CENTRO UNIVERSITÁRIO Uni – ANHANGUERA
CURSO DE DIREITO

INFILTRAÇÃO VIRTUAL DE AGENTES POLICIAIS NO COMBATE AOS CRIMES CIBERNÉTICOS NA *DEEP WEB* E *DARK WEB*

GLEICE KELLY PAIXÃO SILVA

GOIÂNIA
Abril/2019

GLEICE KELLY PAIXÃO SILVA

INFILTRAÇÃO VIRTUAL DE AGENTES POLICIAIS NO COMBATE AOS CRIMES CIBERNÉTICOS NA *DEEP WEB* E *DARK WEB*

Trabalho de Conclusão de Curso apresentado ao Centro Universitário de Goiás – Uni Anhanguera, sob orientação da Professora Ms. Cinthya Amaral Santos, como requisito parcial para obtenção do título de bacharel em direito.

GOIÂNIA
Abril/2019

FOLHA DE APROVAÇÃO

GLEICE KELLY PAIXÃO SILVA

INFILTRAÇÃO VIRTUAL DE AGENTES POLICIAIS NO COMBATE AOS CRIMES CIBERNÉTICOS NA *DEEP WEB* E *DARK WEB*

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

_____

Ms. (a)
Orientadora (a)

_____

Prof. (a).
Membro

_____

Prof. (a).
Membro

Dedico este trabalho a minha família e amigos, que sempre me apoiaram e que me fortalecem cada dia mais para seguir em frente com meus sonhos.

AGRADECIMENTOS

Dedico este trabalho primeiramente a Deus que me guiou nesta jornada, me fortalecendo e iluminando meu caminho. Agradeço também a minha mãe, meu pai e meu irmão, por sempre me apoiarem nas minhas escolhas, a meus amigos, que apesar de algumas decepções os verdadeiros sempre estiveram ao meu lado e a meus companheiros de trabalho que sempre foram pacientes e atenciosos comigo.

“O mais corajoso dos atos ainda é pensar com a própria cabeça.”
Coco Chanel

RESUMO

O presente trabalho foi pautado na análise acerca da técnica especial de investigação denominada infiltração policial, com enfoque na persecução penal de crimes praticados no ambiente virtual. Assim, foi analisado o desenvolvimento do espaço cibernético como facilitador da prática delitiva, apresentando a infiltração policial como uma técnica investigativa viável no combate aos crimes estrategicamente planejados e a importância para a solução dos crimes virtuais. Com o intuito de maior debate sobre o tema, apresentou-se a dificuldade em navegar pelo ambiente virtual, uma vez que este ambiente vasto dificulta a identificação dos criminosos, o método para compor o estudo foi através de pesquisa feita por meio de livros, artigos e leis esparsas. De modo a facilitar a compreensão do tema, fez-se um estudo acerca dos crimes cibernéticos, demonstrando os artifícios da criminalidade em dificultar a atividade investigativa, através da *Deep Web* e da *Dark Web.* Após, analisou-se o instituto da infiltração policial, de forma ampla, expondo seus requisitos, limites e demais aspectos. Ao final, fez-se uma abordagem sobre a importância deste meio investigativo e os riscos em que os agentes se expõem ao adentrar este ambiente, e a importância da cooperação internacional para a solução destes crimes.

PALAVRAS-CHAVE: Investigação. Criminalidade. Ambiente. Riscos.

SUMÁRIO

INTRODUÇÃO

O presente trabalho fez uma abordagem dos novos meios de a criminalidade disseminarem seus produtos provenientes do crime organizado através da rede mundial de computadores, a internet. Sabemos que os criminosos estão se aperfeiçoando para acompanhar as tecnologias e se introduzirem no comércio on-line do crime.

O objetivo principal foi fazer uma análise sobre os meios de investigação dos crimes cibernéticos, compreender como os criminosos abordam as vítimas, a disseminação desses criminosos no ciberespaço e como os agentes policias lidam com a infiltração e a cooperação internacional que os agentes recebem nos casos de crimes virtuais praticados em outros países.

O surgimento dos crimes cibernéticos veio atraves do avanço tecnológico, do surgimento do computador e a disseminação dos conteúdos online, o que chamou a atenção dos criminosos vendo uma oportunidade a mais de conseguirem vítimas. A facilidade no acesso e na obtenção de informações é um fato que chama a atenção dos criminosos.

A infiltração dos agentes policias no combate aos crimes cibernéticos está cada vez mais encontrando dificuldades na hora de ser colocada em prática, visto a legislação em alguns aspectos falha e a dificuldade de rastrear os criminosos que usam uma espécie de internet profunda, conhecida como *Dark Web e Deep Web (a* Deep Web é composta por todo domínio não indexado, ou seja, que não é encontrado nos buscadores comuns, já a Dark Web é uma pequena parte da Deep Web, na qual podem ocorrer crimes e compartilhamento de situações e informações ilegais, como comercialização de drogas, negociações com hackers e assassinos, pornografia infantil e demais delitos) para comercializar armas, drogas, serviços sexuais, tráfico de órgãos e pessoas.

Para que a infiltração policial se torne eficiente é necessário que saibamos como esse ambiente da internet profunda funciona, quais os seus mecanismos, para que os agentes não cainham em armadilhas feitas pelos criminosos, para isso foi usado a pesquisa bibliográfica atraves de livros, artigos e reportagens acerca do assunto. Vimos neste trabalho, quais os métodos e procedimentos os agentes brasileiros usam para se infiltrarem neste ambiente inóspito para elucidar crimes deste tipo numa rede onde é possível encontrar criminosos de todos os países.

Por fim, como o Estado lida com os riscos da infiltração do agente neste meio criminoso, visto o perigo que podem encontrar sendo seduzidos ou perturbados psicologicamente com as situações que em muitos casos imaginaram se quer existir, os riscos de serem descobertos em meio a infiltração e como funciona as provas conseguidas caso a infiltração tenha sucesso.

1 DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos não são fatos que surgiram recentemente, e sim, ganharam notoriedade e mídia atualmente, uma vez que, com a evolução dos equipamentos eletrônicos e nossa eventual dependência dos mesmos, nos tornamos mais propensos a estes tipos de crimes.

1.1 Surgimento e Evolução

Os crimes cibernéticos surgiram através do avanço tecnológico que se desenvolveu e evoluiu com o intuito de auxiliar o homem a progredir. O ciberespaço está associado a internet, ou seja, é o espaço virtual onde os crimes cibernéticos são propagados. Na visão de Lévy (1999, p. 32) o ciberespaço:

> […] 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 juntamente com o crescimento do ciberespaço.

Segundo Lévy (1999), as tecnologias digitais surgiram coma a estrutura do ciberespaço, tornando assim, um novo ambiente de comunicação, de sociabilidade, de organização e de transação, mas também se tornou um novo mercado de informação e de conhecimento. Ou seja, a internet é a infraestrutura que sustenta o ciberespaço, tornando possível assim, todo o portfólio de informações que conhecemos.

Com o advento da internet a rapidez na propagação de conteúdo e informações se tornou o maior atrativo para os usuários que a utilizam em diversos dispositivos moveis que os auxiliam no trabalho e para se comunicarem com pessoas de várias partes do mundo através de redes sociais.

A facilidade no acesso através da rede é um chamativo para os usuários o que para Inellas (2004), pode se tornar um chamativo para criminosos visto que, a Internet é uma rede de computadores integrada por outros menores que se comunicam entre si, através de uma rede lógica, chamado de IP, onde uma gama de informações são trocadas, surgindo assim o problema da quantidade de informações pessoas que estão na rede, ficando assim a disposição de milhares de usuários na internet, e quando não abertas ao público são procuradas por

outros usuários com o intuito de usar essas informações para cometer os denominados crimes virtuais.

Diante do crescimento da propagação de informações através da internet, este fenômeno chamou a atenção da criminalidade, que viu a oportunidade de agir num ambiente novo e cheio de oportunidades.

