FACULDADES INTEGRADAS DE PONTA PORÃ FIP MAGSUL

JULIANE DE FREITAS ORTIZ

OS DESAFIOS DA PERSECUÇÃO PENAL DO CRIME DE DISSEMINAÇÃO DE PORNOGRAFIA INFANTIL NA *DARK WEB*

PONTA PORÃ/MS

2019

JULIANE DE FREITAS ORTIZ

OS DESAFIOS DA PERSECUÇÃO PENAL DO CRIME DE DISSEMINAÇÃO DE PORNOGRAFIA INFANTIL NA *DARK WEB*

Trabalho de Conclusão de Curso apresentado à Banca Examinadora das Faculdades Integradas de Ponta Porã/FIP Magsul, como requisito a obtenção do título de Bacharel em Direito.
Orientador: Prof. Esp. Arquimedes Alez Jara.

PONTA PORÃ/MS

2019

Dados Internacionais de Catalogação na Publicação (CIP)

—

O77d Ortiz, Juliane de Freitas.
Os desafios da persecução penal do crime de disseminação de pornografia infantil na Dark Web / Juliane de Freitas Ortiz – Ponta Porã, MS, 2019.
68p.; 30 cm.

Orientador (a): Profº. Esp. Arquimedes Alez Jara.
Monografia (graduação) – Faculdades Integradas de Ponta Porã - MS. Curso de Direito.
1. Pornografia infantil. 2. Dark Web. 3. Deep Web. 4. Investigação. 5. Prova. I. Jara, Arquimedes Alez. II. Título.

CDD:

343.541

OS DESAFIOS DA PERSECUÇÃO PENAL DO CRIME DE DISSEMINAÇÃO DE PORNOGRAFIA INFANTIL NA *DARK WEB*

BANCA EXAMINADORA DA MONOGRAFIA PARA A OBTENÇÃO DO GRAU DE BACHAREL EM DIREITO DAS FACULDADES INTEGRADAS DE PONTA PORÃ – FIP MAGSUL

BANCA EXAMINADORA:

_____

Profª. Ma. Janaína Ohlweiler Milani

_____

Profº. Esp. Mauro Alcides Lopes Vargas

_____

Profº Orientador. Arquimedes Alez Jara.

_____

Juliane de Freitas Ortiz

PONTA PORÃ/MS

2019

AGRADECIMENTOS

A etapa final do presente curso foi atribulada e árdua, sendo que por momentos julguei-me incapaz de concluir o curso, porém minha fé sempre me guiou e me concedeu força para continuar perseguindo meus objetivos. Em razão disso em primeiro lugar agradeço a Deus por minha vida, saúde, oportunidades, sabedoria e amor. Sem Ele nada seria possível.

Agradeço a minha mãe, Rosana, pelo amor e apoio incondicionais sem os quais jamais poderia ter cursado ensino superior. Nunca me esquecerei dos seus sacrifícios para oportunizar-me vida de qualidade e educação acadêmica, bem como da sua crença no meu potencial e incentivo constante, sendo que o jamais serei capaz de expressar minha gratidão. Espero um dia poder recompensá-la por tudo que fez por mim e sou eternamente grata por ser meu exemplo de força e bondade.

Ao meu irmão, Thales, agradeço por sempre prestar-me auxílio e se alegrar com as minhas conquistas. Em especial lhe agradeço pela preocupação com meu bem-estar e pelo zelo com nossa mãe.

Agradeço aos meus demais familiares pelo afeto e paciência que sempre demonstraram e pela disposição para ajudar-me nos momentos de dificuldade. Sou grata por se orgulharem de minhas conquistas.

Agradeço ao meu orientador, Arquimedes Alez Jara, pela paciência, disposição e orientação que contribuíram para a elaboração do presente trabalho.

Aos integrantes dos órgãos judiciais em que tive a oportunidade estagiar durante o curso representados na figura do Procurador da República, Luiz Paulo, agradeço pelos conhecimentos transmitidos e pela cordialidade com que sempre foi tratada que foram significativos para minha formação acadêmica e profissional.

Agradeço aos meus amigos pelo apoio psicológico e palavras de incentivo proferidas no decorrer do curso principalmente em momentos de dificuldade. Em especial às minhas colegas de turma que embora também tivessem suas obrigações, inseguranças, incertezas e problemas sempre dispuseram de paciência e companheirismo para me auxiliar.

Por fim, sou grata a todo o corpo docente da FIP/MAGSUL por todos os conhecimentos compartilhados e pelo apreço pela docência que transpareceram. Agradeço pelo incentivo dado a todos os alunos.

Enfim, sou muito grata a todos aqueles que contribuíram para a minha formação.

RESUMO

O presente estudo teve como propósito identificar os desafios da persecução penal no combate ao crime de disseminação de pornografia infantil praticada na *Dark Web*. O sistema de funcionamento da *Dark Web* mostra-se como obstáculo à investigação criminal em razão do véu de anonimato proporcionado pelo *software* TOR ao usuário. Para alcançar o objetivo, o estudo buscou a compreensão dos aspectos que permeiam a *Dark Web*, bem como da tutela legislativa e as ferramentas investigativas utilizadas na persecução com enfoque na Operação Darknet. Portanto, realizou-se uma pesquisa bibliográfica qualitativa com a exploração dos direitos das crianças e do investigado em obras doutrinárias, artigos científicos e na legislação, bem como um exame acórdão emanado do Tribunal Regional Federal da 3ª Região. Atualmente entende-se pela licitude da prova produzida por meio da infiltração de policiais diante de prévia autorização judicial. O equilíbrio entre os direitos e liberdades individuais das pessoas e a reposta jurisdicional à cibercriminalidade é o principal desafio da investigação penal do crime de disseminação de pornografia infantil no ambiente da *Dark Web.*

Palavras-chave: Pornografia Infantil. *Dark Web. Deep Web*. Investigação. Provas.

ABSTRACT

The purpose of this study was to identify the challenges of criminal prosecution against the crime of dissemination of child pornography practiced in the Dark Web. The Dark Web's operating system is seen as an obstacle to criminal investigation because of the veil of anonymity provided by the software TOR to the user. In order to reach the objective, the research sought an understanding of the aspects that permeate the Dark Web, as well as the legislation and investigative tools used in the persecution focused on Operation Darknet. Therefore, was made a qualitative bibliographic research of the children's and suspect's rights in doctrinal literature, scientific articles and legislation, as well as an examination of a court decision emanated from the Federal Regional Court of the 3rd Region. Nowadays it is understood that the criminal proof obtained by police infiltration is legal if it is based on a prior judicial decision. The balance between the rights and freedom of individuals and jurisdictional response to cybercrime is the main challenge of criminal investigation of the crime of dissemination of child pornography in the Dark Web's environment.

Key words: Child Pornography. Dark Web. Deep Web. Investigation. Proof.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

CP – CÓDIGO PENAL
ECA – ESTATUTO DA CRIANÇA E DO ADOLESCENTE
FBI – FEDERAL BUREAU OF INVESTIGATION
IP – INTERNET PROTOCOL
MPF – MINISTÉRIO PÚBLICO FEDERAL
ONG – ORGANIZAÇÃO NÃO GOVERNAMENTAL
TOR – THE ONION ROUTER
TRF 3 – TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO
URL – UNIFORM RESOURCE LOCATOR

SUMÁRIO

INTRODUÇÃO

Nas últimas duas décadas o excepcional avanço tecnológico e científico conduziu a mudanças significativas na forma organizacional e comportamental da sociedade. Nesse sentido, a *Internet* tornou-se o principal meio para troca de informações e conteúdos entre os indivíduos, uma vez que além de facilitar a comunicação entre locais fisicamente distantes, também proporciona, a depender do mecanismo utilizado, a proteção dos dados insertos no mundo digital.

Por outro lado, os progressos tecnológicos também conduziram ao surgimento de inúmeros crimes propriamente digitais e transcendência de crimes para o ambiente digital que originalmente não eram cometidos por intermédio da *Internet.*

A inserção da sociedade no mundo digital fez surgir uma nova classe de crimes denominados, ainda sem precisão terminológica pacífica, como crimes digitais, crimes virtuais, crimes cibernéticos, delito informáticos, dentre outros (SPINIELI, 2018). Podem ser entendidos por crimes digitais as condutas ilícitas que são praticadas por meio da *Internet* ou com seu auxílio que causam dano à vítima (FIORILLO; CONTE, 2016).

Nos últimos anos, tonaram-se recorrentes notícias jornalísticas acerca de crimes envolvendo o ambiente digital. Nessa perspectiva, ocupa recorrente destaque casos de vídeos e imagens envolvendo crianças em cenas de sexo explícito ou com alguma conotação sexual, uma vez que seu compartilhamento pode se dar de forma aparentemente anônima e instantânea.

Dessa forma, a *Internet* propiciou a expansão e facilitação da disseminação de pornografia infantil. Conforme os Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos disponível no *site SaferNet* Brasil[1]*,* no ano de 2016 a Polícia Federal recebeu 35.303 (trinta e cinco mil e trezentos e três) denúncias anônimas de pornografia infantil relacionadas à *Internet* envolvendo IPs de 37 (trinta e sete) países em 5 (cinco) continentes (SAFERNET BRASIL, 2016).

A *Internet* é dividida em três níveis: *Surface Web, Deep Web e Dark Web*. Nesse sentido, a terceira camada é considerada a mais sombria e classificada como *Dark Web,* uma vez que é nela em que se concentram a grande variedade de delitos oferecidos, negociados e praticados (ROCHA, 2018).

[1] A *SaferNet* Brasil é uma organização sem fins lucrativos e sem vinculação com o governo que atua no Brasil no combate aos crimes e violações aos Direitos Humanos na *Internet.*

Nos últimos anos houve a transição da prática de crimes relacionados com pornografia infantil para a chamada *Dark Web,* em virtude de sua maneira de funcionamento que dificulta a constatação da autoria e materialidade do crime. Estudos realizados por Gareth Owen e Jamie Bartlett indicam que cerca de 80% (oitenta por cento) do conteúdo da *Dark Web* consiste em pornografia infantil.

Diante de recorrência dessas condutas a dignidade sexual e a imagem da criança são mundialmente salvaguardadas por tratados e convenções, como a Convenção das Crianças sobre Direito das Crianças e o Protocolo Facultativo sobre a Venda de Crianças, Prostituição e Pornografia Infantis, visando garantir o crescimento digno na fase de desenvolvimento púbere.

No Brasil a Lei nº 11.829/2008 promoveu alteração nos artigos 240 e 241 do Estatuto da Criança e Adolescente com o intuito de aperfeiçoar o enfrentamento da produção, venda e distribuição de pornografia infantil (ISHIDA, 2014). O artigo 241-A do ECA criminaliza no ordenamento jurídico brasileiro a disseminação de pornografia infantojuvenil por meios telemáticos e informáticos.

Dessa maneira, percebe-se de crimes virtuais se expandiram, impondo ao Estado a necessidade de desenvolver tecnologias e métodos de investigações aptos a acompanhar as evoluções criminológicas. Constitui objetivo do direito regular as relações humanas, sendo assim deve buscar evoluir na medida em que a sociedade se transforma.

O crescimento da investigação desses crimes no Brasil ocorreu com a deflagração da Operação Carrossel pela Polícia Federal em 2007 onde foram cumpridos 102 (cento e dois) mandados de busca e apreensão e contou com o auxílio do FBI e da Interpol (FIORILLO; CONTE, 2016). Após diversas outras operações foram deflagradas objetivando a repressão da pornografia infantojuvenil na *Internet,* como a Operação Darknet I e II nos anos de 2014 e 2016 que teve enfoque a apuração dessa espécie de crime cometidos no espaço da *Deep Web* (MPF, 2018).

A operação Darknet em sua primeira fase efetuou o cumprimento de mais de 100 (cem) mandados de busca e apreensão, sendo 51 (cinquenta e uma) pessoas foram presas em razão do armazenamento de material que continha pornografia infantil. Na segunda fase da operação cerca de 70 (setenta) suspeitos foram investigados, sendo que a competência foi declinada para diversas subseções judiciárias em 17 (dezessete) estados brasileiros. Ainda, com a investigação 5 (cinco) crianças foram resgatadas em situações de abuso (MPF, 2017).

No entanto, em razão do aperfeiçoamento dos meios de cometimento dos delitos no ambiente digital por seus usuários e da grande quantidade de conteúdo pornográfico infantojuvenil disponível na *Internet,* o ordenamento brasileiro ainda encontra dificuldade para a identificação e repressão dos agentes que praticam condutas relacionadas à pornografia infantojuvenil (CALADO; CALADO, 2018).

Nessa perspectiva, a presente pesquisa visa, principalmente, identificar os desafios da persecução penal no combate ao crime de disseminação de pornografia infantil praticada na *Dark Web* com base em pesquisa bibliográfica e na observação de decisão judicial proferida em caso concreto apreciado pelo Tribunal Regional Federal da 3ª Região.

O presente estudo mostra-se relevante uma vez que o campo do direito digital apresenta demanda cada vez mais crescente, porém ainda, embora tenha sido mais explorado nos últimos anos, não é temática comum em especial no tocante aos crimes praticados na *Dark Web*.

Em pesquisa ao site *Google* Acadêmico, verificou-se que há moderado número de artigos científicos e trabalhos acadêmicos no campo do estudo da pornografia infantil na *Dark Web*, porém não foi possível localizar trabalho com enfoque no exame de acórdão judicial proferido pelo Tribunal Regional da 3ª Região, o qual exerce jurisdição sobre as Seções Judiciárias dos estados de São Paulo e de Mato Grosso do Sul. Assim, não há ainda pesquisa acerca do entendimento de tribunal responsável pelo julgamento de futuros casos de disseminação de pornografia infantil na *Dark Web* no estado de Mato Grosso do Sul.

A partir disso, estabeleceu-se como questionamento orientador do projeto: Quais são os desafios do ordenamento jurídico brasileiro no combate ao crime de disseminação de pornografia infantil praticado no ambiente da *Dark Web.*

Neste ponto, realizar-se-á estudo com pesquisa bibliográfica sobre o tema. Para tanto a pesquisa será baseada em material científico, ou seja, em artigos científicos publicados em revistas jurídicas e informáticas, livros, dados estatais e pesquisas realizadas no campo acadêmico. Além disso, serão utilizados elementos contidos na legislação pátria e em estudo de acórdão judicial proferido pelo Tribunal Regional Federal da 3ª Região.

Isto posto, visando responder à problemática serão desenvolvidos três capítulos. No primeiro capítulo será exposta a gênese da *Internet* e sua evolução, bem como o desenvolvimento tecnológico que deu azo a criação da chamada sociedade

de informação. Ademais, serão exibidos os principais aspectos acerca dos crimes informáticos e as complexidades que permeiam a *Dark Web*.

No segundo capítulo busca-se tecer noções sintéticas acerca do abuso sexual e do comportamento do pedófilo, a fim de entender as peculiaridades das motivações do agente criminoso. Ainda, faz se necessária a exibição da tutela jurídica aos direitos da criança à luz da Constituição Federal, do Estatuto da Criança e do Adolescente e convenções internacionais. Neste capítulo também pretende-se demonstrar o paralelo entre a pornografia infantil e a *Dark Web*, bem como tecer breves considerações acerca dos direitos constitucionalmente assegurados aos indivíduos que devem ser observados na investigação criminal, como os direitos à privacidade e liberdade de comunicação.

Por derradeiro, no último capítulo proceder-se-á a observação acerca de posicionamento de acórdão julgado pela 11ª Turma do Tribunal Regional Federal da 3ª Região conjuntamente com as disposições legislativas acerca da persecução penal da temática no âmbito jurídico brasileiro. Para tanto, necessária a identificação dos procedimentos utilizados para a investigação de caso concreto e exame da licitude das provas produzidas no procedimento judicial.

Diante o exposto, visa-se traçar panorama do atual quadro investigativo a fim de identificar os desafios que a persecução penal encontra para o combate do crime de disseminação de pornografia infantil praticado por intermédio de *Dark Web*.

CAPÍTULO 1 - A SOCIEDADE DE INFORMAÇÃO E A EVOLUÇÃO DA *INTERNET*

Com o desenvolvimento de tecnologia a sociedade modificou não somente seus meios de produção, mas também sua forma comportamental e organizacional, trazendo o surgimento de uma nova gama de relações que necessitam de regulamentação.

Nessa perspectiva, a criação da *Internet* alterou de forma profunda as relações interpessoais e deu azo ao nascimento de delitos, bem como a modificação de crimes já existentes. Além disso, nos últimos anos o Estado e a sociedade têm se atentado para a necessidade do desenvolvimento de tecnologia para o combate do cibercrime.

