia, houveram diversas transformações necessárias para que este fosse aperfeiçoado,

sua engenharia foi estudada, a matemática ajudou muito e a eletrônica também teve sua participação.

Todas elas foram cruciais para que este dispositivo fosse construído, diversas pessoas tiveram uma função essencial para que este fosse criado, desta forma o mesmo não possui apenas um inventor, existem formas que dividem a história dos computadores em gerações, pois separam as ferramentas que foram utilizadas e os métodos de construção. São 4 as gerações que marcam a criação do computador,que abrangem o príodo de 1951 a 1959.

Quando foram criados, os computadores de primeira geração, estes funcionavam através de válvulas e circuitos eletrônicos, estes eram imensos e muito pesados, temos como exemplo o *Eletronic Numerical Integrator and Computer* (ENIAC) em português Computador Integrador Numérico Eletrônico, sua construção foi para uso militar, consumia uma quantidade grande de energia em torno de 200 quilowatts. Já na segunda geração que ocorreu entre os anos de 1959 e 1965 os computadores funcionavam por meio de transistores deixando a utilização das válvulas sendo que estas foram consideradas um grande avanço para a época pois os transistores faziam as operações de forma muito mais rápida que as válvulas além de começarem a ser usados comercialmente neste mesmo período.

A terceira geração dos computadores se caracterizou pelos circuitos integrados que fizeram a substituição dos transistores pois estes circuitos possuíam um tamanho menor que os transistores e também uma capacidade de processamento maior, dando-se início à criação dos chips e sua utilização em computadores pessoais, aumentando a expansão de seu uso no mundo.

Mas na quarta geração é onde vemos o computador realmente se popularizar no planeta, a medida em que o computador se desenvolveu o mesmo reduziu seu tamanho e aumentou exponencialmente a velocidade do processamento de dados, nesta geração ocorre o aparecimento dos microprocessadores os quais consumiam muito menos energia.

Com a chegada dos sistemas operacionais deu-se o desenvolvimento dos computadores de mão os quais são smartphones e tablets, celulares inteligentes que executam atividades similares ao computador e também realizam chamadas de

telefone, além do acesso à rede mundial de computadores, atualmente o ser humano encontra-se na quarta geração.

A computação de bolso tem passado a ser realidade e se faz presente na vida das pessoas cada vez mais, estes podem ser carregados no bolso do usuário por serem portáteis, sendo estes os celulares também conhecidos como smartphone e tablets, os quais executam diversas tarefas e também sistemas operacionais próprios, sendo estes, tendência para o futuro.

FIGURA 1 – EVOLUÇÃO DOS COMPUTADORES

FONTE: HISTÓRIA..., 2017, disponível em: <https://www.todamateria.com.br/historia-e-evolucao-dos-computadores/>

1.2 A CRIAÇÃO DA INTERNET E SUA FUNÇÃO

A internet, também conhecida como rede mundial de computadores, foi criada na época da guerra fria, possuía fins militares, assim como o computador, seria utilizada como um meio alternativo de comunicação do exército norte americano caso os meios de comunicação convencionais da época fossem destruídos em ataques promovidos pelos inimigos.

Assim, foi criada a ARPANET (*Advanced Research Projects Administration* – Administração de Projetos e Pesquisas Avançados), esta foi a primeira rede nacional de computadores, criada em 1969 pelo departamento de defesa dos Estados Unidos da América tendo a função de conectar os computadores dos centros de pesquisa, universidades e principalmente instituições militares americanas, fazendo assim com que se compartilhasse informações, pesquisas e estratégias militares, no ano de 1972 o governo apresentou a internet à sociedade.

Também com a ideia de difundí-la nas universidades americanas passando a conectar os computadores respectivos aos centros de pesquisa, no ano de 1980 esta passou a adotar o protocolo aberto (TCP IP) *Transmission Control Protocol - Internet Protocol* , em português Protocolo de Controle de Transmissão - Protocolo de Internet que realizava uma conexão de sistemas heterogêneos.

Fazendo assim com que a rede fosse ampliada para que pudesse ser acessada por diferentes equipamentos, tais como super computadores, microcomputadores *workstations* e *mainframes* mas foi no ano de 1983 que ocorreu uma separação da aplicação da internet na área civil e militar e foi aí que realmente surgiu a definição internet.

No ano de 1991 a *World Wide Web* (WWW) em português: rede mundial de computadores, é lançada, a qual permitiu que imagens, vídeos e sons fossem transmitidos pela rede, pois até este ponto a internet poderia transmitir apenas textos, assim a internet popularizou-se entre os usuários de computador, ocorrendo a criação dos provedores que concedem o acesso à internet, para que pudessem “navegar na internet”

Sua estrutura foi melhorada e atualizada à medida em que o tempo passou e esta se expandiu, chegando em um nível global alcançando diversos países, no Brasil a internet começou a ser utilizada na década de 90, segundo a (ABRANET) Associação Brasileira dos Provedores de Acesso, em 1996, cerca de 300 mil brasileiros utilizavam a internet, esse número mudou muito.

Hoje em dia segundo o IBGE (Instituto Brasileiro de Geografia e Estatística), mais da metade dos domicílios brasileiros já possuem acesso à internet, a pesquisa que data de 2014 aponta que 36,8 milhões de residências no país possuem internet, representando 54,9 % no ano de 2013 apenas 48% das casas tinham acesso.

Um dos fatores que aumentaram muito o acesso foi o acesso à internet em smartphones, tablets, televisões, dentre outros dispositivos. O computador por muito tempo esteve em primeiro colocado na posição de acesso à internet, mas caiu para a segunda colocação no ano de 2014, ano em que os smartphones foram os preferidos pelos usuários para acesso à web.

Inclusive o acesso à internet por meio de tablets e celulares foi superior ao utilizado por meio de computadores convencionais pela primeira vez no ano de 2016

de acordo com a empresa StatCounter a qual monitora o tráfico na web, ou seja, é um avanço significativo no aumento do acesso a ambientes virtuais por meio de dispositivos móveis, mas sendo considerável ainda o uso do computador.

1.3 SURGIMENTO DO CIBERESPAÇO

A palavra “ciberespaço” dá uma ideia de seu significado, é um termo utilizado inclusive na mídia em debates sobre tecnologia e o alcance desta palavra está além da internet e abrange toda a estrutura das redes telemáticas.

Segundo LÉVY o conceito de ciberespaço se caracteriza como:

> O ciberespaço (que também chamarei de ‘rede’) é o novo meio de comunicação que surge da interconexão mundial de computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ele abriga, assim como os seres humanos que navegam e alimentam esse universo. Quanto ao neologismo ‘cibercultura’’, especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem no juntamente com o crescimento do ciberespaço. (2000 p.17)

A Internet está associada ao ciberespaço em virtude da mesma ser a rede mundial de computadores, esta criou um novo espaço onde o ser humano pode se expressar e comunicar, este espaço não existe fisicamente e sim virtualmente, usuários de computador e internet podem acessar este ambiente virtual, a revolução cibernética-tecnológica afetou os mais variados aspectos do cotidiano do ser humano, pois com o surgimento desta houve a introdução ao ambiente virtual.

Foi apresentada a possibilidade de amizades virtuais, comunidades, a “navegação” deste ambiente, a partir disto o ser humano se viu utilizando a virtualização, para as práticas sociais.

2. CRIMES NOS AMBIENTES CIBERNÉTICOS

2.1 CONCEITO

Da mesma forma que um crime tradicional, o crime no ambiente virtual pode se apresentar de várias formas podendo acontecer a qualquer tempo e lugar, o criminoso virtual se utiliza de habilidades e formas para a prática do delito, um crime cibernético se caracteriza como um crime adicionado de uma conduta informática ou cibernética.

Para SHARIFF (2010. pg.276) “... o ciberespaço se tornou um verdadeiro lugar sem regras de civilidade virtuais claramente definidas...”

De acordo com ROSSINI:

> [...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança Informática, que tem por elementos a integridade, disponibilidade a confidencialidade.(2004, p. 110.).

Para Rossini o delito informático se baseia em uma conduta ou prática considerada ilícita e típica, algo que é intrinsecamente ligado àquilo que acontece na vida real, pois é um fundamento básico da tipificação dos crimes, não importando a forma que é praticada, sendo esta tanto com dolo ou culpa, podendo esta ação ser praticada tanto por pessoas físicas ou jurídicas.

Interessante notar que este ressaltou a prática do delito virtual tanto em um ambiente provido de rede tanto sem a rede, ou seja independerá da internet para caracterizar um crime virtual, pois basta o dispositivo que acesse o ciberespaço, este tipo de conduta afeta tanto usuários quanto sistemas, afetando diretamente a segurança no ambiente virtual, inclusive corrompendo sua integridade e confidencialidade.

De acordo com CASTRO (2003, p.9), um dos aspectos mais visados no ambiente cibernético é a confidencialidade das informações, as quais são muito difundidas. Outra forma de conceituar um crime cibernético é a de que estes são cometidos por meio de computadores ou contra os mesmos, grande parte dos crimes sendo praticados pela internet, sendo comumente utilizando um computador.

Para FELICIANO, o crime cibernético possui a seguinte conceituação:

> Conheço por criminalidade informática o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware, software, redes, etc.) (2000 p.42).

