PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES
INTERNACIONAIS NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

PROTEÇÃO CONTRA OS CRIMES CIBERNÉTICOS NO BRASIL

A NECESSIDADE DE UMA LEGISLAÇÃO ESPECÍFICA E ATUALIZADA

ORIENTANDA: EVA CRISTINA DE SOUZA SILVA
ORIENTADOR: PROF. MS. WEILER JORGE CINTRA

GOIÂNIA
2021

EVA CRISTINA DE SOUZA SILVA

PROTEÇÃO CONTRA OS CRIMES CIBERNÉTICOS NO BRASIL

A NECESSIDADE DE UMA LEGISLAÇÃO ESPECÍFICA E ATUALIZADA

Artigo Científico apresentado à disciplina deTrabalho de Curso II, da Escola de Direito e Relações Internacionais, curso de Direito da Pontifícia Universidade Católica de Goiás(PUCGOIÁS).
Prof. Orientador: Ms. Weiler Jorge Cintra.

GOIÂNIA

2021

EVA CRISTINA DE SOUZA SILVA

PROTEÇÃO CONTRA OS CRIMES CIBERNÉTICOS NO BRASIL

A NECESSIDADE DE UMA LEGISLAÇÃO ESPECÍFICA E ATUALIZADA

Data da Defesa: 26 de maio de 2021.

BANCA EXAMINADORA

_____

Orientador: Prof. Ms. Weiler Jorge Cintra nota

_____

Examinador Convidado: Prof. Ms. José Eduardo Barbieri nota

Dedico este trabalho a Deus, o maior orientador da minha vida. Ele nunca me abandonou nos momentos de necessidade. E a minha mãe que foi e continua sendo minha inspiração, agradeço por todo carinho, dedicação e cuidado que me deu durante toda a minha existência.

A cada um de meus professores que dedicaram suas vidas para lecionar, e assim dividindo seus conhecimentos e estudos, para com que eu me descubre-se no Direito.

A universidade PUC em sua direção e administração, que abriu suas portas para me receber da melhor forma, dando assim um voto de confiança.

Sou grata por todo o apoio que recebi do meu orientador Weleir Jorge Cintra, que esteve junto comigo desde a escolha do tema, até o momento da conclusão do TCC. Me orientou durante a pesquisa fazendo com que o estudo fosse além do que eu imaginava.

Minha mãe que lutou sua vida toda para com que eu tivesse a oportunidade de tero estudo que tenho hoje, por acreditar em mim, sempre estando ao meu lado para com que meus objetivos fossem alcançados. Minha inspiração de mulher guerreira que em seus dias e noites batalhou para que eu permanecesse no meu objetivo.

A Orgasnização das Voluntária de Goiás que confiou em mim, dando a bolsa parcial para que assim eu me formasse na área que tanto amo e sonho atuar todos os dias de minha vida.

Aos meus padrinhos Josy e Dawillan que me apoiaram emocionante e financeiramente para que eu desse continuidade aos meus estudos, e meu grande sonho.

E ao mais importante, a Deus, que através de sua graça permitiu para que eu tivesse a oportunidade que tive e estou tendo. Me dando saúde e livrando de todos os impedimentos que mecercavam.

E a todos que participaram diretamente ou indiretamente na minha formação, o meu muito obrigada.

SUMÁRIO

PROTEÇÃO CONTRA OS CRIMES CIBERNÉTICOS NO BRASIL

A NECESSIDADE DE UMA LEGISLAÇÃO ESPECÍFICA E ATUALIZADA

EVA CRISTINA DE SOUZA SILVA [1]

RESUMO

Os crimes virtuais foram estudados no presente trabalho, que apresentou os seus diversos tipos, bem como o ordenamento jurídico brasileiro repreende os meliantes, que cometem tais crimes. Inclusive no mundo virtual existe duas denominações, os crackers, que são sujeitos que cometem o crime, e os hackers que protegem a rede virtual, abordados ao longo do presente artigo científico. Assim, a polícia tem que investiar os crimes virtuais e é necessário ter uma legislação específica para tratar sobre os tais crimes.

Palavras-chave: crimes virtuais; ciberespaço; cibercriminoso; Hacker; Cracker; DeepWeb.

INTRODUÇÃO

O presente trabalho estudará como são os crimes virtuais, sua origem, lugar do crime, os diversos tipos e quem são sujeitos que os praticam; para assim entrar no ponto principal, as leis que os sancionar, se elas são eficaz, se trazem justiça e segurança as vítimas.

A criação da internet e a tecnologia foi um momento muito importante, por fazer com que barreras fossem derrubadas, unindo pessoas de culturas diversas, diminuído o uso do papel, gerando novos empregos etc, mas infelizmente facilitou para os criminosos que logo tiraram vantagem.

Não era de se imaginar que os delinquentes tirariam aproveito do ciberespaço, ainda mais que não precisa gerar esforço físico, porém é necessário inteligência e os mais espertos crackers causam danos bem maiores, principalmente

[1] Acadêmica do Curso de Direito da Pontifícia Universidade Católica de Goiás, e-mail. evaaamanhecer@hotmail.com

nas empresas que possuem uma rede de computadores.

Os crimes virtuais ocorrem no ambiente conhecido como ciberespaço, sendo a arma do crime o computador ou o celular, onde os meliantes adentram no meio virtual e ali consegue dados pessoais das vítimas e que acarretaram enormes prejuízos, os quais serão abordados aos longo do presente trabalho.

Entender como cada crime virtual é cometido permitirá analisar onde as leis não estão dando certo, como elas deveriam ser aplicadas ou até mesmo a criação de novas leis. Mas para ter o devido sucesso a formação de uma legislação específica e atualizada vai ser fundamental.

1. CRIMES VIRTUAIS

Para entender sobre o que é crimes virtuais deve-se olhar como tudo se inciou, e foi no ano de 1960 o começo, diga-se que a origem do termo e definição de crimes virtuais, durante a tão imblemática e falada guerra fria, e que logo ápos no ano de 1969 para ter um avanço importante, a internet surgiu, com uso restrito aos militares do Estados Unidos. Tal fato para poder acontecer foi através da criação dos computadores em 1946, que nos dias de hoje tiveram uma grande evolução.

Os crimes em 1960 não foram grande coisa, eram manipulações, sabotagem ou espionagem, mas não tiveram grande viabilização. O marco para os crimes virtuais se deram no ano de 1980, os delitos ficaram cada vez mais grave, sendo eles, manipulação nos bancos, pornografia infantil, pirataria de programa, dentre outos.

O Brasil teve acesso as redes internacionais para pesquisa em 1991, mas somente em 1995 que teve acesso para o consumo e logo sentiu o impacto dos crimes virtuais e tiveram a consciência do que eles seriam em 1996, quando os sites ligados ao governo foram invadidos por criminosos.

Segundo Inellas (2009, p.05):

> A internet é uma rede de computadores, ligadas por redes menores, portanto comunica-se entre si, assim através de um endereço IP, onde variadas informações é trocada, é quando surge o problema, existe uma quantidade enorme de informações pessoais disponíveis na rede, ficando a mercê de milhares de pessoas que possuem acesso à internet, e quando não é disponibilizada pelo próprio usuário, são procuradas por outros usuários que busquem na rede o cometimento de crimes, os denominado Crimes Cibernéticos.

Com o avanço da tecnologia e o grande acesso de usuários cada vez maior, os delitos virtuais também tiveram mais vítimas e assim tendo casos que não podiam ser solucionados por falta de lei. O Brasil se preocupou e através da Constituição Federal de 1988 normas sobre questões informática foram feitas.

Asssim depois de entender como tudo se iniciou, deve entender o que seria os crimes virtuais, que podem ocorrem pela intenert, onde o criminoso pode difamar a sua vítima ou divulgar pornografia infantil; já a outra forma é pelo computador, que seria roubar dados ou instalar vírus.

