UNIFG – CENTRO UNIVERSITÁRIO FG
DIREITO

MARIA LUIZA BEZERRA COSTA

CRIMES VIRTUAIS: OS DESAFIOS DA INVESTIGAÇÃO CRIMINAL NO COMBATE À PORNOGRAFIA INFANTIL NO BRASIL

Guanambi-BA
2021. 1

MARIA LUIZA BEZERRA COSTA

CRIMES VIRTUAIS: OS DESAFIOS DA INVESTIGAÇÃO CRIMINAL NO COMBATE À PORNOGRAFIA INFANTIL NO BRASIL

Artigo Científico apresentado ao curso de Direito do Centro Universitário FG- UNIFG como requisito de avaliação da disciplina de Trabalho de Conclusão de Curso II.

Orientador: Matheus Vídero Caldas da Silva.

Guanambi-BA
2021.1

SUMÁRIO

CRIMES VIRTUAIS: OS DESAFIOS DA INVESTIGAÇÃO CRIMINAL NO COMBATE À PORNOGRAFIA INFANTIL NO BRASIL

Maria Luiza Bezerra Costa[1], Matheus Vídero Caldas da Silva[2]

[1] Graduanda do Curso de Direito. Centro Universitário FG- UNIFG
[2] Docente do Curso de Direito do Centro Universitário FG - UNIFG

RESUMO: Com o surgimento e evolução do meio virtual, que trouxe inúmeros benefícios, houve o surgimento de novos crimes praticados por meio da internet, e a utilização desse novo espaço para a prática de crimes já existentes e tipificados no ordenamento Jurídico brasileiro. Dentre os crimes mais comuns nesse meio, está a pornografia infantil, que consiste na comercialização e compartilhamento de fotos, vídeos pornográficos envolvendo crianças e adolescentes. As vantagens proporcionadas pelo anonimato de servidores e IP's, em ambientes como a Dark Web e a Deep Web, dificulta o papel da polícia na hora de identificar e combater os criminosos. Além da dificuldade de acesso a ambientes virtuais que permitem a navegação anônima, utilizando muitas vezes da criptografia para esconder sua localização e seus acessos, a polícia brasileira que combate a crimes cibernéticos, encontra outros obstáculos como a falta de leis mais específicas e eficazes em relação a tais crimes. Desse modo é importante analisar e identificar os obstáculos existentes, a fim de promover uma repressão efetiva a essas práticas delituosas e garantir a segurança no meio virtual e a integridade dos bens jurídicos de crianças e adolescentes.

PALAVRAS- CHAVE: Ambiente Virtual. Pornografia Infantil. Dificuldades. Crime. Investigação.

ABSTRACT: With the emergence and evolution of the virtual environment, which brought countless benefits, there was the emergence of new crimes practiced through the internet, and the use of this new space for the practice of crimes already existing and typified in the Brazilian Legal system. Among the most common crimes in this environment is child pornography, which consists in the commercialization and sharing of photos, pornographic videos involving children and adolescents. The advantages provided by the anonymity of servers and IP's, in environments such as the Dark Web and the Deep Web, make it difficult for the police to identify and combat criminals. In addition to the difficulty of accessing virtual environments that allow anonymous browsing, often using cryptography to hide their location and access, the Brazilian police, which fight cyber crimes, encounter other obstacles such as the lack of more specific and effective laws in relation to to such crimes. Thus, it is important to analyze and

identify the existing obstacles, in order to promote an effective repression of these criminal practices and to guarantee security in the virtual environment and the integrity of the legal assets of children and adolescents.

KEY WORDS: Virtual Environment. Child Pornography. Difficulties. Crime. Investigation.

1 INTRODUÇÃO

O presente texto analisará as dificuldades enfrentadas pela polícia nas investigações em combate aos crimes virtuais, sobretudo, a pornografia infantil, que tem aumentado de forma significativa nos últimos anos. Com a globalização, e evolução dos aparatos tecnológicos, a internet proporcionou uma comunicação em tempo real, conectando pessoas de várias partes do mundo, e devido a essa facilidade houve um aumento da interação social. Mas da mesma maneira que a internet trouxe inúmeros benefícios para a sociedade, também serviu de meio para que criminosos praticassem atos ilícitos.

A imaterialidade do meio virtual que proporciona a ausência de limites espaciais e temporais, contribuiu, portanto, para o surgimento dos chamados crimes virtuais. Dentre os diversos crimes existentes no contexto virtual, há a pornografia infantil, que consiste no compartilhamento ou comercialização de fotos e vídeos pornográficos envolvendo crianças e adolescentes. Esta prática criminosa está tipificada na legislação Penal e no Estatuto da Criança e do Adolescente (ECA).

O objetivo principal do texto foi analisar os métodos utilizados na persecução criminal do crime de pornografia infantil e a legislação vigente sobre tal conduta delitiva, além de esclarecer quais são os desafios encontrados pelos aplicadores do Direito e autoridades no combate da pratica delituosa, demonstrando quais pontos podem ser melhorados.