O presente capítulo tem como objetivo abordar a evolução da *Internet* até os dias atuais, destacando as mudanças causadas pela sua difusão. Além disso, trazemos um aparato geral acerca dos crimes informáticos como conceituação e classificação. Por derradeiro, busca-se fazer a diferenciação entre *Surface Web, Deep Web* e *Dark Web*.

1.1 Surgimento e aspectos técnicos acerca da *Internet*

A *Internet* nasceu durante a Guerra Fria, em 1960, quando os norte-americanos, no meio do conflito com os soviéticos, verificaram a necessidade de criação de um mecanismo que oportunizasse comunicação em longas distâncias e que não pudesse ser interceptado por terceiros desautorizados. A partir disso, o estadunidense Paul Baran idealizou uma rede com diversas trajetórias para lograr êxito em chegar ao seu destino, por esta razão tem-se a expressão *Web* que em inglês significa "teia de aranha" (MARCON, DIAS, 2014).

Após alguns anos cientistas norte-americanos iniciaram o projeto com base na ideia de Baran que consistiu na *ARPAnet*, derivado do termo *Advanced Research Projects Agency*[2]. Nesse mecanismo inexistia um comando central de maneira que caso algum dos computadores fosse destruído não afetaria o funcionamento dos demais equipamentos (MPF, 2006).

Deste modo, percebe-se que a *Internet* foi desenvolvida para atender a fins militares já que em guerra os combatentes necessitavam de um sistema de

[2] Agência de Projetos de Pesquisa Avançada

comunicação que não ficasse prejudicado se caso alguma base militar fosse destruída ou invadida. Logo, o projeto da *Internet*, como hoje conhecemos, surgiu para garantir também autonomia de comunicação.

A criação da *ARPAnet* ocorreu com propósito de oportunizar estudos em que os Estados Unidos ultrapassassem a União Soviética em tecnologia militar. Nesse sentido, na apresentação ao Pentágono a *ARPAnet* foi exposta como uma maneira de comunicação descentralizada apta a garantir o sigilo de dados até mesmo em ataques nucleares (FIORILLO; CONTE, 2016).

A versão inicial da *ARPAnet* foi projetada para conectar alguns centros de pesquisas e algumas universidades, objetivando o armazenamento de forma virtual do conteúdo sem que fosse perdido, bem como rápida comunicação. A primeira mensagem transmitida com êxito por meio da *ARPAnet* ocorreu em outubro de 1969 entre a Universidade de Los Angeles e o Instituto de Stanford, os quais ficam à uma distância aproximada de 650 (seiscentos e cinquenta) quilômetros (MARCON; DIAS, 2014).

Deste modo, desde o seu surgimento a *Internet* assumiu um caráter inovador para sua utilização, principalmente no campo militar em virtude de sua característica principal de autonomia de um sistema mãe, permitindo que fosse operado independentemente do sistema central. Entretanto, diante da sua potencialidade passou a ser explorado para fins científico e acadêmicos, uma vez que proporciona a troca de informações de maneira rápida e simultânea.

Os anos seguintes foram dedicados ao melhoramento e estabilização do que hoje denomina-se *Internet*, oriunda da ideia central de uma espécie de agremiação mundial de computadores que se interligam por intermédio de um grupo de regras padronizadas que determinam o formato, a sincronização e fiscalizam os erros em comunicação de dados.

A liberação do uso da *Internet* ao público conduziu à privatização. Assim, empresas provedoras de *Internet* destinaram seus esforços para a sua comercialização e, consequentemente, expansão. No início da década de 90 o programador inglês Tim Berners-Lee desenvolveu um sistema chamado Hipertexto de *World Wide Web* (FIORILLO; CONTE, 2016). Logo, não demorou para que a iniciativa privada observasse o potencial da *Internet* para a exploração comercial e passasse a investir, gerando, consequentemente, mais estudo e desenvolvimento da ferramenta.

O crescimento do uso da *Internet* conduziu a necessidade de ampliar a rede em virtude disso foram criados mecanismos que possibilitassem a troca de informações nos mais diversos formatos, textos e mídias, de forma organizada e que fosse acessível ao público. Essa rede é denominada *World Wide Web*, também conhecida como *WWW* ou *Web*, armazena dados e informações em um servidor que podem ser reproduzidos através de hipertextos ou mídias, as quais são lidas por intermédio de um programa de navegação que direciona o usuário a páginas de acesso (POMPÉO; SEEFELDT, 2013).

A *Internet* como hoje conhecemos, que permite o envio de mensagens de texto e arquivos multimídia, pode ser acessada utilizando uma ferramenta denominada navegador. As informações na Web, via de regra, são agrupadas em sites que consistem em páginas organizadas acerca de um determinado tema. O *Internet Explorer*, o *Mozilla Firefox*, o *Google Chrome* são exemplos de *browsers*, ou seja, programas de navegação que permitem o acesso aos *sites*.

Nessa perspectiva, o acesso, por meio desses programas de navegação, se dá pelo URL, abreviação de *Uniform Resource Locator*[3], que funcionam como uma espécie de endereço do *site* e que seguem uma estrutura ordenada formada por domínios (MPF, 2006).

Com efeito, para que este sistema funcione é necessário que os URLs digitados nos navegadores sejam convertidos para um endereço numérico chamado endereço IP. Assim, um endereço eletrônico é composto de três domínios, respectivamente, os chamados nomes de domínio como *Google, Yahoo*, Globo; domínios de nível superior como .gov, .com, .org; e por fim domínios de países como .br, .fr. Cumpre destacar que *sites* de origem estadunidense não possuem domínio de países, uma vez que quando da criação da *Web* os desenvolvedores norte-americanos não julgaram necessária a inserção de nenhuma sigla para o país de origem (MPF, 2006).

O IP, o acrônimo de *Internet Protocol*[4], "é um número que um computador ou equipamento conectado à *Internet* recebe". Nesse ponto, por intermédio do IP agregado a uma hora e data é possível encontrar um usuário da *Internet* em qualquer localidade (SHIMABUKURO, 2017, p. 21).

É necessária a identificação da conexão e fuso horário do sistema, uma vez que somente no período em que o usuário está conectado o IP pertence a ele, sendo

[3] Localizador Padrão de Recursos
[4] Protocolo de Internet

que posteriormente é conferido a outro usuário de forma aleatória (MPF, 2006). Nesse sentido, todos os *sites* passíveis de acesso encontram-se hospedados em um computador ligado à um servidor que é identificado por um endereço numérico de IP.

Desta maneira, o IP é como uma digital temporária capaz de identificar e individualizar o usuário na rede mundial de computadores enquanto este encontra-se *online.* Este aspecto é essencial para a investigação de crime praticado na *Internet* e por esta razão as autoridades policiais assim que são noticiadas acerca da possível prática de um crime no ambiente digital devem diligenciar para conseguir informações sobre o IP ou preservá-las.

É imprescindível que a organização dos endereços ocorra de forma extremamente organizada, a fim de assegurar que um dispositivo conectado à rede seja localizado dentre milhões. Isto significa dizer que cada usuário deve possuir seu endereço de IP na *Internet*, em virtude disso é adotado um sistema hierárquico com a organização denominada *Internet Assigned Numbers Authority*[5], que fica situada nos Estados Unidos, no topo dessa pirâmide:

> [...] de sorte que uma organização localizada nos Estados Unidos, denominada IANA (Internet Assigned Numbers Authority) ou Autoridade para Atribuição de Números da Internet, aparece no nível mais alto desta estrutura. A IANA aloca grandes blocos de endereçamento IP para organizações conhecidas como RIRs (Regional Internet Registries) ou Registros Regionais de Internet , que por sua vez alocam sub-blocos para os NIRs (National Internet Registries) ou Registros Nacionais de Internet , para os LIRs (Local Internet Registries) ou Registros Locais de Internet ou diretamente para grandes operadores de rede e provedores de acesso à Internet (também conhecidos por ISPs - Internet Service Providers). Os ISPs finalmente são os responsáveis pelo fornecimento de IPs para as residências, empresas e outras organizações menores, que no jargão técnico são refereciados como Sítios ou Usuários Finais (MPF, 2016, p. 26-27).

Assim, dentro da complexidade da *Internet* e da quantidade de pessoas que a ela se conectam diariamente imprescindível que sua organização ocorresse de forma extremamente metódica e sistemática, a fim de assegurar que as informações acerca do IP serão localizadas caso sejam necessárias. Destarte, para tanto o sistema de organização e armazenamento das informações foi fracionado.

Importante ressaltar que alguns computadores utilizam classes de endereço reservadas que não estão acessíveis para usuários de *Internet*. Nessa perspectiva, alguns provedores de acesso disponibilizam endereços de IP para uso de redes

[5]Autoridade para Atribuição de Números da Internet

privadas, oportunizada por meio de técnicas de mapeamento de endereços. Assim um IP público pode dar acesso à diversos computadores com IPs privados (MPF, 2006).

Embora esse sistema proporcione mais segurança ao usuário, ajudando na proteção contra invasões, traduz-se em dificuldade de investigação para as autoridades. Isso porque a quebra do sigilo telemático do IP de um único usuário poderia atingir os demais clientes do provedor. Em razão disto, o provedor deve guardar os logs, que consiste no armazenamento dos eventos ocorridos no sistema computacional dos seus usuários, a fim de garantir que seja possível localizar o cliente posteriormente (MPF, 2006).

Assim, visando não atingir a privacidade e intimidade de um número indeterminado de pessoas a autoridade responsável por conduzir investigações criminais e julgar processos que envolvam a necessidade de quebra de dados devem assegurar a individualização do usuário objeto da quebra. Nessa perspectiva, a decisão que autoriza a quebra dos dados telemáticos deve indicar a necessidade da medida para a investigação, bem como indicar de forma determinada ou determinável o suspeito investigado.

Na *Internet* há a tráfego de dados por pequenos fragmentos que saem de um ponto de origem até alcançar seu destino na rede, entretanto, antes de atingi-lo há o encontro desses grupos de dados nos chamados roteadores. Os roteadores, usualmente, "indicam qual o melhor caminho que os dados devem seguir a partir daquele ponto, buscando alcançar o seu destino de forma eficiente" (MPF, 2006, p. 41).

Em virtude de sua proporção algumas organizações requerem um mecanismo de roteamento específico para suas redes internas. Deste modo, conclui-se que a *Internet* possui dois níveis de roteamento, sendo que o primeiro é constituído por roteadores que conectam redes menores que se conectam à *Internet*, porém em razão do caminho estático que propiciam não se adequam a complexidade e dinamicidade do fluxo de dados da rede de computadores mundial (MPF, 2013).

Para a investigação criminal de um crime cibernético a identificação do IP é o passo mais importante, uma vez que conduz à autoria delitiva. Importante destacar que a autoridade investigatória deve tratar a identificação do IP responsável pela prática delitiva como prioridade da investigação, tomando para tanto as cautelas

necessárias, já que as informações relativas aos IPs não permanecem armazenadas por muito tempo.

Assim, a maior parte da prova que interessa a persecução criminal pode ser perdida, tornando a comprovação do delito muito custosa ou impossível. Nesse sentido, a instrução dos profissionais do direito acerca das peculiaridades da investigação criminal no ambiente digital é crucial para a persecução penal e defesa sejam realizadas com êxito.

1.2 A sociedade de informação e a criminalidade

A Sociedade de Informação resultou de um processo de desenvolvimento iniciado na Revolução Industrial que trouxe mudanças tecnológicas que afetaram, em níveis econômico e social, o sistema de produção. Esta transformação teve gênese na Inglaterra no século XVIII e difundiu-se pelo mundo durante o século XX, caracterizando-se principalmente pela substituição da força de trabalho humana pelas máquinas (CRESPO, 2011).

O desenvolvimento não trouxe apenas a informatização da sociedade, mas também formou a Sociedade de Informação que tem como marca a valorização dos bens imateriais, como propriedade intelectual e segredo industrial, de maneira que nos tornamos, como sociedade, mais dependentes da tecnologia (CRESPO, 2011).

A chamada Sociedade de Informação surgiu após a Revolução Industrial e é caracterizada por uma evolução tecnológica tão revolucionária que deu azo a uma nova concepção de vida em sociedade, atingindo diretamente as relações sociais. Nessa linha, houve transformação de conceitos já estabelecidos na sociedade, bem como das relações entre indivíduos (FIORILLO; CONTE, 2016).

Evidente que a tecnologia tem impacto direto na vida dos indivíduos, desde a produção de produtos para consumo como quanto nas relações interpessoais. No mundo moderno nada mais é realizado sem que haja algum tipo de tecnologia envolvida no processo. Esse avanço tecnológico não é percebido no cotidiano pela população, mas se observada a evolução histórica veremos que não conheceríamos a sociedade em seu estado atual se não fosse graças a tecnologia.

É necessário esclarecer que é inviável discutir a Sociedade de Informação dissociada da importância da *Internet* e de seus reflexos jurídicos na sociedade. A partir das tecnologias de informação e comunicação surgiu a indispensabilidade de

nova visão acerca de direitos como informação, liberdade de expressão, comunicação e privacidade. Além disso, foi imposta a necessidade de tutelas jurídicas específicas que abarcassem, por exemplo, a integridade de informações lançada na rede mundial de computadores (FIORILLO; CONTE, 2016).

Assim, a evolução social não pode ser analisada sem também realizar o avanço da *Internet.* Os impactos do seu uso já são percebidos e serão percebidos nas próximas décadas, sendo incabível imaginar a vida em sociedade sem sua presença. Logo, a existência da *Internet* impõe ao direito a necessidade de ajustamento as mudanças dela oriundas.

Na *Internet* todos seriam iguais, anônimos e de aparência irrelevante, sendo, em tese, a sociedade ideal. Nessa perspectiva, enquanto no mundo material seria necessário passar por um detector de metal para ingressar em um espaço governamental na *Internet* basta um *click* (SYDOW, 2015). A ideia basilar da *Internet* parte da concepção de formar uma sociedade diferente da que vivemos, com o rompimento de paradigmas e barreiras, não só sociais, mas também físicas.

Desta maneira, a rede de computadores trouxe a seus usuários a percepção do princípio da igualdade, uma vez que tanto um milionário quanto um assalariado podem acessar o mesmo *site* e obter as mesmas informações. Por óbvio, que há partes exclusivas e que demandam assinatura, porém, ao contrário do que acontece na sociedade material, é acessível a uma pessoa com algum tipo de crédito (SYDOW, 2015). Assim, diferentemente do mundo físico onde o acesso é extremamente limitado, na *Internet* as informações e oportunidades são bem mais acessíveis a todos.

A *Internet* passou a representar dificuldade quando começou a interferir, de forma negativa, nas relações sociais e a ser utilizada para a prática de crimes. Nessa perspectiva, a evolução tecnológica não aproveitou apenas indivíduos interessados em acesso a informações, mas também àqueles voltados à criminalidade que observaram na *Internet* um novo instrumento delitivo.

No Brasil a *Internet* passou a ser utilizada a princípio no ambiente acadêmico, especificamente na Universidade de São Paulo, em 1988 com interligação de universidades. Contudo somente sete anos mais tarde houve a autorização dos Ministérios das Comunicações e da Ciência e Tecnologia para a disseminação comercial da *Internet* (FIORILLO; CONTE, 2016).

O papel do direito sempre foi adaptar-se às mudanças sociais, sob pena de perder sua função social, sendo que a relação com *Internet* não se apresenta como

um fenômeno passageiro, no entanto, ainda pouco explorado. Com o surgimento da *Internet*, em especial do ciberespaço, e a troca instantânea de informações e dados modificou a concepção de território.

Em virtude desse dinamismo, a interação no ciberespaço desconhece fronteiras, sendo que a informação na rede passa a ser elemento identificador de território no espaço digital (FIORILLO; CONTE, 2016). O ambiente digital funciona de forma às vezes bem diversa do ambiente físico já que não há o estabelecimento de territórios e nações.

O termo sociedade de risco foi utilizado por Ulrich Beck que trouxe a ideia de que existe *trade off*[6] em razão da evolução social ao tratar dos acidentes com gases letais ocorridos na revolução industrial. Ao desenvolver as tecnologias o ser humano também é capaz de identificar riscos oriundos desse avanço, bem como assumir posturas para minimizá-los (SYDOW, 2015).

A rede mundial de computadores proporciona ao criminoso percepção de anonimato e à vítima impressão de segurança, pois não visualiza claramente os riscos. Ainda, acrescido a esses fatores, encontra-se a dificuldade do usuário em compreender a importâncias das informações disponibilizadas e produzidas no ambiente digital, montando um ambiente propício para a prática de um crime (SYDOW, 2015).