Segundo Lévy (2000, p.17) 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 oceânicodeinformaçõesqueeleabriga,assimcomoos seres humanos que navegam e alimentam esse universo. Quanto ao neologismo ‘cibercultura’’, especifica aqui o conjunto de té cnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem no juntamente com o crescimento do ciberespaço.

O ciberespaço tem sua existência virtualmente, que logo após com o surgimento da Internet ele passou a existir passando a ser um meio de comunicação, sendo assim, onde as pessoas podem se interagir com outros usuários, até mesmo de longa distância, possibilitando o começo de amizades virtuais, a criação de comunidades, lives dentre outros.

Segundo a pesquisa TIC (Tecnologias da informação e da comunicação) domicílio 2019, mostrou que 134 milhões de pessoas tem acesso a internet. Não é um número que asssusta porque nos dias de hoje é um fato normal, a tecnologia cresce a todo instante, cada vez mais é usada. Esse nivel de usuário aumentou bastante nesse ano de 2020, por causa da pandemia gerada pelo Coronavírus (COVID-19).

De acordo com Rossini (2004, p. 110):

> [...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa,comissivaouomissiva,praticadaporpessoa 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.

Como todo o crime, o virtual também é aconduta onde o criminoso não segue a lei, atingindo a sua vítima de forma dolosa ou culposa. O fato que diferencia de outros crimes é a questão que ele ocorre no ciberespaço, ou seja, virtualmente, o que torna mais dificil de punir o agente, mas não impossível.

A associação SaferNet Brasil, em parceria com o Ministério Público Federal, em 2018 registrou pelo menos 366 crimes virtuais por dia no Brasil. Agora imagine esse indice nos dias de hoje, onde a pandemia fez com que todos ficassem em casa, várias pessoas acessando a intenert para trabalhar, estudar ou se comunicar com outros. E preciso entender que os criminosos iram se aproveitar de qualquer situação para tirar vantagem, então deve ter leis que realmente irão proteger as vítimas afetadas por esses delitos.

1.1 TIPOS DE CRIMES VIRTUAIS

Os crimes virtuais mistos é onde a internet e o sistema informático são importantes para que o fato criminoso aconteça, mesmo que o objetivo não seja a rede e sim meios não relacionados ao meio virtual. Já os crime virtuais comuns é o qual o uso da informática é apenas a forma pelo qual o crime é praticado, sendo este, já tipificado pela lei.

Os crime virtuais próprio é a conduta ilícita com objetivo de causar dano ao sistema informático da vítima. Já o delito impróprio é o qual através da informática o deliquente irar danificar o patrimônio ou bem jurídico comum da vítima.

Segundo dispõe Vianna e Machado (2013, p. 35) “crimes cibernéticos mediatos ou indiretos são aqueles delito-fim não informático que herdou as características do delito-meio informático, realizado para configurar a própria consumação do ato em si”.

Abaixo alguns crimes que ocorrem na rede com acesso ou foram da rede, de forma resumida para compreender um pouco de cada um que será citado:

Invasão de dispositivo (art.154-A do Código Penal) sem a devida autorização do proprietario, que nele pode gerar outros delitos que é o furto (art, 155 do Código Penal) de dados que podem ser usados para prejudicar o dono, já o furto mediante abuso de confiança (art. 155, § 4º, inciso II, do Código Penal), através da segura da vítima com criminoso por exemplo passa os seus dados bancários, que acabam sendo utilizados sem a permissão do dono.

Os crimes de ódio é comentar de forma preconceituosa ou qualquer outro tipo de discriminação, sendo praticado por si ou induzido e incitando terceiro ao crime. Com objetivo de retaliação a raça, cor, etnia, religião ou procedência nacional. (art. 20, da Lei nº 7.716/89, art. 3º, IV da Constituição Federal, nos arts. 1º e 2º da DUDH, e a Lei nº 9.459/97 e art. 14, § 3º Código Penal).

Divulgar por internet, parcial ou total sem autorização o nome, documento ou o ato de adolescente ou criança de procedimento policial, judicial ou administrativo que se deve manter em confidência. (art. 245 da Lei nº 8.069/90).

Os mais comuns são contra a honra, sendo elas, calúnia (art. 138 do Código Penal) que é noticias incriminadoras falsas, as famosas fakenews é um bom exemplo; injúria (art. 140, Código Penal) é quando ofende a dignidade da pessoa, podem ser por meio de comentários; e a difamação (art. 139 do Código Penal) onde ofende a reputação da pessoa, por comentário ou até mesmo vídeos.

O crime de ameaça (art. 147 do Código Penal) também acontece pela internet, quando o ameaçador por meio de conversa ou ligação ameaça a vítima, sua vida, entes queridos ou seus bens.

A revelação de segredo (art. 153, Código Penal) é a divulgação de informação, sendo documento ou correspondência particular e confidencial que pode gerar danos a quem lhe pertence.

Apologia ao crime (art. 287 do Código Penal) criar comunidades para ensinar a infringir a lei ou vangloriar crimes cometidos por si ou terceiro. Também pode ser quando apoia o autor do crime.

Incitação ao crime (art. 286 do Código Penal) incentivar a prática certo tipo de crime pela internet. De forma pública e sem um grupo específico. Por exemplo, no meio de uma greve incentivar as pessoas ao redor a cometer vandalização.

Estelionato (art. 171 do Código Penal) promoções falsas com o propósito de atrair as pessoas que ao acessar o site ou link, o dispositivo terá furtado os seus dados. Obtem a vantagem ilícita sobre a vítima ao induzir ou mantiver ao erro.

Já a fraude virtual é através da invasão ou qualquer tipo de adulteração no dispositivo em seus sistemas de dados (art. 155, do Código Penal), conforme Gil (2000, p.144):

> 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.

Falsificação de medicamentos (art. 273, § 1º do Código Penal), produto adulterado para fins terapêutico ou medicinais, vendendo estes, divulgado ou exportando.

A falsa identidade virtual (art. 307 do Código Penal), com objetivo de obter vantagem para si ou terceiro ou causar dano a outro, são os chamados perfis fakes. Segundo Régis (2004, p. 278):

> No artigo 307 o Código prevê uma forma de falsidade não mais documental, nem mesmo material ou ideológica, mas pessoal: ilude alguém a respeito da própria identidade ou da identidade de terceiro, para obter vantagem ou causar-lhe dano.

O plágio (art. 12 da Lei nº 9.610/98) cópia informação ou texto sem colocar a fonte de quem a publicou ou escreveu, o bom exemplo são alunos em seus trabalhos que copiam o texto como se fosse de si próprio, sem seguir a norma da ABNT colocando com citação e sua fonte.

A pornografia infantil divulgar,obter ou salvar vídeo, foto ou qualquer tipo relacionado, de criança ou adolescente realizando atividades sexuais ou se expondo de forma pornográfica. (art. 241-A c/c art. 241-E da Lei nº 8.069/90). O indivíduo é um adulto que possue a falha em sentir atração por crianças ou adolescentes. A conduta criminosa tem que ocorrer junto com a doença, para configurar crime (art. 240, Código Penal).

E a pornografia de vingança (“revenge porn”), quando sem autorização expõem da intimidade sexual de alguém por vídeo ou qualquer outro meio, costumam ser obtidos através de relacionamento afetivo ou vínculo emocional que o sujeito teve com a vítima (art. 140-A Código Penal).

O estupro ou “sextorsão” (art. 213, Código Penal) consiste em constranger a vítima por meio de chantagem ou violência, para fazer com que satisfaça desejos sexuais do sujeito por videoconferência, com atos libidinosos.