A metodologia utilizada na pesquisa foi a bibliográfica, de caráter qualitativo, tendo em vista um levantamento de dados mediante artigos científicos, documentos e legislação sobre o tema proposto, com a finalidade de se desenvolver uma análise crítica fundamentada sobre a temática. Assim, esse estudo investigativo busca analisar e debater questões que se entrelaçam na atuação penal no combate à pornografia infantil no Brasil inserido no meio dos impactos dos crimes virtuais.

Por fim diante das dificuldades encontradas pela Polícia investigativa e autoridades de um modo geral no Brasil, no combate aos crimes cibernéticos, se faz mister o papel da sociedade em buscar soluções junto ao Poder Legislativo para que leis mais específicas sejam criadas, a fim de punir com mais eficácia as práticas delituosas e resguardar a segurança de dados e informações pessoais no ambiente virtual.

2 MATERIAIS E MÉTODOS

A metodologia utilizada na pesquisa é a bibliográfica, de caráter qualitativo, tendo em vista um levantamento de dados mediante artigos científicos, documentos e legislação sobre o tema proposto, com a finalidade de se desenvolver uma análise crítica fundamentada.

Assim, esse estudo investigativo busca analisar e debater questões que se entrelaçam na atuação penal no combate à pornografia infantil no Brasil inserido no meio dos impactos dos crimes virtuais. Dessa maneira, o trabalho proposto utilizará de análise de dados através do método dedutivo, buscando primeiramente analisar as fontes de pesquisa que versem sobre o tema a ser analisado. Pesquisa bibliográfica, do tipo de compilação de dados (coleta de dados) com análise de materiais já publicados, constituído de artigos de periódicos e legislação vigente.

Ademais, o método dedutivo proposto neste trabalho parte das teorias e leis consideradas gerais e universais buscando explicar a ocorrência de fenômenos particulares. O exercício metódico da dedução parte de enunciados gerais (leis universais) que supostos constituem as premissas do pensamento racional e deduzidas chegam a conclusões. O exercício do pensamento, conforme Lakatos e Marconi (2000) pela razão cria uma operação na qual são formuladas premissas e as regras de conclusão que se denominam demonstração.

3 CRIMES VIRTUAIS

Os crimes realizados no meio virtual são denominados de crimes virtuais, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, delitos cibernéticos, crimes transnacionais, dentre outras nomenclaturas. Estes se dividem em puros (ou próprios) sendo aqueles praticados por meio eletrônico em sentido amplo, onde a informática é o objeto jurídico tutelado, enquanto os impuros (ou impróprios) são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens diversos da informática [1].

De acordo com (ROSSINI,2004) o conceito de "delito informático" poderia ser delimitado como uma conduta típica e ilícita, constituindo um crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por qualquer pessoa, seja ela física ou jurídica, utilizando da informática, dentro ou fora de uma rede, e que agrida, direta ou indiretamente, a segurança digital, que tem por elementos a integridade, a disponibilidade a confidencialidade[2].

Neste sentido o crime cibernético abrange toda conduta criminosa, tipificada que é cometida através da internet. Segundo Nigre (2000, p. 32) o crime virtual: "é um ato lesivo cometido através de um computador ou de um periférico com a intenção de se obter uma

[1] ALBUQUERQUE, Roberto Chacon de. **A Criminalidade Informática**. São Paulo: Editora Juarez de Oliveira, p.40-41, 2006.
[2] ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2004.

vantagem indevida". Portanto, o conceito de crime cibernético não engloba somente o que para muitos estudiosos seriam apenas os crimes de roubo ou alteração de dados pessoais ou de software, mas inclui também crimes como pedofilia, tráfico de drogas, tráfico de pessoas, pedofilia, tráfico de órgãos, calúnia, difamação, injúria. [3]

4 PORNOGRAFIA INFANTIL

A pornografia infantil, é uma forma de violência sexual contra crianças e adolescentes. No Brasil, a prática desse crime está tipificada no Estatuto da Criança e do Adolescente (ECA), e no Código Penal, assim como também na Convenção dos Direitos da Criança da ONU, de 1989[4].

É necessário esclarecer que o crime de Pornografia Infantil não se confunde com Pedofilia, que de acordo com a Organização Mundial da Saúde (OMS) é uma doença, transtorno psicológico, onde o indivíduo apresenta desejo sexual por crianças pré-púberes. Sendo assim o Pedófilo não é um criminoso, mas sim um doente, porém quando exterioriza sua patologia e esta se enquadra em algum crime previsto no ordenamento jurídico, o pedófilo se torna um criminoso.[5] No crime de Pornografia Infantil, não há necessidade da ocorrência de relação sexual, sendo suficiente para a tipificação a comercialização e o compartilhamento de fotos, vídeos pornográficos envolvendo crianças e adolescentes[6].