Nessa perspectiva, a maior parte da população não compreende a magnitude e seriedade das informações que são inseridas na *Internet*. As informações que são fornecidas pelos indivíduos, que nas suas concepções estão inacessíveis, podem ser invadidas por terceiros não autorizados e com as mais diversas intenções. Logo, é importante que o indivíduo ao acessar a *Internet* se conscientize a respeito de seus riscos e da necessidade de cautela para que sua vida privada não esteja à mercê de criminosos.

Importante ressaltar que a ampla liberdade confere ao criminoso o direito de transitar livremente por onde desejar e a igualdade incialmente faz que não seja possível verificar vestígios do crime. Desta forma, o agente criminoso tem sensação de segurança dentro do mundo digital do que na realidade física, pois corre riscos significativamente menores (SYDOW, 2015).

---

[6]permuta

Os criminosos digitais não possuem o estereótipo padrão daqueles da realidade física já que não necessariamente são advindos de classes sociais com renda mais baixa e geralmente não necessitam da prática de crimes como meio de sobrevivência (SYDOW, 2015). Ao contrário do estereótipo formado acerca dos indivíduos que cometem delitos como roubo e furto, o criminoso informático geralmente é pessoa com mais instrução acadêmica e mais recursos financeiros, pois embora a *Internet* hodiernamente seja mais acessível ainda requer um certo grau de dedicação e expertise para que seja utilizada como meio para a prática de crimes.

Os avanços tecnológicos provocaram mudanças progressivas nas terminologias e nos conceitos em diversas áreas, não podendo ser diferente no direito. Nesse sentido, a criminalidade também encontrou novos métodos, já que, por algumas vezes, há lacuna na legislação e em razão da vedação presente na *in malem partem* existem condutas prejudiciais que ainda não se encontram penalmente previstas (CRESPO, 2011).

A tecnologia, como a maioria dos recursos, pode acarretar em aspectos positivos e negativos, porém é patente que toda evolução requer alguma espécie de renúncia a bens do passado e representa mudanças no presente com reflexos no futuro. Assim, cabe ao Direito, como uma ciência essencialmente social, a evolução na medida de evolução da sociedade.

1.3 Conceituação e classificação dos crimes informáticos

O crescimento da *Internet* também conduziu a sua utilização para a prática de delitos, fazendo surgir uma nova classe de crimes denominados, ainda sem precisão terminológica pacífica, como crimes digitais, crimes virtuais, crimes cibernéticos, delito informáticos, dentre outros (SPINIELI, 2018). No entanto, a doutrina majoritária defende a utilização da nomenclatura delitos informáticos.

O ciberespaço caracteriza-se como, dentre outras utilidades, um campo para cometimento de delitos em virtude da sua capacidade de processamento, armazenamento e circulação de informação em formato digital. A estrutura descentralizada da *Internet* proporciona isso, uma vez que impossibilita a atuação de órgão de controle de circulação de informações, sendo impossível supervisionar a quantidade e conteúdo de informações.

Ainda nessa perspectiva, a grande quantidade de potenciais vítimas e criminosos é potencializada em virtude do vasto número de usuários e a frequência de acesso. Outro ponto é que as tecnologias de informação e comunicação podem ter seu conteúdo alterado, por acesso ilegítimo, em razão de suas próprias características físicas, técnicas e lógicas (CRESPO, 2011).

O último aspecto é que pela sua própria estrutura as tecnologias de informação podem potencializar de forma gigantesca a multiplicação de ações ilícitas, como ocorre em crimes contra a honra que quando cometidos, por exemplo, em fóruns na *Internet* ganham maior repercussão e disseminação (CRESPO, 2011).

Segundo Rossini (2004) entende-se por crime virtual o comportamento ilícito e penalmente previsto praticado por meio de utilização de informática:

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

Há crimes digitais tanto quando a conduta for prevista em lei cujo tipo contenha pena cominada e envolva aparelhos tecnológicos, bem como quando a tecnologia seja uma nova forma de cometimento do delito.

A doutrina majoritária divide os crimes digitais em duas categorias: crime digitais próprios ou puros e em impróprios ou impuros. Os crimes digitais próprios ou puros são ações penalmente incriminadas em desfavor dos sistemas informáticos e dados. Assim, o acesso não autorizado e a disseminação de vírus caracterizam-se como crimes digitais (CRESPO, 2011).

Quanto aos crimes impróprios ou mistos podem ser definidos como condutas criminosas que atingem bens jurídicos tradicionalmente já protegidos pela legislação. Caracterizam como crimes digitais impróprios aqueles contra a honra praticados por meio da *Internet*, compartilhamento de pornografia infantil e estelionato (CRESPO, 2011).

Assim, verifica-se que os crimes digitais próprios são aqueles desde sua concepção são cometidos por meios digitais ou envolvendo equipamentos digitais. Por outro lado, os crimes digitais impróprios são aqueles que tutelam outros bens jurídicos que não apenas digitais.

Além disso, para Fiorillo e Conte (2016) os crimes digitais podem ser definidos como os ilícitos perpetrados por intermédio da *Internet* ou com o auxílio desta que causem alguma modalidade de dano à vítima. Ainda, dentro desse amplo conceito estão inseridos os crimes praticados por meio do uso de computadores e as práticas contra os sistemas informáticos e às relações contidas no equipamento.

Os crimes digitais puros caracterizam como aqueles que agridem o sistema informático, seja por meio do programa informático, componentes físicos, dados ou sistemas de armazenamento. Por sua vez, nos crimes mistos as tecnologias de informação constituem uma condição que permite a prática do crime, como, por exemplo, a transferência ilícita de valores de uma *homebanking,* serviço bancário que permite acesso a conta bancário por meio da *Internet* na residência do cliente, ou o *salemislacing,* que consiste na retirada de quantias diminutas de milhares de contas (FIORILLO; CONTE, 2016).

Finalmente, os crimes comuns caracterizam-se como aqueles que estão previstos na legislação brasileira, sendo que a rede mundial de computadores auxilia a execução desses delitos. Nesse sentido, são exemplos: o estelionato (art. 171 do CP), a ameaça (art. 147 do CP), os crimes contra a honra (arts. 138-140 do CP), o homicídio (art. 121 do CP), a veiculação de pornografia infantil (Estatuto da Criança e do Adolescente - ECA - Lei n. 8.069/90), o crime de violação ao direito autoral (art. 184 do CP) (FIORILLO, CONTE, 2016).

Em que pese essas pequenas diferenciações entre doutrinadores é possível visualizar que os crimes informáticos são aqueles que utilizam de alguma forma sistemas informáticos ou telemáticos. Ainda, percebemos que crimes que em sua gênese não eram informáticos evoluíram e se adaptaram a uma nova sociedade, utilizando a tecnologia como instrumento delitivo.

Ainda, Jesus e Milagre (2016) definem que os crimes informáticos próprios são aqueles em que o bem jurídico afetado é a tecnologia de informação em si e crimes informáticos impróprios são aqueles em que a tecnologia é utilizada como meio utilizado para agredir os bens jurídicos já tutelados pela legislação penalista brasileira. Por sua vez, entende crimes informáticos mistos como aqueles em que há a proteção ao bem jurídico informático e a outro bem jurídico, acarretando na existência de dois tipos penais diversos.

No que tange a classificação dos delitos informáticos Sydow (2015) conceitua delitos informáticos impróprios como crimes comuns que são praticados por meio de

tecnologia, sendo que poderia também ser praticado por outra ferramenta. Logo, são delitos de forma livre. Por outro lado, os delitos informáticos próprios são condutas típicas e antijurídicas que buscam alcançar um sistema informático ou seus dados, sendo delitos de forma vinculada.

Assim, percebe-se que existem diversas modalidades de delitos informáticos, impondo ao Estado a necessidade de desenvolver tecnologias aptas a acompanhar as evoluções criminológicas. A sociedade sempre vai evoluir antes da Poder Público, considerando que a sociedade civil é composta pela maior parte da população, entretanto, o Estado não pode quedar-se inerte e deve ao buscar métodos para acompanhar esse desenvolvimento.

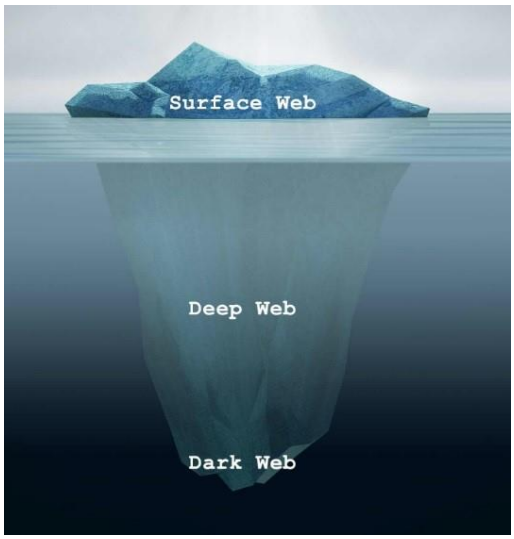
1.4 Distinções entre *Surface Web, Deep Web e Dark Web*

Diferentemente do que acontecia no passado hoje não é mais absoluta a afirmação de que a *Internet* é terra sem lei. Nessa perspectiva, na parte mais conhecida e utilizada pelos usuários a *Internet* possui legislação de regulamentação e métodos de identificação, responsabilização e punição do agente em caso de incidentes, mesmo que mediante desafios impostos pelo sistema tecnológico (ROCHA, 2018).

Ao longo dos anos foi aperfeiçoado aquilo que hoje conhecemos como *Internet.* Nessa perspectiva, na *World Wide Web,* conforme já exposto no item 1.1 deste capítulo, há o armazenamento de dados e informações em um servidor, os quais são apresentados ao leitor em navegador visível por intermédio de provedores de pesquisa. Deste modo, qualquer indivíduo com um computador com acesso à Internet pode acessar as informações de modo fácil por meio de pesquisas no buscador Google.

Por outro lado, a esfera não indexada da *Internet,* ou seja, não mapeado ou de difícil acesso, trata-se de ambiente que exige cuidados redobrados em razão de sua inacessibilidade. Os estudos relacionados a este assunto geralmente fazem uma analogia do uso da *Internet* com a imagem de um *iceberg,* pois nesses blocos de gelo que flutuam na superfície dos oceanos a maior parte de seu conteúdo fica submerso embaixo d’água (POMPÉO; SEEFELDT, 2013).

Imagem 1 – *Iceberg* das divisões da *Internet*



Fonte: *Site* Tecmundo. 2018. Disponível em: <https://www.tecmundo.com.br/internet/131843-historia-deep-web-submundo-da-internet-video.htm>

Cumpre esclarecer que alguns autores como Pompéo e Seefeldt (2013) defendem que a busca dessas informações ocorre em duas categorias: a *Surface Web e* a *Deep Web*, sendo que a primeira representaria uma seção da *Web* de fácil acesso e a segunda parte dela de acesso restrito:

> Enquanto a *Surface Web* é um termo técnico que resume a coletânea de páginas facilmente encontradas por mecanismos de busca, a *Deep Web* resume as páginas que, por algum motivo, ficam alheias a esses provedores, não podendo serem listadas como resultados (2013, p. 439).

A expressão *Deep Web* foi criada em 2001 por Michael K. Bergman, criador do *Bright Planet*[7]*,* programa especializado em acessar dados não estruturados da *Surface Web*, *Deep Web* e até *Dark Web.*

A tradução de *Deep Web*, *Web* Profunda, remete ao sentido profundeza justamente o oposto da *Surface Web* que dirige ao sentido de superficialidade. Nesse sentido, entende-se por *Deep Web sites* intencionalmente não indexados nas ferramentas de busca como *Google, Firefox, Mozilla, Yahoo, Bing*, dentre outros, a fim de garantir a não localização. Deste modo, os referidos *sites* ficam inacessíveis a maior parte dos usuários da *Internet* (POMPÉO; SEEFELDT, 2013).

Com efeito, a *Deep Web* ou *Dark Web* ganhou destaque no cenário mundial nos últimos dez anos, principalmente com os acontecimentos relacionados a assuntos políticos quando informações confidenciais do governo dos Estados Unidos da América acerca de seu sistema de vigilância global foram vazadas por Edward Joseph Snowden.

Ainda acerca da conceituação Pinheiro (2016) adepta da divisão suprarreferida, define que a *Deep Web* é a *Internet* não indexada pelos buscadores convencionais,

[7] Planeta Brilhante

agrupando grande quantidade de dados muitas vezes só localizados por meio do uso de alguma ferramenta específica como o navegador *TOR,* que possui como símbolo uma cebola, fazendo analogia às suas camadas.

Por outro lado, a maioria dos estudiosos do tema, classificam a *Internet* em *Surface Web, Deep Web e Dark Web.* A primeira camada é a superfície e pode ser acessada por qualquer navegador de busca já que seu conteúdo foi previamente indexado, sendo seu acesso possível numa busca no *Google* (ROCHA, 2018).

Nesse cenário é possível afirmar que a *Surface Web* é a camada mais utilizada pela maior parte dos usuários da *Internet* considerando que grande parte de materiais culturais, acadêmicos, profissionais e de entretenimento estão nela contidos. Além disso, por meio da *Surface Web* permite a acessibilidade a maior parte da população que não possuem conhecimento aprofundado sobre equipamentos tecnológicos.

A segunda camada, chamada *Deep Web,* armazena larga quantidade de informação, de caráter legal e ilegal, resultante de pesquisas médicas e científicas e outros conteúdos que são alvo dos grandes buscadores. Nesta camada também se encontra o compartilhamento de resultados de pesquisas e debate de temas relevantes como moedas virtuais (ROCHA, 2018). Assim, esta segunda camada é mais comumente utilizada para compartilhamento e armazenamento de dados com certo grau de confidencialidade, porém na maioria das vezes de cunho lícito.

A terceira camada é considerada a mais sombria e classificada como *Dark Web,* uma vez que é nela em que se concentram a grande variedade de delitos oferecidos, negociados e praticados. Nessa camada é comum encontrar pornografia infantil, negociação para contratação de assassinos de aluguel e vítima de trabalho sexual (ROCHA, 2018).

Para Shimabukuro (2017) a da *Dark Web* ou *Darknet,* que consiste em “uma rede fechada, usada para compartilhar conteúdo de forma anônima”. Nesse sentido, o acesso a *Dark Web* ocorre por intermédio de *softwares* como TOR, o *Freenet* e a rede I2P dentre muitos outros existentes (2017, p. 21).

A *Dark Web* é conhecida por conter majoritariamente conteúdo de cunho ilícito e por ser parte acessada apenas por meio de programas específicos, os quais não são utilizados normalmente pelo usuário médio da *Internet*. Isso porque o acesso a *Dark Web* requer cautela do usuário já que seu computador e consequentemente seus dados estão mais expostos à invasores.

1.5 Acesso a *Dark Web* por intermédio do programa *TOR*

Os indivíduos que já tiveram acesso a *Dark Web* geralmente relatam que a disponibilidade de serviços, conteúdos e materiais ilícitos é imensa e completamente irrestrita. Nesse segmento, a *Silk Road* é um ótimo exemplo dessa afirmação, pois consiste em um mercado que opera na *Dark Web,* por meio da rede TOR, e oferece anonimato aos vendedores e compradores que busquem a negociação de produtos ilícitos, como drogas e armas.

Ainda, há informações de que o grupo denominado Estado Islâmico tem utilizado a *Dark Web* para promover a ampliação do recrutamento de futuros integrantes em todos os continentes e organização de atentados terroristas em diversos países.

Essas plataformas foram responsáveis por grandes movimentos políticos e sociais nos últimos anos, como, por exemplo, como a exposição do sistema de vigilância mundial mantido pelos Estados Unidos. Assim, a *Deep Web* se mostra como importante espaço para conjuntura política, como *Anonymous* e do *Wikeleaks,* ante a liberdade de expressão e privacidade.

Além disso, outro ponto que merece destaque é diversidade e quantidade de conteúdos intelectuais raros disponibilizados de forma gratuita por intermédio da rede TOR. Ainda, a *Dark Web* constitui ferramenta relevante para indivíduos que vivem em países em regime de censura como China e Coreia do Norte, permitindo a troca de informações que não estariam acessíveis pelos meios de comunicação convencionais. Por intermédio do TOR é possível o acesso ao *site* Wikipédia em países que vivem em regimes ditatoriais.

Os fóruns de discussão na *Dark Web* são apontados como ponto de nascimento do movimento chamado Primavera Árabe no qual pessoas residentes em países do oriente médio protestaram acerca das condições sociais e econômicas de suas nações em virtude da ausência de democracia.