Este afirma que a criminalidade informática se consolida por um fenômeno que é recente, informação esta, essencial, pois o advento dos meios tecnológicos não é antigo, mas sim algo que fora criado recentemente,e mesmo recente, já se é utilizado para a prática de atos criminosos, os sistemas, as máquinas as redes e o aparato tecnológico são utilizados com o fim do cometimento do ilícito por parte do praticante.

De acordo com ROSA (2005, p. 53) o crime virtual é conceituado como algo que desvirtua os dados que são característicos em um sistema que processa dados ou os armazena, ou seja, tem o intuito de prejudicar as informações.

Segundo NIGRI (2000.p. 34) o crime virtual é: “um ato lesivo cometido através de um computador ou de um periférico com a intenção de se obter uma vantagem indevida”.

Outra definição de crime virtual se dá por BARRETO (2007, p. 71):

Com o advento da Internet da Sociedade da Informação, surgiu uma nova modalidade de crimes cometidos no espaço virtual da rede através de e-mails (correio eletrônico), web sites (sítios pessoais, institucionais ou apócrifos) ou mesmo ocorridos em comunidades de relacionamento na Internet.

As transações comerciais eletrônicas, envolvendo compras que exigem a identificação do número de cartão de credito, as transações bancarias, que solicitam registro de dados referentes as contas correntes bancarias, além do uso de senha se demais mecanismos de segurança, assim como a profusão de novas modalidades relacionais mantidas em sociedade, através da Internet,propiciaram o surgimento de novas modalidades de crimes na web,batizados de crimes virtuais.

No ponto de vista de Irineu, os crimes virtuais surgiram em virtude da internet e da sociedade da informação que por fim gerou o espaço virtual, interligado à e-mails, sites na internet ou até mesmo em redes sociais, juntamente com transações comerciais realizadas eletronicamente e compras, pelas quais é necessário uso de cartão de crédito e também de senhas.

Segundo ele, todos esses são fundamentados por novas modalidades de relação em sociedade, esta interrelação proporcionou com que através de novas formas, ocorresse o cometimento de crime na internet sendo caracterizados como crimes virtuais.

Os crimes virtuais possuem diversas denominações podendo ser chamados de: crimes da computação, delitos da informática, abuso de computador, fraude informática, dentre muitos outros, ainda assim não alcançam todos os crimes atrelados à tecnologia em virtude da complexidade do ambiente virtual.

Em virtude de novas condutas criminosas surgirem nos computadores e na internet, as classificações que existem para os crimes cibernéticos tornam-se ineficazes, mas, na doutrina existem classificações presentes, as quais caracterizam o crime cibernético como puros, mistos e comuns e crimes cibernéticos próprios e impróprios.

O crime cibernético puro tem como objetivo atingir o computador os dados ou o sistema informático e seus dados, hackers se utilizam deste tipo de conduta, os mesmos possuem alto conhecimento da informática, invadem ou prejudicam sistemas.

Crimes cibernéticos mistos se caracterizam como aqueles em que a internet ou o sistema informático é de fundamental importância para que a conduta criminosa seja realizada, mesmo que aquilo que o criminoso tenha interesse não tenha relação com componentes da informática ou sistemas. Crime cibernético comum é aquele no qual o uso da informática é apenas um instrumento pelo qual o crime é praticado, sendo que este já esteja tipificado pela lei.

Um crime Cibernético próprio se configura como aquele que a conduta ilícita praticada visa prejudicar o sistema informático do sujeito passivo, conduta esta praticada por hackers que visam corromper os dados da vítima.

Crime Cibernético impróprio se caracteriza como aquele que visa atingir o patrimônio ou bem jurídico comum e que se utiliza da informática uma forma de se executar.

2.2 PROGRAMAS MALICIOSOS NO CIBERESPAÇO

Como exemplo das formas do cometimento destes ilícitos existe vários programas maliciosos que infectam um sistema, semelhante a vírus biológico que infecta pessoas. O mesmo inclusive se multiplica e cria cópias para se propagar para outros computadores de diversas formas, e conforme veremos a seguir, existem ferramentas para que o crime seja perpetrado.

Vírus, são programas maliciosos que são desenvolvidos por programadores. O vírus de computador tem o propósito de se instalar em um computador com a intenção de danificar e prejudicar o desenvolvimento da máquina, também destrói arquivos e também ser passado para outros computadores.

Ou seja, um computador que possuir um vírus dentro de si torna-se vulnerável e exposto para que outras pessoas de má intenção se utilizem deste, busquem ou roubem dados da máquina tais como senhas ou dados de cartão de crédito.

O vírus se propaga no ambiente virtual através da contaminação, na maioria das vezes esta contaminação ocorre quando por uma ação do usuário, este executa um arquivo infectado, podendo ser este um anexo de e-mail ou através de arquivos infectados transmitidos por pen drives ou CDs.

O sistema desatualizado também propicia a contaminação do computador pois o mesmo não possuirá correções de segurança que podem corrigem (corrigir concordância) as vulnerabilidades do sistema operacional ou também de aplicações, fazendo assim com que o vírus adentre e seja executado no sistema.

Outros tipos de vírus que infectam máquinas e sistemas podem manter-se ocultos durante algum período de tempo, para que no momento determinado se execute, os desenvolvedores e criadores destes tipos de vírus são indivíduos que possuem um alto domínio de conhecimento tanto de sistemas quanto de programações de computadores. Poucos anos atrás os vírus eram espalhados por meio do uso e compartilhamento dos disquetes, mas em virtude do avanço da internet, foram desenvolvidos novos meios com os quais os vírus são transmitidos, tais como e-mails, páginas de sites, dentre outros, formas do usuário se proteger destes vírus é possuir antivírus em seu computador e também não utilizar arquivos enviados por estranhos.

Worm (verme em português), se assemelha ao vírus se diferenciando na parte em que pode se propagar sozinho, já o vírus necessita de um hospedeiro para poder se replicar, o worm invade o sistema e pode apagar arquivos ou enviá-los através de e-mail. Tornando assim vulnerável o computador no qual infectar e também gerar danos no tráfego de rede, os usuários devem tomar muito cuidado quando acessar a internet e inclusive utilizar arquivos compartilhados mesmo que por pessoas conhecidas em virtude da possibilidade dos mesmos estarem de alguma forma infectados por um worm.

Spam, este é uma abreviação em inglês “spiced ham” (presunto condimentado) sendo uma mensagem de cunho eletrônico no qual é enviado de forma em larga escala, conhecido de maneira popular, são mensagens de e-mail com intuito de publicidade, em caráter geral estes são na maioria das vezes incômodos e consistem em propagandas, mas podem conter vírus em algumas situações, desta forma é preciso cuidado por parte dos usuários mesmo que pareçam simples propagandas.

Spyware (programa ou aplicativo espião) este programa coleta dados e informações do usuário e realiza o envio destas informações para alguém na internet, sem o conhecimento ou permissão do dono.

Por vezes o Spyware é utilizado por firmas que monitoram o comportamento dos usuários e avaliam seus hábitos e a partir daí vendem essas informações, por outras o único intuito deste programa espião é roubar informações e arquivos confidenciais pertencentes ao usuário inclusive dados pessoais ou bancários, ou seja de uma forma clara este programa tem a clara intenção de espionar.

Phishing, uma expressão de origem em inglês da palavra “fish” (pescar em português) ou seja é uma espécie de fraude virtual é realizada com a intenção de obter informações confidenciais, o criminoso se passa por alguém de confiança ou uma empresa enviando e-mails ou mensagens instantâneas, com a intenção de “pescar informações” do usuário, tais como senhas, ou números de cartão de crédito.

Botnet ou Storm Worm, é um programa de extrema dificuldade para ser identificado, pois o mesmo realiza constantes alterações em si mesmo, propaga-se por links de sites que já estão infectados, pode atingir muitas vítimas e é considerado um dos mais perigosos.

Rootkit, se trata de várias ferramentas que um hacker domina ao garantir um acesso remoto ao computador da vítima, pois este poderá causar dano à máquina na hipótese de ser retirado e também prejudicar o desempenho do computador, estas ferramentas dão ao hacker poder para alterar o sistema, arquivos e processos do computador infectado, por isso é de fundamental importância que os usuários utilizem antivírus em suas máquinas e tomem diversas outras precauções para evitar as ameaças virtuais.

Ransomware, também de origem da palavra inglesa “ransom” (resgate em português), é um programa malicioso que limita o uso do sistema e dos dados que for contaminado por este, após ser infectado, quando o usuário do computador utilizar o mesmo, aparecerá um alerta de que será necessário o pagamento de um valor para o resgate dos arquivos, para que assim o usuário possa ter acesso novamente aos dados e recursos do computador, é um programa malicioso que sequestra computadores.

De acordo com relatórios que mapeiam brechas e vulnerabilidades, o Brasil foi identificado como o país da américa latina que mais é atacado por ransomware e também Online Banking, também é o segundo na questão de aplicativos maliciosos, apenas nos dois primeiros semestres do ano de 2017 foram registrados mais de 82 milhões de ameaças deste tipo, este também afeta empresas, causando danos e prejuízos de grande quantia.

Este age criptografando e comprimindo os arquivos da vítima, de forma que este não consiga perceber que isto está ocorrendo, após este processo ser finalizado, uma mensagem é exibida na tela do computador, informando que o dono do computador não poderá se utilizar do mesmo.