A lei 11.829/08 alterou a lei 8.069/90 Estatuto da Criança e do Adolescente afim de aprimorar o combate à produção, venda e distribuição de pornografia infantil, como também criminalizar a aquisição e a posse de tal material dentre outras condutas relacionadas à pornografia infantil na internet.

A divulgação deste tipo de conteúdo na internet torna complexa a identificação da origem de quem as espalhou. Esta prática delituosa é frequente na Deep Web, local este que torna quase impossível a identificação do criminoso, além disso a facilidade de viralização oferecida pela internet, bem como o envio e recebimento de arquivos, como fotos e vídeos, para qualquer lugar, favorece ainda mais essa pratica.[7]

---

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

[4] LANDINI, Tatiana Savoia. **Pornografia infantil na Internet: violência sexual ou pornografia?** Sociologia, USP. S.Paulo, 2000.

[5] CARAMIGO, Denis. **Pedofilia não é um crime, mas, sim uma doença**. Conjur,2017. Disponível em: https://www.conjur.com.br/2017-nov-10/denis-caramigo-pedofilia-nao-crime-sim-doenca. Acesso em: 14 de junho, 2021.

[6] INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004.

[7] PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia, 2019.

A utilização do meio virtual por crianças e adolescentes, principalmente as redes sociais e jogos online, sem o monitoramento dos pais ou responsáveis, facilita ainda mais a existência deste crime, tornando esses menores alvos fáceis para os criminosos, uma vez que muitos criam perfis falsos nas redes sociais, para se comunicar com as vítimas de forma fácil e sem apresentar suspeitas.

Além disso, é importante que os pais, ou a família se atentem para fotos que são tiradas no cotidiano, em que essas crianças ou adolescentes, se encontrem despidos, visto que tais arquivos podem ser facilmente violados e utilizados por criminosos, através da invasão de dispositivo informático, e espalhados na Deep Web.

5 DEEP WEB E DARK WEB

É chamado de Deep Web o local onde se encontra os materiais de difícil acesso contidos na internet. Esses materiais são para usuários selecionados, e para acessar a tais conteúdos é necessário links próprios, fator que dificulta o acesso por leigos.[8]

De acordo com Shimabukuro e Silva (2017), a Deep Web, também conhecida como, as profundezas da internet, é o local em que seu conteúdo não está disponível tão facilmente, como nos buscadores populares da internet o Google ou o Yahoo, para qualquer utilizador, porém sua extensão é igual à da internet convencional.[9]

A internet usual, para Borges (2018)[10] a Surface Web[11] é composta por computadores que possuem seus conteúdos conectados, através da uma rede mundial. Neste ambiente é possível acessar a localização de qualquer computador, utilizando o endereço de IP (Internet Protocol) que é um endereço único presente em cada máquina para que se possa acessar a rede de internet. Já para se ter acesso aos conteúdos da Deep Web, é preciso de mecanismos específicos, não bastando ter apenas o endereço de IP, desta forma fica claro o quanto o acesso a esse ambiente virtual é restrito.[12]

---

[8] PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia, 2019.
[9] SHIMABUKURO, A.; SILVA, M. G. B. de A. **Internet, Deep Web e Dark Web**. In SILVA, Ângelo Roberto Ilha da (Org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado. 2017.
[10] BORGES, C. B.; SARTORI, L. P.; BARROS, S. M. **A Deep Web e a relação com a criminalidade na internet**. Direito & TI. Porto Alegre, 07 de dezembro de 2018.
[11] Surface Web – superfície, em português – é toda a parte da internet indexada, possibilitando que os canais de busca (Google, Bing, entre outros) encontrem o domínio, e todo o público tenha acesso livre às informações lá postadas.
[12] PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia, 2019.

De acordo com Shimabukuru e Silva (2017) a Dark Web, uma rede ainda mais anônima, surgiu devido a propagação da existência da internet profunda, que com o passar do tempo, foi atraindo cada vez mais a atenção de usuários. A Dark Web é muito utilizada em países onde o governo restringe e bloqueia o acesso a determinados sites, e esse ambiente ainda mais "profundo" da rede utiliza a criptografia, como uma forma de dificultar ainda mais a identificação de seus usuários e crimes. [13]

Este ambiente, em relação a Deep Web, é muito mais favorável para a prática de crimes, uma vez que proporciona o anonimato de seus agentes. Infelizmente, na Dark Web é muito comum a prática de diversos crimes, como tráfico de drogas, fraudes bancárias, assassinos de aluguel, e principalmente a pornografia infantil, justamente devido o sigilo das informações dos usuários nesse ambiente.