A *Deep Web* passou a ser a principal forma de compartilhamento de informação, em razão da dificuldade em rastreamento da origem e usuário responsável pela publicação do material. Além disso, a *Deep Web* reúne cerca de dois terços de todo o conteúdo da *Internet* e para que seja possível acessá-lo foi criada a *Hiden Wiki*, uma espécie de Wikipédia, que foi derrubada, mas já possui outras variações (PINHEIRO, 2016).

Para o iniciante no uso da *Deep Web* é essencial o uso da *The Hidden Wiki,* que é uma espécie de diretório da *Deep Web* que classifica e separa diversos *links* de acordo com algum tema que possa interessar ao usuário. Neste diretório pode-se encontrar livros raros, materiais pornográficos, vídeos de estupros reais, compra e venda de drogas, ferramentas para derrubar outros *sites,* entre outras diversas variedades de conteúdo (ROCHA, 2018).

Nessa perspectiva, o usuário que deseje usar a rede TOR deve ter precauções para que seu dispositivo não seja invadido por outros usuários, bem como conhecer o funcionamento para o acesso às páginas que desejar visitar.

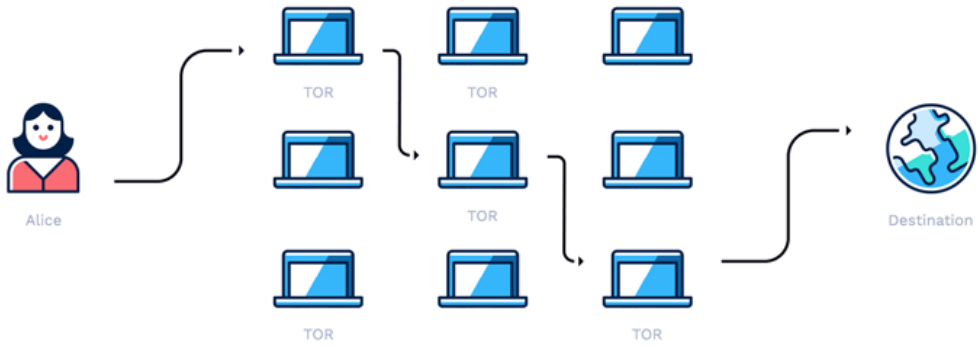
Em virtude do grau de privacidade e proteção que essas redes possuem o conteúdo constante na *Deep Web* é praticamente irremovível. A remoção e identificação do agente que publicou o material é objeto de desafio para as principais autoridades de investigação do mundo como o *Federal Bereau of Investigation* (FBI) e a *Interpol* que cada vez mais se associam a empresas de tecnologia para a investigação desses crimes (ROCHA, 2018).

Nesse ponto, é necessária compreensão acerca do modo de funcionamento da *Dark Web* por meio do *software The Onion Router* (TOR). O programa TOR acrônimo de *The Onion Router*, que pode ser traduzido como Roteamento Cebola, é mantido por uma organização sem fins lucrativos e conta com a ajuda de voluntários ao redor do mundo.

Para a utilização do *software* é necessário que o indivíduo baixe o programa, disponível de forma gratuita na *Internet,* no computador. O programa garante anonimato ao usuário devido ao seu sistema de funcionamento que faz com que o IP utilizado para acessar determinado conteúdo seja camuflado em níveis de criptografia. Essa característica de funcionamento em camadas é apontada como razão do nome do programa, fazendo analogia as camadas de uma cebola.

Nessa perspectiva, diferentemente do que ocorre na *Surface Web,* na *Dark Web* é possível publicar material em algum *site* sem que se releve o IP responsável pela postagem. Em síntese, quando um computador acessa algum *site* e/ou envia uma mensagem utilizando a rede TOR o conteúdo passa por três níveis de criptografia por meio de *relays,* retransmissores*,* também conhecidos como *nodes*, nós, que são computadores mantidos voluntariamente por outras pessoas.

Imagem 2 – Funcionamento do TOR



Fonte: Site Hotspotshield. https://www.hotspotshield.com/pt/resources/tor-vs-vpn/

O sistema funciona de forma com que apenas o usuário remetente e o usuário destinatário tenham acesso ao conteúdo da mensagem, que tem seu caminho ocultado por meio de criptografia e técnicas matemáticas.

Segundo Lotufo (2018):

> Como o próprio nome sugere, *The Onion Router* (TOR) significa o roteamento cebola: o usuário que está enviando a mensagem seleciona um caminho de roteadores da rede e “encripta” a mensagem diversas vezes via *encriptação assimétrica*; e, a cada servidor, o pacote recebido (a cebola) é “desencriptada” como se retirasse uma camada da cebola, abrindo um novo caminho randômico. Isso possibilita que apenas o remetente, o último servidor e o receptor vejam a mensagem original (2018, p. 262-263).

Assim, quando o indivíduo envia uma mensagem ela passa por diversos nós de forma aleatória antes de chegar ao destino final, sendo que o mesmo ocorre no sentido contrário. Deste modo, é assegurado o anonimato da identidade do usuário, pois somente cada nó tem informação acerca do nó anterior. Soma-se isso ao fato de que durante a passagem entre os nós os dados são criptografados, tornando impossível o rastreamento dos IPs de origem e final.

No entanto, como todo sistema o software possui alguns pontos fracos que podem ser utilizados no momento da investigação criminal pelas autoridades, como vulnerabilidade do último nó e o descuido do usuário.

CAPÍTULO 2 - O CRIME DE DISSEMINAÇÃO DE PORNOGRAFIA INFANTIL NA *DARK WEB*

Os aspectos que contornam o comportamento de indivíduos interessados em pornografia envolvendo crianças e adolescentes não são tão delimitados, uma vez que o pedófilo geralmente não é guiado pelas mesmas motivações que o criminoso considerado convencional. Cumpre destacar que embora a pedofilia seja considerada doença por si só não retira do caráter ilícito da conduta do agente.

O pedófilo diagnosticado geralmente age motivado pela vontade de satisfação da lascívia. Nessa perspectiva, a *Internet* nas últimas décadas tem sido corriqueiramente utilizada como ferramenta para a prática de crimes envolvendo a dignidade sexual da criança como a disseminação de pornografia infantil.

No entanto, a busca pelo combate dos crimes envolvendo pornografia infantil não pode ser dissociada dos direitos assegurados constitucionalmente ao suspeito.

Deste modo, mostra-se necessária breve compreensão no que concerne as principais características e comportamentos do pedófilo. Além disso, traçaremos breve panorama acerca da relação da *Internet*, da *Surface Web* até a *Dark Web,* e o crime de compartilhamento de pornografia infantil.

Ainda, será realizada a exposição da legislação pátria que tutela os direitos relativos a dignidade sexual da criança, bem como a criminalização da disseminação de pornografia infantil nos meios telemáticos e informáticos. Por derradeiro, busca-se realizar breve exposição acerca da proteção constitucional aos direitos da privacidade e liberdade de comunicação.

2.1 Considerações sobre o abuso sexual infantil

É inegável, infelizmente, que o abuso sexual contra crianças e adolescentes existe no Brasil, mesmo que de forma velada. Neste ponto, surge dificuldade em registrar a quantidade e dimensão destes abusos, uma vez que grande parte deles não são comunicados aos órgãos oficiais. Diversos são os fatores que ocasionam esse fenômeno como o desinteresse da vítima, descrédito no sistema punitivo, temor da vitimização social e inefetividade do Estado.

Deste modo, assim como acontece com os casos de violência doméstica, onde as vítimas são submetidas a situações semelhantes, as estatísticas acerca de

abusos sexuais envolvendo crianças e adolescentes não retratam de fato a realidade. Assim, devido a forma oculta com que os abusos usualmente são cometidos em várias oportunidades nunca são relevados às autoridades.

Além disso, por diversas vezes os abusos são cometidos dentro da casa da criança e do adolescente e estes sentem receio de contar aos responsáveis. Um cenário ainda mais grave ocorre quando os abusos são cometidos por aqueles que deveriam garantir proteção e o crescimento saudável do menor como pais, tutores e demais familiares.

Ainda, há casos em que a vítima não possui condições de perceber a anormalidade da situação vivenciada (SILVA, 2013). Nesse ponto, devido à pouca idade ou falta de instrução dos responsáveis acerca de abusos sexuais muitas vezes a vítima não percebe a situação a qual foi exposta. Com frequência são noticiados casos de pessoas que foram abusadas sexualmente quando crianças e adolescentes, mas somente anos mais tarde denunciaram os agressores por desconhecimento sobre o abuso sofrido ou medo.

Assim, é essencial que os responsáveis legais e demais indivíduos envolvidos no desenvolvimento da criança e adolescente os instruam sobre as possíveis formas de abusos sexuais, dos níveis considerados mais leves até os mais graves. Ademais, os pais devem sempre estar atentos ao comportamento da criança, que muitas vezes é instruída pelo agressor a não relatar nada aos pais.

O abuso sexual infantil ofende os direitos e garantias fundamentais da criança e do adolescente além de deixar marcas permanentes na vida da vítima, sendo considerado como uma das formas mais graves de violência. Importante destacar que a maior parte dos especialistas classifica o abuso sexual como gênero de duas espécies: violência e exploração. A exploração se dá com a prostituição infantil, turismo sexual, tráfico para fins sexuais e pornografia infantil (SILVA, 2013).

O abuso sexual interessa ao âmbito jurídico, pois além de seus números expressivos trata-se de conduta que tem graves repercussões na vida da vítima nas esferas físicas e psíquicas.

2.2 Os principais aspectos acerca da pedofilia

De início, cumpre destacar que o pedófilo não é necessariamente um criminoso, não possui característica físicas caracterizadoras específicas e pode

possuir bom convívio familiar. Logo, não há como, via de regra, identificar um pedófilo apenas com base em características aparentes, ambiente social, renda, profissão ou idade.

Por outro lado, a Medicina Legal indica que a perversão sexual se mostra mais frequente em homens que possuem graves problemas em sua vida sexual. Na maioria são homens com personalidade com traços de timidez acentuados que não conseguem manter relações com mulheres adultas. Ademais, podem apresentar sentimento ou pensamentos de inferioridade (SILVA, 2013).

Nessa perspectiva, há algum tempo especialistas buscam identificar se o pedófilo é um criminoso em potencial ou doente. Acerca disso, o psicólogo Antônio Pádua Serafim esclarece que conforme a psicologia cerca de 75% (setenta e cinco por cento) dos pedófilos nunca chegam a concretizar suas fantasias, ou seja, praticando crimes. Conforme o referido estudioso é preciso vigilância constante e não há cura para a pedofilia, somente tratamento (SILVA, 2013). Deste modo, o pedófilo apresenta um risco em potencial e deve receber acompanhamento constante.

As pesquisas realizadas acerca do comportamento do pedófilo geralmente não tem apenas um viés criminal, mas multidimensional englobando aspectos éticos, morais, biológicos e religiosos. É uníssono entre os especialistas que o enfoque deve ser a tutela dos direitos da criança e do adolescente que são vítimas dos crimes, tendo seu desenvolvimento psicológico e físicos afetados.

No entanto, é importante dar atenção ao agente, no caso o pedófilo, pois apesar do estigma de monstro criado na sociedade, trata-se de um indivíduo portador de direitos e garantias (SILVA, 2013). Logo, para que um pedófilo tenha a atitude extrema de abusar sexualmente de uma criança o distúrbio mental provavelmente está em um estágio avançado. São comuns relatos de pedófilos que apresentam sentimentos como culpa e vergonha. Inclusive, alguns até mesmo se sentem aliviados quando tem suas condutas criminosas descobertas.

Nessa perspectiva, o pedófilo deve ser responsabilizado pelas condutas criminosas que cometer, porém isso não afasta a necessidade de criação pelo Estado de políticas de tratamento, a fim de minimizar os efeitos e evitar a prática de crimes contra crianças e adolescentes. Deste modo, a partir do abuso sexual surge para o Estado tanto a obrigação de dar apoio para a recuperação física e mental da criança e do adolescente, mas também de contribuir para o tratamento do pedófilo.

Deve ser esclarecido os meios de comunicação erroneamente utilizam os termos pedofilia e pedófilo relacionando-os à crimes sexuais envolvendo crianças. No entanto, não existe crime de pedofilia, mas sim trata-se de um transtorno psíquico qualificado como doença e que recebe tratamento de psiquiatria. Vale ressalta que estes termos não têm origem jurídica, mas sim da medicina, uma vez que a pedofilia compõe os denominados comportamentos sexuais anormais (SILVA, 2013).

Desta forma, a pedofilia é integrante do gênero parafilia que pode ser entendida como “qualquer interesse sexual intenso e persistente que não aquele voltado para a estimulação genital ou para carícias preliminares com parceiros humanos que consentem e apresentam fenótipo normal e maturidade física” (APA, 2014, p. 685).

Por sua vez, segundo a APA (2014) o transtorno pedofílico caracteriza-se quando um indivíduo apresenta:

> Por um período de pelo menos seis meses, fantasias sexualmente excitantes, impulsos sexuais ou comportamentos intensos e recorrentes envolvendo atividade sexual com criança ou crianças pré-púberes (em geral, 13 anos ou menos) (2014, p. 689).

Nesse sentido, a pedofilia consiste no desejo sexual de indivíduo que tem, “no mínimo, 16 anos de idade e é pelo menos cinco anos mais velho que a criança” (APA, 2014, p. 689), envolvendo crianças de até 13 anos.

Ainda, é possível a divisão desse transtorno em subtipos de pessoas que tem atração exclusiva por crianças e as que não. Além disso, é viável a identificação um indivíduo como possuidor desse transtorno desde àqueles que assumem abertamente a atração sexual por crianças, bem como os que negam essa situação embora existam indícios.

Ainda, cumpre esclarecer que a pedofilia pode manifestar-se nas formas hétero ou homossexual e que não é necessária a presença de diversas vítimas para a caracterização da patologia. Assim percebe-se que os referidos conceitos não são inequívocos e estão sujeitos a variações e transformações.

Por derradeiro, cumpre destacar que o Direito Penal não prevê condutas voltadas a um crime de pedofilia, mas sim ações que possam ser praticadas por qualquer indivíduo e não apenas àqueles que apresentam perversão sexual pedófila (SILVA, 2013). O crime de estupro de vulnerável previsto no artigo 217-A do Código Penal que tipifica a prática de ato libidinoso ou de conjunção carnal com menor de 14 anos como crime independentemente da presença ou não do transtorno da pedofilia.

2.3 A relação entre a pornografia infantil e a *Internet*

Nos últimos anos a sociedade vivenciou mudanças comportamentais e organizacionais drásticas em razão do crescimento expansivo do uso de tecnologia, principalmente, da ampliação do acesso à *Internet.* A rede mundial de computadores propiciou rompimento de barreiras físicas e temporais, permitindo o acesso a conteúdo produzido há milhares de anos, bem como interação simultânea com pessoas residentes em outros países (SANTOS, 2018).

Nesse sentido, a *Internet* tornou-se o principal meio para troca de informações e conteúdos entre os indivíduos, uma vez que além de facilitar a comunicação também possui proteção dos dados a depender do mecanismo utilizado. Os desenvolvedores de tecnologias criaram ferramentas de proteção dos dados dos usuários, visando assegurar o direito à privacidade destes.

Por conseguinte, foram criados os aplicativos criptografados e desenvolvidos *softwares* que tem a função de proteger os dados dos usuários de possíveis invasores, chamados antivírus. A preocupação acerca da proteção de informações de cunho pessoal não é apenas dos integrantes da sociedade, mas também do Estado.

Assim, como no mundo físico a *Internet* também exige precauções, no entanto, em razão de não visualizar os riscos tão claramente como no ambiente físico os usuários deixam de agir de forma diligente (SYDOW, 2015). Nesse sentido, alguns pais não monitoram o conteúdo acessado pelas crianças na *Internet,* tampouco instruem as crianças acerca dos perigos que estão expostas no ambiente digital.

Nessa perspectiva, muitos indivíduos utilizam redes sociais para se aproximar de crianças com o intuito de induzi-las a mandar fotos e vídeos de cunho sexual ou pornográfico. Deste modo, é possível dizer que mais importante que apenas vigiar o acesso das crianças à *Internet* é orientá-las sobre esse tipo de abordagem, uma vez que é extremamente difícil controlar totalmente o conteúdo com o qual a criança pode ter contato.

Desta maneira, apesar dos avanços tecnológicos representarem evolução para diversos nichos da sociedade também podem operar como instrumentos para as mais diversas práticas delitivas. Nos últimos tempos, tonaram-se recorrentes notícias acerca de crimes praticados por meios digitais, implicando necessariamente no crescimento da seara do Direito Penal Digital. A maior exposição na mídia acerca da

Deep e Dark Web promoveu sua popularização e voltou a atenção da sociedade e das autoridades para os riscos crescentes delas advindos.