1.2 COMO OCORREM OS CRIMES VIRTUAIS

Os crimes virtuais podem ocorrer em acesso a internet ou fora dela, pois os delitos podem ocorrer no dispositivo que é usado para entrar na rede que é o ciberespaço. A conduta tem por objetivo afertar o sistema da vítima e a própria, para roubar dados, divulgar informações sigilosas, dentre diversas infrações.

Conforme Cunha (2016, p.248) a ação penal será:

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

A punição será por violação do dispositivo eletrônico de terceiros ou a instalação de vulnerabilidade que poderá causar dano. Tal dispositivo é atefato que possue armazenamento, processa informações, dados, e ou propagadas.

O agente agira em duas etapas, na primeira irá derrubar a proteção que a no dispositivo para que assim posssa furtar dados, alterar ou destruir, já na segunda ele fará a instalação de vírus ou meios para danificar o bem da vítima.

As partes vão ser o sujeito passivo, onde qualquer pessoa poderá ser, sem a necessidade de qualidades ou condições especiais. Já o sujeito ativo será pessoa física ou jurídica proprietária do dispositivo eletrônico que foi invadido ou vítima do delito.

Conforme explica Filho (2000, p.85):

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes), e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou.

A consumação do ciberataque se dá no exato momento de sua entrada ao dispositivo eletrônico da vítima, com o propósito de obter, destruir, alterar os

dados ou as informações. Já a tentativa de apropriação do criminoso virtual nesse aparelho eletrônico será constituída em todas às vezes em que, houver vestígios da execução da invasão.

O arrependimento eficaz é possível no delito dos crimes virtuais, quando em vontade própria desiste de cometer o ato ou impede a produção do ato, segundo o art. 15 do Código Penal. A também previsão de crime impossível em que o agente não será penalmente punido, por realizar uma conduta e não atinge o seu objetivo ou por absoluta ineficácia do meio, bem como absoluto erro do objeto material utilizado na conduta criminosa, mediante disposição do art. 17 do referido Código.

2. A INTERNET E O DIREITO

A internet é um aplicativo que está presente em todos os computadores do nosso planeta, fazendo com que se tenha uma conexão entre eles, havendo uma troca de informações e comunicação, sendo ela feita na mesma cidade ou do outro lado do mundo.

Sendo o principal meio de comunicação que existe, ela foi criada pelos norte-americanos dentre 1960 a 1970. Primeiro veio ARPANET (Advanced Research Projects Agency Network), que era ligada a somente quatro computares, que logo mais outros se juntaram a esses, bem diferente da internet que é ligada a todos os computadores, mais eficaz e com uma velocidade maior.

De acordo com Moherdaui (2002, p. 19):

> A internet é um conjunto de recursos tecnológicos que coloca à disposição de qualquer cidadão que possui computador, um modem e uma linha telefônica uma enorme quantidade de informação e possibilidades de acesso a serviços diversificados.

A internet é como um novo mundo onde nos permite diversas formas de expressa ideias, informações, ensinamentos e transações econômicas. Como o seu objetivo de manter todos conectados a liga distância, as informações circulam de uma forma anônima e sem a devida regulação, em que se ignoram regras e fugindo de legislações e jurisdições.

O Governo Federal começou a disponibilizar a Internet ao público brasileiro em 1995, mas com o Laboratório Nacional de Computação Científica (LNCC) no ano de 1998 no Rio de janeiro que teve a Bitnet, estabelecida através da

Universidade Maryland, onde a conexão era 9 600 bits por segundo.

A internet está em atos simples desde o dia-a-dia de um jovem a econômia de grandes bancos ou na saúde, sendo assim um direito fundamental como água, à luz, à informação, à saúde, à privacidade,eentre outros que são essenciais.

Sendo algo tão fantástico a internet também tem seus defeitos, um deles sendo a grande liberdade em qualquer um ter acesso e ser considerado um “lugar sem lei”, o direito entrou em cena para mudar esse fato.

Como se sabe o direito é justo e correto, com o objetivo de criar legislações, jurisprudência e doutrinas que iram fiscalizar um determinado objetivo, nesse caso a internet que cresce a cada dia.

Assim o Congresso Nacional criar Leis para os crimes informáticos, onde certas condutas deram consideradas criminosas, que o caso de invasão de computadores, roubo de dados, bullying virtual, e dentre outras que são citadas na legislação.

O bem nesse caso que será protegido é a privacidade da pessoa, ou seja, será assegurado que a privacidade não seja violada, por exemplo o furto de dados. Tal bem esta amparado pelo artigo 5º, X da Constituição Federal de 1988.

2.1 CIBERCRIMINOSO

Aproximadamente no final dos anos 90 na reunião do subgrupo G-8, ao qual composto por oito grandes paises, em quesito de riquesa (Estados Unidos, Japão, Alemanha, Canadá, França, Itália, Reino Unido e Rússia), é que surgiu o termo cibercrime. Tal reunião discutia sobre como combater as maneiras ilícitas na internet, para que houvesse solução para o caso deve-se dar um uma classificação ao delito, o que foi feito.

Cibercrime é todos os crimes cibernéticos cometidos de maneira que conforme a lei é proibida, dentro da rede, ou seja, em objetos eletronicos conectados a internet ou não, de acordo com Simas (2014, p. 12), “quem que o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital”.

Suas principais características é predominância transnacional, que ultrapassa a froteira de sua nacionalidade atigindo outros países, tonando díficil a investigação para coleta de prova contra o acusado. A outra é que como a população possui acesso aos computadores, onde é possível de qualquer pessoal cometer o fato visando o lucro ou não, com motivação pessoal ou até mesmo política.

Muitas vezes se usa computadores para atingir outros computadores, já o que visam esse aparelho envolvendo com virus ou malware (qualquer pograma ou código que prejudica o sistema).

Phishing também é considerado um crime cibernético, onde tanto na caixa de entrada de e-mails ou na opção *spam* ou outros meios de comunicação são utilizados para enviar em grande quantidade algo que induza as pessoas que receberem essa mensagem, a prejudica a sua segurança ou até mesmo a empresa em que essa pessoa trabalha.

Ele funciona com uma propaganda sem fundo de verdade, muitas vezes a pessoa com a simples curiosidade ao clicar tem seus dados pessoais roubados, gerando graves danos.

A “spear – phishing” atinge especificamente a segurança da empresa que a pessoa trabalha, através de campanhas que chamam a atenção do funcionário, que acaba atingindo a organização.

As mensagens parecem ser muito confiáveis com um público alvo com maior segurança. Já a phishing que atinge grupos em massa não se preocupa tanto em demostrar que a informação é verídica.

Os ataques Ddos são às vezes iniciados por dispositivos conectados a internet das coisas, onde o ataque tem o objetivo de paralisar a rede ou um sistema, envia vários pedidos de conexão por spam. As ameaças tem o objetivo de extorquir dinheiro ou uma distração para que outro crime cibernético aconteça sem que seja percebido.

2.2 HACKERS X CRACKERS

Os crackers visam infringir a segurança eletrônica para conseguir algum lucro, em benefício próprio ou causar dano às pessoas e as empresas. São vistos

como cibercriminosos, pois usam a sua inteligência com informática de forma ilegal.

O termo foi dado pelos próprios hackers em 1985 para não associar essas pessoas com eles. Oliveira (2006, p. 26) explica:

> [...] Cracker: possui tanto conhecimento quanto aos hackers, mas com a diferença de que, para eles, não basta entrar em sistemas, quebrar senhas e descobrir falhas: precisam deixar um aviso de que estiveram por lá. Geralmente são recados malcriados, mas, algumas vezes, podem destruir partes do sistema, ou aniquilar tudo o que veem pela frente. Também são atribuídos aos crackers programas que retiram travas de softwares, bem como os que alteram suas características, adicionando, ou modificando, opções, muitas vezes relacionadas à pirataria.