Na visão de Levy (1999, p. 49-50):

> […] a extensão do ciberespaço acompanha e acelera uma virtualização geral da economia e da sociedade. Das substâncias e dos objetivos voltamos aos processos que o produzem. Dos territórios, pulamos para o nascente, em direção às redes móveis que os valorizam e as desenham. Dos processos e das redes, passamos à competências e aos cenários que as determinam, mais ainda. Os suportes de inteligência coletiva do ciberespaço multiplicam e colocam em sinergia as competências. Do design à estratégia, os cenários são alimentados pelas simulações e pelos dados colocados à disposição pelo universo digital. Ubiquidade da informação, documentos interativos interconectados, telecomunicação recíproca e assíncrona em grupo e entre grupos: ciberespaço faz dele o vetor de um universo aberto. Simetricamente a extensão de um novo espaço universal dilata o campo de ação dos processos de virtualização.

Como demonstrado, o crescimento e a disseminação da internet pelos usuários foi um processo rápido, hoje busca-se a internet para quase todas as atividades do nosso dia a dia, nos tornando assim vulnerareis a criminosos virtuais. No começo os crimes praticados eram os roubos de dados pessoais, uma vez, que todos os nossos arquivos pessoais ficam gravados no banco de dados da internet e que na maioria das vezes não temos controles sobre onde esses dados vão parar, desta forma é que o criminoso virtual vê a oportunidade perfeita para extrair essas informações pessoais do usuário.

1.2 Conceito De Crimes Cibernéticos

Crimes cibernéticos são todos os crimes tipificados que são cometidos por meio da internet, crimes estes que se diversificaram a partir dos avanços tecnológicos que ocorrem na sociedade, uma vez que podem ser cometidos através de qualquer dispositivo que tenha acesso à internet.

De acordo com Rossini (2004), o denominado "delito informático" pode ser comparado com a conduta típica e ilícita constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, podendo ser praticada por pessoa física ou jurídica, usando dispositivos informáticos em ambiente de rede ou fora dele, ofendendo direta ou indiretamente a segurança informática.

Os crimes tipificados como cibernéticos engloba todos os que utilizam meios informáticos para serem cometidos, sendo que desta forma, os criminosos se aproveitam do

anonimato para praticarem os atos ilícitos, tornando assim, a internet como uma ferramenta essencial para dificultar a identificação.

Vale ressaltar que não necessariamente o instrumento para a prática do crime deverá ser por meio da internet, uma vez que o crime poderá ser consumado tanto por dispositivo com internet como sem internet, como corrobora Feliciano (2000), a criminalidade informática é o recente fenômeno histórico-social cultural se caracterizando pela grande incidência de ilícitos penais como, delitos, crimes e contravenções, que tem o objetivo material ou meio de execução objeto tecnológico informático como, hardware, software, redes, entre outros.

Entende o referido doutrinador, que a criminalidade virtual é um fenômeno recente, visto que os meios tecnológicos se dissiparam recentemente, e já é utilizado para a prática de delitos criminosos. Ao contrário deste pensamento, observamos que estudos científicos mostram que os primeiros crimes cibernéticos começaram a tomar forma a partir dos anos 70, quando os hackers ganharam destaque por praticar ataques a sistemas de software.

Leciona Nigre (2000, p. 32) que 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”. Podemos observar que este conceito abrange não só o que para muito estudiosos seriam apenas os crimes caracterizados pelo roubo ou alteração de dados pessoais ou de software, mas também os crimes como pedofilia, tráfico de drogas, tráfico de órgãos, difamação, injuria, pornografia infantil entre outros.

1.3 Classificação e Tipos De Crimes Cibernéticos

A classificação dos crimes cibernéticos, na doutrina não é um consenso, sendo que vários autores possuem uma classificação distinta uma da outra acerca do tema. Correa (2010) conceitua como, sendo a tecnologia digital uma realidade que possui lacunas objetivas aos quais o direito tem o dever de estudar, compreender e preencher essas lacunas. Com a popularidade da grande rede de computadores, evidentemente observamos a criação de novos conceitos sobre tradições e valores, sendo eles a liberdade, a privacidade e o crescimento dos crimes digitais.

Para Fragoso (1983, p 5), a classificação deve observar o bem jurídico tutelado: “A classificação dos crimes na parte especial do código é a questão ativa, e é feita com base no

bem jurídico tutelado pela lei penal, ou seja, a objetividade jurídica dos vários delitos ou das diversas classes de intenções".

Pinheiro (2002) define como Direito digital a evolução do Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes até hoje, assim como introduzindo novos institutos e elementos para o direito em todas as suas áreas sendo elas, no direito cível, autoral, comercial, constitucional, econômico, financeiro, tributário, penal, internacional e etc.

A classificação mais aceita pelos doutrinadores, que é dividida em crimes virtuais próprios e impróprios. A esta diferenciação por conta da diferença dos crimes e a sua finalidade, podendo acarretar em consequências apenas na esfera virtual, apenas na física ou em ambas. Para Lima (2011), analisando a internet, pode-se considerar dois pontos de vista sendo eles crimes ou ações que merecem incriminações praticadas por meio da Internet e os crimes ou ações que são praticados contra a internet, enquanto bem jurídico autônomo.

Esta classificação é a mais aceita, uma vez que é a mais objetiva para se enquadrar às condutas ilícitas disseminadas atualmente, apresentadas como: a) condutas perpetradas contra um sistema informático. b) condutas perpetradas contra outros bens jurídicos.

1.3.1 *Crimes Próprios*

Nos crimes virtuais próprios o principal instrumento pelo qual é consumado o crime é o computador. Desta forma, o bem jurídico tutelado é a informática, visto que a conduta criminosa é praticada unicamente e objetivamente com intuito de corromper os dados da vítima, causando prejuízo a segurança de sistemas, titularidade das informações, lesando dados entre outros.

Crespo (2011), afirma que não se pode negar que a informação, os dados, a confiabilidade e a segurança dos sistemas informáticos e de comunicação sejam novas formas que necessitam serem legislados pelo Direito Penal. Com a evolução dos meios de comunicação e a evolução da internet, observamos que a legislação penal em certos momentos se encontra atrasada em relação a tutela jurídica a respeito dos crimes cibernéticos.

No ano de 2012, foi sancionada pela presidenta Dilma Rousseff a lei que entrou em vigor para combater os crimes cibernéticos no País (Leis 12.737/12 e 12.735/12), aprovação esta que demonstrou o avanço para a segurança no País, uma vez que era uma área que a muito tempo estava sendo explorada pelos criminosos.

Sobre a Lei dos Crimes Cibernéticos Capette (2018), nota que a Lei 12. 737/12 acabou sendo apelidada de Lei Carolina Dieckmann, atriz da Rede Globo de televisão que teve o computador invadido por Hackers que vazaram fotos íntimas da mesma. Esta situação acabou acelerando o andamento de projetos que estavam para ser votados com o intuito de criminalizar os denominados crimes cometidos por meio de dispositivo informático. Antes deste acontecimento, era necessário tipificar os crimes virtuais em condutas já existentes no Código Penal, esta situação foi regularizada através da Lei 12. 737/12.

O referido autor (2018), afirma que o bem jurídico tutelado é a liberdade individual, que esta inserida no capítulo que regula os crimes contra a liberdade individual (artigos 146 e 154, CP) na seção IV – Dos Crimes Contra a Inviolabilidade dos Segredos (artigos 153 e 154 – B, CP). É tutelada a privacidade das pessoas (intimidade e vida privada), bem jurídico assegurado pela Constituição Federal em seu artigo 5º, inciso X.

Na Lei 12.737/12, o artigo 154-A apresenta apenas uma conduta criminosa que é a de invadir dispositivo informático alheio, podendo ou não estar conectado a rede de computadores, mediante a violação de mecanismo de segurança para obter sem o consentimento do proprietário dados informáticos. Pode-se afirmar que também se tutela neste crime, a privacidade das pessoas, no que concerne a sua intimidade e vida privada, que é bem jurídico protegido no art. 5º, inciso X, da Constituição Federal. Dessa forma, observamos que a tutela assegurada é a individual, envolvendo interesses de pessoas físicas ou jurídicas, não tendo a ver com a proteção à rede mundial de computadores (BRASIL, 2012).

Apesar da criação da Lei 12.737/12, já existiam leis que disciplinavam os crimes próprios, no caso a Lei do Software e outras leis esparsas. A grande inovação da Lei dos Crimes Cibernéticos é prevê a conduta da inovação do dispositivo informático de uma pessoa, burlando o sistema que protege os dados salvos na máquina sem a autorização previa.