Nos últimos anos casos abusos sexuais de crianças têm sido frequentemente noticiados. No entanto, se por um lado a *Internet* trouxe mais facilidade e amplitude as condutas dos criminosos em razão do anonimato que a *Internet* proporciona, também colaborou no combate à pornografia na *Internet.*

Em 2007 foi deflagrada a primeira operação policial, denominada Operação Carrossel, visando o combate da pornografia infantil no Brasil, que foi realizada simultaneamente em 56 (cinquenta e seis) cidades e contou com ajuda do FBI e da *Interpol*. O ponto mais importante da operação foi a utilização de tecnologia de rastreamento dos IPs dos criminosos (FIORILLO; CONTE, 2016).

Além desses mecanismos de rastreamento, a *Internet* também possibilitou a criação de uma central unificada para denúncias de crimes digitais na rede mundial de computadores. Para tanto foi celebrado um acordo entre a Secretaria Especial de Direitos Humanos, a Polícia Federal e a ONG *SaferNet* que promoveu a criação de uma central com acesso permitido à Polícia Federal para que promova a investigação de eventuais práticas criminosas (FIORILLO; CONTE, 2016).

Segundo Indicadores da Central Nacional de Denúncia de Crimes Cibernéticos do *site* da ONG *SaferNet* em 12 (doze) anos a central de denúncia recebeu e processou 1.552.028 (um milhão quinhentos e cinquenta e dois mil e vinte e oito) denúncias anônimas envolvendo pornografia infantil. Dentre estas denúncias, 126.443 (cento e vinte e seis mil quatrocentas e quarenta e três) páginas (URLs) distintas foram removidas por conter conteúdo inapropriado (SAFERNET, 2018).

Ainda conforme os indicadores, destas denúncias foram identificados 46.969 (quarenta e seis mil novecentos e sessenta e nove) números IPs distintos e distribuídos em 97 (noventa e sete) países em 5 (cinco) continentes.

Assim, mesmo na *Surface Web* é complexo verificar todas as denúncias de conteúdo pornográfico infantil e estabelecer dados estatísticos, mas os órgãos e especialistas que estudam essa temática afirmam que a quantidade de material pornográfico envolvendo crianças é imenso. Ainda, a estimativa do alcance dessas informações torna-se mais dificultosa, pois como acima exposto o material uma vez colocado na rede mundial de computadores pode ser acessado por qualquer indivíduo em qualquer localidade do planeta.

Outro ponto importante que deve ser apontado é a rapidez com que as informações circulam no ambiente digital, podendo um arquivo ser postado, salvo, compartilhado e apagado em questão de alguns minutos. Por outro lado, importante destacar que nos últimos anos os administradores de *sites* famosos, como *Twitter* e *Facebook*, tem tomado cuidado e monitorado o conteúdo que é postado por meio da criação de ferramentas para denúncia de conteúdo inapropriado ou suspeito.

Desta forma, fica visível que se na *Surface Web* é necessário esforço para identificação de casos de pornografia infantil na *Dark Web* a dificuldade é aumentada. Conforme exposto no primeiro capítulo na *Dark Web* a identificação do usuário é extremamente difícil o que torna o ambiente propício para a atuação dos produtores e consumidores de conteúdo pornográfico infantil.

Cumpre destacar que por se tratar de um novo seguimento de pesquisa na maioria das ciências ainda não existem muitos dados estatísticos acerca da quantidade de material pornográfico infantil na *Dark Web* utilizando a ferramenta TOR. No entanto, estudos de observação realizados por Gareth Owen e Jamie Bartlett indicam que a maioria do conteúdo da *Dark Web* é composto por pornografia infantil.

Conforme Bartlett (2014) a maioria dos indivíduos que assistem pornografia infantil iniciam com pornografia que envolvam jovens e adolescentes. Posteriormente, passam a assistir, devido a forma de funcionamento da *Internet* que proporciona conteúdos ilegais com facilidade, pornografia envolvendo crianças cada vez mais jovens.

Ainda, conforme Bartlett (2014) o sistema TOR funciona como um ciclo reciclagem. É extremamente simples suprir a demanda de pornografia infantil na *Dark Web,* sendo possível acessar esse conteúdo numa espécie de *Wikipédia* com a categoria *hard candy*[8] com diversos *links* para páginas de pornografia infantil. Assim, quando os *sites* são derrubados os indivíduos que já baixaram os arquivos e salvaram em seus equipamentos de armazenamento repostam o conteúdo para outros indivíduos.

Nessa perspectiva, o termo *hard candy* é utilizado pelos usuários para se referirem a *sites* de pornografia infantil (PINHEIRO, 2016). Os estudiosos do tema são unânimes em dizer que na *Dark Web* é de fácil localização *sites* referentes a pornografia infantil.

[8] doce difícil

Deste modo, a distribuição do material pornográfico está tão fragmentada que é impossível removê-la completamente da *Internet.* Diante disso, surge um dilema para a polícia acerca de sua atuação no combate ao crime de pornografia infantil na *Internet* considerando os limitados recursos tecnológicos disponíveis e a dificuldade em remover este conteúdo.

2.4 Tutela dos direitos e garantias fundamentais da criança

A infância faz parte do processo de formação física e psíquica do indivíduo, funcionando como uma fase transitória, posto que ninguém nasce completamente desenvolvido, mas sim evolui suas características ao longo dos anos (SILVA, 2013). Logo, a infância é essencial para a construção da pessoa que irá viver em sociedade e por esta razão, dentre outras, merece zelo especial.

Assim, se a criança é tratada de forma amorosa e respeitosa tende a repetir esse comportamento diante da sociedade, porém se a criança é exposta a situação de abuso dentro do próprio lar, como ocorre em grande parte dos casos, podem reproduzir o que foi vivenciado posteriormente (SILVA, 2013). Logo, se a criança sofre situação de abuso sexual para a produção de material pornográfico ou se tem sua imagem exposta de forma abusiva na *Internet* provavelmente repercutirá negativamente no seu processo de formação.

De início, cumpre destacar que a dignidade da pessoa humana se apresenta como um dos princípios basilares dos ordenamentos jurídicos modernos. Com o fim da Segunda Guerra Mundial surgiu a necessidade e tendência de assegurar a todos os indivíduos o nascimento e desenvolvimento saudável, com observâncias de direitos e garantias ditas fundamentais.

Nessa perspectiva, o constituinte da Constituição Federal de 1988 diferentemente de alguns outros princípios que estão implicitamente contidos na carta magna, decidiu por inserir a dignidade da pessoa humana no inciso III, do artigo 1º. Desta maneira, devido ao contexto de regime militar que precedeu o processo constituinte, é manifesta a preocupação do constituinte em garantir segurança jurídica e expressividade a dignidade da pessoa humana. Não suficiente, em seu artigo 24, inciso XV, define a competência concorrente da União, Estados e Distrito Federal para legislar sobre a proteção da criança e adolescente (BRASIL, 1988).

Nesse sentido, visando salvaguardar os direitos da criança o Protocolo Facultativo sobre a Venda de Crianças, Prostituição e Pornografia Infantis, ratificado pelo Brasil em janeiro de 2004, determina que os Estados signatários reprimam a venda de crianças, a prostituição e a pornografia infantil. Este mesmo protocolo estabelece em seu artigo 3º que as referidas condutas sejam criminalizadas (PIOVESAN, 2012).

Por conseguinte, a Convenção das Crianças sobre Direito das Crianças, ratificada em 24 de setembro de 1990 e com entrada em vigor no ordenamento jurídico brasileiro em 23 de outubro de 1990, impõe em seu artigo 34 que os Estados tomem providências visando proteger as crianças de material pornográfico (BRASIL, 1990).

Ainda, em âmbito internacional a Convenção de Budapeste sobre Cibercrime estabelece que os membros partes deverão tomar atitudes para promover a redução de pornografia infantil na *Internet,* bem como indica em seu artigo 9º as condutas que devem ser criminalizadas. Ademais, aponta que menor é todo indivíduo menor de 18 (dezoito) anos de idade (FIORILLO, CONTE, 2016). Cumpre destacar que embora o Brasil não seja signatário da referida convenção há pressão de órgãos nacionais e juristas para a adesão do Estado brasileiro à Convenção, porém sem grandes avanços.

Com efeito, visando a melhor proteção dos direitos da criança e adolescente foi criada a Lei nº 8.069/1990 também conhecida como Estatuto da Criança e do Adolescente (ECA) que contém as mais diversas disposições concernentes à criança e ao adolescente. Nessa perspectiva, o ECA é conhecido pelo seu paradigma de proteção integral da criança e do adolescente que visa priorizar o bem-estar e os direitos dos menores que se encontram em fase de desenvolvimento.

Neste ponto, é essencial esclarecer que o artigo 2º do ECA estabelece que “considera-se criança, para efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade” (BRASIL, 1990). Importante a referida diferenciação visto que são fases de desenvolvimento distintas e que possuem características peculiares, devendo, portanto, ser tratadas de maneira diversa.

O artigo 18 do referido estatuto define que se constitui ônus de toda a sociedade zelar pela dignidade da criança e do adolescente, resguardando-os de tratamento “desumano, violento, aterrorizante, vexatório ou constrangedor” (BRASIL, 1990). Nessa conjuntura, chama a atenção que o legislador não deixou a encargo apenas

dos pais e familiares o dever de proteger a criança, mas também incumbiu essa função a sociedade como um conjunto.

Além disso, o artigo 15 do ECA estabelece o direito da criança ao respeito, liberdade e dignidade estabelecendo que “a criança e o adolescente têm direito à liberdade, ao respeito e à dignidade como pessoas humanas em processo de desenvolvimento e como sujeitos de direitos civis, humanos e sociais garantidos na Constituição e nas leis” (BRASIL, 1990).

Desse modo, conforme leciona Ishida (2014) o princípio da dignidade da pessoa humana e os direitos à vida e liberdade contidos na Constituição Federal foram adotados pelo legislador na criação do ECA. Nesse cenário, a intenção do referido artigo é sensibilizar a sociedade acerca da proteção da criança e do adolescente como um dever social.

Deste modo, o legislador buscou garantir proteção integral à criança, tutelando seus direitos em todos os campos e garantindo direito à crescimento digno. Além disso, restou previsto no ECA que é dever da sociedade como um todo o zelo com a criança.

2.5 Criminalização no ordenamento jurídico brasileiro de disseminação de pornografia infantil

Com base nas disposições jurídicas referentes à criança e ao adolescente, a Lei nº 11.829/2008 promoveu alteração nos artigos 240 e 241 do ECA com o intuito de aperfeiçoar o enfrentamento da produção, venda e distribuição de pornografia infantil. Ainda, criminalizou-se a compra e posse de pornografia infantil. Além disso, a alteração visou criminalizar as condutas realizadas na *Internet* (arts. 241-A, 241-B, 241-C e 241-D).

Cumpre salientar ainda que houve a definição da expressão “sexo explícito ou pornográfico’’ no artigo 241-E. As alterações trazidas entraram em vigor na data de sua publicação em 26 de novembro de 2008. Ainda, verifica-se que possuem como ponto comum a tutela cumulativa ou individual dos bens jurídicos da integridade física, psíquica ou moral da criança e do adolescente (ISHIDA, 2014).

A pornografia infantil não é somente imagens reais que contenham crianças e adolescentes, mas também imagens que aparentem envolver menor em cenas de sexo explícito (ROSSINI, 2004).

A referida alteração legislativa buscou tutelar a dignidade, integridade física, psíquica e moral da criança e do adolescente, bem com a honra e a dignidade sexual. Assim, percebe-se que o direito à livre expressão intelectual e artística, consagrado pela Constituição Federal, não é absoluto diante das garantias da criança também asseguradas pela Constituição em seu artigo 227 (AMIN; MACIEL, 2018). Logo, embora a Constituição Federal assegure o direito à liberdade criativa este não pode ser sobreposto sobre o direito da criança ao desenvolvimento físico e mental saudáveis.

Cumpre destacar que por cena pornográfica entende-se qualquer uma de caráter libidinoso que tenha como objetivo satisfazer a lascívia ainda que não envolva a conjunção carnal em si. Por outro lado, cenas em que haja a exposição de crianças a situação vexatória estão excluídas tendo em vista que tuteladas pelo artigo 232 do ECA (AMIN; MACIEL, 2018).

Embora os tipos penais sejam bem amplos e diversos, com o intuito de pesquisa será abordado no presente estudo o crime previsto no artigo 241-A do ECA que é comumente praticado na *Dark Web* em virtude do compartilhamento gratuito e constante de material pornográfico entre os usuários.

No tocante ao crime previsto artigo 241-A do ECA verifica-se que criminaliza a conduta daqueles que difundem o material pornográfico:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> § 1o Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; (Incluído pela Lei nº 11.829, de 2008)
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
> § 2o As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008) (BRASIL, 1990).

O tipo penal é misto alternativo e está representado pelas ações de oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar as cenas de sexo explícito ou de cunho sexual envolvendo criança ou adolescente. Deste modo, não é

necessário que o agente pratique todas as condutas previstas no *caput*, pois caso o agente cometa apenas uma das referidas ações incidirá na prática do delito.

Na figura equiparada prevista §1º prevê como crime ainda a ação de assegurar o armazenamento ou acesso ao conteúdo pornográfico. Devido a equiparação das condutas do referido parágrafo com o *caput* o agente está sujeito as mesmas penas que podem variar de 3 a 6 anos. No inciso I incrimina-se aquele que assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens pornográficas, como os sócios das empresas que hospedam *sites* na *Internet* onde esteja sendo disponibilizado este tipo de material. Por derradeiro, o inciso II visa punir àqueles que possibilitem o acesso a este tipo de conteúdo como por exemplo os provedores de *Internet* (AMIN; MACIEL, 2018).

Importante destacar que, ao contrário do que acontece com o delito previsto no artigo 241, o crime pode ser praticado por qualquer meio, incluindo sistema de informática ou telemático. Além disso, essencial a presença do dolo, direto ou eventual. Ainda, caracteriza-se como crime formal, ou seja, consuma-se com a prática da conduta independentemente da ocorrência de dano (FULLER; DEZEM; NUNES JÚNIOR, 2013).

Deste modo, percebe-se que o agente incidirá na prática delitiva mesmo não haja dano à vítima, sendo suficiente a conduta de propagar o material pornográfico infantil, em virtude de classificar-se como crime formal. Além disso, indiferente o meio informático ou telemático pelo qual é praticada a conduta ilícita.

O Supremo Tribunal Federal já assentou o entendimento de que compete a Justiça Federal processar e julgar o crime tipificado no artigo 241 do ECA, mesmo que as imagens tenham sido inseridas em um *site* brasileiro e não tenham sido acessadas necessariamente no exterior, pois o simples fato de inserir na *Internet* é suficiente para atrair a competência (FIORILLO, CONTE, 2016). Isso porque o fato de que as imagens estejam inseridas na rede mundial de computadores possibilita o acesso por indivíduo de qualquer país o que demonstra a transnacionalidade do delito.

No tocante a competência territorial, o crime deve ser processado no local onde foi postado o compartilhamento do conteúdo de cunho pornográfico nos termos do artigo 70, *caput*, do Código de Processo Penal. Nesta perspectiva, é irrelevante a localização do provedor de acesso ou do local onde as imagens estavam armazenadas (FULLER; DEZEM; NUNES JÚNIOR, 2013).

Por derradeiro, a competência territorial também é definida em razão do local da postagem do conteúdo ilícito não importando o local do provedor de *Internet*. Isso porque é no referido local em que há a consumação do crime, uma vez que como já mencionado, trata-se de delito formal.

2.6 Proteção dos direitos fundamentais da liberdade, honra, vida privada

De início, cumpre esclarecer que a Constituição Federal tutela de forma intergeracional o meio ambiente, garantindo, assim, às pessoas também a dignidade humana, que é um dos pilares do Estado Democrático de Direito, uma vez que esta encontra-se ligada ao ambiente. Nesse sentido, a Constituição Federal funciona como base para a criação de normas infraconstitucionais (FIORILLO; CONTE, 2016).

Assim, o ordenamento jurídico brasileiro se funda nos direitos fundamentais, dentre eles, a dignidade da pessoa humana. Um dos papéis da Constituição Federal é traçar parâmetros para a criação das leis infraconstitucionais que irão regular as relações humanas. Importante destacar que na seara do direito penal é preciso atenção para que os direitos e garantias fundamentais sejam respeitadas, principalmente, diante da evolução dos meios criminosos.

