BUSCA E APREENSÃO INFORMÁTICA E PERÍCIA DIGITAL: A SUA IMPORTÂNCIA PARA A APURAÇÃO DA MATERIALIDADE E AUTORIA NO DELITO CIBERNÉTICO DA CIBERPEDOFILIA

Loyse Aracelli Silva Rocha Vieira[1]

RESUMO: Tendo em vista a necessidade de uma rediscussão de questões emergentes e de interesse social amplo, como é o caso da pedofilia, especialmente quando reiteradas ações e práticas indevidas são perpetradas por meio da rede mundial de computadores em evidente afronta aos direitos fundamentais em face da criança e do adolescente, é imperioso que o Direito acompanhe essas transformações e fatos sociais. É nesse cenário que a pesquisa em alusão se debruçará na problemática de cunho predominantemente jurídico, e será realizada através de uma pesquisa multidisciplinar, haja vista que os estudos que envolvem a Ciberpedofilia rompem as barreiras do entendimento jurídico e perpassam áreas de conhecimento como a Psicologia, a Sociologia, Tecnologia da Informação e demais campos da Ciência, viabilizando uma análise mais profunda e indispensável à construção de novas abordagens que promovam a real proteção dessas pessoas em formação. A metodologia empregada é predominantemente teórica, tendo por coleta de dados pesquisa na doutrina, legislação e jurisprudência pátrias; e métodos de pesquisa conceitual, histórico, bem como estudo de caso. O objetivo geral do artigo em epígrafe conforma-se em pesquisar o caminho percorrido pela Polícia e pelo Judiciário na persecução de delinquentes informáticos por meio da busca e apreensão informática e perícia digital; sendo objetivos específicos trazer proposições que possam colaborar para a evolução do Direito Digital e da Perícia Forense Digital. Resultados demonstram que muito ainda deve e precisa ser feito no combate à pedofilia, especialmente na seara do Direito Digital e da Perícia Forense Digital.

Palavras-chave: Crianças e Adolescentes. Direito Penal. Cibercrime. Ciberpedofilia. Direito Digital.

ABSTRACT: Considering the necessity of a discussion on outcoming questions of wide social interest, such as pedophilia, especially when repeated acts and undue practices are perpetrated through the global computer network in clear violation of fundamental rights in the face of the child and the adolescent, it is imperative that the law accompany these transformations and social facts. It is in this scenario that the research in allusion will focus on the predominantly juridical problem, and will be performed through a multidisciplinary research, since the studies that involve Cyberpedophilia break the barriers of the legal understanding and pass through areas of knowledge such as Psychology, Sociology, Information Technology and other fields of science, enabling a deeper and indispensable analysis to the construction of new approaches that promote the real protection of these people in formation. The methodology used is predominantly theoretical, having as data collection research in doctrine, legislation and Brazilian jurisprudence; and conceptual, historical research methods as well as case study. The general objective of this article is to investigate the path taken by the Police and the Judiciary in the prosecution of computer criminals through computer search and seizure and digital expertise; being specific objectives to bring propositions that can collaborate for the evolution of the Digital law and the Digital

[1] E-mail: loyse_jurista@outlook.com.
Revista de Direito UNIFACEX, Natal-RN, v.7, n.1, 2018. ISSN: 2179-216X. Paper avaliado pelo sistema blind review, recebido em 27 de novembro, 2017; Aprovado em 9 de fevereiro, 2018.

Forensic Expertise. Results demonstrate that much still needs to be done in the fight against pedophilia, especially in Digital Law and Digital Forensic Expertise.

Keywords: Children and adolescents. Criminal law. Cybercrime. Cyberpedophilia. Digital law.

1 INTRODUÇÃO

A escolha do tema que norteou a pesquisa em epígrafe resultou da constatação de reiteradas ações e práticas indevidas perpetradas por meio da rede mundial de computadores em evidente afronta aos direitos fundamentais em face da criança e do adolescente, pessoas humanas em formação.

Assim, a Constituição da República Federativa do Brasil, promulgada em 5 de outubro de 1988, encontrou um dos seus maiores desafios: concretizar os direitos fundamentais, frutos de conquistas históricas gradativas da pessoa humana, a nível mundial, constitucionalizados a partir da Segunda Guerra Mundial e internalizados nos ordenamentos jurídicos de diversos países em todo o mundo.

A Constituição pátria além de expressar vasta previsão normativa de direitos e garantias fundamentais e sociais, instituiu um Estado Democrático de Direito destinado a garantir o pleno exercício dos Direitos Fundamentais Sociais, consoante prolata seu Preâmbulo Constitucional.

É nesse cenário que o presente trabalho, à luz da Constituição Federal pátria, tratará da proteção à criança e ao adolescente ante a nova ferramenta utilizada por criminosos para o cometimento da pornografia e exploração sexual infantil amplamente disseminado por meio da rede mundial de computadores: a *Ciberpedofilia*.

A suscitada problemática é de cunho predominantemente jurídico, merecendo espaço para discussão e será realizada através de uma pesquisa multidisciplinar percorrendo áreas de Direito Constitucional, Estatuto da Criança e do Adolescente, Direito Penal, correlacionando-os com a Psicologia, Sociologia, Tecnologia da Informação, entre outros, a respeito da *Ciberpedofilia*.

Serão apresentadas proposições para a casuística em análise, na compreensão de que se faz extremamente necessário que o Direito transcenda do plano teórico para a realidade.

A justificativa para a abordagem proposta revela-se na pertinência do tema para a nossa sociedade, vez que as crianças e adolescentes são pessoas humanas em formação, merecendo apreço e tratamento prioritário e diferenciado como consigna a Constituição Federal, assegurando-lhes que é dever da família, do Estado e de toda a sociedade à proteção integral aos mesmos.

A metodologia empregada para a consecução dos objetivos traçados para o trabalho em alusão é a de análise normativa, doutrinária e jurisprudencial; tendo como métodos de pesquisa conceitual, histórico, bem como estudo de caso.

O objetivo geral do trabalho em alusão conforma-se em pesquisar o caminho percorrido pela Polícia e pelo Judiciário na persecução de delinquentes informáticos por meio da busca e apreensão informática e perícia digital; sendo objetivos específicos trazer proposições que possam colaborar para a evolução do Direito Digital e da Perícia Forense Digital, bem como aproximar o Ordenamento Jurídico brasileiro dessa realidade cometida em ambiente virtual.

Deseja-se despertar a sociedade para defesa, maior cuidado e proteção a essas pessoas em formação, tão carentes de serem ouvidas, acreditadas, e libertadas de feridas tão profundas, que têm sido sufocadas e caladas pela insensibilidade e negligência daqueles que devem garantir com prioridade e integralidade seus direitos fundamentais.