Para que se possa utiliza-lo são necessários mecanismos que assegurem o anonimato do usuário, entre estes o mais conhecido é o TOR (The Onion Router), que de acordo com Shimabukuru e Silva (2017) consiste em uma rede de túneis virtuais que dificulta a identificação das máquinas ao acessarem certos conteúdos, mecanismo que foi criado pela marinha dos Estados Unidos, com a intenção de estabelecer uma comunicação segura pela internet.[14]

É importante mencionar que nenhum desses mecanismos de acesso a esses ambientes, que mascaram a identificação dos equipamentos utilizados, são totalmente seguros, sendo possível sim a violação de dados e a descoberta do servidor ou computador utilizado. Ainda assim, é quase que impossível que esses ambientes da internet profunda sejam combatidos pelas autoridades, como também a identificação dos criminosos que atuam nestes ambientes.[15]

Devido a existência desses ambientes virtuais de difícil acesso, é que a prática de crimes, em especial a pornografia infantil, é tão grande. O compartilhamento e obtenção de fotos de abuso sexual de crianças e adolescentes na Dark Web e Deep Web ocorre constantemente, sem que as autoridades consigam identificar a origem desses arquivos, e quem está acessando.

---

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

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

[15] PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia, 2019.

6 LEGISLAÇÃO BRASILEIRA E CRIMES CIBERNÉTICOS

No ambiente informático, os usuários buscam segurança e privacidade para que possam desfrutar com tranquilidade da facilidade e dos benefícios que a rede mundial proporciona no cotidiano, tanto nas relações sociais e comerciais. De acordo com Abreu (2011, p.12) as condutas ilícitas por sua vez, como a fraude, roubo e uso indevido de dados, e tantos outros crimes cometidos por intermédio da internet, com cada vez mais frequência, traz a insegurança e a sensação de que as autoridades se encontram impotentes em relação a isso.[16]

Ao analisar a legislação brasileira, percebe-se que esta ainda carece de normas que tipifiquem as condutas ilícitas cometidas no ambiente virtual, neste sentido Crespo (2011), menciona que a informação, os dados, a confiabilidade e a segurança dos sistemas informáticos e de comunicação necessitam de serem tutelados pelo Direito Penal. Observando a evolução dos meios de comunicação e a evolução da informática, observamos que a legislação penal em certos momentos não está adequada em relação a tutela jurídica a respeito dos crimes cibernéticos.[17]

A criação das leis 12.735/2012, 12.737/2012 e 12.965/2014 não foram suficientes para o combate efetivo dos delitos que são cometidos através da internet, principalmente devido a vasta gama de crimes virtuais e a falta de leis específicas. Além disso a natureza taxativa do Código Penal brasileiro, dificulta a aplicação de suas normas por analogia, aos crimes cibernéticos.[18]

Quando o delito se relaciona a contratos virtuais, utilizam -se o Código Civil brasileiro e o Código de Defesa do Consumidor, devido a falta de normas específicas, já em relação a esfera penal, há também a aplicação de normas já tipificadas no Código Penal, entre estes os artigos 240 e 241 da Lei nº 11.829/2008 do Estatuto da Criança e do Adolescente; artigo 12 da Lei nº 9.609/98 que versa sobre crimes contra Software- "Pirataria"; artigos 138,139,140 e 147 do Código Penal brasileiro, que tipificam respectivamente os crimes de Calúnia, Difamação, Injúria e Ameaça.[19]

6.1 Marco Civil da Internet

O Marco Civil da Internet ("MCI") lei 12.965/14, foi criado com o objetivo de combater os crimes virtuais e auxiliar na investigação destes crimes, procurando enfrentar temas que

[16] ABREU, Leandro Farias dos. **A Segurança das Informações nas Redes Sociais**. 2011.
[17] CRESPO, M. X. de F. **Crimes Digitais**. São Paulo: Saraiva, 2011.
[18] MAIA, Teymisso Sebastian Fernandes**. Análise dos Mecanismos de Combate aos Crimes Cibernéticos no Sistema Penal Brasileiro** / Teymisso Sebastian Fernandes Maia. – 2017.
[19] MAIA, Teymisso Sebastian Fernandes**. Análise dos Mecanismos de Combate aos Crimes Cibernéticos no Sistema Penal Brasileiro** / Teymisso Sebastian Fernandes Maia. – 2017.

ainda estavam em aberto, e trazendo impactos diretos sob os interesses comerciais. A norma busca a proteção aos registros, dados pessoais e comunicações privadas, a neutralidade da rede, e a responsabilidade civil dos provedores de rede, a guarda de dados e registros, e a requisição judicial de registros.[20]

> Com os avanços tecnológicos e as constantes trocas de informações e ideologias nos meios virtuais, a sociedade contemporânea carece da interferência do Estado, para ditar as regras e preceitos constitucionais, com o intuito de estender os princípios supracitados a todas as áreas onde a democracia deposita seus pressupostos básicos de existência.[21]

Ao analisar o art. 3º do MCI, pode-se observar que a internet brasileira se estabelece sobre três pilares, formados pelos princípios da neutralidade da rede, da privacidade e da liberdade de expressão, que estão relacionados entre si. A neutralidade da rede versa sobre a garantia de que as operadoras não cobrem de forma diferenciada, a depender do conteúdo que transporta, exceto em relação às velocidades que oferecem, este princípio tem como objetivo proporcionar a democratização do acesso a internet no país.