Os hackers utilizam seu conhecimento em informática para protegerem dados pessoais, verificar o nível de danos causados pelos crackers, ou seja, só tem a intenção de torna o mundo da informática seguro dos delinquentes que habita esse espaço.

Em relação ao hacker Nogueira (2008, p. 61) explica que:

> Este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver que consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual. Várias empresas estão contratando há tempos os Hacker's para proteção de seus sistemas, banco de dados, seus segredos profissionais, fraudes eletrônicas etc.

Em 1960 nós Estados Unidos foi criado o termo hack, para as pessoas que descobriam algo diferente para qualquer tipo de problema, logo associou a programadores de computadores. Já programador é o que escreve, cria ou faz manutenção de software em um grande sistema ou alguém com seu computador pessoal criar um software.

O hacker exige formação em alguma área conectada à informática, pois a maioria dos cursos tem matérias associadas à segurança da informação. Entre elas, estão as graduações de Tecnologia da Informática, Redes de Computadores, Sistema de Informação, Engenharia de Software, Ciência da Computação, Engenharia da Computação.

Desenvolvendo e modificando softwares, hardwares de computadores, novas funcionalidades em relação a sistemas de informática. Quem possuí algum conhecimento avançado em áreas específicas da computação ou descubra algo

novo, pode ser considerado hackers.

Já White hats são os hackers com especialidade em TI ou possibilidades semelhantes, com preferência na área de segurança e que aproveita suas competências para auxiliar empresas. São especialistas com princípios e que costumam ser contratados como analistas de sistemas.

Tem por objetivo encontra uma instabilidade na segurança, logo a demostra ao desenvolvedor, dando a vantagem para que ele corriga o erro de seu produto e tornar a sua segurança mais eficaz, antes que seja prejudicado.

Conforme diz Assunção (2008, p. 13):

> Hacker White-Hat seria o “hacker do bem”, chamado de “hacker chapéu branco”. É aquela pessoa que se destaca nas empresas e instituições por ter um conhecimento mais elevado que seus colegas, devido ao autodidatismoe à paixão pelo que faz. Não chega a invadir sistemas e causar estragos, exceto ao realizar testes de intrusão. Resumindo: tem um vasto conhecimento, mas não o usa de forma banal e irresponsável.

Outro termo conhecido é o Black hats e as pessoas que enganam os sistemas e são experientes em apropriação de sites, porém, com objetivos duvidosos, suas atitudes os fazem ser desmoralizados pelos outros grupos, acabando sendo comparados aos crackers.

O Black hats não possui paciência para tratar em vantagem de seus objetivos e pensando que pode ser melhor que os outros, utiliza de ferramentas incertas para infringir os mecanismos de busca e manter-se sempre na frente.

Agora o Gray hats realizam testes de credibilidade em sistemas e redes de computadores, mas sem precisão de ter a permissão do proprietário para isso, sendo assim, seus métodos não eram sempre éticos, podem tentar danificar um sistema de computador sem permissão, comunicando logo a empresa dando a possibilidade para reparar o erro.

Os Newbies são individuos em aprendizagem na área de hacking, pois na maioria das vezes têm um grande interesse e desejo de aprender e de participar desse espaço. Por esse fato, os noobs são ignorados ou caçoados, alias de não possuírem, ainda, uma característica definida.

Lammers não possuem conhecimento algum sobre hacking ou que sabem um pouco do assunto, e acabam usando meios progetados por outros que realmente são hacking, para operarem ataques. Esse termo surgiu entre o final da década de

80 e no período da década de 90.

Os ataques de lammers a maioria das vezes não são experientes, pois pelo pouco conhecimento que tem sobre programação e tecnologia. Alguns deles são apenas audaciosos da internet e do mundo virtual, em busca de diversão, ou novos métodos de se agradarem na internet.

Buscam por fama, seus meios de ataques são utilizados através de exploits, trojans e outras invenções de cracking, usam o disfarce, para realizar atentados envolvendo transações bancárias e de dados, fraudar cartões de crédito, alterar sites, entre outros.

Wares, eles exploram os software com disposição de cópias e passwords falsos, de costume através de sites de baixa segurança. Bem diferente dos Coders, que sao codificadores, entendedores de uma ou mais linguagens que torna possível escrever segurança, exploits, programas, e ferramentas de invasão, em busca de fragilidade que possam ser analisadas.

Phreakers são individuos crackers que possuem habilidades na área de telefonia e dispositivos móveis, onde acabam fazendo seus atacam dentro desses meios. Ficaram conhecidos operadoras de telefone estavam entrando em cena na década de 70.

Antes eles criaram um método para fazer ligações gratuitas, que hoje em dia não funciona mais. Agora na atualidade seus crimes são a clonagem de chips, espionagem de ligações e mensagens e entre outros.

Carder é a pessoa que através de informações bancárias como números de cartões de conta corrente, de crédito ou poupança, ou até mesmo contas em sites movimentam contas bancárias, para privilégio de si mesmo, como comprar algo, fazer transferência para abrir contas de laranjas (pessoa que de forma, voluntária ou involuntariamente, recebe transações financeiras criminosas), entre outros atos ilícitos.

Script Kiddies são como discípulos de Crackers costumam usar técnicas que ainda não possuem controle para danificar computadores e também ganhar vantagens próprias. Acontece que o Cracker viola um sistema grande usando um script kiddie como um faixada primário, tornando ele o principal culpado que dá invasão.

O Cheater é dado às pessoas que trapaça, usa cheats, que são códigos que infringem o sistema de certo jogo, para obter alguma vantagem no jogo online

ou local. Diferente dos VIRRI que são criadores e colecionadores de programas, de vírus e jogos.

3. DA INVESTIGAÇÃO POLICIAL

No começo da investigação compete a instauração do inquérito policial, onde será feito depois a denúncia do crime em uma delegacia especializada em crimes virtuais, sendo assim, dá se inicio a fase da examinação de provas colhidas durante o fato.

A definição da competência penal, ou seja, o foro do local do delito, assim ensina Capez (2012, p 254), será:

> […] competência é a delimitação do poder jurisdicional (fixa os limites dentro dos quais o juiz pode prestar jurisdição). Aponta quais os casos que podem ser julgados pelo órgão do Poder Judiciário. É, portanto, uma verdadeira medida da extensão do poder de julgar.

O delegado deve buscar permanecer na plena confirmação probatória obtida, pelo fato que este tipo penal, em toda ação feita através de algum aparelho eletrônico, acaba deixando algum tipo de indício de codificação em uma rede de dados, podendo sem até mesmo na *deep web*, em mensagens criptografadas (protocolos que impedem terceiros de lerem mensagens privadas), ou nos *ips* (tem a objetivo de identificar um computador em uma rede) das máquinas usadas para cometer os delitos.

Com isso, o profissional deve buscar investigar as provas encontradas, para assim desvendar a sua autoria, sendo de grande importância, que as pessoas que usam dispositivos eletrônicos não excluam arquivos, ou joguem fora o aparelho que foi atacado ou bulado, por algum vírus, para as provas não serem perdidas.

A investigação dos crimes cibernético ocorre pela inspeção técnica, que pode examinar a autoria e materialidade dos delitos executados através de uma rede que conecta os computadores.

O meio digital chega a atingir tanto o direito individual quanto o direito coletivo, pois os delitos prejudicam a todos, pelo fato que os crimes cibernéticos são capazes de alcançar uma pessoa ou várias.

Conforme Lima (2014, p. 497):

> Diferencia-se a investigação preliminar da instrução processual por este motivo: enquanto a investigação criminal tem por objetivo a obtenção de dados informativos para que o órgão acusatório examine a viabilidade de

> propositura da ação penal, a instrução em juízo tem como escopo colher provas sob o crivo do contraditório e da ampla defesa para demonstrar a legitimidade da pretensão punitiva ou do direito de defesa.