É crescente o clamor social por punições mais severas e redução dos direitos fundamentais dos criminosos, pois são vistos como privilégios e até mesmo incentivadores de práticas criminosas. No entanto, é essencial recordar que o Direito Penal e Processual Penal não tem a função de revanchismo, tampouco a repressão a criminalidade pode vir a qualquer custo. Deste modo, justificar a violação de garantias fundamentais em troca de sensação de segurança constitui retrocesso social e jurídico, sendo que seus efeitos repercutem a curto e longo prazo.

O direito penal ambiental possui características próprias como o caráter preventivo, conduzindo a criação de tipos penais de perigo concreto, mas principalmente, abstrato, de mera conduta e tipos penais em branco (FIORILLO, CONTE, 2016). Diante disso, a asseguração dos direitos fundamentais é essencial em especial diante das peculiaridades existentes no meio ambiente digital.

A criminalidade e suas respectivas mudanças ocorrem ao redor do mundo de forma semelhante, porém no ambiente digital amplia a facilidade e extensão dos efeitos, uma vez que podem repercutir em qualquer localidade do mundo. Nesse

ponto, é essencial que para a evolução do direito penal e da investigação criminal os países promovam integração e assistência mútua.

Nessa perspectiva, as práticas delitivas desconhecessem divisões geográficas e cada vez mais a criminalidade tem se tornado globalizada. Assim, os crimes transnacionais ganham destaque, sendo que dentre eles está o compartilhamento de pornografia infantil por meio da *Internet.* A forma fluída e livre como a *Internet* funciona impõe o desenvolvimento de mecanismos eficazes de combate à criminalidade nela ocorrida.

Na era da informação há discussão acerca do direito à liberdade de expressão *versus* o direito à privacidade, intimidade ou honra, por exemplo, em casos em que *sites* coletam informações dos usuários sem autorização expressa e fornecem a outros desautorizados como ocorreu durante a eleição do presidente norte-americano Donald Trump.

A Constituição Federal tutela em seu artigo 5° os referidos direitos nos incisos IV, IX, X, XII, XIV, estabelecendo ampla proteção a indivíduo no que tange a sua liberdade de comunicação e expressão, mas também traçando limites para o exercício desse direito:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
> (...)
> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> (...)
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)
> (...)
> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional (BRASIL, 1988)

Deste modo, é assegurado o direito à liberdade artística e de expressão, à privacidade e inviolabilidade, mas também são impostas limitações a esses direitos, bem como hipóteses de interferência estatal. Nesse cenário, é possível a colisão de

direitos fundamentais, que é ainda mais frequente no ambiente digital em virtude da dinamicidade e autonomia que os usuários experimentam a ferramenta.

Assim, as colisões entre direitos fundamentais podem ser resolvidas por meio de conciliação ou pela avaliação de peso de importância, hipótese em que somente um dos direitos irá preponderar (FIORILLO, CONTE, 2016). Em casos em que há a colisão entre a liberdade do indivíduo em compartilhar e armazenar arquivos de mídia e a intimidade e a honra da criança e adolescente há a primazia pela integridade física e mental da criança e seu desenvolvimento regular.

CAPÍTULO 3 - ESTUDO DE CASO

Este capítulo visa analisar decisão judicial proferida pela 11ª Turma do Tribunal Regional Federal da 3ª Região referente ao crime de disseminação de pornografia infantil na *Dark Web*. A decisão judicial selecionada refere-se a caso concreto investigado a partir da operação *DarkNet* deflagrada pela Polícia Federal do Rio Grande do Sul em 2016. Na presente análise serão analisados os aspectos formais e legais referentes ao caso.

Deste modo, a avaliação terá como finalidade verificar os métodos investigativos utilizados como mecanismos de busca e infiltração de agentes, bem como a legalidade das provas produzidas. Além disso, será realizado breve demonstrativo acerca da produção de provas no ambiente digital.

Com esta análise busca-se traçar um panorama da resposta jurisdicional do Tribunal Regional Federal que possui jurisdição no estado de Mato Grosso do Sul frente a contemporaneidade dessa prática delitiva no ambiente digital da *Dark Web*.

3.1 Análise do julgamento do Recurso em Sentido Estrito 0013241-15.2014.4.03.6181/SP

O Ministério Público Federal interpôs recurso em sentido estrito registrado sob o n. 0013241-15.2014.4.03.6181/SP em razão de decisão prolatado pela 8ª Vara Federal de São Paulo/SP, buscando a reforma da referida decisão que rejeitou a denúncia oferecida em desfavor de P.R.S.M pelo cometimento dos crimes previstos no artigo 241-A e 241-B do ECA.

O juízo *a quo* julgou que não havia justa causa para o recebimento da denúncia e início da ação penal, uma vez que a peça acusatória estava embasada em provas ilícitas e que os crimes apurados pela Operação *Darknet* constituíram crime impossível.

Por sua vez, o Ministério Público Federal sustentou que não houve flagrante preparado, pois a infiltração de agentes já estava autorizada judicialmente, bem como as técnicas de identificação de usuários. Além disso, argumentou que não era cabível a tese de crime impossível, tendo em vista que houve a consumação dos crimes de disseminação e armazenamento de pornografia infantil.

Após os atos processuais devidos, sendo a decisão recorrida mantida pelo juízo de origem, o Tribunal Regional da Terceira Região reformou a referida decisão a fim de receber a denúncia oferecida em desfavor do recorrido e dar prosseguimento ao feito, considerando lícita a prova produzida nos autos.

Nesse ponto importante realizar uma ressalva de que um dos maiores desafios da investigação criminal no ambiente digital é a colheita de provas suficientes de materialidade e autoria (justa causa) para o oferecimento de denúncia. Nesse seguimento, as dificuldades são encontradas na identificação e localização do provável autor, uma vez que conhecer apenas o IP responsável pela conduta criminosa não significa necessariamente identificar o sujeito que cometeu a conduta. Além disso, é necessário observar a legalidade da prova produzida (FIORILLO; CONTE, 2016).

Nesse sentido, os obstáculos encontrados na investigação criminal, e eventualmente durante a ação penal, de crimes informáticos exigem que a autoridade responsável tome precauções para preservação das provas, tendo em vista que no ambiente digital podem ser corrompidas, destruídas e apagadas com maior facilidade. Ademais, é fundamental que sejam respeitados os direitos fundamentais do investigado, como privacidade e inviolabilidade, a fim de que a prova não seja maculada por vício de ilegalidade.

Segundo já mencionado por diversas vezes a prática de crime digital envolve mais de um país, tornando, eventualmente, difícil de precisar onde as provas deverão ser colhidas e envolvendo mais de um regramento jurídico. Com a criação da Lei nº 12.965/2014 também conhecido como Marco Civil da *Internet* foram estabelecidos direitos, diretrizes, princípios e deveres para o uso da *Internet* no Brasil. A gênese dessa legislação também fixa orientações para a atuação do Estado em questões relativas ao tema.

Conforme já destacado existem diversas dificuldades na investigação criminal no âmbito digital, pois além da facilidade na alteração e ocultação do domicílio digital também exige cooperação e compartilhamento de informações. Nesse sentido, o artigo 13 do Marco Civil da *Internet* define que o administrador de sistema deve guardar, observando o sigilo, os registros de conexão pelo prazo de um ano. Ainda, o § 2º do referido artigo garante a faculdade a autoridade policial ou administrativa ou o Ministério Público de requerer a manutenção dessas informações por tempo superior a um ano (BRASIL, 2014).

Embora o Marco Civil da *Internet* tenha representado um avanço na seara do Direito Digital no Brasil ainda não é suficiente para regular a atividade na *Internet,* principalmente no campo penal, existindo diversas lacunas. Além disso, o Brasil não é signatário da Convenção de Budapeste que é única que aborda a temática dos delitos cometidos por meio digital, porém esta é usada como diretriz para investigações nacionais.

Nessa perspectiva, em que pese o relativo atraso do Estado na resposta aos crimes digitais, nos últimos anos houve avanço no tocante a esta matéria e foram desenvolvidos métodos de investigações mais eficazes diante da complexidade do ambiente digital e da atuação dos criminosos. Assim, os agentes infiltrados ganharam atuação de destaque, em especial na investigação na *Dark Web*.

Conforme destacado pelo Relator Nino Toldo em seu voto no presente caso o recorrido foi rastreado a partir da denominada Operação DarkNet. A referida operação foi a primeira operação no Brasil com o objetivo de investigar crimes de pornografia infantil na *Dark Web*, acessada por meio da rede TOR. A investigação foi iniciada em 2013 e teve duas fases que foram deflagradas em 15 de outubro de 2014 e 22 de novembro de 2016.

A investigação foi conduzida pela Polícia Federal, sendo desenvolvida com auxílio de um mecanismo de busca e identificação de conteúdos de interesse. Além disso, a investigação contou com a participação do Ministério Público Federal que tinha como objetivo acompanhar a licitude das provas, bem como resolver questões incidentais que surgissem ao longo do processo investigatório (MPF, 2017).

Em outro momento da investigação foi requerida a quebra dos dados cadastrais dos usuários, visando identificação da autoria e local da prática do crime para a fixação da competência territorial. As autoridades envolvidas decidiram que o declínio de competência somente ocorreria após a identificação desses elementos (MPF, 2017).

Diante do pioneirismo desse tipo de operação no Brasil foi essencial a assistência e orientação de especialistas na *Deep Web* que instruíram as autoridades policiais e membros do Ministério Público acerca das peculiaridades da rede TOR e as medidas que deveriam ser tomadas para a colheita de provas.

Deste modo, assim como no presente caso, a operação teve desdobramentos em diversos estados da federação. Ademais, durante a investigação foram identificados autores delitivos com IPs cadastrados em outros países, sendo encaminhadas informações para a Interpol (MPF, 2017).

Além disso, na fundamentação do voto, foi destacado que a *Dark Web*, no acórdão tratada como *Deep Web,* apresenta dificuldade para a investigação criminal, ante a complexidade para a identificação dos autores. Destacando ainda que o *TOR* possui espécies de túneis pelos quais a informação é percorrida anonimamente, com a modificação do número de IP da origem até o destino final. Ademais esse mecanismo consegue se ocultar de *plug-ins* como *Flash, Real Player* e *Quick Time*, que são capazes de identificar IPs (TRF3, 2018).

Nesse sentido, houve autorização judicial da 11ª Vara Federal de Porto Alegre no estado do Rio Grande do Sul para a infiltração dos agentes da Polícia Federal, com fulcro nos artigos 1º, § 2º, I, e 10 da Lei nº 12.850/2013, na *Dark Web* com o intuito identificação de indivíduos que estivessem praticando crimes envolvendo pornografia infantil com o auxílio de ferramentas desenvolvidas pela inteligência policial.

Nesse cenário, vê-se que o agente infiltrado tem sua origem apontada desde os tempos de Luís XIV em virtude da figura do delator indivíduo que em troca de vantagens fornecidas pelo príncipe descobria seus inimigos políticos (CAMILO, 2012). Logo, o agente infiltrado sempre teve a função de encontrar informações se passando por indivíduo característico do ambiente em que está inserido.

É possível encontrar a figura do agente infiltrado em diversos ordenamentos jurídicos, mas sua atuação sempre depende de autorização judicial prévia. Nesse sentido, a Convenção das Nações Unidas sobre Crime Organizado Transnacional, ratificada pelo Brasil em 12 de março de 2004, prevê em seu artigo 20 que se os princípios fundamentais do ordenamento jurídico autorizarem o Estado poderá adotar medidas para permitir técnicas especiais de investigação criminal como operações de infiltração de agentes (BRASIL, 2004).

Conforme Neisten (2006) o agente infiltrado, integrante da polícia, insere-se no ambiente criminoso, a fim de conseguir acesso a informações para obter elementos probatórios acerca da prática de um crime:

> o agente infiltrado é o membro da polícia, que autorizado por um Juiz, oculta sua identidade e se insere, de forma estável, em determinada organização criminosa, na qual ganha confiança de seus membros, por ser aparentado a eles, tendo acesso a informações sigilosas, com a finalidade de comprovar o eventual cometimento do delito, assegurar fontes de prova e identificar seus autores (2006, p. 44).

Deste modo, pode-se entender como a agente infiltrado o membro da força policial que é inserido dentro de uma organização criminosa, a fim de que atue como

um membro dessa organização com o intuito de colher provas para amparar a persecução penal.

No Brasil o modelo persecutório penal é a investigação policial realizada de forma preliminar pela polícia judiciária. A Constituição Federal de 1988 passou a limitar a atuação discricionária da autoridade policial, porém ainda contava com liberdade absoluta na investigação, tendo apenas o dever de observar os prazos processuais penais. Por outro lado, com o advento da Lei nº 8.625/93 e Lei Complementar Federal nº 75/1993 a investigação criminal passou a ser submetida a fiscalização direta do Ministério Público (SOUZA, 2012).

O instituto do agente infiltrado foi inserido na legislação pátria por intermédio da Lei nº 9.034/1995 com a alteração promovida pela Lei nº 10.217/2001. Atualmente, a figura do agente infiltrado na investigação de crimes organizados tem previsão legal na Lei nº 12.850/2013 em seu artigo 3º, inciso VII que autoriza, qualquer fase da persecução penal, como meio de obtenção de prova a “infiltração, por policiais, em atividade de investigação, na forma do art. 11” (BRASIL, 2013).

Conforme já destacado a *Dark Web* propicia, em razão de seu anonimato, ambiente geográfico e custo/benefício rentável já que a informação se propaga de forma rápida a custo baixo, ferramenta eficaz para a prática do delito de compartilhamento de pornografia infantil. Logo, a atuação do agente infiltrado virtual passa a ser método importante para a repressão dessa espécie de delito (BUFFON, 2018).

Nesse cenário, verifica-se a razão pela adesão do uso da *Dark Web* por pessoas com intenção criminosa, uma vez que além de proporcionar a rápida e fácil disseminação do conteúdo ainda dificulta a localização do agente da conduta, bem como do receptor do material.

No início a infiltração de agente em nosso ordenamento jurídico somente era permitida em casos de associações criminosas, associações criminosas para o tráfico de drogas, roubo e quadrilha. No entanto, com a promulgação da Lei nº 12.850/2013 foi autorizada, no § 2º, a sua aplicação em casos envolvendo pornografia infantil (BRASIL, 2013).

Essa previsão legal foi essencial para a utilização do instituto, pois embora algumas vezes o acesso desse material esteja organizado em fóruns compostos por diversos indivíduos não necessariamente estes compõem uma organização criminosa.

Nesse sentido, é importante que o sigilo da investigação criminal, principalmente, acerca da infiltração do agente seja resguardado, tanto para garantir o êxito da investigação quanto para proteger a integridade física e privacidade do agente infiltrado. Isso porque estando inserido no ambiente criminoso o agente está exposto a diversos riscos em especial se os integrantes descobrirem sua verdadeira identidade.

A Lei nº 13.441/2017, alterou o ECA para acrescentar capítulo regulamentando a infiltração de agentes para investigação de crimes envolvendo a dignidade sexual da criança e adolescente, ou seja, aqueles previstos nos artigos 240, 241, 241-A, 241-B, 241-C e 241-D do ECA e nos artigos 154-A, 217-A, 218, 218-A e 218-B Código Penal (BRASIL, 2017).

A infiltração judicial somente será realizada diante de autorização judicial fundamentada, estabelecendo-se limites para a infiltração. Além disso, o inciso II do artigo 190-A definiu que o requerimento que pode ser feito pelo Ministério Público ou autoridade policial, "conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas" (BRASIL, 2017).

Cumpre ressaltar que a autorização de infiltração policial deve ser proferida por juiz aparentemente competente para processar e julgar os crimes investigados. Outro requisito para a infiltração de agentes é a existência de indícios de materialidade. Ainda, como último requisito está a concordância do agente que será infiltrado, sendo que é um direito do agente recusar ou fazer cessar a prática da infiltração.

Ainda, foi estabelecido como prazo para a infiltração 90 (noventa) dias passíveis de prorrogação, não podendo exceder 720 (setecentos e vinte) dias em sua totalidade e desde que demonstrada a necessidade da continuidade da investigação. Além disso, confirmando a corrente de excepcionalidade, o § 3º do artigo 190-A estabelece que a infiltração não será autorizada se houver outros meios probatórios (BRASIL, 2017).

A utilização da infiltração de agentes tem como objetivo a obtenção de provas criminais que dificilmente poderiam ser produzidas de outra maneira. No entanto, cumpre destacar que o agente infiltrado enquanto inserido no ambiente criminoso, em virtude do papel desempenhado, pode ser compelido a prática de delitos.