1.3.2 *Crimes Impróprios*

Os crimes impróprios são os que o agente utiliza o computador como um meio para chegar ao resultado esperado, assim, causando prejuízo no mundo físico ou real. Para Castro (2003), são crimes informáticos aqueles que são concretizados de qualquer forma, inclusive atraves da informática. A internet é uma ferramenta associada aos dispositivos informáticos, pode ser usada por qualquer pessoa, por mais leigo que seja, para a prática de delitos através da informática.

Os crimes impróprios já são tipificados na legislação vigente, apenas é utilizado dispositivos informáticos para facilitar o *modus operandi* do criminoso, que anonimamente comete o crime visando a dificuldade para ser identificado.

1.4 Crimes Tipificados Pela Lei Brasileira

1.4.1 *Crime de Pedofilia e Pornografia Infantil*

Na Legislação brasileira, o crime de Pedofilia Infantil está tipificado no ECA[1] (Lei 8.069/90), que especifica as penalidades para quem dissemina ou comercializa imagens ou vídeos que exponha crianças em cenas eróticas, com pena de reclusão de 4 (quatro) a 8 (oito) anos e multa, podendo aumentar a pena a 1/3 se o agente comete o crime no exercício do cargo ou função pública, relações domésticas ou de hospitalidade e de relações de parentesco para cometer o crime (BRASIL, 1990).

Vale ressaltar, que veremos mais a frente que o crime de pedofilia e o de pornografia infantil não se tratam do mesmo crime, esclarece Inellas (2004), é necessário fazer uma diferenciação entre o crime de Pedofilia e a Pornografia Infantil, na primeira existe uma perversão sexual, sendo que o adulto experimenta sentimentos eróticos com a criança ou adolescente, sendo que na Pornografia Infantil não é necessário acontecer a relação sexual entre o adulto e a criança, mas apenas a circulação de fotos eróticas envolvendo crianças e adolescentes.

A propagação deste tipo de conteúdo na internet torna complexa a elucidação da origem de quem as espalhou. Este delito é muito comum na *Deep Web*[2]*,* local este que torna quase impossível a identificação, como veremos mais adiante.

1.4.2 *Crimes Contra a Honra*

Os crimes contra a honra se caracteriza através da internet por meio de postagens nas redes sociais, seja por publicar uma foto ou por meio de comentários. O que se observa é que

[1]ECA é a sigla do Estatuto da Criança e do Adolescente, um documento formado por um conjunto de leis que garantem os direitos das crianças e dos adolescentes no Brasil.
[2]A internet profunda, ou *Deep Web* nada mais é do que a parte da rede cujo conteúdo não está disponível ou indexado nos principais mecanismos de pesquisa (Google, Bing, Yahoo). Ela é formada por milhões de páginas, com dimensão inimaginável e com crescimento similar ao da Internet Visível.

muitos usuários acreditam que por estarem na internet podem fazer qualquer tipo de comentário que ofenda a terceiros sem uma devida punição, é o que acontece nos dias atuais onde se utilizam de perfis *Fakes*[3] para ofender certas pessoas.

Os referidos crime se encontram tipificados no Capítulo V Dos Crimes Contra a Honra do Código Penal, onde são encontrados 3 (três) espécies de crimes, a Calúnia artigo 138 parágrafos 1º e 2º que prevê a calúnia a alguém imputando falsamente fato definido como crime, a Difamação artigo 139 que tipifica a conduta de difamar alguém imputando fato ofensivo à sua reputação, e a injúria artigo 140 parágrafos 1º e 2º, que prevê a injuria a alguém ofendendo a dignidade ou o decoro (BRASIL, 1940).

Conforme Masi (2016), no ambiente virtual o autor da informação é chamado de "provedor de informação". O que disponibiliza as informações criadas ou desenvolvidas pelos provedores de informação, se utiliza de servidores próprios ou de terceiros ("provedores de hospedagem") para armazená-las é chamado de "provedor de conteúdo". A autoria das informações compartilhadas pode ser altamente complexa dificultando a apuração dos fatos, sobretudo porque os meios para a prática delitiva são também ilimitadas e aumentam com a velocidade com que surgem novas tecnologias. Dessa forma, os autores dos fatos se sentem protegidos pelo anonimato ou pela facilidade de publicações a partir de qualquer lugar.

Apesar de não haver uma tipificação específica em caso de ocorrência destes delitos no âmbito cibernético, a interpretação dos dispositivos legais deve ser adaptada aos dias atuais, o que se enquadra perfeitamente nos crimes cibernéticos.

1.4.3 *Invasão de Dispositivo Informático*

Em 2012 foi sancionada a lei n. 12.737, intitulada Carolina Dieckmann, alterou o Código Penal o que originou a tipificação penal do crime de Invasão de dispositivo informático, art. 154-A, que tipifica a conduta de invadir dispositivo informático de outra pessoa podendo estar conectado ou não a rede de computadores, violando mecanismo de segurança com a intenção de obter, adulterar dados ou informações sem a autorização do titular, ou instalar vulnerabilidades para obter vantagem.

[3]Fake em inglês é um termo usado para denominar contas ou perfis usados na Internet para ocultar a identidade real de um usuário, para proteger-se de spams, ou simplesmente passar o tempo. Para isso, são usadas identidades de famosos, cantores, personagens de filme ou até mesmo outras pessoas anônimas.

O artigo supracitado ampara a inviolabilidade dos dados informáticos, assegurando a preservação da intimidade do indivíduo. Qualquer pessoa que seja proprietária de dados computacionais que se encontrem violados pode denunciar o caso, desta forma se caracteriza como criminoso o indivíduo que se encontre violando estes dados aos quais não possui licença.

Vale ressaltar que a lei Carolina Dieckmann encontra um fato curioso a cerca do meio pelo qual o crime vai se concretizar, a atividade criminosa se torna atípica caso os dados da vítima estejam por algum motivo no computador do criminoso, outro caso que causa a atipicidade é o fato de a vítima não utilizar antivírus ou outro mecanismo de segurança no momento da invasão. Desta forma, fica evidente que ainda existe uma certa fragilidade acerca dos crimes virtuais, por mais que existam leis que qualifiquem a conduta delitiva, ainda se encontram brechas na lei que em certas situações podem livrar o indivíduo da conduta criminosa.

2 DA ATUAÇÃO DAS ORGANIZAÇÕES CRIMINOSAS NA INTERNET

2.1 Surgimento da Internet

O surgimento da internet se concretizou através de um projeto denominado (*ARPA: Advanced Research Projects Agency*) se tratava de uma pesquisa militar do período da guerra fria. Este projeto surgiu como resposta do governo americano ao lançamento do Sputnik pela ex-União Soviética (LIMA, 2011).

A ideia inicial era conectar os mais importantes centros universitários de pesquisa americanos com o Pentágono para permitir não só a troca de informações rápidas e protegidas, mas também para instrumentalizar o país com uma tecnologia que possibilitasse a sobrevivência de canais de informação no caso de uma guerra nuclear, assim, no dia 29 de outubro de 1969 foi estabelecida a primeira conexão entre a Universidade da Califórnia e o Instituto de Pesquisa de Stanford, ocorrendo o primeiro envio de e-mail (CARVALHO, 2006).

No ano de 1972 o governo apresentou a internet à sociedade, com a ideia de difundi-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 (OLIVEIRA, 2017).

Dessa forma, foi feita a ampliação da rede para que fosse acessada por diferentes equipamentos, tais como supercomputadores, 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 de internet (OLIVEIRA, 2017).

Em 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” (CASTRO, 2003).

A expansão da internet se tornou global alcançando ate o Brasil na década de 90, segundo a ABRANET – Associação Brasileira dos Provedores de Acesso, em 1996 cerca de 300 mil brasileiros utilizavam a internet. Nos dias atuais, é praticamente absoluto o número de

pessoas conectadas na internet através de smartphones e tablets, aparelhos esses que facilitam a conectividade dos usuários, ultrapassando até mesmo os computadores, que hoje em dia foram deixados de lados (OLIVEIRA, 2017).

2.2 Conceito de Organização Criminosa

Conforme a lei n. 12.850/13, seu art. 1º, §1º, entende-se como organização criminosa a associação de 4 (quatro) ou mais pessoas estruturadas e caracterizada pela divisão de deveres, mesmo sendo informal, com o objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza cometidas através de infrações penais cujas penas sejam superiores a 4 (quatro) anos (BRASIL, 2013).