Em relação ao princípio da privacidade do usuário, a lei busca proteger os dados das pessoas em relação aos provedores, permitindo a quebra do sigilo apenas em ocasiões excepcionais. A liberdade de expressão além de ser assegurada constitucionalmente, apresenta tutela destacada no MCI, sendo um fundamento que disciplina o uso da internet no Brasil e pleno exercício do direito de acesso.[22]

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

A referida Lei n.º 12.737/2012 ficou conhecida como Lei Carolina Dieckmann, em decorrência do episódio da divulgação de imagens em sites de pornografia, após hackers terem invadido os arquivos e acessado indevidamente os dados da atriz da rede de televisão brasileira, Rede Globo, a vítima recusou à chantagem de pagar a quantia em dinheiro para que suas fotografias em poses íntimas não fossem amplamente divulgadas. De acordo com Brito (2013), o surgimento da norma sobre delitos informáticos representou um marco na história do ordenamento jurídico brasileiro, pois trouxe um avanço significativo no que concerne à criminalidade informática.[23]

---

[20] TEFFÉ, C.S; MORAES, Maria Celina B. **Redes Sociais Virtuais: privacidade e responsabilidade civil análise a partir do marco civil da internet.** Pensar, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017.

[21] SILVA, *et al*. **Livre Manifestação do Pensamento Correlato ao Marco Civil da Internet**. Revista de Direito do Centro Universitário FG- UNIFG, ano 1, nº1, out.2015.

[22] TEFFÉ, C.S; MORAES, Maria Celina B. **Redes Sociais Virtuais: privacidade e responsabilidade civil análise a partir do marco civil da internet.** Pensar, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017.

[23] PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia, 2019

A Lei n. 12.737/2012 dispõe sobre a tipificação criminal de delitos informáticos, com o intenção de atualizar a legislação penal em vigência, previsto no art. 154-A do Código Penal, introduzido pelo art. 2º da Lei 12.737, explicita a conduta criminosa de invadir dispositivo informático alheio, podendo estar ou não conectado à rede de computadores, através da violação indevida de mecanismos de segurança para obter, adulterar, ou destruir dados ou informações sem autorização do dono do dispositivo para obter vantagem ilícita.[24]

Nas palavras de Cabette (2013, p. 01):

> Não é qualquer dispositivo informático invadido que conta com a proteção legal. Para que haja o crime é necessário que o dispositivo conte com 'mecanismo de segurança' (v.g. antivírus, 'firewall', senhas etc.). Assim sendo, o dispositivo informático despido de mecanismo de segurança não pode ser objeto material das condutas incriminadas, já que o crime exige que haja 'violação indevida de mecanismo de segurança'. Dessa maneira, a invasão ou instalação de vulnerabilidades em sistemas desprotegidos é fato atípico. […] Sinceramente não se compreende essa desproteção legislativa exatamente aos mais desprotegidos. É como se o legislador considerasse não haver violação de domicílio se alguém invadisse uma casa que estive com as portas abertas e ali permanecesse sem a autorização do morador e mesmo contra a sua vontade expressa! Não parece justo nem racional presumir que quem não instala proteções em seu computador está permitindo tacitamente uma invasão, assim como deixar a porta ou o portão de casa abertos ou destrancados não significa de modo algum que se pretenda permitir a entrada de qualquer pessoa em sua moradia. A forma vinculada disposta no tipo penal ('mediante violação indevida de mecanismo de segurança') poderia muito bem não ter sido utilizada pelo legislador que somente deveria chamar a atenção para a invasão ou instalação desautorizadas e/ou sem justa causa. Isso seria feito simplesmente com a locução 'mediante violação indevida' sem necessidade de menção a mecanismos de segurança.[25]

O contexto que envolveu o surgimento da Lei 12.737/12, demonstra que havia uma lacuna legislativa para tipificar os crimes ocorridos na internet, e que só após a notoriedade do crime ocorrido com a atriz Carolina Dieckmann, a questão foi discutida efetivamente e a lei foi aprovada com urgência, o que significou um grande avanço na legislação brasileira, no que diz respeito ao combate aos crimes cibernéticos.[26]

7 INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

A investigação e o combate aos crimes virtuais não são tarefas fáceis, pois as práticas desses crimes podem ocorrer em qualquer lugar, para isso bastando que o criminoso tenha acesso à rede. Nesse contexto, a internet desempenha o papel de grande facilitadora para prática desses crimes em razão da dificuldade de se encontrar o responsável pelo delito. Além disso, é

[24] BRASIL. **Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckman).**
[25] CABETTE, E. L. S, NAHUR, M. T. M. **Criminalidade Organizada & Globalização Desorganizada**. Rio de Janeiro: Freitas Bastos.
[26] PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia- GO, 2019

necessário que as investigações sejam realizadas por profissionais capacitados, que tenham conhecimento técnico informático.