Em virtude dessa possibilidade, o artigo 190-C estabelece que não cometerá crime o agente que se oculta para a investigação dos referidos crimes, mas o parágrafo único do referido artigo prevê a responsabilização do agente pelos excessos cometidos (BRASIL, 2017).

Um dos métodos de investigação do crime de pornografia infantil no ambiente digital é a chamada ciberpatrulha, em que o agente busca indicativos dessa prática delitiva em ambientes digitais públicos. A busca pode ser dar pelo próprio agente ou como o auxílio de sistemas eletrônicos.

Conforme destaca Buffon (2018) o sucesso da investigação pode depender da busca e análise integrada de informações na rede TOR e na *Surface Web:*

> Para o êxito de uma investigação, na maioria das vezes, é necessário o uso concomitante dos dois ambientes a fim de obter a autoria e materialidade dos delitos. O cruzamento de informações entre redes abertas e fechadas, inclusive com informações obtidas na rede TOR, pode ser decisivo no esclarecimento dos delitos que ocorrem no mundo virtual. Portanto, é possível ser necessária a devida decisão judicial para o uso do meio da infiltração policial propriamente dita, após a descoberta, em ação de ciberpatrulha, de indícios de materialidade e autoria, que necessitem de acessos em redes fechadas, para esclarecimento e alcance dos fatos e delimitação dos responsáveis pela atividade ilícita (BUFFON, 2018, p. 81).

Deste modo, a atuação investigatória do agente deverá ser balizada na autorização judicial. Nesse sentido, foi o entendimento da turma do TRF3 que destacou que a infiltração dos agentes era necessária para identificar os agentes que navegavam sob o véu do anonimato e criptografia compartilhando material pornográfico infantil em nível da *Internet* não atingido anteriormente pelo Poder Judiciário.

Ainda, restou demonstrada a maneira em que se procedeu a ação investigatória, pois foi autorizada pelo magistrado da 11ª Vara Federal de Porto Alegre a criação de página na *Dark Web* planejada para permitir que o programa desenvolvido pela Polícia Federal realizasse o rastreamento de usuários. Posteriormente, após autorização, foram introduzidos agentes da Polícia Federal na *Dark Web*, sendo observado que no ambiente estavam sendo praticadas condutas ilícitas envolvendo a dignidade sexual e imagem de crianças e adolescentes.

O tribunal entendeu que as provas produzidas eram lícitas e ao contrário do alegado pelo recorrido não houve a indução dos agentes para a prática criminosa, uma vez que restou comprovado que o réu constantemente compartilhava arquivos de pornografia infantil. Nessa perspectiva, destacou-se que se tratou do chamado

flagrante esperado, que é lícito no ordenamento jurídico brasileiro, e não de flagrante preparado.

Acerca da ilicitude de prova em razão de flagrante preparado é imprescindível realizar a distinção entre agente infiltrado e agente provocador. Conforme Buffon (2018) “o primeiro está albergado pela lei e com os limites bem determinados pela decisão judicial, enquanto que as ações decorrentes do agente provocador tornarão a prova inválida” (2018, p. 88).

O agente infiltrado tem o objetivo de coletar informações para a investigação acerca da autoria e materialidade, adotando atitude passiva e com a confiança do investigado. Deste modo, em razão de sua atitude passiva, o agente infiltrado não tem como objetivo levar o investigado ao cometimento da prática delitiva, sendo possível que o agente cometa alguma prática delitiva, nos limites estabelecidos na decisão judicial, para a colheita de provas.

Por sua vez, o agente provocador instiga e induz o investigado ao cometimento do delito, agindo de forma ativa e sendo essencial para a execução do crime. Nesse sentido, diferentemente do agente infiltrado as ações do agente provocador têm interferência na consumação do delito:

Nesse sentido, leciona Buffon (2018):

> As ações do agente provocador terão como consequência a impossibilidade da consumação do delito, exatamente o oposto do resultado obtido pelo agente infiltrado, o qual não interfere na prática do crime. Para haver a nulidade dessa prova, também, há a necessidade, concomitantemente, de o agente provocador ter tomado todas as providências necessárias capazes de tornar impossível o crime (2018, p. 89).

Deste modo, não restou caracterizado flagrante preparado, mas sim flagrante esperado, que é legítimo. Ainda, na referida investigação foi apenas realizada a vigilância e a criação de página dentro do sistema com conteúdo pornográfico infantil aguardando-se que houvesse a prática do crime de difusão de pornografia infantil.

Nesse sentido, importante visualizar a ementa de julgamento do recurso:

> RECURSO EM SENTIDO ESTRITO. PORNOGRAFIA INFANTIL. ART. 241-A e 241-B DA LEI 8069/90. RECEBIMENTO DA DENÚNCIA. OPERAÇÃO DARKNET.
> 1. O acusado foi rastreado em decorrência da denominada "Operação DARKNET", deflagrada para investigar a produção e circulação de imagens e vídeos pornográficos envolvendo crianças e adolescentes na deep web, também conhecida como internet profunda. Tal operação consistiu na primeira investigação brasileira realizada na deep web e objetivou identificar usuários da rede Tor (The Onion Router) que a utilizavam para compartilhar pornografia infantil.

> 2. Inexistência da figura do flagrante preparado ou provocado, uma vez que não se vislumbra a presença de agente provocador a instigar a consecução do crime, tampouco a incutir ou induzir a prática do crime de pedofilia virtual nos agentes. Na realidade, depreende-se dos autos a inserção da polícia no ambiente virtual de forma legítima, sob a forma da lei, com técnicas e mecanismos inovadores e pedagógicos na busca pela repressão a crimes perversos que destroem a vida de milhares de crianças e adolescentes em situação de vulnerabilidade.
> 3. Afigura-se precipitada a rejeição da denúncia, que atende aos requisitos do art. 41 do Código de Processo Penal e não se amolda a qualquer das hipóteses descritas em seu art. 395, não se podendo, por ora, afirmar, com a segurança necessária, a ausência de justa causa.
> 4. Recurso em sentido estrito provido.
> (TRF 3ª Região, DÉCIMA PRIMEIRA TURMA, RSE - RECURSO EM SENTIDO ESTRITO - 8271 - 0013241-15.2014.4.03.6181, Rel. DESEMBARGADOR FEDERAL NINO TOLDO, julgado em 04/09/2018, e-DJF3 Judicial 1 DATA:12/09/2018)

Nesse cenário, não houve o flagrante preparado já que os criminosos espontaneamente realizaram o compartilhamento das imagens. Deste modo, a atuação do agente infiltrado encontra respaldo legal no ordenamento jurídico brasileiro, desde que as condutas do agente infiltrado ocorram dentro dos limites estabelecidos legalmente e na decisão judicial que autorizou a infiltração.

No caso em tela o recorrido publicou em 25 de novembro de 2013 vídeo de abuso sexual de uma menina de aproximadamente 06 (seis) anos de idade por um adulto. Após, por meio da infiltração de agentes e com a criação da página foram verificados o IP e a localização do endereço do recorrido, sendo que a partir deste ponto foi requerida autorização judicial para a investigação de forma individualizada ao recorrido.

Na fundamentação do voto foi destacado trecho de parecer do MPF no bojo da investigação que apontou a efetividade da infiltração dos agentes e a licitude da prova produzida:

> Como se vê, o procedimento adotado tinha apenas a finalidade de verificar qual o IP utilizado por criminosos. Como constou dos autos, ao se utilizar a Deep Web valendo-se do programa TOR, é muito difícil haver rastreamento (aliás, a própria sentença compreende isso, a fls. 3), pois o IP muda a cada navegação. Portanto, é fundamental ver que a finalidade da técnica de investigação era, naquele momento, localizar o IP verdadeiro e, assim, saber o endereço físico daquele IP.
> Analisando os autos, observo que não houve ilicitude na colheita das provas. Igualmente, não há ilicitude por derivação, uma vez que, após a identificação do acusado, foi requerido de forma autônoma o mandado de busca e apreensão em sua casa, respeitando-se a reserva de jurisdição (TRF3, 2018).

Conforme demonstrado a infiltração de agentes é situação excepcional em razão da existência de três pontos. O primeiro deles é a necessidade de assegurar os

direitos fundamentais, pois há, mesmo que de forma judicialmente autorizada, a restrição dos direitos do investigado. Nesse sentido, é essencial que a autoridade judicial não só delimite a atuação do agente infiltrado, mas que também acompanhe de forma detalhada as atividades por aquele desenvolvidas. Assim, em caso de eventual violação dos direitos do acusado a infiltração deve ser cessada.

A persecução penal não pode se sobrepor a integridade física e psicológica do agente policial. Diante dos riscos a que o agente pode encontrar é essencial que o próprio agente avalie as condutas por ele praticadas, devendo se negar a praticá-las caso julgue inapropriadas.

Cumpre ressaltar que se durante a instrução criminal não restar confirmado pelos elementos de prova que o recorrido no caso em tela foi o autor dos crimes a ele imputados deverá ser absolvido. Isso porque conforme destacado anteriormente a identificação do IP responsável pela postagem não necessariamente implica no conhecimento acerca da autoria. Logo, caso o réu comprove que no momento do acesso não fez uso do aparelho eletrônico rastreado, embora esteja provada a materialidade a autoria será incerta.

Nessa perspectiva, outra medida muito importante para a produção de provas é a busca e apreensão, devidamente autorizada judicialmente, na residência do investigado, a fim de coletar aparelhos que possam armazenar material pornográfico infantil, reforçando assim os elementos coletados por meio da investigação.

Cumpre destacar que em razão da Operação DarkNet foram identificados indivíduos que prometiam abusar sexualmente de seus filhos, que na época ainda estavam em estado de gestação. Além disso, 06 (seis) crianças foram resgatadas de situações de risco. Dessa maneira, vislumbra-se o significativo impacto da operação.

Por derradeiro, importante destacar que a persecução penal no ambiente da *Dark Web* ainda se trata de novidade no Brasil e seus desdobramentos ainda não são conhecidos por completo. Por outro lado, embora seja medida excepcional a infiltração dos agentes como método investigativo criativo e efetivo diante dos desafios impostos pela *Dark Web*, bem como dentro dos ditames legais do ordenamento jurídico brasileiro.

CONSIDERAÇÕES FINAIS

Os avanços tecnológicos contribuíram para mudanças significativas na sociedade em vários aspectos, impondo ao Estado a necessidade de adequação a fim de acompanhar a evolução social. A partir da Revolução Industrial a tecnologia passou a gerir tanto a produção e quanto prestação de serviços. O comportamento e a forma de se relacionar dos indivíduos também sofreram grandes transformações, sendo incabível imaginar a vida em sociedade sem o uso de tecnologia.

A gênese da *Internet* ocorreu durante a Guerra Fria quando militares estadunidenses idealizaram e criaram um mecanismo com a independência de um sistema central para seu funcionamento. Logo, mesmo que um computador da rede seja destruído não prejudicaria, via de regra, o funcionamento dos demais. Essa é umas das principais características da *Internet*, uma vez que garante mais autonomia ao usuário.

Nesse cenário, a *Internet* atualmente é acessada por grande parte da população mundial e essencial na maioria das atividades cotidianas, inclusive, alguns serviços privados e públicos funcionam apenas por meio de acesso à *Internet.* A inserção da sociedade no ambiente digital trouxe diversos benefícios e facilidades para o cotidiano, porém a transferência para o espaço virtual também acarretou novas situações problemas.

Nessa perspectiva, com esse progresso tecnológico os crimes e as formas de cometimento também sofreram alteração. Nos últimos anos a maioria dos países têm desenvolvido mecanismos de combate aos crimes cometidos no ciberespaço, sendo a pornografia infantil protagonista na incidência de crimes cibernéticos. O desafio na persecução penal do crime de pornografia infantil se torna ainda mais complicado na *Dark Web* em razão do véu de anonimato proporcionado ao usuário pelo seu sistema de funcionamento.

Essa é a problemática assumida no presente estudo que buscou identificar os desafios que permeiam a persecução penal da prática delitiva de disseminação de pornografia infantil na *Dark Web.* Para tanto, a pesquisa foi dividida em três capítulos, que consistiram na pesquisa bibliográfica a respeito dos aspectos concernentes à *Internet* e aos direitos da criança, bem como em estudo de caso com a análise de decisão judicial acerca da temática.

O presente estudo em breve exibição apresentou histórico acerca do surgimento da *Internet* e como esta afetou a sociedade, bem como aspectos técnicos básicos sobre seu funcionamento. Nessa perspectiva, verificou-se que é essencial para a investigação criminal que as autoridades responsáveis possuam conhecimento básico acerca dos principais aspectos técnicos da *Internet,* pois é importante para a identificação, preservação e produção de provas.

Nesse sentido, a *Surface Web,* a *Deep Web e* a *Dark Web* possuem características peculiares que influenciam na forma em que o agente criminoso age e também como o operador do direito deve proceder para a investigação ou defesa criminal. Logo, uma prova importante pode ser perdida em razão do desconhecimento acerca, por exemplo, o tempo de armazenamento de dados pelo provedor.

A investigação na *Surface Web* de certa forma já se encontra consolidada, entretanto o mesmo não se pode dizer acerca da investigação de crimes cibernéticos na *Dark Web,* sendo que se trata de ambiente pouco conhecido e acessado por grande parte da população. Além disso, o funcionamento da *Dark Web* por meio do programa TOR, com a ocultação da identidade do usuário, constitui peculiaridade que dificulta a investigação criminal.

Nesse ponto, o programa TOR assegura ao usuário que o utiliza a camuflagem do IP utilizado para a postagem ou acesso a determinado conteúdo em vários níveis de criptografia. Deste modo, o percurso da mensagem enviada é ocultado, sendo que apenas o usuário remetente e o usuário destinatário têm acesso ao conteúdo da mensagem. Esse sistema dificulta a interceptação da mensagem pelas autoridades, bem como o rastreamento do responsável pela postagem.

A partir da elaboração do segundo capítulo buscou-se demonstrar que a criança possui a tutela dos seus direitos assegurada em âmbito internacional e nacional, sendo que em razão do seu estado de formação as crianças necessitam de proteção especial. Nesse sentido, a Constituição Federal de 1998, Protocolo Facultativo sobre a Venda de Crianças, Prostituição e Pornografia Infantis e a Convenção das Crianças sobre Direito das Crianças, ambas ratificadas pelo Brasil, e o Estatuto da Criança e do Adolescente estabelecem que medidas devem ser tomadas para a repressão da pornografia infantil.

Nesse sentido, é na fase da infância que a criança molda seu comportamento em sociedade, sendo essencial um assegurar um crescimento digno e saudável.

Assim, é quase imensurável o impacto que abusos sexuais e exposição sexual possam ter na vida de um indivíduo na infância e na fase adulta.

Ainda o estudo verificou que embora nos últimos anos tenha ocorrido avanço no campo do direito informático e legislação relativa ao tema, o ordenamento jurídico brasileiro ainda não regulamenta de forma satisfatória as relações jurídicas, em especial, no âmbito criminal ante a ausência de lei que trate sobre os procedimentos investigatórios criminais no ambiente digital.

Além disso, não há dados concretos acerca da dimensão de material pornográfico infantil contido na *Dark Web.* Existem poucos estudos e pesquisadores que adentraram na *Dark Web* com essa finalidade relatam que cerca de 80% (oitenta por cento) do fluxo da *Hidden Web* é de pornografia infantil. Cumpre destacar que a escassez de dados estatísticos acerca da quantidade desse tipo de conteúdo se dá, principalmente, em razão da dificuldade de mensuração dos dados já que demanda acesso a diversos *sites* ocultos, uma vez que não é possível fazer uma busca geral.

O presente estudo identificou que repressão à disseminação de pornografia infantil na *Dark Web* encontra obstáculo no ocultamento do agente emissor e agente destinatário do conteúdo. Conforme demonstrado a rede TOR funciona como uma espécie de labirinto que dificulta muito a identificação e localização dos IPs, ou seja, os autores envolvidos no crime.

Assim, é fundamental para a persecução penal que os integrantes do poder judiciário conheçam os procedimentos e limites da investigação em casos de pornografia infantil. Ademais, a infraestrutura deve ser compatível com as necessidades dessas investigações que demandam maior empenho e aparato. Nesse sentido, para a persecução desse crime é necessário que haja investimento no setor de inteligência e capacitação dos integrantes dos órgãos investigativos, acusatórios, defensivos e julgadores.

Nesse panorama, a fim de garantir reposta jurisdicional ao alto nível de circulação de material de pornografia infantil na *Dark Web* os membros do sistema persecutório penal encontraram como medida a criação de programas específicos de vasculhamento do conteúdo de interesse para o referido ambiente digital, bem como ocupa destaque a atuação de agentes infiltrados.