É essa, destarte, a proposta que se pretende desenvolver, dentro da objetividade que a matéria e a pedagogia do presente artigo permitem.

2 O QUE É PEDOFILIA?

Não raro, infelizmente, noticiam-se casos sobre pedofilia por meio da televisão, rádio e, atualmente, largamente explorado na rede mundial de computadores. É um assunto doloroso, que causa grande repercussão em toda sociedade, e que precisa ser tratado com todo cuidado por tratar-se de violência que atinge diretamente a criança e o adolescente.

É imperioso destacar que o nosso ordenamento jurídico pátrio tem legislação própria para a proteção da criança e do adolescente (BRASIL, 2017, p. 925), proteção também consagrada pela Constituição de 1988 (BRASIL, 2017, p. 74) como garantia fundamental. A propósito, alude o artigo 5° do Estatuto da Criança e do Adolescente a respeito de tal proteção, que “Nenhuma criança ou adolescente será objeto de qualquer forma de negligência,

Revista de Direito UNIFACEX, Natal-RN, v.7, n.1, 2018. ISSN: 2179-216X. Paper avaliado pelo sistema blind review, recebido em 27 de novembro, 2017; Aprovado em 9 de fevereiro, 2018.

discriminação, exploração, violência, crueldade e opressão, punido na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais." (BRASIL, 1990, p. 925).

Mas, afinal, o que é pedofilia? Nas palavras de Lillian Ponchio e Silva et al. (2013, p. 9), pedofilia "é uma perversão". Seguem ainda os autores trazendo a distinção entre o que é pedofilia e quem é o pedófilo: Pedofilia é uma perversão. O perverso sofre de um desvio de comportamento. O indivíduo pedófilo é um adolescente ou um adulto que padece de perversidade. Esses indivíduos sentem-se sexualmente atraídos por crianças impúberes (sem características femininas ou masculinas adultas). Acrescentam que a Organização Mundial da Saúde (OMS) considera a pedofilia não só como desvio sexual, mas como desordenamento mental e também de personalidade do indivíduo.

Jane Felipe (2006, online), no artigo "Afinal, quem é mesmo pedófilo?" oferece uma abordagem importante sobre essa questão. Enuncia a referida autora, que é imperioso lembrar que, o termo pedofilia, em suas origens, designava o amor de um adulto pelas crianças (do grego *paidophilos*: pais = criança e *phileo* = amar). Ressalta, no entanto, que a palavra tomou outro sentido e que passou a ser designada para caracterizar comportamentos socialmente inadequados e cita que, de acordo com o Catálogo Internacional de Doenças (CID), a pedofilia é considerada um transtorno de preferência sexual, classificada como parafilia (para = desvio; filia = aquilo para que a pessoa é atraída), bem como uma perversão sexual. O CID é bastante minucioso no que se refere à classificação de tais transtornos, sendo a pedofilia assim definida como:

> Uma preferência sexual por crianças, usualmente de idade pré-puberal ou no início da puberdade. Alguns pedófilos são atraídos apenas por meninas, outros apenas por meninos e outros ainda estão interessados em ambos os sexos. A pedofilia raramente é identificada em mulheres. Contatos entre adultos e adolescentes sexualmente maduros são socialmente reprovados, sobretudo se os participantes são do mesmo sexo, mas não estão necessariamente associados à pedofilia. Um incidente isolado, especialmente se quem o comete é ele próprio um adolescente, não estabelece a presença da tendência persistente ou predominante requerida para o diagnóstico. Incluídos entre os pedófilos, entretanto, estão homens que mantêm uma preferência por parceiros sexuais adultos, mas que, por serem cronicamente frustrados em conseguir contatos apropriados, habitualmente voltam-se para crianças como substitutos. Homens que molestam seus próprios filhos pré-púberes, ocasionalmente seduzem outras crianças também, mas em qualquer caso seu comportamento é indicativo de pedofilia. (FELIPE, 2006, p. 213).

Como se pôde observar, há divergências no que tange o conceito de pedofilia. A Organização Mundial da Saúde (OMS) define pedofilia como desvio sexual, desordem mental e de personalidade, ao passo que o Catálogo Internacional de Doenças (CID) a define como

um transtorno de preferência sexual e perversão sexual. Mas, entende-se, para o que se destina a problemática do trabalho em alusão que tanto a OMS quanto o CID concordam em um ponto: a pedofilia é um transtorno, ou mesmo em outras palavras, um desvio sexual.

Para reforçar tal conclusão, segundo o Míni Aurélio – O Dicionário da Língua Portuguesa, o termo desvio (FERREIRA, 2010, p. 249), em síntese significa "ato ou efeito de desviar (-se) da posição normal", já o termo transtorno (FERREIRA, 2010, p.752), seria "1. Ato ou efeito de transtornar (-se); 2. Contrariedade; 3. Desarranjo, desordem."

Desta feita, adota-se para fins didáticos e práticos no presente artigo, o termo pedofilia como sendo um transtorno e perversão sexual. Após direcionamento do trabalho em epígrafe sobre o entendimento adotado para o termo pedofilia, uma questão surge: A pedofilia é uma perversão, um transtorno de preferência sexual; mas, quem é o pedófilo?

Sobre esse questionamento, Lillian Ponchio et al. (2013, p. 47-48) assinalam que:

> Um pedófilo não é, necessariamente, um criminoso. Uma pessoa pode sentir atração por crianças e manter-se afastada delas, sem cometer nenhum abuso sexual. Além disso, o pedófilo não possui características físicas que o distinguem. (...). Assim, por fora, ninguém desconfia de um pedófilo que, internamente e com frequência, pensa em sexo com crianças, violência e demais formas de abuso sexual.

No entanto, os referidos autores salientam ainda:

> Não há dúvidas de que o foco principal deve ser sempre a criança, a pessoa em desenvolvimento físico, psicológico e sexual, isto é, a vítima do crime. No entanto, é preciso conferir atenção também ao pedófilo, isto é, tratá-lo realmente como pessoa, e não como "monstro". O abuso sexual que ele (eventualmente) materializa é decorrente da doença que o acomete, ainda que geralmente se manifeste de modo a causar asco social. (...). Todavia, a pessoa que sofre dessa doença carrega um fardo muito pesado. O pedófilo não comete o crime "por safadeza" (como se costuma ouvir normalmente). Muitas vezes o pedófilo não procura tratamento assim que percebe que está tendo fantasias sexuais envolvendo criança e depois não consegue se controlar. (PONCHIO et al., 2013, p.49).