RAT, é um termo em inglês abreviado “Remote Administration Tool” (Ferramenta de Administração Remota em português), sendo um programa que permite um acesso remoto ao sistema, da mesma forma que se utilizasse fisicamente, mas é um programa utilizado de forma ilegal, pois não há permissão do dono para que seja utilizado por outra pessoa, o usuário que possui o acesso remoto pode executar ações e inclusive obter todos os dados e informações da vítima, configurando assim um crime cibernético.

Backdoor se caracteriza como a prática para que programas maliciosos se instalem em um ou mais computadores, utilizado para conceder o acesso remoto de um sistema ou de uma rede, procura por brechas ou falhas que podem ser encontradas nos sistemas, buscando vulnerabilidades de programas ou sistemas que se encontrem desatualizados, para que assim se instale sem o usuário perceber, fazendo com que o computador fique desprevenido, pois as informações podem ser facilmente roubadas.

Malware trata-se de um software (programa) malicioso que é instalado no computador da vítima, sem a permissão do usuário, o mesmo age da mesma forma que um vírus, tem a intenção de roubar informações.

Um malware(software malicioso)acrescentar recentemente criado pelos criminosos, tem a capacidade de realizar o bloqueio do computador do usuário e liberar o computador no momento em que o criminoso permitir, criminosos estão se utilizando deste programa malicioso para cobrar nudes (fotos nuas) dos usuários e só liberam o acesso deste, caso as fotos sejam realmente as do usuário do computador.

Criminosos se aproveitam das brechas em sistemas operacionais de computadores, como exemplo o Windows, estas vulnerabilidades permitem que o sistema seja invadido e todos os dados da máquina sejam roubados, e também espionar a vítima em tempo real no computador, inclusive criminosos nos dias atuais vendem e comercializam ferramentas que permitem praticar estes delitos por um valor de 18 mil reais.

Espionar e roubar dados de outros sistemas se torna fácil com esta ferramenta, para que um usuário esteja protegido deste tipo de programa malicioso é necessário máximo cuidado ao navegar por páginas ou links suspeitos e inclusive adquirir ferramentas de proteção contra essa ferramenta maliciosa.

Não apenas computadores estão vulneráveis a ataques desses programas, celulares que possuem sistema operacional também podem ser atacados por programas maliciosos, recentemente pesquisadores descobriram vulnerabilidades no sistema Android, pelo qual os criminosos são capazes de criar telas falsas no smartphone.

Assim, são burladas as defesas do sistema Android, criminosos ofertam aplicativos que criam as telas falsas, ou seja, o usuário acaba por ser enganado e

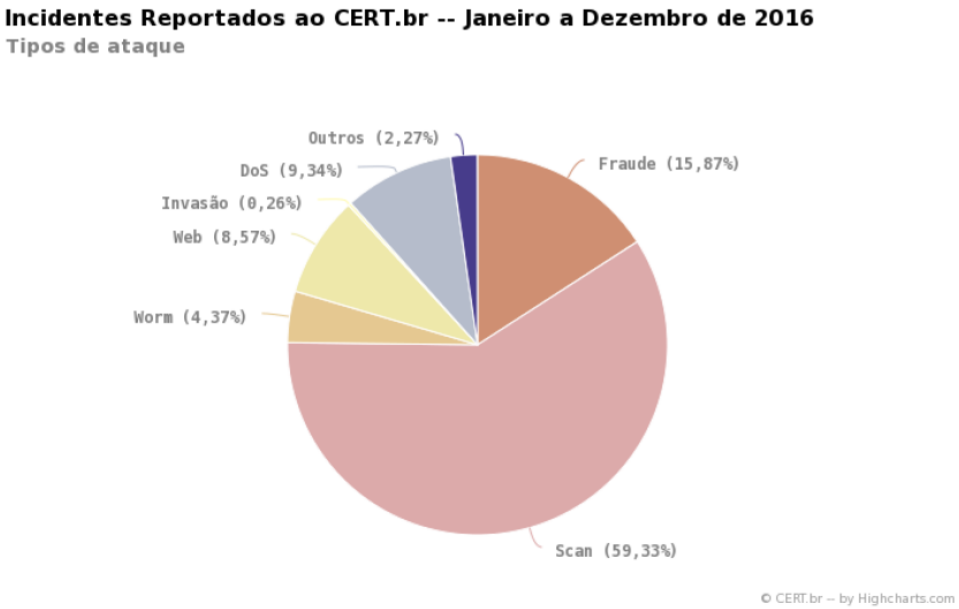
tendo suas informações roubadas, ou até mesmo sendo bloqueadas de ter acesso, algo muito similar ao Ransomware, o qual sequestra arquivos, para que o usuário se proteja deste tipo de programa é necessário manter o sistema atualizado e utilizar aplicativos oficiais do sistema Android.

O sistema de celulares da empresa norte americana Apple também tem sido afetado por cibercriminosos, hackers invadem contas de usuários com a intenção de roubar os dados pessoais e após isso bloqueiam todos os dados do aparelho, acessam a função “Buscar Iphone” e após isso solicitam dinheiro para pagar o resgate do acesso ao celular, isso é considerado um sequestro digital, pois as informações e dados se encontra em poder dos hackers.

Muitas vítimas relatam que são pedidos valores para a devolução do acesso aos aparelhos, este golpe é semelhante ao Ransomware, mas com a pequena diferença de que o criminoso se aproveita de ferramentas da própria Apple para cometer o ilícito, autoridades tem recomendado que as vítimas não realizem pagamentos de valores, tendo em vista o estímulo deste crime.

A CERT-BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, divulgou dados de incidentes reportados datando de janeiro até dezembro do ano de 2016 contendo os seguintes dados:

FIGURA 2: INCIDENTES REPORTADOS AO CERT



FONTE: INCIDENTES..., 2017. Disponível em: <https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html>

Legenda:

Worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

Dos (DoS -- Denial of Service): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

Invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.

Web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

Scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

Fraude: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

Outros: notificações de incidentes que não se enquadram nas categorias anteriores.

Deve-se tomar como observação o fato de que a palavra: scam não deve ser confundida com a palavra: scan, a palavra scam (com a letra “m”) significa ataque à uma vítima com intenção de obter vantagem financeira.

2.3 PRATICANTES DE CRIMES VIRTUAIS

Em sua obra, FELIZARDO (2010.p.135) nos exemplifica os tipos de criminosos virtuais sendo eles:

Cracker – expert em computador que tem domínio e habilidade em programações e desenvolvimento de sistemas. Invade o sistema de computação de outra pessoa, ou rede, quebrando palavras-chave, licenças, senhas e proteções: age de forma ilegal e sem ética, com intenção de dolo. Os crimes virtuais geralmente atribuídos a eles podem subdividir-se em:

Pichadores Digitais (que geralmente invadem sites para expor sua “marca”.

Cyberpunk (agem pelo simples prazer de causar danos à vítima. Esse dano pode consistir na simples queda do servidor- deixando a máquina momentaneamente desconectada da internet – ou até mesmo a destruição total dos dados armazenados).

Espiões (agem para adquirir informações confidenciais armazenadas no computador da vítima. Os dados podem ter conteúdo comercial- segredos industriais-, políticos- dados do governo – ou militar).

Ciberterroristas (suas motivações são em geral políticas e suas armas são muitas, desde o furto de informações confidenciais até a queda do sistema telefônico local ou outras ações do gênero),

Estelionatários (também em geral com objetivos financeiros, procuram adquirir números de cartões de crédito armazenados em grandes sites comerciais. Geralmente utilizam uma técnica chamada “Phishing Scam”, enviando por e-mail um programa que é executado por algum usuário, tendo acesso às suas informações. Também podem atacar instituições financeiras desviando dinheiro para sua conta).

Hacker – expert em computador que tem domínio e habilidade em programações e sistemas e desenvolvimento de proteções. O hacker utiliza todo seu conhecimento para melhorar softwares, de forma legal, e criar soluções inteligentes para um problema de programação e segurança. O hacker é necessário para a sobrevivência da informática e na busca cada vez maior da tecnologia, que a cada dia apresenta novas descobertas. Ele geralmente é de classe média ou alta, com idade de 12 a 28 anos. Também pode ser chamado de White Hat Hacker (hacker do chapéu branco), em alusão ao serviço benéfico que faz (BlackHat e Gray Hat se enquadram no perfil do cracker).

Segundo SPYER E AVORIO (2015 p 189) o cibercrime surgiu na forma de uma brincadeira de criança, no ano de 1982 um estudante desenvolveu um vírus de computador para pregar uma peça em seus colegas.

Após alguns anos este vírus seria utilizado como base para estudo e o desenvolvimento de novas ferramentas que pudessem invadir secretamente outros sistemas de computadores, serem transferidos para outras máquinas e redes.

3 PRINCIPAIS FORMAS DE CRIMES CIBERNÉTICOS

No ambiente virtual diariamente são praticados os mais diversos tipos de crimes, segundo o site estadão houve um crescimento de 10% na prática dos cibercrimes no Brasil do ano de 2015 para 2016, cerca de 42,4 milhões de pessoas foram alvo dos criminosos através da internet no ano de 2016, os prejuízos dos crimes virtuais chegaram a um valor de 10 bilhões de dólares , estes estão se multiplicando de uma forma espantosa e praticamente sem controle.