A consumação do crime de organização criminosa ocorre com a associação de quatro ou mais pessoas a fim de praticarem crimes com pena máxima superior a quatro anos, ou de caráter transnacional, ou seja, trata-se de um crime formal que independente da prática de outro ilícito pelos integrantes da organização, onde a repressão legal encontra-se no fato de um agente integrar a organização criminosa.

Para Lima (2017, p. 491):

> À evidência, para que os integrantes da *societas criminis* respondam pelos delitos praticados pela organização criminosa, é indispensável que tais infrações penais tenham ingressado na esfera de conhecimento de cada um deles, sob pena de verdadeira responsabilidade penal objetiva. Logo, o agente não poderá ser responsabilizado por um homicídio praticado pelos demais integrantes da organização criminosa à qual associou caso não soubesse, de antemão, que tal delito seria executado pelo grupo.

Assim, se os agentes delituosos, ao se associarem a uma organização criminosa, e praticarem ilícitos penais, responderão pelo crime do art. 2º, *caput*, da Lei nº 12.850/13, que traz as condutas criminosas de promover, constituir, financiar ou integrar, pessoalmente ou por interposta pessoa, organizações criminosas, em concurso material com as infrações que praticarem (BRASIL, 2013).

2.3 Deep Web e Dark Web

Os conteúdos de difícil acesso que se encontram na internet é denominado *Deep Web*. Os materiais encontrados neste local são para usuários selecionados, necessitam de links próprios para acessar aos conteúdos, o que dificulta o acesso aos leigos. No entendimento de

Shimabukuro e Silva (2017), a internet profunda, conhecida como *Deep Web* é uma parte da rede onde seu conteúdo não está disponível nos principais buscadores da internet como o Google ou Yahoo, para qualquer usuário, mas sua dimensão e seu crescimento é similar ao da internet que conhecemos e fazemos pesquisas.

A *Surface Web*[4]*,* internet convencional para Borges (2018), é formada por computadores com seus conteúdos conectados entre si, através de links espalhados pelo mundo. Na internet comum é possível localizar qualquer máquina desde que se conheça o endereço de IP (*Internet Protocol*), o IP é um endereço único de cada computador para acessar a Internet.

Desta forma, fica claro que o acesso a *Deep Web* é extremamente restrito, sendo necessário a utilização de mecanismos específicos para se ter acesso ao conteúdo. Com o passar dos anos, a proliferação de informações acerca da existência da internet profunda aumentou a busca dos usuários a cerca deste assunto, desta forma surgiu uma rede ainda mais anônima, chamada de *Dark Web* (SHIMABUKURU; SILVA, 2017).

A *Dark Web* tem como cargo chefe a criptografia que se mostra como obstáculo para as autoridades identificarem condutas criminosas e seus agentes. É utilizada em países nos quais os governos bloqueiam o acesso a diversos sites, o que facilita muito o anonimato de criminosos que usam esses mecanismos para a prática de crimes (SHIMABUKURU; SILVA, 2017).

Em contrapartida a *Deep Web,* a *Dark Web* é um ambiente muito mais propício para a proliferação de crimes como a pornografia infantil, fraudes bancarias, assassinos de aluguel, tráfico de drogas, entre outros, visto o sigilo de informações que são totalmente protegidos neste ambiente.

Para se navegar tanto na *Deep Web* como na *Dark Web,* é necessários mecanismos de navegação que asseguram o anonimato que são eles o TOR, *Invisible Internet Project* e *FreeNet,* mas o mais popular é o TOR – The Onion Router, para Shimabukuro e Silva (2017), a Rede denominada TOR tem três aspectos positivos que garantem a privacidade para quem a utiliza: remetente e destinatário da comunicação não conhecem os servidores que utilizados para a transmissão da mensagem; o número de nós utilizados é fluente, o que dificulta a espionagem; e os usuários podem se tornar nós de si próprios, o que acaba dificultando o

[4]Surface Web – superfície, em português – é toda a parte da internet indexada, possibilitando que os canais de busca (Google, Bing, entre outros) encontrem o domínio, e todo o público tenha acesso livre às informações lá postadas.

monitoramento e aumentando a eficiência da estrutura. Apesar de todas as vantagens e de ser uma ferramenta fácil, o TOR é facilmente bloqueável.

O TOR (*The Onion Router*), é uma rede de túneis virtuais que dificulta e faz um mascaramento da identificação dos equipamentos ao acessarem determinado conteúdo, foi criado pela marinha norte-americana objetivando meios seguros de comunicação via internet. O TOR dificulta o rastreamento, mas não garante a inviolabilidade dos dados nem da identidade da máquina (computador ou servidor) porque não é criptografado (SHIMABUKURU; SILVA, 2017).

O anonimato propiciado pelo TOR foi o meio pelo qual tornou possível a comunicação entre ativistas de vários países no movimento revolucionário conhecido em 2010 a meados de 2012 por Primavera Árabe. Essas revoltas aconteceram em mais de 10 países no Oriente Médio e no Norte da África. Este movimento aconteceu em prol da oposição as altas taxas de desemprego, precárias condições de vida e a corrupção do governo autoritário que ocorriam nesses países (LUZ, 2017).

É importante salientar que nenhuma dos mecanismos citados é totalmente seguro, mas a *Deep Web*, contudo é praticamente impossível de ser combatida pelas autoridades, sendo quase nula a possibilidade de identificação precisa de criminosos que atuam nesse ambiente.

2.4. Ciberterrorismo

O terrorismo não é algo que surgiu recentemente, é um movimento que surgiu nos primórdios da sociedade. Podemos observar sinais de atitudes terroristas no movimento judeu político-religioso denominado “Zelota” que surgiu nos anos de 66 a 70 d. C., rejeitavam a dominação romana e o pagamento de tributos dos israelitas á um imperador pagão, atitude essa que levou a destruição de jerusalém pelos romanos e o suicídio em massa dos Zelotas (HOBSBAWM, 2007).

Com o passar dos anos a globalização trouxe entre 1960 e 1980 uma vasta possibilidade de comunicação entre diversas pessoas espalhadas pelo mundo em razão da revolução da tecnologia. Os primeiros indícios de atitudes ciberterrorista foram observadas no início dos anos 1990 com o rápido crescimento da internet e a proliferação dos primeiros crimes cibernéticos (CASTELLS, 1999).

Para Colarik e Janczewski (2008), o termo “ciberterrorismo” passou a ser usado a partir da reunião do G8 realizada em Lyon, na França, no fim da década de 1990, onde foram

analisados e discutidos os crimes promovidos via aparelhos eletrônicos ou a disseminação de informações pela internet.

A dependência da população em relação a tecnologia deu brecha para a disseminação de atos terroristas no ambiente virtual e consequentemente ficou nítido as deficiências tecnológicas que possibilitam a execução de ataques ciberterroristas. Shimeall (apud LIMA, 2006), entende terrorismo informático como qualquer ato que se enquadre numa das seguintes situações, podendo ser a destruição ou a tentativa de infraestrutura de rede a ponto da perda parcial ou total do controle das funções vitais; acesso não autorizado à informação classificada em formato eletrônico; ou a distorção intencional de informação eletrônica com o objetivo de perder a credibilidade com o publico da instituição.

Deve-se atentar que a uma diferença entre "acesso não autorizado à informação classificada em formato eletrônico" que é a invasão de hackers sem propósitos terroristas a contas bancárias e correntistas efetuando verdadeiros furtos, muitas vezes de valores imperceptíveis de várias contas que é considerado um crime cibernético, do ciberterrorismo que se caracterizaria através de furtos a contas bancárias com o intuito de desviar o dinheiro para financiar ações terroristas diversas (SHIMEALL, 2002 apud LIMA, 2006).

O ciberterrorismo é configurado pelo uso da tecnologia para se concretizar o ato, não correndo a utilização de suicidas, conhecidos com "homem-bomba" que ocasiona destruição de determinado ponto e com fins religiosos, mas sim, a utilização de uma rede de computadores para atacar, na maior parte das vezes, sites de entidades governamentais.

2.5 Ciberpedofilia

A Pedofilia é uma psicopatologia, se trata de uma condição em que o indivíduo se sente atraído por menores que demonstram características físicas de criança muito marcantes, independente do sexo, podendo ou não executar o ato libidinoso. A ciberpedofilia é caracterizada pela facilidade e a confiança em que o indivíduo tem de executar atos libidinosos com as vítimas por meio do ambiente virtual.