Ante as definições aqui abordadas concernentes aos termos pedofilia (substantivo) e pedófilo (adjetivo), por óbvio que os meios de comunicação fazem uso equivocado dos mesmos e tornaram-se costumeiros quando se trata de infrações penais contra crianças ligadas às questões de sexo e outras formas de abusos sexuais. (PONCHIO et al., 2013, p. 28).

Após o destaque sobre a divergência quanto aos sentidos dos termos aqui tratados, Lillian Ponchio et al. (2013, p.29) ressaltam que a Medicina Legal considera a pedofilia como uma perversão sexual e que não se trata de um termo ontologicamente jurídico, mas de origem médica.

Diante da exposição feita até aqui e estabelecidas as necessárias distinções terminológicas, já é possível afirmar-se que o Direito Penal brasileiro não protege a criança e o adolescente em relação à um crime de pedofilia, mas apenas dos comportamentos que podem ser praticados pelo indivíduo que apresenta perversão sexual pedófila, e que, no entanto, também podem ser perpetrados por quem não é pedófilo. (PONCHIO et al., 2013, p.30)

Assim, observa-se que o Direito Penal pune a ação pedófila, bem como resta configurado que esta pode ser perpetrada por um indivíduo doente, com transtorno mental; e também por quem não é pedófilo.

3 CRIMES INFORMÁTICOS

A informática é a ciência dedicada ao tratamento da informação mediante o uso de computadores e demais dispositivos de processamento de dados. E, neste sentido, a boa prática impõe que os tipos sejam nominados de acordo com o bem jurídico que visam proteger. (JESUS; MILAGRE, 2016, p. 49) Desta feita, Crime Informático é um fenômeno inerente às transformações tecnológicas que a sociedade experimenta e que influenciam diretamente no Direito Penal. (JESUS; MILAGRE, 2016, p.48)

No entendimento de Stein Schjolberg:

> As recomendações da *Organization for Economic Cooperation and Development* (OECD), de 1986, conceituam crime eletrônico no seguinte sentido: "qualquer comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados e, transmissão de dados, podendo implicar a manipulação de dados ou informações, a falsificação de programas, o acesso e/ou o uso não autorizado de computadores e redes. (SCHJOLBERG apud JESUS; MILAGRE, 2016, p. 48).

Damásio de Jesus e José Antônio Milagre (2016, p. 49) conceituam crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal.

No Brasil, escolheu-se nomear crimes cometidos contra a informática de "delitos informáticos", termo usual em países de língua espanhola que se relaciona à ideia de proteção do objeto jurídico informática e informação. (JESUS; MILAGRE, 2016, p. 49)

O crime virtual, em tese, era considerado um crime-meio, em que se utiliza um meio virtual. Assim reforçava Patrícia Peck Pinheiro (2014, p. 307) que o mesmo não é crime-fim por natureza, isto é, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por *hackers*, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros.

Diversamente entendem Jesus e Milagre (2016, p. 49) a respeito de crime virtual. Os mesmos preceituam que o crime virtual pode ser um crime-meio, mas vem se desenvolvendo como crime-fim, o que, aliás, demandou a tipificação de alguns crimes informáticos próprios, promovendo a edição das Leis n°. 12.735/2012 (BRASIL, 2012, online) e n°. 12.737/2012 (BRASIL, 2012, online). Ademais, prosseguem os professores, "não só *hackers* podem praticar um crime-fim informático, mas qualquer pessoa".

Consoante as palavras de Jesus e Milagre (2016, p. 50), o "fato é que a maior parte dos crimes eletrônicos está relacionada a delitos em que o meio para a realização da conduta é virtual, mas o crime em si não." É a partir daqui que se aprofundará a problemática do trabalho em alusão.

A *Ciberpedofilia* pode então ser definida como um delito informático em que a conduta do agente é virtual, mas o crime em si não. Pois veja-se que, primeiramente houve crime real de abuso/violência sexual infantil quer seja através de sexo com a criança, fotografias em cenas de sexo com criança ou na presença delas, gravação em vídeos ou outros meios em que a criança sofreu um abuso/violência real e, que, posteriormente teve sua imagem, honra, sexualidade, dignidade, inocência expostos e violados via ambiente virtual. Há, destarte, um crime que cresce sem proporções em todo o mundo via rede mundial de computadores: um cibercrime.

Sobre a nomenclatura, doutrinadores em todo o mundo procuram classificar os crimes digitais. No entendimento de Fabrízio Roza apud Jesus e Milagre:

> Kohn, utiliza *computer criminals* para designar seus praticantes. Jean Pearl e Cristian Feuliard referem-se a 'infrações cometidas por meio de computador'. Há ainda quem prefira a expressão 'crimes de computador', 'cybercrimes', 'computer

> crimes', 'delito informático', 'crimes virtuais', 'crimes eletrônicos' ou, ainda, 'crimes digitais', 'crimes cibernéticos', 'infocrimes', 'crimes perpetrados pela internet', denominações distintas, mas, que, no fundo, acabam por significar basicamente a mesma coisa. (ROZA apud JESUS; MILAGRE, 2016, p. 50).

Damásio de Jesus e José Antônio Milagre classificam os crimes informáticos da seguinte forma:

> *a) crimes informáticos próprios*: em que o bem jurídico ofendido é a tecnologia da informação em si. Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente;
> *b) crimes informáticos impróprios*: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais;
> *c) crimes informáticos mistos*: são crimes complexos em que, além da proteção do bem jurídico informático (inviolabilidade de dados), a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico;
> *d) crime informático mediato ou indireto*: trata-se de delito informático praticado para a ocorrência de um delito não informático consumado ao final. Em Direito Informático, comumente um delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial. Como, por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consunção, o agente só será punido pelo delito-fim (furto). (JESUS; MILAGRE, 2016, p.52) (grifos dos autores).

Marcelo Xavier de Freitas Crespo (2011, p. 63), entende que a simples utilização de um computador para a perpetração de um delito como um estelionato não deveria ser considerada, com precisão técnica, um crime informático. Alude o referido autor, que não só autores, mas as mídias em geral, convencionaram denominar crimes informáticos quaisquer delitos praticados com o uso da tecnologia informática, seja ela o instrumento da conduta, seja o objeto do ilícito. Destarte, concorda o autor, que apesar de não ser a precisão mais técnica, é impossível ignorá-la, dada sua particularidade acadêmica e, por que não, social, vez que mesmo a mídia em geral vale-se de tal classificação.