Isto acontece porque o cibercrime pode ocorrer em qualquer lugar, não existindo barreiras para sua prática, este tipo de criminalidade em nada diverge da realizada na vida real, o criminoso emprega diversos artifícios para a prática do crime virtual, esta espécie de delito não se diferencia também na questão dos efeitos e danos gerados à vítima.

Existem muitas formas e espécies de cometimento de um crime cibernético, conforme conceitua COLARES:

> Crime contra a segurança nacional, preconceito, discriminação de raça-cor e etnias,pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software,calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano,apropriação indébita, estelionato, violação de direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, incitação ao crime, apologia ao crime ou criminoso, falsa identidade, inserção de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões e jogo de azar (2002, p. 02)

Os crimes cibernéticos podem ser praticados das mais diferentes formas possíveis, é interessante reforçar que os crimes e as contravenções penais são compreendidos tanto as praticadas na internet quanto em sistemas informáticos, pois estes se difundem em um ambiente virtual, o qual está repleto de usuários mal-intencionados que buscam oportunidades para o cometimento de ilícitos.

Segundo FELIZARDO (2010.p.56) os crimes cometidos virtualmente possuem uma lista extensa e com a universalização da internet sua prática aumentou consideravelmente, abaixo veremos os principais.

3.1 INVASÃO DE PRIVACIDADE

A rede mundial com suas facilidades trazem riscos que não podem ser vistos aos usuários, especialistas afirmam que é necessário ter conhecimento dos perigos e estar com atenção sempre, pois a partir de um clique algo que é privado pode se tornar público na internet.

O crime de invasão à privacidade deu um salto imenso nos últimos anos, a quantidade de informações e dados privados que são violados é imensa, documentos, fotos, vídeos e todo tipo de arquivos são roubados pelos criminosos, esses dados dizem respeito tanto a intimidade da pessoa física quanto dados privados de pessoa jurídica, tais como bancos, empresas e diversas outras instituições.

Infelizmente indivíduos de conduta repudiável se utilizam dos meios tecnológicos para acessar informações privadas e sigilosas e obter para si ou para outrem vantagem ilícita, no Brasil o Direito já começa a se movimentar para o combate deste tipo de crime, no ano de 2012 ocorreu um crime virtual que foi notícia em todo o país, e serviu de exemplo para a criação de uma lei que combate os crimes virtuais.

Este crime fora praticado contra a atriz Carolina Dieckmann a qual teve mais de 30 fotos íntimas publicadas na internet as quais foram furtadas de seu computador pessoal através de seu e-mail, hackers fizeram chantagem com a mesma por meio de mensagens anônimas e solicitaram dinheiro para deletarem as imagens, tal crime repercutiu de forma nacional e demonstrou a necessidade de uma lei que combatesse este tipo de crime, felizmente a legislação através do congresso nacional se movimentou e promulgou a criação de uma nova lei sendo esta a Lei 12.737/2012 que fora batizada como Lei Carolina Dieckmann.

O código penal passou por acréscimos de artigos com a criação da Lei 12.737/2012 sendo o artigo 154-A e 154-B.

Abaixo podemos verificar no Código Penal lei n° 2.848/1940 a atualização do artigo e como sua tipificação se estabelece:

> 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.
>
> § 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.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Vigência Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

> § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Com a atualização deste artigo do Código Penal percebe-se que a invasão de dispositivos informáticos alheios passou a ser configurada crime, o legislador aponta que independe de o dispositivo estar ou não conectado à rede mundial de computadores, também conhecida como internet, configura o crime a simples invasão do dispositivo sem a autorização do proprietário.

O praticante desta conduta antijurídica poderá ser preso ou pagar multa caso venha a cometê-la, inclusive poderá ter sua pena majorada de, caso o crime seja cometido em acordo com as hipóteses previstas no artigo, sendo as vítimas políticos, a pena poderá variar de 6(seis) meses à 2 (dois) anos.

Recentemente sites de Tribunais e Órgãos brasileiros foram alvo de ataques e ameaças de invasão por hackers, o TRT 8º Região informou que seu site foi hackeado de uma forma superficial, mas que atingiu sua página principal, a equipe de informática e segurança do Tribunal teve que agir rapidamente e tomar as providencias para que a página fosse restabelecida e também identificar a origem do ataque hacker.

O site do Tribunal de Justiça da Paraíba também foi invadido por hackers, durante a invasão a página inicial do site fora substituída por uma bandeira e uma mensagem em inglês a qual dizia que o site do tribunal havia sido hackeado por Muhmad Emad e logo abaixo da bandeira do Curdistão havia uma citação de que: “Hackers Curdos estiveram aqui” e palavras contra o estado islâmico, logo após o departamento de Tecnologia e Informação fora avisado desta situação o site fora retirado do ar para após um tempo retornar normalmente.

Outro grande ataque ocorreu contra os sites do Ministério Público de São Paulo, INSS (previdência) e Tribunal de Justiça de São Paulo, fazendo com que ficassem fora do ar, inclusive não apenas no Brasil, mas boa parte da Europa também fora vítima deste ataque massivo, a Coordenação de Tecnologia da Informação e

Comunicação (CTIC) chegou a orientar que fossem desligados os computadores do Ministério Público de São Paulo, tamanho fora o ataque sofrido.

Este incidente se espalhou pela rede do estado e por isso houveram avaliações para descobrir se a segurança da rede fora comprometida, o site do INSS (Instituto Nacional do Seguro Social) também ficou inativo tendo em vista o ataque hacker, neste ataque o programa malicioso ransomware foi utilizado.

Os arquivos foram compactados e criptografados, assim as companhias só poderão obter novamente seus arquivos caso paguem o valor que o invasor solicita, este se mostra um modus operandi de cometer um crime de uma forma totalmente sofisticada, este tipo de criminoso não costuma deixar rastros, algo que dificulta na sua punição.

Esses ataques aos órgãos oficiais por vezes possuem a intenção de demonstrar as fragilidades do sistema ou também de os criminosos desafiarem a segurança dos sites do governo.

Criminosos também disponibilizaram dados de usuários de sites de compras virtuais na internet, com os nomes de usuários e senhas, clientes de diversas lojas foram vítimas desta invasão de privacidade, cerca de 360 logins e senhas de usuários estavam disponíveis na internet, isto configura crime, pois além da invasão da conta privada, as lojas armazenam dados como endereços de clientes, telefone, cartão de crédito, dentre muitos outros.

3.2 FRAUDES VIRTUAIS

Para entendermos as fraudes virtuais vejamos o conceito segundo LIMA (2005.p.60):

Fraudes eletrônicas – invasão de sistemas computadorizados e posterior modificação de dados, com o intuito da obtenção de vantagem sobre bens, físicos ou não, por exemplo, a adulteração de depósitos bancários, aprovações em universidades, resultados de balanços financeiros, pesquisas eleitorais, entre outros.

De acordo com o entendimento de GIL (1999.p. 15) as fraudes virtuais se conceituam como:

Ação intencional e prejudicial a um ativo intangível causada por procedimentos e informações (software e bancos de dados), de propriedade de

pessoa física, ou jurídica, com o objetivo de alcançar benefício, ou satisfação psicológica, financeira e material.

Para que a fraude virtual se consuma segundo LIMA (2005.p.134), é necessário que um agente realize a prática da invasão, modificação, supressão ou pagamento de informações, dados eletrônicos ou programas, ou qualquer outro meio que possa realizar alterações em um sistema de processamento de dados. Este tipo de crime é cometido com a intenção de enganar a vítima e assim obter a vantagem ilícita, este tipo de conduta criminosa só tem aumentado, em virtude do aumento constante de usuários na internet e ambientes virtuais, os golpes se multiplicaram, e nem mesmo os usuários mais avançados escapam de ser vítimas desses golpes, criminosos empenham-se para conseguir novos modos da prática criminosa nesses ambientes.

Uma modalidade desse tipo de crime é a simulação de um e-mail enviado por uma instituição financeira para a vítima, como exemplo Bancos, a vítima já deve possuir vínculo com a instituição, é solicitado que usuário atualize informações, ao clicar no link acompanhado no e-mail a vítima é direcionada à uma página falsa da instituição financeira para que a mesma escreva suas informações bancárias, tais como cartão de crédito e senha, após isso o criminoso recebe estas informações e poderá causar prejuízos à vítima.

O crime de fraude também está associado ao phishing(mensagens falsas com links fraudulentos), no qual os criminosos se aproveitam da situação para roubar informações ou dinheiro, por ser difícil por vezes os usuários comuns dos ambientes cibernéticos acabam por cair nestas fraudes ou golpes, certos aplicativos para smartphones possuem o único propósito de roubar dados dos celulares, enganando assim o usuário.

Lojas virtuais são muito visadas pelos criminosos para a prática destes delitos, em virtude do crescimento de compras realizadas por meio da internet, os criminosos atraem as vítimas com ofertas e descontos falsos, em virtude de estes serem muito atrativos ao usuário, alguns produtos são desejo de vários usuários, portanto muitos caem nestes golpes. Outras vezes criminosos ficam sabendo que clientes reservaram hotéis por meio online, enviam e-mails falsos solicitando o preenchimento ao usuário para a confirmação de reserva em hotéis, prática também fraudulenta.