Para o Código Internacional de Doenças CID – 10 (1998), a definição da pedofilia é a preferência sexual por crianças, usualmente de idade pré-puberal ou no início da puberdade. Alguns pedófilos são atraídos apenas por menias e outros por meninos e alguns se interessam por crianças dos dois sexos. Raramente a pedofilia é identificada em mulheres, mas pode

ocorrer. Homens com essa condição podem molestar sexualmente seus filhos e também outras crianças, qualquer desses comportamentos é um indicativo de pedofilia (FELIPE, 2006).

Este transtorno mental pode se desenvolver em indivíduos de ambos os sexos, homem ou mulher, não se observando classe social. Em muitos casos, o indivíduo que prática o ato libidinoso é conhecido ou parente da família da vítima, o que facilitava a consumação do fato por conquistarem a confiança da vítima. Com o avanço da tecnologia, a internet se tornou ferramenta de sucesso dos pedófilos que vem um alvo fácil em crianças que já possuem perfis nas redes sociais.

Esses indivíduos criam perfis falsos para se comunicar com as vítimas de uma forma mais fácil e que não levante suspeitas, no caso de crianças que usam as redes sociais sem o controle dos pais estes pedófilos encontram alvos fáceis. No âmbito virtual, observamos não só a crescente de casos de pedofilia, mas também os casos de proliferação da pornografia infantil em fóruns, principalmente na *Deep Web* que acaba dificultando a localização e a identidade dos usuários que divulgam esse conteúdo.

2.6 Tráfico de Drogas

Com a facilidade em se ter acesso a produtos ilícitos de forma facilitada e anônima na *deep web,* o mercado de tráfico de drogas encontrou um amplo espaço agindo no mercado negro, uma vez que nesse ambiente é praticamente impossível identificar os usuários que participam dessas transações.

Sem contar que a moeda utilizada nas negociações não é rastreável, se trata do *bitcoin* esta é utilizada não só na *deep web*, mas na internet comum que é utiliza pelas massas. A facilidade na compra de entorpecentes neste ambiente é o atrativo e movimenta milhões de reais durante o ano (SILVA, 2017).

Um exemplo clássico é uma das maiores redes americanas de comércio ilegal, acessada pela rede *TOR,* denominada de *Silk Road*, que era administrada por uma pessoa cujo *nickname* era *Dread Pirate Roberts*. Apos uma investigação a polícia conseguiu identificar os donos do site e desativaram o site, mas após algum tempo outros sites maiores que o *Silk Road* surgiram (SILVA, 2017).

2.7 Lei Carolina Dieckmann (Lei n. 12.737/2012)

A referida Lei n.º 12.737/2012 ficou conhecida como Lei Carolina Dieckmann, em decorrência do episódio da divulgação de imagens em *sites* de pornografia, após *hackes* terem invadido os arquivos e acessado indevidamente os dados da vítima, a atriz que se recusou à chantagem de pagar a quantia em dinheiro para que suas fotografias em poses íntimas não fossem ilicitamente divulgadas.

Segundo Brito (2013), a entrada em vigor do diploma legal sobre delitos informáticos representou um marco na história do ordenamento jurídico pátrio, tendo em vista o substancial avanço no que concerne à criminalidade informática. A Lei n.º 12.735/12 foi sancionada pela presidente Dilma Rousseff com a dura missão de estreitar as lacunas existentes sobre a matéria, bem como evitar a impunidade dos crimes cibernéticos.

Em 7 de maio de 2012, a atriz Carolina Dieckmann foi até a delegacia comandada pelo delegado Gilson Perdigão, denunciar o vazamento de 36 (trinta e seis) fotos pessoais que foram publicadas na internet sem o seu consentimento no dia 4 do mês de maio. A atriz recebeu ameaças de extorsão desde o final de março, mas decidiu não registrar queixa para evitar exposição (VEJA, 2012).

Foram feitas 3 ligações para a atriz solicitando R$ 10 mil reais para não divulgar as fotos, como não cedeu as chantagens, a mesma se recusou a efetuar o pagamento e as fotos foram vazadas pelos criminosos, sendo compartilhadas por vários sites de conteúdo adulto. Na época do fato, não havia lei específica para crimes ocorridos através de dispositivo informático, com isso, a justiça se baseou no código penal para resolver o caso e os criminosos foram indiciados por furto, extorsão qualificada e difamação (VEJA, 2012).

Com a cobertura da imprensa nacional, o Projeto de Lei 2.793/2011, de autoria do Deputado Paulo Teixeira foi acelerado, uma vez que possuía a previsão de delitos cibernéticos aos quais o episódio com a atriz se encaixava. Em decorrência deste fato, a Câmara dos Deputados aprovou o projeto com urgência.

Dispõe a Lei n. 12.737/2012 sobre a tipificação criminal de delitos informáticos, com o intuito de atualizar a legislação penal vigente, em razão do defasamento do Código Penal com o passar dos anos. Previsto no art. 154-A do Código Penal, introduzido pelo art. 2º da Lei 12.737, de 30 de novembro de 2012 explicita a conduta repreendida de invadir dispositivo informático alheio, podendo estar ou não conectado à rede de computadores, através de violação indevida de mecanismos de segurança para obter, adulterar, ou destruir dados ou

informações sem autorização do dono do dispositivo para obter vantagem ilícita (BRASIL, 2012).

O crime é tipificado como formal, na conduta de invadir o sistema como de instalar vulnerabilidades, em eventual obtenção de dados ou informações, adulterações ou destruição, assim como a obtenção de vantagens ilícitas constituirão mero exaurimento. O crime de "Invasão de Dispositivo Informático" se consuma com apenas a invasão ou a instalação de vulnerabilidades no computador (BRASIL, 1940).

Entende como dispositivo informático qualquer computador ou aparelho que possua a capacidade de armazenar dados ou informações passiveis da violação prevista no tipo penal como computador pessoal, de empresas ou institucionais.

Constitui elemento normativo do tipo que é "dispositivo informático alheio" estar protegido por "mecanismo de segurança", como antivírus, *firewall* e senhas entre outros mecanismos. Assevera Cabette (2013, p. 01):

> Não é qualquer dispositivo informático invadido que conta com a proteção legal. Para que haja o crime é necessário que o dispositivo conte com 'mecanismo de segurança' (v.g. antivírus, 'firewall', senhas etc.). Assim sendo, o dispositivo informático despido de mecanismo de segurança não pode ser objeto material das condutas incriminadas, já que o crime exige que haja 'violação indevida de mecanismo de segurança'. Dessa maneira, a invasão ou instalação de vulnerabilidades em sistemas desprotegidos é fato atípico. […] Sinceramente não se compreende essa desproteção legislativa exatamente aos mais desprotegidos. É como se o legislador considerasse não haver violação de domicílio se alguém invadisse uma casa que estive com as portas abertas e ali permanecesse sem a autorização do morador e mesmo contra a sua vontade expressa! Não parece justo nem racional presumir que quem não instala proteções em seu computador está permitindo tacitamente uma invasão, assim como deixar a porta ou o portão de casa abertos ou destrancados não significa de modo algum que se pretenda permitir a entrada de qualquer pessoa em sua moradia. A forma vinculada disposta no tipo penal ('mediante violação indevida de mecanismo de segurança') poderia muito bem não ter sido utilizada pelo legislador que somente deveria chamar a atenção para a invasão ou instalação desautorizadas e/ou sem justa causa. Isso seria feito simplesmente com a locução 'mediante violação indevida' sem necessidade de menção a mecanismos de segurança.

Diante do exposto, fica evidente a eficacia da proteção do Estado em resguardar e tipificar os crimes dispostos na Lei 12.737/2012, a legislação tipificando os crimes ocorridos na internet sempre foi uma discussão que se desenrolou por muitos anos, mas com o caso da invasão do computador da atriz Carolina Dieckmann deu notoriedade a falha legislativa no caso de crimes cibernéticos.