Ante o demonstrado, resta claro que com o advento da informática e a velocidade de informação, o compartilhamento de material que expõe a criança e o adolescente, afrontando sua imagem, intimidade e privacidade, dissemina-se em tempo real, propiciando ao delinquente informático um mercado amplamente lucrativo para a prática da *Ciberpedofilia*, delito em que a dignidade dessas pessoas em formação é ignorada.

4 CIBERPEDOFILIA E O ESTATUTO DA CRIANÇA E DO ADOLESCENTE

O art. 241-A tipifica vários comportamentos, que vão desde o oferecimento, troca, disponibilização, transmissão até divulgação de imagens envolvendo pornografia ou cenas de sexo explícito com crianças e adolescentes, via rede mundial de computadores (ROSSATO; LÉPORE; CUNHA, 2012, p. 565), conceituados no presente artigo como *Ciberpedofilia*.

> 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:
> *Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa*. [*Caput* acrescentado pela Lei n. 11.829, de 25 de novembro de 2008]
> § 1° Nas mesmas penas incorre quem: [Incluído pela Lei 11.829, de 25 de novembro 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 n. 11.829, de 25 de novembro 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 n. 11.829, de 25 de novembro de 2008]
> § 2° As condutas tipificadas nos incisos I e II do § 1° 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 n. 11.829, de 25 de novembro de 2008]. (BRASIL, 2017, p. 954).

O sujeito ativo do delito *in supra* é qualquer pessoa (crime comum).

O sujeito passivo é a criança (até doze anos incompletos) ou o adolescente (até dezoito anos incompletos).

São sete as ações nucleares típicas referidas no art. 241-A. São elas: oferecer (propor para aceitação); trocar (substituir); disponibilizar (permitir o acesso); transmitir (remeter de um local ao outro); distribuir (proporcionar a entrega); publicar (tornar manifesto); divulgar (difundir, propagar).

O aludido artigo apresenta o dolo como tipo subjetivo, isto é, a vontade consciente de praticar uma das condutas previstas no tipo penal (tipo misto alternativo).

Concernente a consumação e tentativa, revela-se na prática de uma das ações nucleares típicas. O tipo penal não exige comprovação do efetivo acesso do usuário ao material relacionado à pedofilia divulgado pelo agente.

No que diz respeito à disponibilização ou divulgação, atos de disponibilizar e divulgar, a consumação pode se prolongar no tempo.

Ressalta-se que todas as ações nucleares estão ligadas à difusão do material pornográfico já produzido, recaindo assim, sobre fotografia, vídeo, ou outro registro que contenha cena de sexo explícito ou pornográfica que envolva crianças e adolescentes. (ROSSATO; LÉPORE; CUNHA, 2012, p. 566-567).

Ante estudo detalhado do artigo 241-A, para que não se torne cansativa ou demasiadamente longa a leitura, cita-se o art. 241-C, elucidando-se que é punido o agente que simula a participação de criança e adolescente em cena de sexo explícito ou pornográfica por meio de adulteração (falsificação), montagem (sobreposição de imagens) ou modificação (alteração) de fotografia, vídeo ou quaisquer formas de representação visual (PONCHIO et al., 2013, p. 138).

Por sua vez, o art. 241-D, prolata que é crime aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso. Os incisos I e II acrescentam: a) quem facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso; b) quem pratica as condutas descritas no *caput* do referido artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita. (PONCHIO et al., p. 139-140).

Jesus e Milagre ressaltam ainda que é frequente o tipo de assédio a que se refere o art. 241-D pela internet e redes sociais, seja por meio de salas de bate-papo ou programas de relacionamento tais como MSN, MySpace, Facebook, Skype, dentre outros, e que, na maioria dos casos, o pedófilo se aproxima virtualmente da criança e pede para que ela fique nua ou mostre algumas partes do corpo via webcam. (PONCHIO et al., 2013, p. 140).

Infere-se nos tipos aqui abordados o quanto se faz necessária uma maior discussão em toda sociedade sobre a problemática de que trata a pesquisa em epígrafe: “BUSCA E APREENSÃO INFORMÁTICA E PERÍCIA DIGITAL: A SUA IMPORTÂNCIA PARA A APURAÇÃO DA MATERIALIDADE E AUTORIA NO DELITO CIBERNÉTICO DA CIBERPEDOFILIA”.

É imperioso lembrar que o nosso Código Penal vigente (BRASIL, 2017, p. 516) também expressa tipos penais cometidos contra crianças e adolescentes, como por exemplo, ‘a satisfação de lascívia mediante presença de criança ou adolescente’, constante no art. 218-A; ‘favorecimento da prostituição ou outra forma de exploração sexual de vulnerável’, consoante art. 218-B do referido *Códex* e outros tipos de abuso/violência sexual em face da criança e do adolescente que não serão detalhados aqui por tratar-se o trabalho em alusão de formas de abuso/violência em face da criança e do adolescente na seara digital, virtual, informática, no *ciberespaço*.

5 CIBERPEDOFILIA E A INVESTIGAÇÃO CIBERNÉTICA

Aborda-se aqui, ainda que sucintamente, a Lei que é considerada a “Constituição da Internet” – Lei n° 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil; bem como se apresentam propostas ou caminhos para inibição do crime de pornografia infantil on-line e caso prático de ação e combate a pornografia infantil via internet. (BRASIL, 2014, p. 1638).

5.1 MARCO CIVIL DA INTERNET E A INVESTIGAÇÃO CIBERNÉTICA

Embora muito necessite evoluir o Direito Digital pátrio para solucionar os problemas relativos ao cometimento de crimes cibernéticos, a Lei n°. 12.965/2014, “O Marco Civil da Internet”, é considerada uma grande conquista para a sociedade brasileira.

Nessa linha de pensamento, Jesus e Milagre (2016, p. 168) entendem que a referida lei pode ser considerada a “Constituição da Internet”, garantindo direitos e deveres a todos os atores da Internet brasileira (usuários, provedores de conexão e de serviços em geral), embora reconheçam que a solução para o cometimento de crime cibernético no Brasil não é fácil de ser encontrada, pois envolve educação digital, políticas criminais e estrutura investigativa.

Explicam ainda, os referidos autores que a Lei n°. 12.737/2012 (conhecida como Lei Carolina Dieckmann), tipifica fatos cibernéticos, entretanto, não trata da estrutura investigativa ou deveres dos provedores de Internet e serviços, no que tange à cooperação para com autoridades na investigação de crimes digitais. (JESUS; MILAGRE, 2016, p. 169) Aludem, por sua vez, ainda, que a Lei n°. 12.735/2012 (BRASIL, 2012, online), prevê que os

órgãos de polícia judiciária poderão estruturar, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. (JESUS; MILAGRE, 2016, p. 168).