Algumas empresas agem de má fé e enviam boletos na residência de clientes de outra empresa que possuem domínios (sites) na internet, cobrando valores, tentando se passar pela empresa original, tudo isso para realizar a cobrança indevida, caracterizando assim claramente uma fraude. Oportunidades de emprego falsas também são fraudes praticadas pelos criminosos os quais oferecem empregos, convencendo as vítimas a descontar cheques ou ordens de pagamento, e iludem muitas pessoas com promessas de salários altíssimos.

Nos ambientes virtuais as fraudes são cometidas com o furto de identidade com fins da obtenção da vantagem ilícita, no ciberespaço é possível acessar contas bancárias utilizando o nome ou criando perfis falsos, ou seja, o criminoso faz se passar pela vítima.

Um usuário teve um caso relatado recentemente sobre uma tentativa de fraude em uma loja virtual, pois o criminoso teve acesso aos seus dados e realizou uma compra em seu nome, imediatamente o mesmo procurou ajuda na central de atendimento da loja, para evitar que o prejuízo se tornasse maior.

3.3 CYBERBULLYING

Para a melhor compreensão do termo cyberbullying vejamos o conceito deste crime segundo FELIZARDO (2010.p.36):

O Cyberbullying é uma extensão do bullying escolar, por sua natureza, é difícil de ser detectado porque, em primeiro lugar, é anônimo, e em segundo, a vítima não denuncia.

Segundo a autora este tipo de crime possui características bastante peculiares que se diferenciam do bullying tradicional em virtude da forma com que este é praticado, pois o criminoso o consuma em anonimato, sem que a vítima realmente saiba que lhe causou este mal, a acessibilidade à prática deste, no bullying normal o agressor só encontra as vítimas durante algumas horas do dia, mas no ambiente virtual a agressão pode ser realizada em qualquer hora.

O medo de serem punidos também inibe que as vítimas denunciem os agressores, pois o acesso ao computador ou ao celular pode ser retirado deste, os espectadores no mundo cibernético podem ser de um número imenso, o comportamento do agressor no ambiente virtual é diferente do praticado

pessoalmente em virtude do anonimato o estar protegendo, aumentando as chances de indivíduos intimidarem os outros.

Diferentemente do bullying praticado na vida real, o processo para se tornar um agressor é mais rápido, tendo em vista que todos os que participam das mensagens se tornam coagressores.

Para SHARIFF (2010. pg.62) o cyberbullying se conceitua como:

Pela sua natureza, os meios eletrônicos permitem que as formas tradicionais do bullying assumam características que são específicas do ciberespaço.

De acordo com a autora o ciberespaço por possuir uma natureza anônima e tornou atraente aos jovens, estes usam apelidos ou pseudônimos os quais acabam por preservar suas identidades dificultando sobremaneira a identificação do mesmo, caso seja praticado em redes sociais, fica mais fácil de realizar a identificação, as consequências desse ato criminoso são devastadoras para as vítimas.

Alunos de vários colégios sofrem com este tipo de crime segundo SHARIFF (pg.63 – 65), pois a vítima sofre e acaba por se afastar dos outros alunos, o ambiente escolar se torna hostil em virtude das ameaças e xingamentos sofridos, no ciberespaço muitos autores podem praticar o abuso, ou seja, a tecnologia esconde estes praticantes, inclusive gêneros sofrem este tipo de crime, pois assédio sexual e perseguição homofóbica são realizados por meio do ciberbullying.

FELIZARDO (2010.p.41-42) em sua obra aponta que o Cyberbullying se apresenta em nove formas mais comuns, sendo estas:

- Injúria
- Difamação
- Ofensa
- Falsa Identidade
- Calúnia
- Ameaça
- Racismo
- Constrangimento ilegal
- Incitação ao suicídio

Todos estes crimes oriundos do cyberbullying estão tipificados no código penal brasileiro, pois caracterizam conduta ilícita e punível, quando uma pessoa tem sua honra insultada a calúnia está presente com previsão legal no artigo138 do código

penal, quando boatos eletrônicos são espalhados sobre uma pessoa configura difamação, artigo 139 do Código Penal.

Insultar uma pessoa por usas características ou apelidar grosseiramente configura injúria presente no artigo 140 do Código Penal, comentários sobre a raça religião ou etnia configura preconceito ou discriminação previsão legal na Lei 7.716/89 em seu artigo 20.

Na Inglaterra não muito tempo atrás o crime de ódio passou a ser julgado como um crime praticado no mundo real, não havendo distinção entre estes tendo como objetivo encorajar penas mais severas aos criminosos que ousarem cometer este delito, a promotora do Ministério Público do Reino Unido citou que o crime de ódio é “subestimado” e por isso muitas pessoas abusam no cometimento, é um tipo de crime online que ofende hostiliza e incita preconceito para com as pessoas.

Independentemente de ser dito nas ruas ou través de pinturas em paredes o impacto na vida da vítima é o mesmo, entre os anos de 2015 e 2016 o Ministério Público do Reino Unido realizou sentença de mais de 15 mil crimes de ódio. No brasil o crime de racismo e injúria racial possuem a pena de 1 até 3 anos de reclusão.

No Brasil o jogo conhecido como “Baleia Azul é utilizado por cibercriminosos para fazer com que crianças e adolescentes sejam coagidos através de ameaças, este jogo que fora iniciado entre 2015 e 2016 na Rússia está ligado supostamente à uma série de suicídios no mundo todo, este jogo tem por objetivo causar danos no participante, o criminoso é chamado de “curador” entrega desafios, sendo o último desafio o suicídio.

Estes cibercriminosos tem por alvo crianças e adolescentes por serem impressionáveis facilmente, estes criminosos se utilizam de engenharia social e ameaçam os menores mostrando os dados destes, como endereço, escola onde estuda, nome de amigos próximos, dentre outros dados pessoais, ameaçam familiares caso a criança ou adolescente não queira cumprir o desafio.

Este tipo de conduta é criminosa e está tipificado no código penal no artigo 122, pois há a indução ao suicídio ou instigação, juntamente com o auxílio ao suicídio, sendo punido de 2 até 6 anos de prisão caso o suicídio ocorra, e 01 até 03 anos caso da tentativa de suicídio ocorra lesão corporal grave.

3.4 PORNOGRAFIA INFANTIL

O artigo 240 do Estatuto da Criança e do Adolescente Lei 8069/90 tipifica claramente este tipo de crime que também é praticado no mundo virtual, o qual prevê:

> Art. 240 – Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
>
> Pena – reclusão de 4 (quatro) a 8 (oito) anos, e multa.
>
> Art. 241 – Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão 4 (quatro) a 8 (oito) anos, e multa.

Esta se caracteriza como uma conduta dolosa tendo em vista o material estar disponibilizado ou à venda, mesmo que outras pessoas não consumam o material, o crime já estará configurado, em virtude da posse do mesmo. O Supremo Tribunal Federal possui o entendimento de que os crimes que são praticados na internet não dependem do meio que foi utilizado e sim de sua publicação, abaixo o julgado da Primeira Turma do STF:

> "Crime de Computador": publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte
>
> 1. O tipo cogitado – na modalidade de “publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente” – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma normal aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.
>
> 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta incriminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da Lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.
>
> 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada do conhecimento do homem comum, impõe-se a realização de prova pericial.

Na Austrália uma força tarefa policial assumiu o controle de um site de pedofilia com a intenção de monitorar e rastrear as atividades de pedófilos em muitas partes do planeta, inclusive fora necessário manter o site em funcionamento para que mais pedófilos fossem capturados, o inspetor chefe da polícia inclusive comentou que os pedófilos se valem do suposto anonimato que o ambiente virtual proporciona para

realizar o compartilhamento de material expondo menores à exploração, cerca de 12 países tiveram resgate de crianças e prisões de pedófilos através desta operação.

Recentemente foi aprovada no Senado uma nova regra para a apuração do crime de pedofilia na internet por parte da polícia, este projeto consistia em modificar o ECA (Estatuto da Criança e do Adolescente), para que policiais pudessem se infiltrar na internet com o objetivo de investigar o crime de pedofilia e crime contra a dignidade sexual de crianças e também adolescentes.

Na investigação, os dados que forem obtidos pelos policiais deverão ser remetidos ao juiz responsável do processo, sendo mantido o sigilo de todas as informações, as investigações terão um prazo de 90 dias podendo ser prorrogados por até dois anos.

4 ÓTICA PENAL PARA COMBATE DO CRIME VIRTUAL

De acordo com NOGUEIRA (2008 p.182-183), a justiça Brasileira e o uso do Código Penal estão totalmente atrelados ao combate ao crime virtual em virtude de a justiça ter adaptado as condutas criminosas virtuais baseadas no código Penal.

Segundo FELIZARDO (2010.p.55-56) por muitas das vezes a legislação específica é necessária, mas esta se encontra ausente, e os tribunais necessitam da mesma para punir os hackers, crackers e também internautas que cometem ilícitos utilizando a internet. Para uma grande parte de magistrados, advogados e consultores jurídicos aproximadamente 95% do Código Penal já tipifica os crimes que são cometidos na internet, a justiça procura se adaptar para utilizar os dispositivos do Código Penal para combater os crimes virtuais.