De uma forma geral a persecução penal pode ser dividida em duas fases, a Investigação Criminal e Processo Penal. A primeira fase delimita-se à colheita de provas, apuração de indícios de autoria e materialidade da ação criminosa, enquanto que a segunda fase tem por escopo a função de processar e julgar [27].

Os conceitos de crime, delito, ato e efeito são os mesmos aplicados tanto no âmbito do direito penal como do direito penal digital, cibernético ou eletrônico, sendo que as principais diferenças se referem à territorialidade e à investigação de provas, bem como a criação de novos tipos penais em virtude do surgimento de crimes que são cometidos exclusivamente através dos meios eletrônicos[28].

De acordo com Wendt (2013) durante a investigação de crimes cibernéticos há uma fase inicial, técnica, e uma fase consequencial, de investigação propriamente dita. O objetivo principal da fase técnica é localizar o computador ou dispositivo que foi utilizado para a prática da conduta criminosa. Durante essa etapa, são realizados alguns procedimentos inicias, que são a análise das informações narradas pela vítima e compreensão do fato ocorrido na internet, orientações à vítima que buscam a preservação do material comprobatório do crime e a sua proteção virtual, iniciação da coleta de provas em ambiente virtual, formalização da conduta criminosa através do registro do boletim de ocorrência, e a instauração do procedimento, investigação inicial de dados na rede mundial de computadores, sobre possíveis autores, origem e-mails, registros e hospedagens de domínios. Formalização das provas coletadas e apuração preliminar, representação ao Poder Judiciário para expedição de autorização judicial para quebra de dados, conexão ou acesso.[29]

Como assegura Wendt (2013, p. 53-54):

> A partir da identificação e localização do computador que permitiu a conexão e o acesso criminoso na internet surge a denominada fase de campo, quando há necessidade de deslocamento de agentes policiais para realização de diligências com o intuito de promover o reconhecimento operacional no local. Essa diligência deverá ocorrer sempre de maneira discreta, pois poderá haver a necessidade de solicitar uma medida processual penal cautelar, em regra a representação para que o Poder Judiciário conceda o mandado de busca e apreensão. Ela ocorrerá de imediato nos casos de identificar o endereço que corresponda a uma residência e/ou rede não corporativa.[30]

---

[27] GRECO, Rogério. **Código Penal: comentado-5. ed**. -Niterói, RJ: Impetus, 2011.

[28] PINHEIRO, Patrícia Peck. **Direito Digital**. 4 ed. Saraiva: São Paulo, 2010.

[29] WENDT, Emerson. **Crimes Cibernéticos: ameaças e procedimentos de investigação**/ Emerson Wendt; Higor Vinicius Nogueira Jorge. -2. Ed. – Rio de Janeiro: Brasport,2013.

[30] WENDT, Emerson. **Crimes Cibernéticos: ameaças e procedimentos de investigação**/ Emerson Wendt; Higor Vinicius Nogueira Jorge. -2. Ed. – Rio de Janeiro: Brasport,2013.

No Brasil a criação de outros métodos para ao combate aos crimes virtuais foram implantados, sendo um deles a criação de divisões especializadas em cibercrimes. Essa atividade policial desempenhada tanto no mundo off-line como no mundo online, sendo atribuição da Polícia Federal ou Civil, deverá ser regulamentada por uma política de segurança pública e organizada a partir de dados e informações característicos ao lugar ou a matéria a qual as autoridades policiais estão vinculadas.[31]

7.1 Infiltração de Agentes Policiais nas Investigações de Cibercrimes

A democratização do uso da rede mundial de computadores além de oferecer enormes vantagens, também facilitou a pratica de crimes, e é evidente a dificuldade que as autoridades possuem para identificar e combater estes criminosos. Com a evolução das condutas criminais no ambiente virtual, houve também a necessidade de aprimoramento da inteligência policial, e a infiltração de agentes no ambiente cibernético, portanto, se tornou essencial para o combate ao cibercrime.[32]

A infiltração de agentes policiais no mundo virtual, é lícita para investigação nos crimes de organização criminosa, tráfico de drogas, pornografia infantil, pedofilia e ciberterrorismo. A Lei 13.441/17[33], regulamenta a infiltração de agentes de polícia na internet com a finalidade de investigar crimes contra a dignidade sexual de criança e de adolescente. Nos procedimentos de investigação, da mesma forma que os criminosos possuem técnicas que os mantém anônimos na rede, as autoridades policiais rastreiam possíveis vulnerabilidades destes criminosos coletando provas dos delitos, utilizando também do anonimato oferecido pela Deep Web e Dark Web.[34]