Até o surgimento do Marco Civil da Internet, no Brasil, inexistia lei que obrigasse os provedores de Internet ou de serviços a registrarem *logs* das atividades de seus usuários. Entretanto, existia apenas "recomendação" do Comitê Gestor Internet do Brasil, para que os provedores (de acesso) passassem a manter, pelo prazo mínimo de 3 (três) anos, dados de conexão e de comunicação realizada por seus equipamentos (identificação do endereço *IP*, data e hora de início e término da conexão e origem da chamada), o que era também o entendimento do Superior Tribunal de Justiça. (JESUS; MILAGRE, 2016, p. 169).

Jesus e Milagre (2016, p. 169) relatam ainda, que, na maioria dos crimes digitais, em que a vítima não é administradora do ativo informático utilizado para a prática do crime ou do ativo atacado, para que se averigue a autoria do delito, é imprescindível a cooperação de terceiros, que geralmente administram e ofertam os serviços, aplicações ou *hosts* utilizados para a prática dos delitos ou que sirvam de ambiente para o crime digital.

Os referidos autores explicam que dentre esses terceiros (cooperadores), os mais solicitados são os provedores de conexão à Internet. Inicialmente, pela ordem, busca-se um contato com aqueles, e, ulteriormente, com estes. (JESUS; MILAGRE, 2016, p. 169).

Ante o que foi explanado, o que ocorre quando um indivíduo se conecta a Internet? Explicam, Jesus e Milagre (2016, p. 169-170), em resposta a tal questionamento, que quando alguém se conecta à rede mundial de computadores, para boas ou más finalidades, o faz através de um *ISP* (*Internet Service Provider*), ou provedor de acesso à Internet. Tal provedor atribui ao usuário um endereço *IP* (*Internet Protocol*), ou protocolo de Internet, em uma determinada faixa de data e horário, comumente enquanto durar a conexão à Internet. Tal atribuição pode ficar registrada no provedor de conexão (registros de conexão associados a dados cadastrais). O usuário, todavia, ao interagir com serviços na Internet (hospedagem, *blogs*, e-mails, *chats*, discos virtuais, redes sociais, mensageiros, serviços de vídeos, aplicativos etc.), tem seus dados registrados por estas aplicações, o que se chama de "registro de acesso a aplicações na Internet", que contém várias informações sobre o uso do serviço *web* por tal usuário (data, hora, *IP*, fuso horário associado ao uso de determinada aplicação).

Neste ponto do trabalho em alusão, pode-se perceber que chegar à autoria de crimes cibernéticos não é impossível, como podem supor usuários da rede mundial de computadores em todo o mundo.

Nessa linha de raciocínio, infere-se que, como explanado *in supra*, diante do uso criminoso de um serviço, ainda que de forma anônima, como, por exemplo, na criação de uma comunidade, grupo, ou página destinada à pornografia infantil, sabe-se que o provedor de serviços (pagos ou gratuitos) registrará os dados de acesso à aplicação (em alguns casos, até mesmo as atividades realizadas – embora muitos afirmem que não), porém, tais registros somente serão fornecidos com ordem judicial, como afirmam Jesus e Milagre. (JESUS; MILAGRE, 2016, p. 170).

Seguem os autores explicando que, obtendo-se os dados de acesso às aplicações daquele que utilizou o serviço para más finalidades, como a prática de crimes cibernéticos, pode-se, através do *IP* (*Internet Protocol*), que será fornecido, descobrir qual o Provedor de Acesso associado ao *IP* (caso o usuário não tenha mascarado a conexão), e, desta feita, oficiá-lo, para que apresente os dados físicos (nome, endereço, RG, CPF, CNPJ, dentre outros) da pessoa responsável pela conta de Internet a qual estava atribuindo o referido *IP*, na exata data e hora da atividade maliciosa. (JESUS; MILAGRE, 2016, p. 170)

Conforme descrito acima, pode-se chegar à autoria de delitos cometidos por meio da Internet, normalmente praticado por pessoas que "não se identificam nos serviços" para criação ou acesso aos mesmos, utilizados para práticas criminosas. Resta claro, destarte, que pode ocorrer de o titular de uma conta de Internet não ser o agente criminoso; neste caso poderá responder por ter negligenciado, permitindo que terceiros acessassem seus ativos, como, por exemplo, no caso de usuário que deixa Internet a rádio, *wireless*, de sua residência, desprotegida, o que permite que terceiros acessem e pratiquem crimes por meio de sua conexão. Neste contexto, como se pode perceber, sem a cooperação dos provedores de Internet ou de serviços, em muitos casos, torna-se praticamente impossível apurar a autoria de delitos cibernéticos, e a questão se agrava quando um destes provedores não está no Brasil, como explicam Jesus e Milagre (2016, p. 170-171).

O Marco Civil expressa em seu artigo 21 e parágrafo único, que somente por ordem judicial os provedores serão obrigados a disponibilizar registros e informações que permitam a identificação de algum usuário, bem como a remoção de conteúdos só será cabível diante de

um mandado, excetuando-se os casos que contêm fotos de nudez, pois para os tais, uma mera notificação extrajudicial deverá ser atendida pelos provedores de conteúdo (JESUS; MILAGRE, 2016, p. 171-172).

No que tange à guarda de registros de conexão pelos provedores de acesso (apenas conectam o usuário à Internet), o Marco Civil prolata em seu artigo 13, que os provedores têm o dever de manter registros pelo prazo de 1 (um) ano. Porém, para os provedores de aplicações ou serviços de Internet (ofertam serviços ou utilidades na Internet), nos termos do artigo 15, deverão guardar os registros de acesso a aplicações por 6 (seis) meses. É imperioso dizer que o fornecimento dos registros somente poderá se dar por ordem judicial, sendo que autoridades administrativas, como Polícia e Ministério Público, poderão requerer aos provedores a guarda por mais tempo do que o previsto em lei, obrigando-se, no entanto, a ingressarem com o requerimento judicial dos dados. (JESUS; MILAGRE, 2016, p.172).

É relevante fazer-se uma observação no que diz respeito à responsabilização dos provedores de aplicações.

Nos moldes do artigo 18 da Lei n°. 12.965/2014, Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, tem-se que o provedor de conexão à Internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros. Entretanto, nos termos do artigo 19 da referida lei, o provedor de aplicações de Internet pode vir a ser considerado responsável por atos de terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente. O artigo, no entanto, consigna: ‘ressalvadas as disposições em contrário’. (JESUS; MILAGRE, 2016, p. 175).