Tem por objetivo na investigação identificar nos tipos de comunicação o endereço do IP que é o endereço lógico de um sistema de identificação global, que faz com que cada computador seja identificado de forma única. O IP é utilizado pelo criminosos em suas ações.

O acesso a informações privadas da vítima ou do acusado é essencial, pois para uma averiguação das provas, é preciso a identificação do IP do computador do local onde foi feito o acesso do aparelho, em que ocorreu a ação criminosa, irá acontecer uma pesquisa para o passo seguinte da investigação, que só efetua através do acesso da polícia no aparelho da vítima.

Segundo Feitoza (2009, p. 820):

> infiltração é a introdução de agente público, dissimuladamente quanto à finalidade investigativa (provas e informações) e/ou operacional (“dado negado” ou de difícil acesso) em quadrilha, bando, organização criminosa ou associação criminosa ou, ainda, em determinadas hipóteses (como crimes de drogas), no âmbito social, profissional ou criminoso do suposto autor de crime, a fim de obter provas que possibilitem, eficazmente, prevenir, detectar, reprimir ou, enfim, combater a atividade criminosa deles

O Estatuto da Criança e do Adolescente (Lei nº 8.069/90) demostra os crimes envolvendo a criança e o adolescente em meio à exploração sexual, a infiltração virtual permite que os criminosos sejam localizados.

A infiltração é feita por agentes de polícia, que devem ser os membros das corporações as quais são: Polícia Federal propriamente dita, rodoviária e ferroviária; e Polícia Estadual, tanto civil, militar e corpo de bombeiros, organizada em cada unidade da federação. È importante, mencionar que nem todos estes órgãos tem competência de investigar.

São habilitados a infiltrar os policiais federais e civis, nós quais a polícia federal possui a tarefa de averiguar as infrações penais, já os polícias civis estaduais tem a tarefa de investigar.

A infiltração virtual como as outras infiltrações, precisa da autorização judicial e oitiva do MP - Ministério Público, quando não ele mesmo o autor do pedido. A autorização é necessária para controlar as ações dos agentes policiais que se inteferem nas atividades criminosas com intuito de investigação, onde colocará limite na forma de colher as provas.

Pode ser feita pelo delegado de polícia (não é parte) ou requerimento do (parte da relação processual). Ambos seram através de um pedido formulado ao juiz, para que seja autorizada a infiltração.

O prazo de duração da investigação é de 90 dias, pode haver renovação, sendo o prazo máximo para as investigações, 2 anos. Nesse prazo, a autoridade policial e os membros do MP poderão pedir relatórios nos quais o agente infiltrado irá conceder contas de sua atividade.

Contudo deve-se demostrar que é necessária à dilação do prazo da investigação, seja para colher mais provas, descobrir as pessoas envolvidas, etc, porém o relatório deve ser feito no prazo de 90 dias, onde será feita a análise para verificar se a necessidade de prorrogar o prazo.

A aquisição da base de conexão do responsável e de seus dados cadastrais é essencial para a investigação de crimes cibernéticos. Através do endereço IP, pode-se identificar de onde veio à conexão e com isso expor a identidade de quem teve acesso a estipuladas páginas, que por meio de download, em certos arquivos ou o material em nuvem.

Se os dados de conexão e cadastrais forem suficientes para servir como prova material do crime e de indícios de autoria, a infiltração não é preciso.

O acesso aos autos da infiltração deve ser acompanhando pelo MP ou pelo delegado de polícia e cabe ao juiz apreciá-las. O sigilo deve ser mantido durante todo o percurso da infiltração, pois a vazamento de informações podem gerar danos à investigação e risco ao policial nela comprometido.

Após a denúncia do MP é aberto prazo para a Defesa, no processo deve ser mantida a identidade do agente infiltrado e das vítimas dos crimes. O agente policial infiltrado que não observar a finalidade da investigação responderá pelos excessos praticados e será punido disciplinarmente e criminalmente.

Com a objetivo de identificar certo criminoso e de confirma que se trata de alguém que armazena e transmite o agente infiltrado pode receber tais imagens, podendo armazená-las para depois juntá-las ao relatório da investigação, como também pode repasa, para manter a confiança dos criminosos da investigação. Se o agente policial mantém, com intuito probatório, algo transmitido via internet não haverá crime de sua parte.

Conforme Guimarães, citado por Cunha e Pinto (2014, p. 114):

> O agente infiltrado mantém sua verdadeira identidade encoberta, adotando

> uma falsa, para ganhar a confiança dos criminosos; passa a viver no submundo do crime, inclusive fazendo parte dos planos e ações ilícitas, sem, no entanto, dar causa diretamente, à prática de um crime (a atividade do agente é limitada). Pode mesmo chegar a prestar apoio moral e material, e praticar atos de execução de crime, como permite o regime legal português de ações encobertas, mas não pode – está proibido – impulsionar o crime.

Costuma ser necessário criar uma identidade para o policial, pois ele trabalha pessoalmente com os criminosos. Segundo Lopes (2011, p. 517):

> Somente os membros da Polícia Judicial poderão atuar como infiltrados e terão seus dados de identidade alterados. Estes dados falsos de identidade serão outorgados pelo Ministro do Interior e terão a duração de seis meses, prorrogáveis por mais seis meses. A resolução de alteração do nome será sigilosa e somente ali constará o nome verdadeiro. Poucos tem acesso ao nome verdadeiro, para uma segurança do agente infiltrado. Poderão adquirir e transportar os objetos dos delitos e estarão habilitados a atuar em tudo que tiver relação com a investigação concreta, atuando na vida social e jurídica sob a falsa identidade. Do mesmo modo, se forem chamados a testemunhar no processo, atuarão com o nome falso.

Existe a possibilidade de que mediante pedido a autoridade judicial, os órgãos de registro e de cadastro públicos adicionem em seus bancos de dados às informações importantes para a efetividade da identidade fictícia criada.

4. DEEPWEB

Em 1980 um funcionário da CERN - Organização Europeia para a Investigação Nuclear, Tim Berners-Lee desenvolveu um sistema capaz de reconhecer e armazenar inúmeras informações, o que gerou o WWW (World Wide Web).

Com o passar dos anos foi desenvolvido por Michael K Bergman o browser (navegador) que poderia ser usado para “surfar” na rede, ele disponibilizou o artigo The Deep Web: Surfacing Hidden Value (A rede profunda: trazendo à tona valores escondidos), fazendo com que o artigo tornasse a origem à palavra Deep Web .

Segundo Borges, Sartori e Barros (2015?):

> A Deep Web é o conjunto de conteúdos da internet não acessível diretamente por sites de busca. Isso inclui, por exemplo e em regra, documentos hospedados dentro de sites que exigem login e senha. Sua origem e sua proposta original são legítimas. Afinal, nem todo material deve ser acessado por qualquer usuário (pode ficar dentro de sites comuns, na forma de arquivos e dados baixáveis, ou escondidos em endereços excluídos propositadamente dos mecanismos de busca).

Na internet é possível estabelecer a localização de qualquer aparelho com acesso à rede, a partir do IP (Internet Protocol), ou seja, o IP é um endereço exclusivo que qualquer computador ou servidor tem para ser ingressado por Internet.

Na Deep Web em alguns casos não é possível localizar o IP do usuário, pois existem várias páginas, que dificultam a localização dos usuários.

Segundo, Pompéo e Seefeldt, (2013, p. 453).