Ainda neste sentido os acordos internacionais ratificados pelo Brasil para cooperação e combate ao Cibercrime, favorece a comunicação entre os países e favorece a assistência e comunicação destes no combate ao crime virtual. Neste sentido, Domingos (2017, p. 247-248) afirma que:

> Nos delitos cibernéticos de disseminação de pornografia infantil via web, é comum que no bojo dessas investigações em determinado país sejam identificados IP's e

[31] SANTOS,L.R; MARTINS, L.B; TYBUCSH,F.B.A. **Os Crimes Cibernéticos e o Direito a Segurança Jurídica: Uma Análise da legislação Vigente no Cenário Brasileiro Contemporâneo**. Anais do 4º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede. Santa Maria-RS, 2017.
[32]PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia- GO, 2019.

[33] BRASIL. **Lei nº 13.441, de 08 de maio de 2017.**
[34] PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia- GO, 2019

> dados de conexão utilizados na prática criminosa de usuários de Internet pertencentes a outro país. Situação em que a polícia desse país e envia as informações para o país onde os IP's identificados são alocados para que as investigações sejam desenvolvidas com relação às imagens e vídeos disseminados a partir desse local, tanto por ser de atribuição do país investigar e processar os delitos cometidos a partir de seu próprio território, quanto por ser mais provável que o criminoso seja identificado no local de onde disseminou as imagens e vídeos. Nesses casos, em que há a troca pelas autoridades competentes de diferentes estados de informações relevantes às investigações que ocorre em geral por intermédio da INTERPOL, há a presunção de regularidade na obtenção e transmissão de tais informações conforme a legislação do país de origem. No entanto, afigura-se prudente que os investigadores submetam a prova ao Judiciário para validação e autorização de uso.[35]

No Brasil a Polícia Federal desencadeou duas grandes operações de combate aos crimes cibernéticos, ambas com o intuito de combater a pornografia infantil. Utilizando um método inédito de investigação, os policias conseguiram burlar o anonimato oferecido pelos ambientes da internet obscura, onde não é possível identificar o IP, e identificaram mais de 90 usuários que acessam e compartilham pornografia infantil. Estas operações demonstram que o serviço de investigação brasileiro tem avançado significativamente no ambiente virtual, apesar das falhas na legislação, e das vantagens oferecidas pela Deep Web e Dark Web aos criminosos.[36]

8 CONSIDERAÇÕES FINAIS

O texto em questão abordou o conceito e as características dos crimes virtuais, que se tornaram tão evidentes nos últimos anos com o surgimento e desenvolvimento do ambiente cibernético, expondo as falhas na legislação vigente e a dificuldade na identificação dos criminosos, devido ao modo como a rede virtual funciona. Com isso, o surgimento de técnicas especiais de investigação no ambiente virtual foi uma prática que acarretou um avanço no combate aos criminosos, dentre elas a infiltração policial.

Ainda que algumas técnicas investigativas tenham avançado, a existência de cibercrimes ainda é um fator alarmante e preocupante, o anonimato oferecido pela internet obscura aos criminosos além de dificultar a identificação dos criminosos, permite que muitos delitos não sejam se quer descobertos. Nestes ambientes, o crime de pornografia infantil é o mais comum, onde pedófilos compartilham e armazenam imagens, vídeos de abuso sexual de crianças, atos libidinosos contra menores, em fóruns na Deep Web. Estes crimes na maioria das vezes são praticados por organizações criminosas, com o objetivo de obter vantagem financeira com a comercialização destes arquivos.

---

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

[36] POLICIA FEDERAL. **Combate a disseminação de pornografia infantil pela deep web no Rio Grande do Sul**. 15 de outubro de 2014.

Com a facilidade com que dados são violados no ambiente virtual, é muito importante que haja cautela no uso da rede informática, devendo sempre estar atento a possíveis ameaças à invasão da privacidade e roubo de dados. Além disso, crianças e adolescentes devem sempre ser monitorados acerca dos sites que frequentam, pois na maioria das vezes são atraídos por perfis falsos que usam da astúcia para engana-los e influencia-los a enviar fotos e vídeos de si mesmo, que contenham nudez ou ato libidinoso, o que certamente será compartilhado e vendido na Deep Web ou Dark Web.

Além da dificuldade de identificar o criminoso há ainda a preocupação em fazer com as provas obtidas na investigação sejam legítimas para ensejar uma decisão judicial favorável a vítima. A perícia deve trabalhar conjuntamente na investigação criminal a fim de auxiliar o caso, para que o inquérito policial apresente legitimidade, e para isso as provas periciais são bastante necessárias. Deste modo o auxílio da Perícia Forense Computacional, especializada na coleta de evidências digitais em computadores se constitui peça chave para a eficácia no combate aos cibercrimes.