Infere-se, desta feita, que poderá haver hipóteses legais em que o provedor de aplicações de Internet possa vir a ser responsabilizado por conteúdo de terceiros, ainda que ausente ordem judicial específica para a remoção de conteúdos infringentes ou violadores. Há decisões divergentes a respeito, sendo que, em muitos casos, provedores foram condenados por não atenderem notificação extrajudicial da vítima para remoção de determinado conteúdo da Internet, e, assim, o Marco Civil vem trazer um parâmetro (ainda que mínimo), evitando decisões contraditórias. (JESUS; MILAGRE, 2016, p. 175).

Não existe óbice, por fim, para eventual responsabilização criminal de diretores ou sócios de provedores de acesso ou de aplicações, desde que comprovada participação ou coautoria em crime informático ou crime cometido por intermédio da informática. (JESUS; MILAGRE, 2016, p. 175).

Ante o que foi discutido até aqui surge uma nova abordagem. A *Ciberpedofilia* é uma das ferramentas utilizadas para o cometimento do abuso sexual em face da criança e do adolescente em todo o mundo, fato impulsionado pelo advento da crescente tecnologia que atua como porta de acesso para que tal crime ganhe espaço na sociedade. Embora no ordenamento jurídico pátrio, leis e medidas estejam avançando em Direito Digital, a prática da *Ciberpedofilia* gera a falsa impressão de que o delinquente informático permanecerá impune e ocultado pela rede mundial de computadores.

Nessa linha de pensamento, Spencer Toth Sydow (2015, p. 142) expressa em sua obra que não há mais regresso na disseminação da informática, mas cabe a sociedade compreender quem dentro deste universo cada vez mais popular propõe-se a agir de modo delinquente e quem estará mais propenso a ser violado.

As linhas de investigação tanto no Brasil como ao redor do mundo se concentram em desmembrar redes de compartilhamento de materiais de conteúdo pornográfico infantil, e, para isso, têm investido em tecnologia a fim de atender a precisão das investigações objetivadas em identificar *Ciberpedófilos*.

5.2 COMPETÊNCIA PARA PROCESSO E JULGAMENTO EM AMBIENTE CIBERESPACIAL

Após breve análise das figuras criminosas relacionadas ao abuso/violência sexual em face da criança e do adolescente elencadas no capítulo 4, analisa-se a competência para o processo e o julgamento desses crimes.

Imperioso é estabelecer a regra sobre a localidade na qual deverá tramitar a ação penal.

Consoante o que foi tratado até aqui no trabalho em apreço, percebe-se que nos crimes relacionados ao abuso/violência sexual em face da criança e do adolescente muitos delitos são

praticados por meio da rede mundial de computadores (aqui tratados como *Ciberpedofilia*), instala-se, desta sorte, um debate doutrinário sobre o Juízo competente: deve ser o local no qual se deu a inserção do material ilícito na rede (efetiva publicação)? Ou o juízo competente é aquele no qual se estabelece o provedor de acesso? Qual o entendimento do Superior Tribunal de Justiça? (PONCHIO et al., 2013, p. 154).

No entendimento do Superior Tribunal de Justiça, é irrelevante o local do armazenamento dos dados. Destarte, o fator determinante é o local no qual se deu a inserção do material. Neste sentido, seguem alguns trechos que importam destacar do voto da Ministra Maria Thereza de Assis Moura (PONCHIO et al., 2013, p. 154-156), conforme aponta-se no ANEXO A do trabalho em epígrafe.

Assim, ante o entendimento do Superior Tribunal de Justiça demonstrado no ANEXO mencionado *in supra*, igualmente pensam Lillian Ponchio e Silva et al. (2013, p.156):

> Portanto, a consumação do crime de publicação de imagens de pornografia infantil na internet ocorre no ato do encaminhamento das imagens pelo agente que comete o delito, ou seja, no local onde está o computador que envia as imagens ilícitas. A localização do provedor de internet no qual as imagens estão armazenadas não interfere na determinação do juízo que processará a ação judicial.

Continuam Lilian Ponchio e Silva et al. apud decisão do Superior Tribunal de Justiça na qual este entendeu que é competência da Justiça Federal julgar crimes de estupro e outros abusos sexuais que possuam conexão com crimes de divulgação de pornografia infantil via internet, sendo, portanto, a pornografia infantil on-line crime de competência federal por ter sido tipificado em cumprimento a Tratados Internacionais ratificados pelo Brasil. (PONCHIO et al., 2013, p. 158).

Pode-se observar que, quanto à competência para o processamento dos delitos praticados via rede mundial de computadores, questões relevantes devem ser levadas em conta: o local da inserção/transmissão do material pedófilo-pornográfico, e a existência ou não da transnacionalidade do delito.

Destarte, a competência pelo lugar em que se consumar a infração (competência territorial/do local do envio dos dados) encontra supedâneo no artigo 70, do Código de Processo Penal (BRASIL, 2017, p. 595). Não sendo identificado este local, a competência recairá ao Juízo que iniciou as investigações correlatas; e compete aos Juízes Federais processar e julgar os crimes previstos em Tratado ou Convenção Internacional, quando

iniciado a execução no país, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente, conforme diligência do artigo 109, inciso V, da Constituição Federal (BRASIL, 2017, p. 44).

Ante o exposto, os maiores desafios frente o cometimento de práticas de abuso/violência sexual que maculam a dignidade de nossos infantes se referem aos avanços da tecnologia da informação, haja vista que a rede mundial de computadores é terreno fértil para violação aos direitos dessas pessoas em formação, pois é seara que o Direito Digital pátrio, que se queda ainda muito jovem, não conseguiu regular com particularidade.

A sociedade está em constante transformação, e a Tecnologia da Informação dita regras e costumes que usuários da rede mundial de computadores em todo o mundo aderem, tornando-se imprescindíveis mais debates envolvendo a proteção de crianças e adolescentes ante essa modalidade de delito cibernético tão impiedoso e que o Direito Digital brasileiro pouco conhece.

5.3 CRIME INFORMÁTICO: BUSCA E APREENSÃO INFORMÁTICA E PERÍCIA DIGITAL

Ante o exposto no subcapítulo anterior, imperioso é tratar-se aqui, ainda que sucintamente, a respeito de busca e apreensão informática e perícia digital, salientando-se que as leis de crimes informáticos não tratam deste instrumento cautelar muito útil na investigação de delitos informáticos. O instituto tem previsão legal nos artigos 240 e seguintes do Código de Processo Penal, Decreto-Lei n. 3.689, de 3 de outubro de 1941. (JESUS; MILAGRE, 2016, p. 177).