> [...] informações públicas na Deep Web são comumente de 400 a 500 vezes maiores que as definidas da World Wide Web. A Deep Web contém 7.500 terabytes de informações comparadas a 19 terabytes de informação da Surface Web. A Deep Web contém aproximadamente 550 bilhões de documentos individuais comparados com 1 bilhão da Surface Web. Existem mais de duzentos mil sites atualmente na Deep Web. Seis das maiores enciclopédias da Deep Web contém cerca de 750 terabytes de informação, suficiente para exceder o tamanho da Surface Web quatro vezes. Em média, os sites da Deep Web recebem 50% mais tráfego mensal, ainda que não sejam conhecidos pelo público em geral. A Deep Web é a categoria que mais cresce no número de novas informações sobre a Internet. Deep Web tende a ser mais estrita, com conteúdo mais profundo, do que sites convencionais. A profundidade de conteúdo de qualidade total da Deep Web é de 1.000 a 2.000 mil vezes maior que a da superfície. O conteúdo da Deep Web é altamente relevante para todas as necessidades de informação, mercado e domínio. Mais da metade do conteúdo da Deep Web reside em tópicos específicos em bancos de dados. Um total 95% da Deep Web é informação acessível ao público não sujeita a taxas ou assinaturas [...]

O uso da *Deep Web* permite que as organizações criminosas desfrutem da rede de computadores para dividir com outros e armazenar arquivos confidenciais e que não devem estar disponíveis na internet popular.

Na Deep Web é possível verificar o local, o tamanho e o tempo dos dados passados, e assim podendo deduzir quem está comunicando com quem, por meio de um aplicativo específico, o TOR (The Onion).

Borges, Sartori e Barros (2015?), explicam que:

> Ao contrário do que muitos podem imaginar, acessar a *Deep Web* não é ilegal. Motivados pela privacidade que o local pode proporcionar, várias pessoas recorrem à “internet invisível” para tratar de assuntos sigilosos e compartilhar arquivos que jamais poderiam “ver à luz do dia”. No entanto, a condição de anonimato (o que é vedado pela Constituição Federal), dessa gigantesca parte da Internet também acaba levando ao surgimento de uma série de atividades ilegais, muitas das quais os órgãos competentes ainda têm muita dificuldade em tratar.

Filipe (2019?) pondera que:

> A Deep Web não é necessariamente ruim. Esse espaço ajuda a proteger o sigilo de milhões de pessoas a partir desse “acordo” de segurança. No entanto, a privacidade garantida aos criadores de conteúdo e quem o acessa atrai criminosos e encoraja a ação de fóruns e de comunidades, o que resulta na veiculação de conteúdos de ódio ou que incentivam a prática

> de crimes. Em geral, espaços como esse na Deep Web são associados à Dark Web

Já o Dark Web abre espaço para a formação de canais e comunidades, com objetivo de troca de informações muito mais anônimas e complexas de serem vigiadas pelas autoridades, fazendo um espaço sem lei na Internet.

Esses espaços relacionados ao Dark Web se tornam, atraente para os criminosos, cometer crimes, repassar material pirata, vender dados vazados ou divulgar conteúdo falso, discursos de homofobia, ódio, racistas, misóginos, etc.

5. LEGISLAÇÃO NACIONAL APLICÁVEL

Conforme o crescimento do uso de aparelhos informáticos e da internet no território brasileiro, ver-se que o sistema jurídico, não esta conseguindo acompanhar a competente evolução digital, sendo evidente que essas lacunas legais geram incerteza e a sensação de que a ausência de punição está inserida nos meios digitais.

Uma das leis da determinação do sistema informático foi a Lei nº 7.232/84, que através dela houve a criação do Conselho Nacional de informática (CONIN), que impôs princípios e orientações na Política Nacional de Informática (PNI). Assim começa a ter leis que procuram defender o domínio digital e suas conexões. A presevação intelectual e a negociação de programas de computadores dispuseram sua ordenação determinada pela Lei nº 7.646/87, e indeferida pela Lei nº 9.609/98.

Verifica-se que o crime virtual passa a ser impedido por legislação especial. Tem como exemplo o Estatuto da Criança e do Adolescente – Lei nº 8.069/90, que reconhece como crime o depósito e o compartilhamento de fotos de sexo sendo visível a participação de crianças e adolescente.

A Lei nº 11.829 de 2008 alterou o Estatuto da Criança e do Adolescente, colocando artigos para melhora o conflito à pornografia infantil e criminalizar a adquirição e a jusrisdição de tal conteúdo e outros procedimentos que se refere à pedofilia na internet.

Ela estabelece, entre outras, pena privativa de liberdade de 3 a 6 anos

para quem oferece trocar, disponibilizar, propaga, compartilha por qualquer meio, sendo através de sistema de informática ou telemático, fotografia, vídeo ou outro tipo de documentação que possua cena de sexo evidente ou pornográfica havendo a participação de criança ou adolescente.

Logo após a Lei nº 11.829/2008, veio a Lei nº 12.015, de 2009 que também modificou o E.C.A. e determina, dentre outras, a pena de reclusão sendo de 1 a 4 para pessoa que se relacione com menores de 18 anos em salas de bate-papo da Internet.

Já a Lei nº 9.609/98 que conceitua a pirataria como crime de falsificação, por sua vez, no que se meciona ao crime virtual próprio, sua especificação se deu através da Lei nº 9.983/2000, promove a introdução dos artigos 313-A e 313-B do Código Penal, onde classificou as condutas de implantação de dados falsos em aparelhos de informações e de mudar ou alterar o que não foi permitido.

Conforme demostra Pinheiro (2013, p. 28):

> Portanto, as condutas chamadas de crimes virtuais (embora inexista legislação específica) encontra-se tipificada em textos legislativos existentes (Código Penal e legislação esparsa) e, ao contrário do que alguns autores afirmam, a aplicação da lei já existente a essas condutas não é caso de analogia, pois não são crimes novos, não são novos bens jurídicos necessitando de tutela penal, a novidade fica por conta do modus operandi, de como o criminoso tem feito uso das novas tecnologias, com foco na Internet, fazendo com que os estudiosos e os aplicadores do Direito tenham que renovar o seu pensamento.

Outro exemplo de lei que específica conduta determinada como própria é a Lei nº 9.296/1996 que tipifica o crime de interceptação de comunicação informática. Muitas atuações determinadas como próprias ainda estão dependendo de norma, sendo essa inexistência de legislação fato grave, causando a impunidade.

Exemplos de atuações que causa dano e até o momento sem tipificação legal são o envio de spam, propagação de vírus ou outros programas danosos e desfiguração de sites.

O que se entende do sistema jurídico brasileiro é que têm um complexo de normas, dispersa e incoerente, que busca tipificar os crimes virtuais. Não impede, é preciso mais do que isso para que se dê uma resposta satisfatória sobre o tema e realmente proteger os bens da sociedade no espaço virtual.

Logo depois, no propósito de considerar o pedido da sociedade, o Poder Legislativo, no ano de 2012 viu-se a ser levado a fazer leis que regularize os crimes virtuais. A grande agitação social deu-se ao fato de fotos intimas da atriz Carolina

Dieckmann ter sido roubadas de seu computador e publicadas na internet. Com esses fatos, aconteceu a divulgação das Leis ns.12.735/12 e 12.737/12.

Primeira delas é a Lei dos crimes virtuais, que é denominada como Lei Carolina Dieckmann, a Lei nº 12.737/2012, que tipifica atitudes como a invasão de computadores por hackings, desrespeitar os dados de usuários, roubar senhas, e espalhar informações privadas sendo fotos, mensagens e outros.

Mesmo ganhando lugar na mídia com o que ocorreu com a atriz, o assunto já era proposto pelo departamento financeiro em face do grande quantidade de ataques e roubos de senhas pela internet.

Os crimes constados na Lei de Crimes Virtuais e juntados no Código Penal em seu art. 298 e a ocupação ilegal de computadores, o roubo de senhas e arquivos através da introdução do art. 154 - A no Código Penal**.**

O ocorrido foi tão comentado de que não tinha leis que seis meses após as fotos serem públicas, foram proclamadas na mesma data a Lei nº 12.735/12 e a Lei nº 12.737/12, sendo modificado o Código Penal Militar, o Código Penal e a Lei de Preconceitos, as quais identificam condutas pelo uso de meios eletrônicos e digital, contrário aparelhos informatizados, sendo nominado de Lei Azeredo fazem refere-se a Eduardo Azeredo, relator do plano 84/99 que deu inicio à referida Lei.