Com o crescente número de crimes perpetrados na internet, por vezes a legislação se torna antiquada, por isso a necessidade de uma normatização de condutas atípicas na ótica penal, é necessária uma abordagem do estado na realidade virtual em virtude de que o ciberespaço não esteja fadado ao estado natural das coisas, no qual não existia lei, e quando não há lei o crime é cometido livremente.

O Direito Penal se firma como o único meio para o controle do aumento da criminalidade no mundo virtual tendo um controle coercitivo o qual sanciona e pune as condutas ilícitas, em relação à internet e os crimes cometidos nos ambientes virtuais. Desta forma é necessário todo um estudo por parte do Direito para que as próximas leis que sejam criadas sejam eficazes no combate ao crime e não sejam ineficazes ou contraditórias.

Por vezes o princípio da analogia é utilizado para que o cibercriminoso não fique impune, sendo estes enquadrados nos tipos já existentes, mas existe uma disparidade grande entre as normas no que diz respeito a aplicabilidade correta das normas já existentes

Com a revolução tecnológica que ocorreu, o direito penal precisou transpor diversos desafios quanto ao tema dos crimes virtuais pois a internet por muitos é considerada uma “terra sem lei”, desta forma os delitos que são praticados no meio virtual passam a adentrar a esfera jurídica, esta é a razão da necessidade que urge da criação de leis específicas que punam o agente criminoso, como exemplo existem as leis 12.735/2012 e também 12.737/2012.

MONTEIRO em sua obra (2008.p.68), afirma que a intervenção do Estado é essencial na fruição dos meios tecnológicos tanto de produção quanto de difusão da informação, conforme consta na Constituição Federal, mas sendo esta intervenção ordenada e não desordenada, e esta intervenção deverá estar focada na fiscalização para que práticas nocivas sejam inibidas.

Para SOUZA NETO (2009.p.58-60) o princípio da territorialidade se apresenta como um dos maiores desafios para o combate do crime virtual, em virtude de a internet possuir um caráter global abrangendo todo o planeta, o artigo 5º do Código Penal Brasileiro tem a previsão de que nos crimes que forem praticados no território brasileiro, será aplicada a lei brasileira, nos crimes que forem perpetrados na Internet. Será aplicada a lei brasileira quando o site for brasileiro, existindo exceção para este dispositivo sendo esta a extraterritorialidade prevista no artigo 7º do Código Penal, pois caso o agente esteja fora do país, será aplicada a lei brasileira nos casos do artigo 5º ou caso haja tratado a respeito.

5 MEDIDAS DE PROTEÇÃO CONTRA O CRIME CIBERNÉTICO

Por mais que pareça difícil se proteger dos crimes cibernéticos, tendo em vista a quantidade de crimes que se classificam, existem mecanismos e formas que impedem a práticas deste tipo, utilizar um programa de antivírus tanto no computador, quanto smartphone ou tablets ajuda a identificar códigos maliciosos que venham a ser instalados nos dispositivos, alguns destes são gratuitos e outros pagos aumentam ainda mais a proteção do usuário.

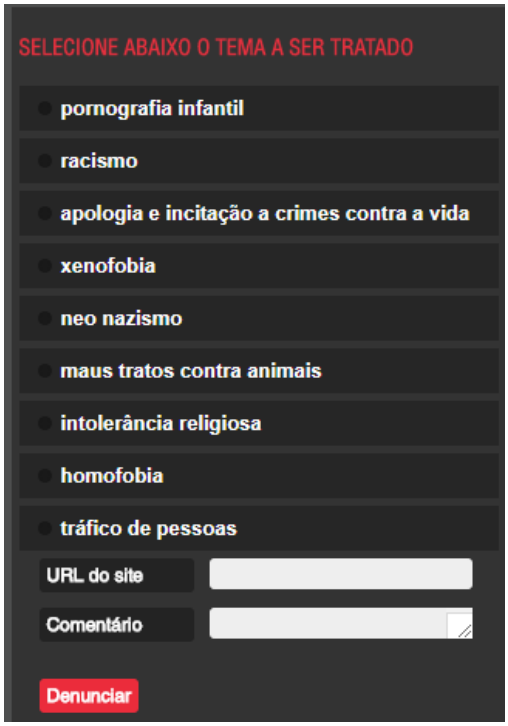
A utilização de cuidados redobrados é sempre importante, o uso de senhas seguras no ambiente virtual é fundamental, deve-se evitar o uso da mesma senha para todos os e-mails ou acesso a bancos e redes sociais, pois com uma única senha um cibercriminoso poderá acessar todos os dados do usuário.

Sempre realizar compras seguras e apenas em sites confiáveis, criminosos virtuais se aproveitam de usuários desatentos para clonarem dados bancários das vítimas. Cuidados com o e-mail são fundamentais, alguns remetentes com assuntos que podem chamar a atenção do usuário podem ser disfarces para golpes.

A desconfiança na internet também é sempre fundamental, tendo em vista os roubos e chantagens, que são perigos constantes, mesmo com todos os cuidados tomados, alguns crimes são difíceis de se evitar, mesmo os usuários mais experientes podem ser vítimas, é necessário entender que qualquer site, aplicativo ou rede social está à mercê de crimes virtuais, caso isso ocorra, a denúncia do crime é fundamental.

A SaferNet Brasil é uma entidade que não possui fins lucrativos e também possui uma cooperação com o Ministério Público Federal além de apoiar o Comitê Gestor da Internet no Brasil e a Justiça Federal, em um período de 11 anos, esta recebeu e também processou 3.861.707 denúncias anônimas, a vítima de crimes virtuais pode realizar uma denúncia anonimamente juntamente à SaferNet, antes da denúncia ser feita basta realizar a escolha da categoria do crime, inserir o site em questão ou adicionar comentários sobre a denúncia. A SaferNet poderá solicitar a retirada do conteúdo do ar para o provedor caso a denúncia proceda.

FIGURA 3 – DENUNCIAR CRIMES CIBERNÉTICOS



FONTE: SAFERNET..., 2017. Disponível em: <http://new.safernet.org.br/denuncie>

Outro meio de realizar denúncias contra crimes virtuais é através das delegacias especializadas em crimes cibernéticos no próprio estado da vítima, são chamadas Delegacias Cibercrimes, estão presentes em vários estados no país, caso esta não atenda ao público, ou nem haja este tipo de serviço na cidade da vítima, esta poderá procurar a Delegacia de Polícia mais próxima ou a Promotoria da Infância e da Juventude para efetuar o Registro de Ocorrência.

De acordo com FELIZARDO (2010.p.44-45) caso a vítima opte pelas medidas judiciais, será necessário dirigir-se ao Cartório de Notas para que o notário descreva o conteúdo do celular, e-mail ou página da internet, pois a ata notarial serve como prova válida perante o juízo.

CONCLUSÃO

No presente trabalho, buscou-se apresentar os crimes virtuais, os quais são subestimados por muitos, mas que existem há tempos e são uma ameaça real, pois se caracterizam como crimes desafiadores às autoridades, tendo em vista a dificuldade na punição destas práticas e o aumento em larga escala das mesmas nos últimos anos, em virtude do aumento do uso de tecnologias por parte da população.

O número de crimes perpetrados na internet e em computadores cresceu absurdamente com o passar do tempo, golpes, fraudes dentre diversos outros ilícitos se proliferam de uma forma que podem afetar milhares de usuários, por isso urge a necessidade da criação de leis específicas para o combate imediato destes.

Aborda-se os principais delitos informáticos que assombram este ambiente, como são conceituados na visão de vários autores e principalmente a forma com que o Direito Penal busca reprimir estes crimes, uma problemática que deve ser abordada, pois da mesma forma que na vida real os crimes virtuais também devem ser passíveis de punição, para que a justiça, os bons costumes e a democracia prevaleçam.

REFERÊNCIAS

AMBITO JURÍDICO - **Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade**. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3> Acesso em: 16/10/2017.

AMBITO JURÍDICO – **Os crimes virtuais e a impunidade real.** Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963> Acesso em: 19 set. 2017.

AVORIO André e SPYER Juliano, **Para Entender a Internet versão revisada e ampliada**, 2015.p.189.

BARRETO, Júnior Irineu. **Atualidade do Conceito de Sociedade da Informação para a Pesquisa Jurídica.** *In*: PAESANI, Liliana Minardi (Coord.). O direito na sociedade da informação. São Paulo: Atlas, 200.p.71.

BRASIL. Supremo Tribunal Federal – **RHC n. 76.689-0 – Pernambuco** – Primeira Turma – Relator: Ministro Sepúlveda Pertence, 22 de setembro de 1998, STF. Disponível em: <http://stf.jusbrasil.com.br/jurisprudencia/740355/habeas-corpus-hc-76689-pb> Acesso em: 14 out. 2017.

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

CERT.BR **- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Incidentes Reportados ao CERT.br** – janeiro a dezembro de 2016. Disponível em: <https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html> Acesso em: 01 out. 2017.

COLARES, Rodrigo Guimarães. **Cybercrimes: os crimes na era da informática** <https://jus.com.br/artigos/3271/cybercrimes-os-crimes-na-era-da-informatica> . Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 7 Acesso em: 13 set. 2017.

DIREITOS BRASIL - **Crimes cibernéticos: o que são e como reagir?** Disponível em: <http://direitosbrasil.com/crimes-ciberneticos/> Acesso em: 14/10/2017.