Sabe-se que diante da suspeita de crimes cibernéticos, ou mesmo com base nos dados fornecidos pelos provedores ou responsáveis pelos ativos de *TI*, pode a autoridade requerer busca e apreensão na sede ou domicílio do suposto autor do delito, para que as máquinas sejam coletadas adequadamente para a realização de perícia técnica (para a apreensão de instrumentos utilizados na prática de crime ou destinados a fim delituoso). (JESUS; MILAGRE, 2016, p. 177).

A busca e apreensão informática seguem logicamente a regra do Código de Processo Penal, sobretudo no que tange à necessidade dos agentes policiais preservarem o local do crime até a chegada dos peritos (art. 6°). A não observância destas regras pode constituir-se em nulidade. (JESUS; MILAGRE, 2016, p. 177). As infrações informáticas deixam vestígios, razão pela qual é indispensável a realização do corpo de delito. Sabe-se que a prova pericial tem importância cada vez maior e sua realização deve se adequar à uma série de cuidados, sobretudo no que diz respeito à forma de realização. O exame de corpo de delito, em verdade, é perícia no escopo de se provar a materialidade de um crime. Em crimes informáticos, comumente o corpo de delito é direto, incidindo sobre os vestígios deixados pela infração. Excepcionalmente, pode ser indireto, quando os vestígios desapareceram. (JESUS; MILAGRE, 2016, p. 178).

A busca e apreensão imprescinde de mandado judicial, nos termos do art. 243 do Código de Processo Penal. É preciso que o mandado considere detalhes específicos da informática, como, por exemplo, a possibilidade de acesso a computadores remotamente administrados da localidade, dispositivos móveis em veículos ou em posse dos residentes, dentre outras características que a autoridade deve atentar para buscas desta natureza. (JESUS; MILAGRE, 2016, p. 178).

Imperioso é destacar a importância da busca e apreensão para apuração da materialidade e autoria dos delitos informáticos. Para ilustrar-se este subcapítulo destaca-se a "Operação Mefisto no Rio Grande do Norte", conforme ANEXO B do artigo em análise. A Operação de combate à exploração sexual de crianças e adolescentes aconteceu em Natal, Mossoró, Caicó e Tibau do Sul e foi deflagrada na manhã do dia 16 de dezembro de 2016, visando identificar suspeitos e levantar dados que confirmem as provas já existentes dos crimes de exploração sexual praticados contra crianças e adolescentes através do assédio, armazenamento, produção e compartilhamento de material contendo cenas de pornografia infanto-juvenil.

Percebe-se como mencionado anteriormente, que o *ciberespaço* se reporta à uma pseudo ideia de anonimato ligada a um sentimento de intangibilidade, fruto da relação do delinquente informático diante do seu aparato tecnológico que lhe transmite uma sensação de não punibilidade face ao seu comportamento criminoso. E, tratando-se de aliciamento de

crianças e adolescentes por meio da rede mundial de computadores, tal ideia impinge-lhes o sentimento de crime perfeito, impossível de serem revelados e de deixarem vestígios.

Ante todo o exposto no trabalho em epígrafe, pode-se definir a *Ciberpedofilia* como sendo a distribuição de conteúdo sexual infantil via Internet (*ciberespaço*), que se apresenta em incontáveis páginas da *web* que podem incluir desde fotos, vídeos, áudios, textos, conversas entre usuários e/ou entre o delinquente informático e a vítima, que vão desde anúncios publicitários que ofertam a pornografia infantil da maneira mais tênue até a mais ofensiva.

A tecnologia da informação integrou o mundo em uma grande teia, onde todos têm acesso a tudo, pouco importando o local físico em que realmente esteja armazenado tal conteúdo. Ocorre que, para a Justiça, o local físico da prática de um ato digital tem relevância para determinar a competência judiciária. Não incomum, os agentes buscam praticar delitos por meio de sistemas hospedados no exterior. Nestes casos, a investigação, no Brasil, necessita da cooperação de provedores (de serviços e de conexão) de fora do país, o que não é uma tarefa fácil, considerando que parte dos provedores costuma alegar que não estão sujeitos às ordens da jurisdição brasileira (isto passa a se relativizar com a aprovação do Marco Civil da Internet). Deste modo, a Cooperação Internacional ainda é um desafio para a eficácia do combate ao crime eletrônico. Os provedores, como "portas" de entrada e saída da Internet, são os primeiros a ter responsabilidade de apurar dados de usuários que sejam seus clientes. Neste contexto, em defesas envolvendo processos de quebras de sigilo de seus usuários, a alegação de que não estão sujeitos à jurisdição brasileira, tem sido desconsiderada pelo Judiciário na grande maioria dos casos, e ainda preocupa a questão do provedor no exterior que não tem filial no Brasil. (JESUS; MILAGRE, 2016, p. 179-180).

Os estudos que envolvem a *Ciberpedofilia* rompem barreiras do entendimento jurídico e perpassam áreas que envolvem diversas vertentes de conhecimento como a Psicologia, a Sociologia, Tecnologia da Informação, Direito Digital, e demais campos da Ciência, viabilizando uma análise cada vez mais profunda e necessária à construção de novas abordagens que promovam a real proteção da criança e adolescente mediante os riscos que correm em ambiente virtual.

A proteção integral à criança e ao adolescente consigna, no artigo 227, *caput*, da Constituição Federal vigente (BRASIL, 2017, p. 74), que é dever da família, da sociedade e

do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de coloca-los à salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

As alternativas objeto de estudo do trabalho em alusão demonstram que muito ainda deve necessariamente ser feito. É uma problemática que importa a todos. A falsa ideia ligada a impunidade faz gerar na sociedade brasileira uma apatia de que denunciar não trará respostas efetivas por parte do Judiciário. Apresentam-se as seguintes proposições:

É imperioso que sejam desenvolvidas políticas públicas de combate à pedofilia e, por óbvio, um investimento maior do Estado na questão de segurança pública; campanhas de conscientização à população no que tange à sua corresponsabilidade na proteção integral e prioritária à criança ao adolescente. Além da imprescindível Cooperação Internacional devido o caráter da transnacionalidade no combate à pornografia e abuso sexual infantil, inclusive na rede mundial de computadores.

Imprescinde maior investimento público no aparelhamento, pessoal e setor de inteligência e investigação das instituições policiais em todas as esferas de sua atuação por parte do Estado, pois correspondem a prestações positivas por parte deste e demandam alocação de recursos para a sua promoção. A informação é uma grande aliada no combate ao cometimento dessa nova arma utilizada em face da criança e do adolescente.