Para a invasão ser caracterizada como crime, deve ela ser cometida sem a permissão clara ou tática do titular do aparelho, e ainda que haja a vontade de conseguir, causar dano, destruir dados ou ainda colocar vulnerabilidades.

Antes da abertura dessa legislação, não tinha dispositivo legal que realmente regular-se tal atitude como crime; não teria outra opção senão a falta de punição.

O crime de invasão de sistema informático pode gerar danos incalculáveis à vítima, por ser crime que atinge contra a liberdade individual e a privacidade, podendo acarretar a exposição pessoal através do roubo de informações ou outros dados privados.

A pena diversa, e intensa, também é executada em condutas de crimes de invasão de aparelho que advenha a conquista de matéria sigilosa, privada, ou de segredo comercial, além do monitoramento remoto não permitido do dispositivo violado, se tornando mais grave nos caso de decorrente negociação ou publicação de tais informações.

É crime de ação pública condicionada, em via de regra, sendo salvo nos

crimes realizados contra patrimônio da administração pública indireta ou direta e a qualquer dos Poderes sendo da União, Estados, Distrito Federal e Municípios, ou além de empresas de serviço público concessionárias; em tais condutas, converte-se-á de ação pública incondicionada conforme art. 154-B, do Código Penal.

Ademais do crime de invasão do aparelho, a lei modificou o definição de crime de interrupção de serviço para ampliar os serviços de informática, conteúdo ou de instrução de serventia pública por meio da alteração do art. 266 do Código Penal, piorando-se a pena por meio de sua aplicabilidade em dobro em caso do crime seja cometido por motivo de calamidade pública, com demostra § 2º do referido artigo.

Crimes de interrupção de serviço informático são cometidos no dia a dia e é realizado por meio de ataques que buscam abalar ou diminuir a capacidade de um serviço proporcionalizado na rede de computadores, e com isso gerarem contrariedade e causa dano ao dispositivo e as pessoas que utiliza este serviço.

Sua tipificação foi muito eficaz em consequência desta conduta ser bastante agregada na comunidade hacker, havendo probabilidade de ser feita sem muitas dificuldades. Por fim, modificou o crime de falsificação de documento particular, segundo art. 298 do Código Penal, para colocar no rol destes documentos os cartões de débito e crédito.

A falsificação de cartões na internet, ainda mais de crédito, é algo bem comum. As fraudes por meio virtual só aumentam e os atacantes alcançar a obtenção dos dados do cartão de crédito, seja através da invasão de um aparelho, pela apreenção de uma conversa ou por meio da engenharia social, empregando-as para cometer novas fraudes.

A instituição da Lei n° 12.737/2012, apenas reparou o Código Penal, tratou-se da tipificação de novas ações e inovação de outras existentes. O texto normativo não gerou grandes mudanças no sistema jurídico, muito menos melhorou o problema confrontado pelo Direito brasileiro sobre o assunto.

Porém, tal lei adquiriu boas conquistas ao tipificar ações muito graves ao povo brasileiro, além disso, pelo fato da lei ter simbolizado pela primeira vez a publicação de um dispositivo normativo voltado exclusivamente para a tutela do bem jurídico no cibernético, abriu lugar para que os conflitos acerca do assuto fossem discutidos.

A Lei nº 12.965/2014 chamada Marco Civil da Internet (MCI), simboliza uma grande avanço para o Sistema Jurídico brasileiro, pois manteve a

ordem civil da internet, diminuindo a falta de segurança jurídica, que está sobre o ordenamento brasileiro. Foi à primeira Lei feita de aspecto parceria entre Governo e sociedade através da internet como espaço de argumentação, e impôs princípios, proteção, direitos e obrigações dos usuários da internet.

O Marco Civil da Internet foi aprovado em 2014 e coloca em ordem nos direitos e obrigações dos internautas. Ele preserva os dados do usuário e a sua privacidade. Assim, exclusivamente pela ordem judicial poderá acontecer rompimento da privacidade de dados e informações pessoais estando em sites ou redes sociais.

Uma das melhorias refere-se à remoção de informações do ar. Antes de entrar em uso, não tinha uma norma específica sobre este fato. Assim, a retirada desses conteúdos do ar só irá ser feita através de uma ordem judicial, salvo os casos de pornografia de vingança.

O Marco Civil da Internet também impôs que os Juizados Especiais estam encarregados pela escolha sobre a ilegalidade ou não dos fatos. Isto se impõe aos casos de ofensa à honra ou injúria, que serão cuidados da mesma maneira como não acontece dentro da rede mundial de computadores.

O estabelecimento da competência não importando o local do aparelho de entrada ao mundo virtual, sendo o lugar da realização do delito, conforme o art. 70 do Código de Processo Penal.

Porém nos casos de crimes como desrespeitando privacidade ou ações que cause danos aos bens, as partes interessadas ou serviço da União ou de suas empresas privadas ou públicas, compete a Justiça Federal, assim como os crimes das convenções internacionais.

Atualmente, não há lei ou órgão do governo que coloque a censura prévia (controle e constrangimento antecedentes a uma manifestação de opinião) na internet. Mas, não ser censurado é bem diferente de não se responsabilizar por suas ações.

Ninguém regula suas condutas previamente na internet, o que não quer dize, que você não irá de paga com os resultados de suas atitudes, além do que refere-se à restauração de danos provocados a outras pessoas. É como realizar um esporte em equipe, ninguém irá te reprime de jogar, mas se você cometer um erro será punido.

Publicar insultos em redes sociais não quer dizer que é um direito à

liberdade de se expressar. Ou seja, não se pode usufruir de um direito seu, a liberdade de expressão nesse caso, como meio de desculpa para infringir os direitos de outros, como a intimidade, a integridade moral e psicológica, a honra ou a dignidade.

Atualmente acontece que a uma lacuna legal grave na ordem social, produzindo vulnerabilidade legal e a falta de segurança no ambiente virtual, tendo vários planos e anteplanos de leis que buscam fazer figuras penais sobre essas ações.

De fato, as lacunas legais cria um espaço de falsa impressão de imunidade, não tão incomum os casos de crimes praticados onde o sujeito ativo tem a falsa sensação de que a internet é um ambiente sem lei.

As lacunas são ainda mais ariscadas no caso dos crimes virtuais próprios, onde as figuras penais não estão formadas e assim as ações praticadas por esta conduta, em muitos de seus casos, não podendo ser alvo de ação penal. As pessoas vítimas da violação da privacidade podem pedir a exclusão do conteúdo, de forma direta, aos sites ou serviços que mantém este conteúdo.

No que se refere ao Ordenamento Jurídico brasileiro quanto aos crimes virtuais, ver-se que o andamento da criação das leis e regularização é lento, em vista do grande mundo cibernético, que a cada dia cresce mais.

Embora haja uma lista de vários tipos de crimes virtuais, necessita-se de legislação específica para tratar os delitos cibernéticos e não apenas leis perdidas e desconectadas.

CONCLUSÃO

O presente estudo indica a importância do debate e da consciência deste deslocamento da criminalidade virtual, solicitando que este evento se estabeleça como um assunto comum da Segurança Pública e de Política Criminal.

O ciberespaço é comentado pelo sistema jurídico brasileiro como uma vantagem necessário para a execução dos direitos e garantias constadas na Constituição Federal a todos os cidadãos. Os obstáculos começam nas circunstâncias atuais da realidade social, com a satisfação deste direito de ingresso a internet indo para o caminho da criminalidade.