E-DOU - **Crimes virtuais: que leis existem?** Disponível em: <https://e-dou.com.br/2016/08/crimes-virtuais-que-leis-existem/> Acesso em: 19 set. 2017.

ESTADÃO – **Crimes virtuais afetam 42 milhões de brasileiros**. Disponível em: <http://economia.estadao.com.br/noticias/releases-ae,crimes-virtuais-afetam-42-milhoes-de-brasileiros,70001644185> Acesso em: 16 set. 2017.

FELIZARDO, Aloma Ribeiro – **Cyberbullying Difamação na Velocidade da Luz**. 1º Ed. São Paulo. Willem Books 2010.

FELICIANO, Guilherme Guimarães. **Informática e Criminalidade: parte I: Lineamentos e Definições.** Boletim do Instituto Manoel Pedro Pimentel, São Paulo, v. 13, n. 2, 2000.

FOLHA DE SÃO PAULO - **Uso de internet em celulares e tablets ultrapassa computador, diz pesquisa**. Disponível em: <http://www1.folha.uol.com.br/mercado/2016/11/1828411-uso-de-internet-em-celulares-e-tablets-ultrapassa-computador-diz-empresa.shtml> Acesso em: 09 set. 2017.

GIL, Antônio de Loureiro. **Fraudes Informatizadas.** 2 ed. São Paulo: Atlas, 1999.

GRUPO ESCOLAR – A Origem da Internet. Disponível em: <http://www.grupoescolar.com/pesquisa/a-origem-da-internet.html>. Acesso em: 06 set. 2017.

G1 - **Internet chega pela 1ª vez a mais de 50% das casas no Brasil, mostra IBGE.** Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/04/internet-chega-pela-1-vez-mais-de-50-das-casas-no-brasil-mostra-ibge.html> Acesso em: 08 set.2017.

G1 - **Série 'Invasão de Privacidade' aborda exposição pela internet e rede social.** Disponível em: <http://g1.globo.com/sao-paulo/itapetininga-regiao/noticia/2015/06/serie-invasao-de-privacidade-aborda-exposicao-pela-internet-e-rede-social.html> Acesso em: 19 set. 2017.

G1 – **Site do TJPB é hackeado e exibe mensagem contra Estado Islâmico**. Disponível em: <http://g1.globo.com/pb/paraiba/noticia/2017/02/site-do-tjpb-e-hackeado-e-exibe-mensagem-contra-estado-islamico.html> Acesso em: 18 set. 2017.

HISTÓRIA e desenvolvimento do computador. Disponível em: <https://www.todamateria.com.br/historia-e-evolucao-dos-computadores/>. Acesso em: 06 set. 2017.

INCIDENTES reportados ao CERT.br—Janeiro a Dezembro de 2016. Disponível em: <https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html> Acesso em: 01 out. 2017.

INFO ESCOLA – **Ciberespaço** Disponível em: <http://www.infoescola.com/internet/ciberespaco/> Acesso em: 13 set. 2017.

JUS BRASIL – **Crimes Cibernéticos.** Disponível em: <http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos> Acesso em: 19 set. 2017.

JUS BRASIL - **Crimes na internet: falta de normatização, dificuldades na regulamentação e entendimentos sobre o assunto.** Disponível em: <https://mikhail.jusbrasil.com.br/artigos/234313175/crimes-na-internet-falta-de-normatizacao-dificuldades-na-regulamentacao-e-entendimentos-sobre-o-assunto> Acesso em: 16/10/2017.

JUSBRASIL - Informe TRT8 - **O site do Tribunal foi hackeado**. Disponível em: <http://oab-pa.jusbrasil.com.br/noticias/112335251/informe-trt8-o-site-do-tribunal-foi-hackeado> Acesso em: 18 set. 2017.

LÉVY, Pierre. **Cibercultura.** Trad. De Carlos Irineu da Costa. 2. Ed São Paulo: Editora 34, 2000.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** Campinas, SP: Ed. Millennium, 2005.

MONOGRAFIAS BRASIL ESCOLA – **Internet.** Disponível em: <http://monografias.brasilescola.uol.com.br/computacao/internet.htm>. Acesso em: 08 set. 2017.

MONTEIRO NETO, J. A**. Aspectos Constitucionais e Legais do Crime Eletrônico.** Fortaleza, 2008.

NIGRI, Deborah Fisch. **Crimes e segurança na internet**. In Verbis, Rio de Janeiro: Instituto dos Magistrados do Brasil, Ano 4, n. 20, 2000.

NOGUEIRA, Sandro D'amato. **Crimes de Informática.** 2 ed. Ver atual. E ampliada, Campinas: BH, 2008.

NORTON - **O que é crime cibernético?** Disponível em: <https://br.norton.com/cybercrime-definition> Acesso em: 12 set. 2017.

OFICINA DA NET – **Diferença entre Ransomware, RAT, Backdoor, Worm e BOT**. Disponível em:<https://www.oficinadanet.com.br/post/18266-diferenca-entre-ransomware-rat-backdoor-worm-e-bot> Acesso em: 14 set. 2017.

OFICINA DA NET - **Diferença entre: vírus, spam, spyware, worm, phishing, botnet, rootkit**. Disponível em: <https://www.oficinadanet.com.br/post/12991-diferenca-entre-virus-spam-spyware-worm-phishing-botnet-rootkit> Acesso em: 14 set. 2017.

OFICINA DA NET – **Golpes da internet: Confira a lista dos principais saiba como evitar cair na armadilha.** Disponível em: <https://www.oficinadanet.com.br/post/12727-golpes-da-internet-confira-a-lista-dos-principais-e-saiba-como-evitar-de-cair-na-armadilha> Acesso em: 21 set.2017.

OFICINA DA NET – **Quais são os crimes virtuais mais comuns?** Disponível em: <https://www.oficinadanet.com.br/post/14450-quais-os-crimes-virtuais-mais-comuns> Acesso em: 14 set. 2017.

ROSA, Fabrizio. **Crimes de informática**. 2. ed. Campinas: Bookseller, 2005.

ROSSINI, Augusto Eduardo de Souza. **Informática Telemática e Direito Penal**. São Paulo: Memória Jurídica 2004.

SAFERNET denuncie. Disponível em: <http://new.safernet.org.br/denuncie> Acesso em: 01 out. 2017.

SEDUC - **Vivendo uma nova era: a tecnologia e o homem, ambos integrantes de uma sociedade que progride rumo ao desenvolvimento**. Disponível em: <http://www.seduc.mt.gov.br/Paginas/Vivendo-uma-nova-era-a-tecnologia-e-o-homem,-ambos-integrantes-de-uma-sociedade-que-progride-rumo-ao-desenvolvimento.aspx> Acesso em:08 set. 2017.

SHARIFF, Shaheen – **Cyberbullying: questões e soluções para a escola, a sala de aula e a família.** Porto Alegre,2010.

SOUZA NETO, P. A. de**. Crimes de Informática.** Itajaí, 2009.

SUA PESQUISA - **História da Internet.** Disponível em: <https://www.suapesquisa.com/internet/> Acesso em: 06 set. 2017.

TECMUNDO - **Acompanhe a linha do tempo do ataque hacker: MPSP, INSS e TJSP fora do ar**. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/116639-mp-tribunal-justica-sp-desligam-maquinas-ataque-hacker.htm> Acesso em: 18 set. 2017.

TECMUNDO - **A história dos computadores e da computação.** Disponível em: <https://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm> Acesso em 06 set. 2017.

TECMUNDO - **Alerta: cibercriminosos obrigam crianças a participar do jogo 'Baleia Azul'.** Disponível em: https://www.tecmundo.com.br/crime-virtual/115715-alerta-cibercriminosos-obrigam-criancas-participar-jogo-baleia-azul.htm> Acesso em: 13 out. 2017.

TECMUNDO – **Brasil é o país da América Latina mais atacado por ransomware.** Disponível em: <https://www.tecmundo.com.br/seguranca/121879-brasil-pais-america-latina-atacado-ransomware.htm> Acesso em: 15 set. 2017.

TECMUNDO - **Crime de ódio na internet será julgado como crime no 'mundo real'** Disponível em: <https://www.tecmundo.com.br/seguranca/121117-crime-odio-internet-julgado-crime-mundo-real.htm> Acesso em: 05 out. 2017.

TECMUNDO – **Criminosos vendem ferramenta para espionar Windows por R$ 18 mil.** Disponível em: <https://www.tecmundo.com.br/seguranca/121708-criminosos-vendem-ferramenta-espionar-windows-r-18-mil.htm> Acesso em: 16 set. 2017.

TECMUNDO - **Crime virtual: o que é e como se proteger das ameaças**. Disponível em: <https://www.tecmundo.com.br/crime-virtual/97401-crime-virtual-proteger-ameacas.htm> Acesso em: 14/10/2017.

TECMUNDO - **Criminosos montam telas falsas para infectar o seu Android; qualquer versão**. Disponível em: <https://www.tecmundo.com.br/seguranca/121890-criminosos-montam-telas-falsas-infectar-android-qualquer-versao.htm> Acesso em: 16 set. 2017.