3 DO PAPEL DO AGENTE POLICIAL INFILTRADO NAS INVESTIGAÇÕES DE CIBERCRIMES

3.1 Imprescindibilidade da Infiltração

O ambiente virtual se tornou um ambiente propício a crimes virtuais desde a disseminação da internet para as várias classes da sociedade. Observamos que a maioria dos crimes praticados no ambiente virtual se trata de crimes já conhecidos no mundo real, de forma que no ambiente virtual os criminosos estão por trás de um computador, o que dificulta a sua identificação.

A infiltração de agentes policiais é permitida no crime de organização criminosa, nas investigações de crimes como o tráfico de drogas, ciberterrorismo, pedofilia, entre outros. Observa-se que no ambiente virtual, ocorre um aprimoramento das condutas delituosas, ocasionando a necessidade do aprimoramento da atividade de inteligência policial.

3.2 A Responsabilidade do Agente Infiltrado

A infiltração virtual do agente policial deve ser bastante analisada antes de ser adotada, de modo que deve ser provado que nenhum outro método deu os resultados esperados. Em vista da infiltração do agente no ambiente criminoso presencial, a infiltração virtual prevista na Lei 13.441/17, esses riscos são bastante abrandados é um método que não proporciona um desgaste físico ao agente (WOLFF, 2017).

Conforme a manifestação de Nahur (2014), a utilização da técnica de infiltração de agentes policiais deve ser utilizada somente depois de esgotada todos os outros meios de investigação, incluindo também a interceptação telefônica que também só pode ser usada quando a prova não puder ser obtida por outros meios. Analisa-se que nas infiltrações policiais não podemos apenas nos preocupar com o sucesso da missão, mas também com o risco de contaminação psíquica, de criação de desequilíbrio emocional e moral, até mesmo com o surgimento de uma crise de identidade pessoal do policial infiltrado.

O autor supracitado ainda salienta que o risco de perversão e corrupção dos agentes é muito grande quando o Estado os coloca no mundo do crime e organizado com seus ganhos financeiros astronômicos, dessa forma, exige do agente uma formação moral praticamente

sobre-humana, mas, ao mesmo tempo flexível o suficiente para permitir uma atuação dissimulada.

Dessa forma, observa-se que um agente com esta flexibilidade na personalidade é extremamente rara, ou impossível de ser encontrada porque seria uma espécie de dupla personalidade do agente policial. Os agentes que se voluntariam para enfrentar esta missão, com o tempo se deparam com o conflito moral e psicológico interno com o decorrer da missão. De qualquer forma, uma orientação cabível é não somente a utilização desse meio investigativo, mas também a formação de equipes especializadas para este trabalho com treinamento e apoio psicológico.

É de suma importância que esses agentes não fiquem muito tempo no exercício dessa espécie de função, para que não sejam facilmente identificados, seja para evitar danos psicológicos a eles e também aquela perigosa associação com o submundo do crime. A pressão psicologia do agente em realizar a missão com êxito e se manter durante a infiltração sem ser descoberto é um dos principais pontos de risco, muitas vezes o indivíduo para manter a veracidade e sobreviver no meio em que na maioria do tempo esta combatendo, faz com que o agente mude de posição e se questione de que lado realmente ele está. Por isso, tal forma de investigação somente deve realmente ser adotada em último caso, esgotados os meios ordinários, de forma que os direitos e garantias individuais, inclusive dos investigados, não podem ser banalizados.

3.3 Da Colheita de Provas na Deep Web

Os criminosos descobrem diversas técnicas para se manterem no anonimato na rede, da mesma forma as autoridades conseguem se manter anônimas atraves de suas técnicas de rastreamento, conseguindo encontrar as vulnerabilidades dos criminosos virtuais e dessa forma coleta provas dos ilícitos causados pelos mesmos.

No Brasil, ocorreram duas grandes operações policiais no combate ao cibercrime. A primeira, denominada *DirtyNet* e a segunda, denominada *DarkNet,* esta que obteve duas fases, uma em 2014 e outra em 2016. A operação *DirtyNet*, ocorreu em 2012 e foi realizada pela Polícia Federal com apoio do Ministério Público Federal e da Interpol. O objetivo era a desarticulação de uma quadrilha que usava a internet para compartilhamento de materiais de pornografia infantojuvenil, fato que deu nome à operação (POLICIA FEDERAL, 2012).

Nesta ocasião, a *Deep Web* não era a rede utilizada pelos criminosos, mas sim um programa de compartilhamento de arquivos através de grupos fechados, denominado *Gigatribe*. No site da Polícia Federal se encontram alguns dados da Operação *Dirtynet:*

> Neste contexto, a partir da investigação de um único individuo descobriu-se uma rede de aproximadamente 160 usuários de conteúdos pornográficos envolvendo crianças e adolescentes, 97 usuários no exterior e 63 no Brasil. Trata-se de uma rede privada, criptografada, onde só é possível entrar com convite e aprovação dos outros membros. Cada usuário possuía a sua coleção privada e compartilhava na rede.

No ano de 2017 foi deflagrada a primeira fase da Operação DarkNet, em 18 (dezoito) Estados e no Distrito Federal, com o objetivo de identificar criminosos, investigar crimes de pornografia infantojuvenil na internet e de abusos sexuais de crianças e adolescentes. No site da Polícia Federal encontramos informações a respeito da primeira operação de combate à pornografia infantil onde a Polícia Federal rastreou o ambiente conhecido como *Deep Web,* considerando um meio seguro para que usuários da internet divulguem anonimamente conteúdos variados. A arquitetura deste ambiente praticamente impossibilita a identificação do ponto de acesso (IP), ocultando o real usuário que acessa a rede (POLICIA FEDERAL, 2014).

Através de metodologia de investigação inédita e ferramentas desenvolvidas, os policiais federais conseguiram quebrar esse sistema e identificar, na operação *DarkNet* mais de 90 usuários que compartilham pornografia infantil. Esta operação é um claro exemplo de como funciona na prática as técnicas de infiltração policial como meio para a obtenção de provas que comprovam os delitos e a inserção dos agentes no ambiente para rastrear os suspeitos (POLICIA FEDERAL, 2014).

A segunda fase da Operação *DarkNet,* ocorrida em 2016, também teve o objetivo de combater à rede *Deep Web* de distribuição de pornografia infantil. Utilizando-se de técnicas similares às aplicadas em sua primeira fase, a Operação *DarkNet* II ocorreu em 16 (dezesseis) unidades da federação. Segundo o site da Polícia Federal: “Poucas polícias no mundo obtiveram êxito em investigações na *Dark Web*, como o FBI, a Scotland Yard e a Polícia Federal Australiana”, fato que demonstra que o Brasil tem avançado nas investigações neste ambiente, apesar das falhas na legislação (POLICIA FEDERAL, 2016).

3.4 Dos Riscos e do Sigilo das Operações

Para a infiltração policial ocorrer de modo eficiente, é necessário medidas que garantam o sigilo por diversos motivos, o principal que é a integridade física do agente infiltrado e a efetividade da operação. Em uma possível descoberta do agente sua integridade física pode ser comprometida, assim como, não haver uma nova oportunidade para se concluir a missão.

O art. 10 da lei 12.850/2013 revela que a infiltração de agente de polícia em tarefas de investigação será precedida de sigilosa autorização judicial, além disso, o art. 12 da referida lei dispõe sobre a necessidade de sigilo do procedimento de infiltração quando expressa que o pedido de infiltração será sigilosamente distribuído, de forma a não conter informações que possam indicar a operação a ser efetivada ou identificar o agente que será infiltrado (BRASIL, 2013).

O sigilo da investigação não fere o princípio o princípio constitucional da publicidade da investigação por parte do investigado, já que a Constituição respalda em seu art. 5º, inciso LX que a "lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou interesse social o exigirem". É inegável o interesse social e a busca pela justiça nos casos de infiltração virtual.

Por mais que o agente infiltrado tenha total suporte, tem o direito de recusar e não se sentir coagido a participar da operação. Os riscos neste tipo de infiltração são menores que os riscos numa infiltração física do agente, mas ainda existem, em função disso o art. 12, §3º, disciplina que a operação de infiltração policial será sustada mediante requisição do Ministério Público ou pelo delegado de policial se houver indícios seguros de que o infiltrado sofre risco iminente, nesta situação proteger a vida do agente é o principal (BRASIL, 2013).