Para que o combate ao cibercrime seja eficiente é importante o comprometimento em relação à criação de Leis mais específicas e efetivas, maior realização de acordos internacionais de cooperação para o fornecimento de informações, além de investir em perícias científicas e especializadas em tecnologia, policias investigativas, melhoramento das estruturas, equipamentos, e treinamento, como também implantar núcleos especializados em combate a crimes cibernéticos em cada estado.

9 REFERÊNCIAS

ABREU, Leandro Farias dos Santos. **A Segurança das Informações nas Redes Sociais**. Disponível em: http://www.fatecsp.br/dti/tcc/tcc0023.pdf. Acesso em: 05 de maio.2021.

ALBUQUERQUE, Roberto Chacon de. **A Criminalidade Informática**. São Paulo: Editora Juarez de Oliveira, 2006.

BRASIL (1990a**). Lei n. 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências (ECA)**. Disponível em: Acesso em: 05 de maio de 2021.

BRASIL. Lei nº 11.829, de 25 de novembro de 2008. **Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007- 2010/2008/lei/l11829.htm. Acesso em: 06 de maio de 2021.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckman).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011 2014/2012/lei/l12737.htm. Acesso em: 05 de maio de 2021.

BRASIL. **Lei nº 13.441, de 08 de maio de 2017.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13441.htm. Acesso em: 05 de maio de 2021.

BORGES, C. B.; SARTORI, L. P.; BARROS, S. M. **A Deep Web e a relação com a criminalidade na internet**. Direito & TI. Porto Alegre, 07 de dezembro de 2018. Disponível em: http://direitoeti.com.br/artigos/a-deep-web-e-a-relacao-com-a-criminalidade-na-internet/. Acesso em: 05 de maio de 2021.

CABETTE, E. L. S, NAHUR, M. T. M. **Criminalidade Organizada & Globalização Desorganizada**. Rio de Janeiro: Freitas Bastos. Disponível em: https://ambitojuridico.com.br/site/?. Acesso em: 05 de maio de 2021.

CARAMIGO, Denis. **Pedofilia não é um crime, mas, sim uma doença**. Conjur, 2017. Disponível em: https://www.conjur.com.br/2017-nov-10/denis-caramigo-pedofilia-nao-crime-sim-doenca. Acesso em: 14 de junho, 2021.

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

GRECO, Rogério. **Código Penal: comentado-5. ed**. -Niterói, RJ: Impetus, 2011.
INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004.

LANDINI, Tatiana Savoia. **Pornografia infantil na Internet: violência sexual ou pornografia?** Sociologia, USP. S.Paulo, 2000.

MAIA, Teymisso Sebastian Fernandes**. Análise dos Mecanismos de Combate aos Crimes Cibernéticos no Sistema Penal Brasileiro** / Teymisso Sebastian Fernandes Maia. – 2017. Disponível em: http://repositorio.ufc.br/bitstream/riufc/31996/1/2017_tcc_tsfmaia.pdf. Acesso em: 06 de maio de 2021.

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

PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia, 2019. Disponível em: http://repositorio.anhanguera.edu.br:8080/bitstream/123456789/227/1/TCC%20CAP.%201%2c%202%20E%203%20GLEICE.pdf. Acesso em: 01 de maio de 2021.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4 ed. Saraiva: São Paulo, 2010.

POLICIA FEDERAL. **Combate a disseminação de pornografia infantil pela deep web no Rio Grande do Sul**. 15 de outubro de 2014. Disponível em:

http://www.pf.gov.br/agencia/noticias/2014/10/pf-combate-a-disseminacao-de-pornografia-infantil-pela-deep-web-. Acesso em: 06 de maio de 2021.

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

SANTOS, L.R; MARTINS, L.B; TYBUCSH, F.B.A. **Os Crimes Cibernéticos e o Direito a Segurança Jurídica: Uma Análise da legislação Vigente no Cenário Brasileiro Contemporâneo**. Anais do 4º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede. Santa Maria-RS, 2017. Disponível em: http://coral.ufsm.br/congressodireito/anais/2017/7-7.pdf. Acesso em: 02 de maio de 2021.

SILVA, *et al*. **Livre Manifestação do Pensamento Correlato ao Marco Civil da Internet**. Revista de Direito do Centro Universitário FG- UNIFG, ano 1, nº1, out.2015. Disponível em: http://revistas.faculdadeguanambi.edu.br/index.php/Revistadedireito/article/view/18/94. Acesso em: 04 de maio de 2021.

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

TEFFÉ, C.S; MORAES, Maria Celina B. **Redes Sociais Virtuais: privacidade e responsabilidade civil análise a partir do marco civil da internet.** Pensar, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017. Disponível em: https://periodicos.unifor.br/rpen/article/view/6272. Acesso em: 02 de maio de 2021.

WENDT, Emerson. **Crimes Cibernéticos: ameaças e procedimentos de investigação**/ Emerson Wendt; Higor Vinicius Nogueira Jorge. -2. Ed. – Rio de Janeiro: Brasport,2013.