TECMUNDO - **Documento com senhas de sites de ecommerce do Brasil aparece no Pastebin**. Disponível em: <https://www.tecmundo.com.br/seguranca/119368-exclusivo-vazam-200-senhas-principais-sites-ecommerce-brasil.htm?utm_source=tecmundo.com.br> Acesso em: 19 set. 2017.

TECMUNDO - **Fique esperto! Não caia nas armadilhas soltas pela Internet**. Disponível em: <https://www.tecmundo.com.br/spyware/107-fique-esperto-nao-caia-nas-armadilhas-soltas-pela-internet.htm> Acesso em: 19 set. 2017.

TECMUNDO - **Golpe de ransomware usa o 'Buscar iPhone' para sequestrar seus aparelhos.** Disponível em: <https://www.tecmundo.com.br/seguranca/122313-golpe-ransomware-usa-buscar-iphone-sequestrar-aparelhos.htm> Acesso em: 15 set. 2017.

TECMUNDO – **Malware bloqueia computador e só libera após o envio de nudes.** Disponível em :<https://www.tecmundo.com.br/seguranca/122320-malware-bloqueia-computador-libera-acesso-envio-nudes.htm> Acesso em: 09 out. 2017.

TECMUNDO **- Onde denunciar crimes na internet?** Disponível em: <https://www.tecmundo.com.br/seguranca/8787-onde-denunciar-crimes-na-internet-.htm> Acesso em: 14/10/2017.

TECMUNDO - **Polícia assume controle de site de pornografia infantil e captura pedófilos**. Disponível em: <https://www.tecmundo.com.br/internet/122870-policia-assume-controle-site-pornografia-infantil-captura-pedofilos.htm> Acesso em: 09 out. 2017.

TECMUNDO - **Senado aprova nova regra para policiais investigarem pedofilia na internet**. Disponível em: <https://www.tecmundo.com.br/crime-virtual/115602-senado-aprova-nova-regra-policiais-investigarem-pedofilia-internet.htm> Acesso em: 10 out. 2017.

TECMUNDO- **Sinta como é ter suas informações roubadas e usadas pelo crime virtual.** Disponível em: <https://www.tecmundo.com.br/seguranca/119607-sinta-ter-informacoes-roubadas-usadas-crime-virtual.htm?utm_source=tecmundo.com.br&utm_medium=home&utm_campaign=tv> Acesso em : 22 set.2017.

TODA MATÉRIA – **História e Evolução dos Computadores**. Disponível em: <https://www.todamateria.com.br/historia-e-evolucao-dos-computadores/> Acesso em: 05 set. 2017.

WEB ARTIGOS - **O que é Ciberespaço?** – Disponível em: <http://www.webartigos.com/artigos/o-que-e-ciberespaco/22537/> Acesso em: 12 set. 2017.

GLOSSÁRIO

Antivírus - Programa de proteção do computador que detecta e elimina os vírus (certos programas danosos) nele existentes, assim como impede sua instalação e propagação.

Aplicativo - Programa de computador concebido para processar dados eletronicamente, facilitando e reduzindo o tempo de execução de uma tarefa pelo usuário.

Backdoor - Porta dos fundos. É uma porta aberta no sistema, não documentada, que permite ao criador ter acesso a ele (legitimamente ou não).

Botnet **-** É uma coleção de programas conectados à Internet que comunicam-se com outros programas similares, a fim de executar tarefas.

Bullying **-** É uma situação que se caracteriza por agressões intencionais, verbais ou físicas, feitas de maneira repetitiva, por um ou mais alunos contra um ou mais colegas

Cibercrime - É o nome dados aos crimes cibernéticos que envolvam qualquer atividade ou prática ilícita na rede.

Cibercriminoso - Criminoso especialista em informática e internet.
Ciberespaço - Espaço das comunicações por redes de computação.
Cibernético - Relativo ao ciberespaço ou à Internet.
Ciberterrorista - Palavra usada para descrever os ataques terroristas executados pela Internet, com o objetivo de causar danos a sistemas ou equipamentos.

Cracker - É o termo usado para designar o indivíduo que pratica a quebra (ou cracking) de um sistema de segurança de forma ilegal ou sem ética.

Criptografia - É um mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos e etc) ininteligível para quem não tem acesso aos códigos de “tradução” da mensagem.

Cyberbullying - É um tipo de violência praticada contra alguém através da internet ou de outras tecnologias relacionadas.

Cyberpunk - Palavra originada a partir da cibernética.
E-mail - Designação de correio eletrônico - sistema que permite o envio e recepção e de mensagens escritas através da internet ou outra rede de computadores.

Engenharia social **–** É um termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

ENIAC - Computador desenvolvido, entre 1942 e 1946, na Universidade da Pensilvânia (EUA), por J. Presper Eckert e John Mauchly, para Departamento de Defesa norte-americano. Possuía 18 mil válvulas, media cerca de 200 m² e pesava 30 toneladas. É considerado o primeiro computador digital eletrônico de alta velocidade.

Hacker - É uma palavra em inglês do âmbito da informática que indica uma pessoa que possui interesse e um bom conhecimento nessa área, sendo capaz de fazer *hack* (uma modificação) em algum sistema informático.

Hardware - É a parte física de um computador, é formado pelos componentes eletrônicos, como por exemplo, circuitos de fios e luz, placas, utensílios, correntes, e qualquer outro material em estado físico, que seja necessário para fazer com o que computador funcione.

Internet - É a rede mundial de computadores que permite comunicação entre pessoas conectadas a ela.

IP - É o principal protocolo de comunicação da Internet. Ele é o responsável por endereçar e encaminhar os pacotes que trafegam pela rede mundial de computadores.

Link - No âmbito da informática, a palavra *link* pode significar hiperligação, ou seja, uma palavra, texto ou imagem que quando é clicada pelo usuário, o encaminha para outra página na internet, que pode conter outros textos ou imagens.

Login **-** É um termo em inglês usado no âmbito da informática, um neologismo que significa ter acesso a uma conta de email, computador, celular ou outro serviço fornecido por um sistema informático.

Mainframes - É um computador de grande porte dedicado normalmente ao processamento de um volume enorme de informações.

Malware - É a combinação das palavras inglesas malicious e software, ou seja, programas maliciosos.

Modus operandi - é uma expressão em latim que significa **"**modo de operação**"**, na tradução literal para a língua portuguesa.

Notebook - Computador portátil, leve, projetado para ser transportado e utilizado em diferentes lugares com facilidade. Geralmente, contém tela de LCD (cristal líquido), teclado, mouse (geralmente um touchpad, área onde se desliza o dedo), unidade de disco rígido, portas para conectividade via rede local ou fax/modem, gravadores de CD/DVD.

Online Banking - Banco online, online banking, às vezes também banco virtual, banco eletrônico ou banco doméstico (do inglês home banking), são termos utilizados para caracterizar transações, pagamentos e outras operações financeiras de dados pela Internet.

Phishing - É uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos.

Ransomware - É um tipo de malware (software malicioso) que afeta sistemas informáticos ou redes inteiras de computadores.

Rootkit - É um software, na maioria das vezes malicioso, criado para esconder ou camuflar a existência de certos processos ou programas de métodos normais de detecção e permitir acesso exclusivo a um computador e suas informações.

Scam - Golpe aplicado no meio virtual. Geralmente é um e-mail com vírus para roubar informações importantes das pessoas.

Site - Página ou conjunto de páginas da Internet com informações diversas, acessível através de computador ou de outro meio eletrônico..

Smartphone - É um telefone celular, e significa telefone inteligente, em português, e é um termo de origem inglesa. O smartphone é um celular com tecnologias avançadas, o que inclui programas executados um sistema operacional, equivalente aos computadores.

Software - É qualquer programa de computador que possa ser utilizado, copiado e etc.

Spam - É um termo de origem inglesa cujo significado designa uma mensagem eletrônica recebida, mas não solicitada pelo usuário.

Spyware - É um software espião de computador, que tem o objetivo de observar e roubar informações pessoais do usuário.

Supercomputador - É um computador com altíssima velocidade de processamento e grande capacidade de memória. Tem aplicação em áreas de pesquisa que grande quantidade de processamento se faz necessária, como pesquisas militares, científica, química e medicina.

Tablet - É um tipo de computador portátil, de tamanho pequeno, fina espessura e com tela sensível ao toque (*touchscreen*). É um dispositivo prático com uso semelhante a um computador portátil convencional, no entanto, é mais destinado para fins de entretenimento que para uso profissional.

Telemática - É o conjunto de tecnologias da informação e da comunicação resultante da junção entre os recursos das telecomunicações (telefonia, satélite, cabo, fibras ópticas etc.) e da informática (computadores, periféricos, softwares e sistemas de redes), que possibilitou o processamento, a compressão, o armazenamento e a comunicação de grandes quantidades de dados (nos formatos texto, imagem e som), em curto prazo de tempo, entre usuários localizados em qualquer ponto do planeta.

Web - Nome pelo qual a rede mundial de computadores internet se tornou conhecida a partir de 1991.

Workstation - é o computador com capacidade de processamento de cálculos e gráficos superior aos comuns. Eles são destinados principalmente a usos profissionais específicos, tais como arquitetura, desenho industrial, criação de filmes 3D ou em laboratórios de física.

Worm - É um programa semelhante aos vírus, com a diferença de este ser auto replicante, ou seja, ele cria cópias funcionais de si mesmo e infecta outros computadores.