3.5 Cooperação Internacional para a Obtenção de Provas

A ratificação pelo Brasil da Convenção sobre Crimes Cibercrimes de modo que ela dispõe de mecanismos de regulação dos procedimentos para a assistência entre países signatários facilita e é de suma importância para a comunicação na parceria ao combate aos cibercrimes.

A Organização Internacional de Polícia Criminal, a conhecida INTERPOL, é uma organização policial internacional que visa o combate a diversos tipos de crimes por meio da

associação de aplicação da lei de muitos países. Com isso a INTERPOL facilita a troca de informações em investigações policiais, principalmente em relação a dados informáticos advindos de outro país.

Neste quesito, entende Domingos (2017, p. 247/248):

> Nos delitos cibernéticos de disseminação de pornografia infantil via web, é comum que no bojo dessas investigações em determinado país sejam identificados IP's e dados de conexão utilizados na prática criminosa de usuários de Internet pertencentes a outro país. Situação em que a polícia desse país e envia as informações para o país onde os IP's identificados são alocados para que as investigações sejam desenvolvidas com relação às imagens e vídeos disseminados a partir desse local, tanto por ser de atribuição do país investigar e processar os delitos cometidos a partir de seu próprio território, quanto por ser mais provável que o criminoso seja identificado no local de onde disseminou as imagens e vídeos.
> Nesses casos, em que há a troca pelas autoridades competentes de diferentes estados de informações relevantes às investigações que ocorre em geral por intermédio da INTERPOL, há a presunção de regularidade na obtenção e transmissão de tais informações conforme a legislação do país de origem. No entanto, afigura-se prudente que os investigadores submetam a prova ao Judiciário para validação e autorização de uso.

Para Domingos, necessário ressaltar a importância da carta rogatória e do pedido de assistência mútua jurídica. A referida carta, direciona requerimentos a uma determinada jurisdição estrangeira para cumprir ato instrutório a fim de colaborar com investigações ou processos do país rogante. Esta assistência tem o objetivo a colheita de provas no combate a criminalidade transnacional, no qual consiste em requerimento de um Estado a outro ultrapassando as medidas de cooperação internacional, a fim de que o Estado que solicita em conformidade com a lei auxilie nas investigações.

Esta cooperação é indispensável principalmente nos casos de crimes cibernéticos, onde muitos crimes ocorrem em diversos países. A investigação de crimes virtuais no Brasil, encontrou diversos impedimentos, uma vez, que não ratificou vários acordos internacionais que colaboram no combate a crimes cibernéticos.

3.6 Convenção de Budapeste

No quesito tipificação de crimes cibernéticos os países Europeus estão muito a frente do Brasil, enquanto o mesmo mostra ter uma falta de dialogo com a sociedade que é a principal propagadora de conteúdos virtuais. A Convenção de Budapeste foi o passo inicial para a tentativa de coibir os crimes virtuais, foi criada em 2001 na Hungria, elaborado por um comitê de peritos nacionais, congregados no Conselho da Europa e entrou em vigor no ano de

2004. Foi ratificada por cinco países e engloba mais de 20 países e trata dos principais crimes virtuais (EDERLY, 2008).

Formada por maioria de países-membros do Conselho da Europa, na sua elaboração participaram vários países de outros continentes como, Estados Unidos, Canadá, África do Sul e Japão, a uma tendência para que mais países do globo se tornem signatários da Convenção, dessa forma, tentando coibir a propagação dos delitos cibernéticos em escala mundial (SOUZA; PEREIRA, 2009).

A convenção trata em seu preâmbulo do que é considerado o cerne do tratado, "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional". O Tratado de 2001 possui quatro Capítulos (Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais) e 48 artigos (SOUZA; PEREIRA, 2009).

A Convenção tem como cargo chefe definir os cibercrimes, tipificando-os como infrações contra sistemas e dados informáticos, infrações relacionadas com computadores, infrações relacionadas com o conteúdo, pornografia infantil e infrações relacionadas com a violação de direitos autorais.

O tratado traz ainda em seu texto regras de cooperação internacional onde é fixado o limite mínimo de um ano de prisão, para que seja admissível a extradição, sendo necessária a dupla incriminação. Em relação à cooperação mútua a Convenção de Budapeste em seu artigo 26º prevê a possibilidade de um país encaminhar informações a outro Estado caso essas informações sejam úteis ou necessárias ao início ou ao desenvolvimento de uma investigação de um crime enquadrado na Convenção. A remessa de informação para outro país signatário deve observar a confidencialidade dos dados (SOUZA; PEREIRA, 2009).

Muito se especulou por qual motivo o Brasil não é signatário da Convenção de Budapeste, mas o Secretário-Geral do Ministério das Relações Exteriores salientou que não se pode apenas aderir a Convenção, mas sim ser convidado pelo Comitê de Ministros do Conselho Europeu, conforme explicita o Artigo 37º da Convenção de Budapeste "(…) O Comitê de Ministros do Conselho da Europa pode (…) convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção" (CONSELHO DA EUROPA, 2001).

A relação do Brasil com os países europeus não é preocupante, ao contrário, a relação é muito harmoniosa e como a adesão deve ser unânime entre os países-membros é praticamente certa uma possível aceitação do Brasil no tratado. O fato do país não ser signatário da Convenção não inibe a legislação brasileira de tipificar os crimes virtuais e combater, mas com a adesão do Brasil no tratado facilitaria a cooperação internacional no auxílio a crimes cometidos em âmbito internacional.

CONCLUSÃO

O trabalho em questão buscou apresentar os crimes virtuais, os quais o desenvolvimento da criminalidade neste ambiente cibernético se tornou evidente nos últimos anos, expondo as falhas na legislação vigente. Com isso, o surgimento de técnicas especiais de investigação no ambiente virtual foi uma prática que acarretou um avanço no combate aos criminosos.

De fato, a infiltração policial surge como uma técnica de investigação polêmica, uma vez que ao se utilizar de métodos não convencionais, como a dissimulação, a criação de uma identidade fictícia, a possibilidade do agente policial praticar crimes, e, também, a violação de direitos fundamentais, como o da privacidade, esbarra-se em aspectos éticos desse instituto. Conforme foi demonstrado no presente estudo, é imperioso que ao deflagrar operações policiais nas quais serão utilizadas técnicas especiais, como a infiltração policial, deve-se observar a essencialidade de cada medida.

O agente que se infiltra no contexto criminoso por meio virtual, mesmo que menores, não está isento de riscos, dessa forma, a infiltração policial assume um caráter excepcional na atividade investigativa, não pode ser utilizada em qualquer caso, mas sim, depois de esgotadas todas as formas convencionais de investigação. Ilícitos penais como o de organização criminosa, tráfico de entorpecentes, terrorismo e pornografia infantojuvenil assumem uma grande periculosidade social, além de um alto grau de reprovabilidade, atingindo bens jurídicos expressivos à sociedade. Por conta disso, importante é o uso de métodos suficientes o bastante no combate aos crimes mais complexos.

Não se trata, contudo, de uma medida que pode ser implementada de forma indiscriminada, mas deve-se observar o seu caráter excepcional, tanto no que se refere ao esgotamento de todos os outros meios convencionais de obtenção de prova, quanto no que tange à natureza da infração. Ou seja, ela só é permitida quando a norma dispuser acerca dos crimes que aceitam, em sua persecução, a referida técnica.

A infiltração virtual é essencial para combater crimes cibernéticos, uma vez que com avanço tecnológico, a criminalidade aprimora seu modo de agir. Se artifícios como a *Deep Web* são utilizados para fins legítimos, a mente criminosa encontrou neste espaço um ambiente propício para realizar seus crimes sem serem descoberto.

Foi realizada uma análise dos principais crimes que ocorrem por meio virtual, um dos principais que é a pornografia infantil, que hoje em dia são comuns de ocorrerem na Deep Web, onde pedófilos propagam imagens de crianças em fóruns online com outras pessoas. Muitos delitos são praticados por organizações criminosas que atuam especificamente na deep web.

A ação do agente infiltrado é de suma importância para o êxito da operação, dependo do crime em rogo é necessário a cooperação internacional das policias com a INTERPOL para se chegar até os criminosos. Observamos assim, a suma importância deste estudo para entendermos melhor como ocorre a infiltração policial no ambiente cibernético.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023**: Informações e documentação: referências: elaboração. Rio Janeiro. 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6024**: Informações e documentação: referências: elaboração. Rio Janeiro. 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 10520**: Informações e documentação: citação em documentos: apresentação. Rio Janeiro. 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 14724**: Informações e documentação: trabalhos acadêmicos: apresentação. Rio Janeiro. 2002.