Nesse sentido, houve grande avanço no âmbito brasileiro a respeito do tema com a Operação Darknet que foi a primeira operação ocorrida no Brasil com o intuito de investigar crimes envolvendo pornografia infantil na *Dark Web.* A referida operação

foi desenvolvida em duas fases denominadas Darknet I e II, deflagradas pela Polícia Federal, respectivamente, em 2014 e 2016.

No bojo da referida investigação diversos autores de crimes envolvendo pornografia infantil foram identificados e localizados, sendo que a operação iniciada no estado do Rio Grande do Sul teve sua competência deslocada também para outros estados brasileiros. No tocante a efetividade verifica-se que diversas pessoas foram presas em flagrante e denunciadas, bem como algumas crianças foram resgatadas de situações de risco.

Nesse cenário, a pesquisa buscou compreender o posicionamento do Tribunal Regional Federal da 3ª Região em caso concreto oriundo da Operação Darknet de disseminação de pornografia infantil na *Dark Web*. Em análise ao Recurso em Sentido Estrito n. 8271 referente ao processo n. 0013241-15.2014.4.03.6181 o estudo observou que o principal ponto de discussão acerca da investigação realizada gira em torno da licitude da prova produzida a partir da infiltração dos agentes.

Com base na pesquisa realizada no presente estudo vê-se que a infiltração de agentes e consequentemente a prova produzida não padece de ilicitude. Isso porque desde o início da Operação Darknet houve a autorização judicial para a infiltração de policiais com o intuito de apurar os crimes relacionados à pornografia infantil, bem como delimitação das condutas que poderiam ser praticadas pelos policiais. Além disso, quando da identificação do possível autor delitivo foi requerida autorização judicial individualizada para continuidade da perquirição investigatória, respeitando, portanto, seus direitos constitucionais.

No tocante à temática o estudo verificou que houve progresso no ordenamento jurídico quanto a infiltração de agentes com a entrada em vigor da Lei nº 13.441, de 8 de maio de 2017, que promoveu alteração no ECA e regulamentou a infiltração de agentes para investigação de crimes envolvendo a dignidade sexual da criança.

Por esse ângulo, acerca do estudo de caso restou constatado que a repressão dessa espécie de crime não pode se dar a qualquer preço, uma vez que o suspeito é titular de direitos e garantias fundamentais assegurados pela Constituição Federal Brasileira. Assim, entende-se que sua privacidade e liberdade de comunicação e criação somente pode ser restrita mediante autorização judicial fundamentada.

Outro ponto verificado na pesquisa sobre a infiltração de agentes na referida situação fática é que o TRF 3 entendeu que não houve o chamado flagrante preparado, que é vedado pelo ordenamento jurídico brasileiro, mas sim o flagrante

esperado já que o acusado da referida ação penal corriqueiramente postava material pornográfico envolvendo crianças na *Dark Web.*

Conforme demonstrado a infiltração de agentes é situação excepcional em razão de constituir método de investigação extremo. Nesse sentido, é necessário assegurar os direitos fundamentais, pois há mesmo que de forma judicialmente autorizada a restrição dos direitos do investigado. Ainda, é essencial que a autoridade judicial não só delimite a atuação do agente infiltrado, mas que também acompanhe de forma detalhada as atividades por aquele desenvolvidas fazendo cessar a medida em caso de violação dos direitos.

Outro ponto importante é que persecução penal não pode se sobrepor ao agente policial. Diante dos riscos a que o agente pode encontrar é essencial que o próprio agente avalie as condutas por ele praticadas, devendo se negar a praticá-las caso julgue inapropriadas. O agente não pode nunca agir de forma desproporcional e excedendo os limites delimitados pela autorização judicial caso em que responderá aos atos ilícitos praticados.

Importante destacar ainda que não se deve vislumbrar a *Dark Web* apenas como um instrumento para prática de crimes informáticos, tampouco defender sua extinção. Conforme já destacado a sociedade evolui a todo instante e a tentativa de barrar o uso da *Dark Web* provavelmente será ineficaz. Alguns países já tentaram banir o uso do TOR, porém acredita-se que caso seja efetivado o banimento que haverá desenvolvimento de outras espécies de tecnologia para suprir o espaço deixado.

Além disso, do ponto de vista constitucional o impedimento da existência desse tipo de mecanismo caminha em sentido contrário com os direitos de privacidade, liberdade de expressão e vida privada, bem como cerceia o acesso à informação.

Cumpre destacar que o Brasil está dentre os poucos países que tiveram êxito nesse tipo de investigação e que o *software* que auxiliou na identificação dos suspeitos foi desenvolvido pela Polícia Federal brasileira. Logo, embora seja uma realidade ainda um pouco distante é possível que no futuro sejam desenvolvidos mecanismos digitais que possibilitem uma investigação mais precisa sem a necessidade de infiltração de agentes.

Outro ponto levantado por Bartlett (2014) diz respeito ao reconhecimento dos órgãos investigativos acerca da impossibilidade de investigação e retirada de todo material contendo pornografia infantil da *Dark Web.* Logo, a tendência dos próximos

anos provavelmente será focada na investigação dos principais produtores de vídeos e imagens pornográficas, bem como dos mantenedores dos *sites.*

Assim, a pesquisa verificou que o paradoxo do equilíbrio entre as liberdades individuais e o controle estatal da criminalidade é o principal desafio à persecução penal do crime de disseminação de pornografia infantil. Nesse ponto, cabe salientar que se trata de campo de pesquisa recente ainda no âmbito tecnológico e jurídico, porém apresentava-se como começo promissor.

Desse modo, é possível concluir que a pesquisa buscou demonstrar que a engenhosidade da *Dark Web* não pode constituir empecilho para a investigação de crime que lesa tanto a dignidade sexual e imagem de crianças, que na maioria das vezes não tem consciência das situações a que estão expostas. Deste modo, o presente estudo buscou destacar que embora a rede TOR seja ferramenta de difícil manipulação ainda sim é possível a identificação de agentes responsáveis pelo compartilhamento de pornografia infantil na *Dark Web*.

REFERÊNCIAS

AMERICAN PSYCHIATRIC ASSOCIATION. **Manual diagnóstico e estatístico de transtornos mentais**: DSM-5 / [American Psychiatric Association; tradução: Maria Inês Corrêa Nascimento ... et al.]; revisão técnica: Aristides Volpato Cordioli ... [et al.]. – 5. ed. – Dados eletrônicos. – Porto Alegre : Artmed, 2014. Disponível em: < https://aempreendedora.com.br/wp-content/uploads/2017/04/Manual-Diagn%C3%B3stico-e-Estat%C3%ADstico-de-Transtornos-Mentais-DSM-5.pdf>. Acesso em: 21/10/2018.

AMIN, Andréia Rodrigues. **Curso de direito da criança e do adolescente: aspectos teóricos e práticos.** São Paulo: Saraiva Educação, 2018. Coordenação Kátia Regina Ferreira Lobo Andrade Maciel. Disponível em < https://app.saraivadigital.com.br/leitor/ebook:625491> Acesso em: 10/11/2018.

BARTLETT. Jamie. **The Dark Net: what happens under the conditions of anonymity?**. Oxford University Scientific Society. YouTube. 5 de nov de 2014. 58min12s. Disponível em: <https://www.youtube.com/watch?v=vSfAhfWW0I0>. Acesso em: 10/11/2018.

BRASIL. **Constituição da República Federativa do Brasil.** Brasília, 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 20/06/2018.

BRASIL, Decreto nº 5.015, de 12 de março de 2004, **Convenção das Nações Unidas contra o Crime Organizado Transnacional**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm> acesso em: 17/12/2018.

BRASIL. Decreto nº 99.710, de 21 de novembro de 1990. **Convenção sobre os Direitos da Criança.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm>. Acesso em: 18/06/2018.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. **Estatuto da Criança e do Adolescente**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/l8069.htm> Acesso em: 18/06/2018.

BRASIL, Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da *Internet*.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 18/07/2018.

BRASIL. Decreto nº 5.007, de 8 março de 2004. **Protocolo Facultativo à Convenção sobre os Direitos da Criança referente à venda de crianças, à prostituição infantil e à pornografia infantil.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5007.htm>. Acesso em: 18/06/2018.

BRASIL, Lei nº 13.441, de 8 de maio de 2017. **Regulamentação da infiltração de agentes nos crimes contra a dignidade sexual infatojuvenil**. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm>. Acesso em: 23/11/2018.

BRASIL, Ministério Público Federal, **Crimes Cibernéticos. Manual Prático de Investigação**. Procuradoria de São Paulo. Grupo de Combate aos Crimes Cibernéticos, 2006. Disponível em: <http://tmp.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf>. Acesso em: 04/09/2018.

BRASIL, Ministério Público Federal, **Operação Darknet**. Disponível em: <http://www.mpf.mp.br/rs/sala-de-imprensa/noticias-rs/operacao-darknet-vence-o-v-premio-republica-na-categoria-201cmpf-2013-criminal201d>. Acesso em: 14/06/2018.

BRASIL, Ministério Público Federal. **Roteiro de Atuação de Crimes Cibernéticos**. 2ª Câmara de Coordenação e Revisão, Criminal. 2013. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf>. Acesso em: 26/08/2018.

BUFFON, Jaqueline Ana. **Agente Infiltrado Virtual**. *In:* BRASIL. MPF. Crimes cibernéticos / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília, 2018. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos>. Acesso em: 06/06/2018.

CALADO, Felipe B. CALADO, Marcelo. **Combate à pornografia infanto-juvenil com o aperfeiçoamento na identificação de suspeitos e na detecção de arquivos de interesse.** *In:* BRASIL. MPF. Crimes cibernéticos / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília, 2018. Disponível em <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos>. Acesso em: 06/06/2018.

CAMILO, Roberta Rodrigues. **A infiltração do agente no crime organizado.** *In:* MESSA, Ana Flávia, CERNEIRO, José Reinaldo Guimarães. Crime Organizado. São Paulo: Saraiva, 2012. Disponível em: <https://app.saraivadigital.com.br/leitor/ebook:600125>.Acesso em: 10/11/2018.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011. Disponível em: <https://app.saraivadigital.com.br/leitor/ebook:583050>. Acesso em:10/07/2018.

FIORILLO, Celso Antonio Pacheco, CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade de informação.** 2. ed. São Paulo: Saraiva, 2016. Disponível em: <https://app.saraivadigital.com.br/leitor/ebook:604677>. Acesso em: 08/08/2018.

FULLER, Paulo Henrique Aranda, DEZEM, Guilherme Madeira, NUNES JÚNIOR, Flávio Martins Alves. **Estatuto da criança e do adolescente: difusos e coletivos.** 1. Ed. São Paulo: Editora Revista dos Tribunais, 2013. Disponível em: < https://portal.mpf.mp.br/rtproview/title.html?redirect=true&titleKey=rt%2Fmonografias

%2F92126100%2Fv3.4&titleStage=F&titleAcct=ia744d779000001593d53a067c09b01c5#sl=0&eid=c1b53fd73cea1705c6ded1f41aef2c84&eat=%5Bbid%3D%221%22%5D&pg=&psl=e&nvgS=false>. Acesso em: 01/11/2018.

Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Disponível em: <http://indicadores.safernet.org.br/>. Acesso em: 13/06/2018.

ISHIDA, Válter Kenji. **Estatuto da criança e do adolescente: doutrina e jurisprudência**. 15 ed. São Paulo: Atlas, 2014.

JESUS, Damásio de. MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. Disponível em: <https://app.saraivadigital.com.br/leitor/ebook:580118>. Acesso em: 12/10/2018.

LOTUFO, Renata Andrade. **Crimes cometidos contra a vulnerabilidade sexual de crianças e adolescentes no ECA e no Código Penal: a Internet como forma de cometimento e aproximação do sujeito ativo e vítima.** *In:* BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados Investigação e prova nos crimes cibernéticos. São Paulo: EMAG, 2017.
352p. (Cadernos de estudos;1). Disponível em: <http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf>. Acesso em: 23/10/2018.

MARCON, João Paulo Falavinha, DIAS, Thais Pereira. **DEEPWEB: O Lado Sombrio da Internet.** Conjuntura Global, Vol.3, n. 4, out./dez., 2014, p. 233-243. Disponível em: <https://revistas.ufpr.br/conjgloblal/article/view/40071/24471>. Acesso em: 18/06/2018.

NEISTEN, Mariângela Lopes. **O agente infiltrado como meio de investigação**. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo, 2006.

PINHEIRO, Patrícia Peck. **Direito digital**. 6 ed. rev. atual e ampl. São Paulo: Saraiva. 2016. Disponível em: <https://app.saraivadigital.com.br/leitor/ebook:604554>. Acesso em: 20/10/2018.

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. 13 ed. rev. e atual. São Paulo: Saraiva, 2012.

PF combate crime de pornografia infantil na Deep Web. Disponível em <http://www.pf.gov.br/agencia/noticias/2016/11/pf-combate-crime-de-pornografia-infantil-na-deep-web>. Acesso em: 07/07/2018.

POMPÉO, Wagner Augusto Hundertmarck, SEEFELDT João Pedro. **Nem tudo está no Google: Deep Web e o Perigo da Invisibilidade**. Anais do 2º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede. 04, 05 e 06 jun / 2013- Santa Maria / RS. ISSN 2238-9121. Disponível em: < http://coral.ufsm.br/congressodireito/anais/>. Acesso em: 18/06/2018.

ROCHA, Henrique. **O lado profundo da internet ("Deep Web").** *In:* PINHEIRO, Patrícia Peck. Direito digital aplicado 3.0. Patrícia Pinheiro Peck. Coordenadora. 1 ed. São Paulo: Thomas Reuters Brasil, 2018. Disponível em: <https://portal.mpf.mp.br/rtproview/title.html?redirect=true&titleKey=rt%2Fmonografias%2F150132880%2Fv1.8&titleStage=F&titleAcct=ia744d779000001593d53a067c09b01c5#sl=e&eid=5ccd1f33de75859b3566aaf60a8856d4&eat=&pg=&psl=&nvgS=false>. Acesso em: 02/08/2018.

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

SANTOS, Marilaine Almeida. **Reflexões sobre o registro de identificação criminal de condenados pela prática de crimes e a liberdade sexual do menor em Portugal.** *In:* BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados Investigação e prova nos crimes cibernéticos. São Paulo: EMAG, 2017. 352p. (Cadernos de estudos;1). Disponível em: <http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf>. Acesso em: 23/10/2018.

SHIMABUKURO, Adriana. **Cibercrime: quando a tecnologia é aliada da lei**. *In:* BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados Investigação e prova nos crimes cibernéticos. São Paulo: EMAG, 2017. 352p. (Cadernos de estudos;1). Disponível em: <http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf>. Acesso em: 23/10/2018.

SILVIA, Lilian Ponchio. **Pedofilia e o abuso sexual de crianças e adolescentes**. Coordenadores Alice Bianchini, Ivan Luís Marques e Luiz Flávio Gomes. São Paulo: Saraiva, 2013. Disponível em: <https://app.saraivadigital.com.br/leitor/ebook:599973>. Acesso em: 18/10/2018.

SOUZA, Luiz Roberto Salles, **A infiltração do agente como técnica de investigação criminal**. *In:* MESSA, Ana Flávia, CERNEIRO, José Reinaldo Guimarães. Crime Organizado. São Paulo: Saraiva, 2012. Disponível em: <https://app.saraivadigital.com.br/leitor/ebook:600125>. Acesso em: 10/11/2018.

SPINELI, André Luiz Pereira. **Crimes Informáticos: Comentários ao Projeto de Lei n. 5.555/2013**. BRASIL. Ministério Público Federal. Crimes cibernéticos / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília, 2018. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos>. Acesso em: 06/06/2018.

Study claims more than 80% of 'dark net' traffic is to child abuse sites. Disponível em: <https://www.theguardian.com/technology/2014/dec/31/dark-web-traffic-child-abuse-sites>. Acesso em: 20/06/2018.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. 2. ed. (Coleção saberes monográficos / coordenadores Aline Bianchini e Luiz Flávio Gomes). São

Paulo: Saraiva, 2015. Disponível em: <https://app.saraivadigital.com.br/leitor/ebook:580813>. Acesso em: 20/10/2018.

TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO. Décima Primeira Turma. **Recurso em Sentido Estrito - 8271 - 0013241-15.2014.4.03.6181**, Relator: Nino Toldo, julgado em 04/09/2018. Disponível em: <http://web.trf3.jus.br/base-textual/home/listacolecao/9?np=3>. Acesso em: 02/12/2018.