A perigosa parceria da tecnologia com a criminalidade, podendo

proporcionar aos criminosos digitais mutiplas formas. As aplicações de novas tecnologias para o exercício da conduta criminosa são um verdadeiro problema social.

E de grande urgência da atuação do Direito Penal e da legislação penal no conflito a essas novas categorias criminosas, buscando a presevação e punição desses atos criminosos.

Com base no desenvolvimento da criminalidade cibernética, a política criminal, colhendo a opinião pública, cria leis mais severas quanto o assunto. Dentre essas, referencia-se a Lei nº 12.965/14, nomiada como o Marco Civil da Internet, que disponibilizam direitos e deveres aos usuários da internet, e a Lei nº 12.737/12 conhecida como Lei Carolina Dieckmann, a qual aumentou a lista dos crimes virtuais ao Código Penal.

A apresentação do controle social é compreensível a declarar que o Brasil, mesmo com a determinação na criação de leis penais com intuito ao combate dos crimes virtuais, não predomina de meios convenientes para evitar a frequente onda de crimes cibernéticos, por vários motivos, como a ausência da classificação de tipos penais de alguns ataques virtuais, bem como pela desorganização tecnológica do Sistema de Justiça para fazer as inspeções ou, ainda, pela falta de agilidade do Poder Judiciário.

Com o desenvolvimento desta atividade criminal na rede, as agências estatais responsáveis pela produção de políticas de monitoração e prevenção continuam com alguma indiferença, não favorecendo condutas e políticas públicas de incorporação virtual, de educação e ética da informática, voltada a esta e outros tempos futuros de sujeitos da internet, visando impor limites aos crimes digitais.

A web é um universo aterrorizante, pois o anonimato governa, dando serventia às condutas delituosas, pois há uma adversidade estatal no reconhecimento de tais criminosos, sendo este um dos mais importantes empecilhos na investigação.

Isto posto, é percebido a necessidade de proteção e cautela primária, secundária e terciária, que buscam uma consideração a respeito da incapacidade, assim, pede de uma análise especial por parte do Estado.

A precisão da colaboração da política criminal especializada, em capacitar os órgãos dos três poderes para compreenderem sob uma otica científica e moderna, sendo possível de decidir de maneira eficaz com esta ação do cibercrime.

Na opinião de política criminal de vigilância, não é eficaz apenas uma legislação que forneça um tipo penal, é preciso à formação de um programa de política criminal de precaução, apoiando-se na educação, na integração social e melhoria do estilo de vida, que qualifica o cidadão a impedir ou evitar eventuais conflitos.

Entende-se que o ordenamento jurídico penal brasileiro ainda está em uma jornada para conseguir eficiência na precaução e punição de tais crimes virtuais, a solução não será uma tarefa simples, mas já é visível que não se solucionará apenas com as leis de leis criminais, o plano inteligente a ser feito é abranger polícias criminais na educação e uma organização de investigação criminal.

Mesmo que já existam algumas condutas que atuem da matéria, ainda sim o sistema brasileiro não se demostra eficiente para que todas as pessoas que usam o meio tecnológico possuam proteção.

O certo se deve que o Direito seguisse as inovações e mudanças da sociedade, sendo assim que ele se ajuste também ao mundo cibernético, ocupando-se sempre da garantia da segurança dos direitos essenciais da pessoa.

Conclui-se que está no momento dos legisladores operarem nesse fato e fazerem uma legislação atualizada e especifica, para assegurar assim a proteção dos usuários a seus computadores e seus aparelhos eletrônicos. Para que as pessoas team seu Direito garantido e obtenham uma segurança, pois caso seja vitimas de crimes ciberneticos elas terão a consciência que os culpados não sairão impunes.

REFERÊNCIAS

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do hacker ético**. 3ª edição. Florianópolis: Visual, 2008.

BRASIL. **Lei 12.965 de 2014.** Disponível em:>http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso: 04 nov. 2020.

BORGES, SARTORI E BARROS. Daniela Cristin, Liane Pioner, Mauricio Sebastião. **A Deep Web e a relação com a criminalidade na internet.** Disponível em:> http://direitoeti.com.br/artigos/a-deep-web-e-a-relacao-com-a-criminalidade-na-internet/ Acesso: 27 mar. 2021.

CARVALHO, Gabriel Chiovetto. **Crimes cibernéticos**. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/51878/crimes-ciberneticos. Acesso: 21 out.2020.

CÓDIGO PENAL BRASILEIRO. 1940 Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso: 06 nov. 2020.

CUNHA, R. S.; PINTO, R. B. **Crime Organizado: Comentários à nova lei sobre o Crime Organizado – Lei nº 12.850/2013.** 2. Ed. Salvador: Jus Podivm. 2014.

CUNHA, Rogério Sanches. **Manual de Direito Penal.** Parte Especial (arts. 121 ao 361). 8ª Ed. Salvador. Editora Jus Podivm, 2016.

CUNHA, Rogério Sanches. **Infiltração de agentes de polícia na internet.** Disponível em: https://www.google.com/amp/s/migalhas.uol.com.br/amp/depeso/258738/infiltracao-de-agentes-de-policia-na-internet. Acesso: 17 mar. 2021.

CAPEZ, Fernando. **Curso de Processo Penal**. 19º ed. São Paulo: SaraivaPodivm.

FEITOZA, Denílson. **Direito processual penal: teoria, crítica e práxis.** 6ª. Ed. Ver., ampl. E atual. Niterói: Impetus, 2009.

GARRETT. Filipe. **Entenda o que é e como funciona a Deep Web, parte da Internet que não pode ser achada no Google**. Disponível em:< https://www.techtudo.com.br/noticias/2019/03/o-que-e-deep-web.ghtml> Acesso em: 27 mar. 2021.

GIL, Antônio de Loureiro. **Fraudes Informatizadas**. 2ª edição, 1ª tiragem, 2000.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet.** Boletim IBCCRIM, v. 8, 2000.

INELLAS, Gabriel Cesar Zaccaria. **Crimes na internet.** 2. Ed., atual. E ampl. São Paulo: Juarez de Oliveira, 2009.

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

LIMA, R. B. de. **Legislação criminal especial comentada.** 2. Ed. Salvador: JusPodivm. 2014.

LOPES, M. T. **A infiltração de agentes do Brasil e na Espanha.** Revista Brasileira De Ciências Criminais. São Paulo. N. 89, ano 2011.

NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo: BH Editora,

2008.

OLIVEIRA, Wilson José. **Dossiê hacker: técnicas profissionais para conhecer e proteger-se de ataques.** São Paulo: Digerati Books, 2006.

POMPÉO, W.A.H; SEEFELDT, J.P. **Nem tudo está no Google: Deep web e o Perigo da invisibilidade.** In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 2., 2013, Santa Maria. Anais… Santa Maria, Rs: Ufsm, 2013.

PRADO, Luiz Régis. **Curso de Direito Penal brasileiro** – 4º Volume – 2º Edição – Editora Revista dos Tribunais, 2004.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal.** São Paulo: Memória Jurídica, 2004.

SIMAS, Diana Viveiros de. **O cibercrime**. 2014. 168f. Dissertação (Mestrado em Ciências JurídicoForenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa. 2014.

SCHAUN, Guilherme. **Uma lista com 24 crimes virtuais.** Disponível em: https://www.google.com/amp/s/guilhermebsschaun.jusbrasil.com.br/artigos/686948017/uma-lista-com-24-crimes-virtuais/amp Acesso: 03 de nov. 2020.

VALENTE, Jonas. **Brasil tem 134 milhões de usuários na internet, aponta pesquisa.** Disponível em: <https://www.google.com/amp/s/agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa%3famp. Acesso: 03 nov. 2020.

VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos.** Belo Horizonte: Fórum, 2013.