AGUIAR, A. **Qual a diferença entre Dark Web e Deep Web?.** Tecmundo. Internet, 09 de março de 2018. Disponível em:< https://www.tecmundo.com.br/internet/128029-diferenca-entre-dark-web-deep-web.htm>. Acesso em: 09 jan. 2019.

BRASIL. **ECA-Estatuto da criança e do adolescente**. Lei nº 8.069, de 13 de julho de 1990. Disponível em < http://www.planalto.gov.br/ccivil_03/leis/L8069.htm > Acesso em: 24 out. 2018.

BRASIL. **Organização Criminosa.** Lei nº 12.850, de 2 de agosto de 2013. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em: 08 jan. 2019.

BRITO, A. **Direito penal informático.** São Paulo: Saraiva, 2013.

BORGES, C. B.; SARTORI, L. P.; BARROS, S. M. **A Deep Web e a relação com a criminalidade na internet.** Direito & TI. Porto Alegre, 07 de dezembro de 2018. Disponível em:< http://direitoeti.com.br/artigos/a-deep-web-e-a-relacao-com-a-criminalidade-na-internet/>. Acesso em: 09 jan. 2019.

CORREA, G. T. **Aspectos jurídicos da internet.** 5 ed. São Paulo: Saraiva, 2010.

CRESPO, M. X. de F. **Crimes Digitais**. São Paulo: Saraiva, 2011.

CABETTE, E. L. S. **Primeiras impressões sobre a Lei 12.737/12 e o crime de invasão de dispositivo informático.** Âmbito Jurídico. Rio Grande, XVI, n. 109, fevereiro de 2013. Disponível em:<http://ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12865>. Acesso em: 19 out. 2018.

_____. **O novo crime de Invasão de Dispositivo Informático**. Consultor Jurídico, São Paulo, 4 fev. 2013. Disponível em: <http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 14 out. 2019.

CASTRO, C. R. A. de. **Crimes de Informática e seus Aspectos Processuais**. 2 ed. rev. ampl e atual. Rio de Janeiro, 2003.

CABETTE, E. L. S, NAHUR, M. T. M. **Criminalidade Organizada & Globalização Desorganizada**. Rio de Janeiro: Freitas Bastos.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança**. 2006. Disponível em: < https://www.cos.ufrj.br/uploadfile/1430748034.pdf>. Acesso em: 22 fev. 2019.

CASTELLS, M. **A Era da Informação**: economia, sociedade e cultura. Vol. 3, São Paulo: Paz e terra, 1999.

CLASSIFICAÇÃO DE TRANSTORNOS MENTAIS E DE COMPORTAMENTO DA CID-10. **Descrições clínicas e diretrizes diagnósticas**. Porto Alegre: Artes Médicas, 1993.

COLARIK, A. M; JANCZEWSKI, L. J. **Cyber Warfare and Cyber Terrorism.** Hershey: IGI Global, 2008.

CONVENÇÃO SOBRE O CIBERCRIME. Disponível em: < http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf >. Acesso em: 15 jan. 2019.

DOMINGOS, F. T. S. **A obtenção das provas digitais na investigação dos delitos de violência e exploração sexual infantil online.** In SILVA, Ângelo Roberto Ilha da (Org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado. 2017.

ERDELY, M. F. Itamaraty ainda estuda adesão à Convenção de Budapeste. **Revista Consultor Jurídico**, maio 2008. Disponível em: <https://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste >. Acesso em: 06 mar. 2019.

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

FELIPE, J. Afinal, quem é mesmo pedófilo? **Cadernos Pagu (26)**, jan/jun. 2006. Disponível em: <http://www.scielo.br/pdf/cpa/n26/30391.pdf>. Acesso em: 15 jan. 2019.

FRAGOSO, H. C. **Lições de direito penal**: Parte Especial. Rio de Janeiro: Forense, 1983.

VEJA. **Polícia caça responsáveis pelo vazamento das fotos de Carolina Dieckmann nua**. Disponível em: <https://veja.abril.com.br/entretenimento/policia-caca-responsaveis-pelo-vazamento-das-fotos-de-carolina-dieckmann-nua/>. Acesso em: 20 jan. 2019.

HOBSBAWM, E. **Globalização democracia e terrorismo**. São Paulo: Companhia das Letras, 2007.

INELLAS, G. C. Z. de. **Crimes na Internet**. São Paulo: Juarez de Oliveira, 2004.

LÉVY, P. **Cibercultura.** Trad. De Carlos Irineu da Costa. 2. ed. São Paulo: 34, 2000.

_____. **Cibercultura**. São Paulo: 34, 1999.

LIMA, P. M. F. **Crimes de Computador e Segurança Computacional**. 2 ed. São Paulo: Atlas, 2011.

LIMA, R. B. de. **Legislação Criminal Especial Comentada**. 5 ed. Vol. Único. Salvador: Juspodivm. 2017.

LUZ, C. **Primavera Árabe: o que aconteceu no oriente Médio?** 2017. Disponível em: <https://www.politize.com.br/primavera-arabe/>. Acesso em: 21 jan. 2019.

MASI, C. V. **Crimes Contra a Honra Pela Internet**. Canal Ciências Criminais. Rio Grande do Sul, 03 de setembro de 2016. Disponível em:<https://canalcienciascriminais.com.br/crimes-contra-honra-pela-internet/>. Acesso em: 30 out. 2018.

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

OLIVEIRA, C. A. G. **Direito Penal e Crimes Cibernéticos**. 2017. 55 f. Trabalho de conclusão de curso de graduação em Direito – Universidade Tuiuti Do Paraná, Curitiba, 2017.

PINHEIRO, P. P. **Direito digital**. São Paulo: Saraiva, 2002.

POLICIA FEDERAL. **Balanço Final da Operação DirtyNet.** 28 de junho de 2012. Disponível em: < http://www.pf.gov.br/agencia/noticias/2012/junho/balanco-final-da-operacao-dirty-net >. Acesso em: 28 jan. 2019.

POLICIA FEDERAL. **Combate a disseminação de pornografia infantil pela deep web no Rio Grande do Sul**. 15 de outubro de 2014. Disponível em: < http://www.pf.gov.br/agencia/noticias/2014/10/pf-combate-a-disseminacao-de-pornografia-infantil-pela-deep-web-no-rs>. Acesso em: 29 jan. 2019.

POLICIA FEDERAL. **Combate crime de pornografia infantil na deep web**. 22 de novembro de 2016. Disponível em: <http://www.pf.gov.br/agencia/noticias/2016/11/pf-combate-crime-de-pornografia-infantil-na-deep-web>. Acesso em: 29 jan. 2019.

ROSSINI, A. E. de S. **Informática Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2004.

SILVA, R. de C. L. **Direito penal e sistema informático.** São Paulo: Revista dos Tribunais, 2003.

SILVA, I. M. **A infiltração policial como técnica especial de investigação no ambiente cibernético**. 2017. 83 f. Trabalho de conclusão de curso de graduação em Direito – Universidade Federal Fluminense, Macaé, 2017.

SHIMABUKURO, A.; SILVA, M. G. B. de A. **Internet, Deep Web e Dark Web**. In SILVA, Ângelo Roberto Ilha da (Org.). Crimes Cibernéticos**.** Porto Alegre: Livraria do Advogado. 2017.

SHIMEALL, T. Cyber Terrorism. CERT Centers, Software Engineering Institute. Pittsburg, PA, 2002. In LIMA, J. **O Impacto do Terrorismo nas Cadeias Globais de Abastecimento**. ed Universidade do Porto, 2006.

SOUZA, G. L. M.; PEREIRA, D. V. **A Convenção de Budapeste e as Leis Brasileiras.**2009. 15 f. Trabalho apresentado para publicação nos Anais do 1° Seminário Cibercrime e Cooperação Penal Internacional, organizado pelo CCJ da UFPB e pela Association Internacionale de Lutte Contra la Cybercriminalite (França), João Pessoa, 2009.

WOLFF, R. **Infiltração de agentes por meio virtual**. In SILVA, Ângelo Roberto Ilha da (Org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado. 2017.