É relevante que crianças e adolescentes tenham educação sexual nas escolas, haja vista que o tema não é obrigatório nas escolas de todo o País. É necessário que os infantes saibam diferenciar carinho de abuso/violência sexual.

Urge que mudanças na legislação sejam discutidas com toda a sociedade. É inconcebível falar em prazos prescricionais quando se trata da dignidade da pessoa humana, especialmente da dignidade sexual de pessoas humanas em formação.

A nossa sociedade precisa ser reeducada no sentido de que a criança e o adolescente são responsabilidade de todos. Não podem permanecer sufocados abusos tão graves cometidos em face de crianças e adolescentes, enquanto os agressores se utilizam de ferramentas cada vez mais nocivas, de fácil acesso e tão complexas como a rede mundial de

computadores para aliciar e seduzir as mesmas diante dos olhos de todos. Pode estar entre nós um agressor. Podem estar entre nós muitas vítimas.

O Direito Digital e a Perícia Forense Digital precisam seguir a direção das leis materiais, vez que estas necessariamente acompanham as modificações que ocorrem na sociedade. Este novo Direito impõe que autoridades das searas penal, processual penal e digital se atualizem em questões de Tecnologia da Informação (*TI*), promovendo segurança e avanços imprescindíveis para a sociedade da Informação, e a criação de novas ferramentas que coíbam o delinquente informático na prática de crimes cibernéticos. A simples tipificação de crimes digitais no Ordenamento Jurídico pátrio não têm a menor significância prática se não houver uma rediscussão sobre o tema *Ciberpedofilia* e formas de combate desse crime tão desumano.

6 CONCLUSÃO

A pedofilia é um transtorno mental, uma perversão sexual: é uma doença. Restou configurado no artigo em apreço que o pedófilo não é necessariamente um criminoso. Um indivíduo pode sentir atração por crianças e adolescentes e manter-se distante delas, sem nunca cometer quaisquer formas de abuso/violência sexual em face das mesmas. O Direito Penal apenas tutela comportamentos que podem ser perpetrados pelo indivíduo que apresenta perversão sexual pedófila, e que, por isto, também pode ser perpetrado por quem não é pedófilo. Pune-se a ação pedófila.

A presente pesquisa, conforme traçada ainda em suas linhas introdutórias, tratou da problemática do consumo sexual infantil via rede mundial de computadores, aqui denominada de *Ciberpedofilia*, com a convicta pretensão de manifestar, em todo o tempo, a partir da análise multidisciplinar da matéria discutida, contribuições na forma de proposições que confiram maior efetividade na proteção de crianças e adolescentes ante essa nova criminalidade.

O tema possui grande relevo no plano acadêmico, doutrinário, jurisprudencial, político, econômico e social, uma vez que trata da necessidade de um maior avanço e aprofundamento do Direito Digital pátrio, cabendo a toda sociedade a imperiosa missão de conferir, por mínima que seja inicialmente, condições de enfrentamento eficazes para a

coibição de práticas delitivas cometidas em ambiente virtual em face dessas pessoas humanas em formação.

Isso porque o cometimento do crime objeto de estudo no trabalho em alusão fere direitos fundamentais, garantidos pelo Direito Constitucional pátrio, bem como pelo Direito Internacional, à essas pessoas em formação para que possuam as mesmas o direito à existência digna e respeitados os seus direitos ao desenvolvimento sexual saudável e livre de toda e qualquer forma de negligência, abuso, violência, exploração e opressão.

Na esteira de buscar proposições, desafios e ferramentas de concretização para maior proteção da criança e do adolescente em face dessa nova criminalidade cometida em ambiente cibernético, e que, porém, se apresenta de forma real e violenta ante a dificuldade de se apurar quem está por trás da tela de um computador ou outros dispositivos conectados à rede mundial de computadores, é que se suscite a debatida importância da sociedade esse desafio, em face de um Direito Digital pátrio que se queda ainda muito recente e carente de maior atenção, bem como, diante das limitações impostas ao Poder Judiciário por necessitar contar com a Cooperação Internacional para se apurar essa verdadeira teia de consumo de exploração sexual e pornografia infantil.

Esse *cibercrime* impiedoso ainda se esconde por trás de uma faceta sórdida, que é o não se poder traçar um perfil claro sobre o delinquente cibernético que alicia e seduz crianças até mesmo dentro de nossas casas, por meio de dispositivo conectado à rede mundial de computadores: “Afinal, quem é mesmo pedófilo?”

Abordou-se, especialmente, leis que tratam de delitos cibernéticos e, foi dada ênfase a Lei considerada a “Constituição da Internet” – O Marco Civil da internet.

É de bom alvitre ressaltar a Operação Mefisto no Rio Grande do Norte, como meio já utilizado pela Polícia e de outros atores do Judiciário na investigação de crimes como o aqui estudado.

É dever da família, do Estado e de toda a sociedade assegurar a proteção integral à criança e ao adolescente, pois estes devem ser tratados com absoluta prioridade. Seus direitos fundamentais correspondem às situações jurídicas necessárias para a concretização de uma vida digna e aos desenvolvimentos moral, intelectual, social e sexual saudáveis e livres de

toda e qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão. Verifica-se que a presente pesquisa alcançou o seu intento de discutir, a partir do caminho percorrido pela Polícia e pelo Judiciário na persecução de delinquentes informáticos por meio da busca e apreensão informática e perícia digital; sendo objetivos específicos trazer proposições que possam colaborar para a evolução do Direito Digital e da Perícia Forense Digital para o enfrentamento do cometimento de abuso sexual infantil perpetrados via rede mundial de computadores: *Ciberpedofilia*.

Revista de Direito UNIFACEX, Natal-RN, v.7, n.1, 2018. ISSN: 2179-216X. Paper avaliado pelo sistema blind review, recebido em 27 de novembro, 2017; Aprovado em 9 de fevereiro, 2018.

REFERÊNCIAS

BRASIL. Constituição [1988]. **Constituição da República Federativa do Brasil de 1988**. *Vade Mecum* Compacto / obra coletiva de autoria da Editora Saraiva com a colaboração de Livia Céspedes e Fabiana Dias da Rocha. 17. ed. São Paulo: Saraiva, 2017.

_____. **Estatuto da Criança e do Adolescente**. Lei nº 8.069, de 13 de julho de 1990, que dispõe sobre o Estatuto da Criança e do Adolescente, e dá outras providências. *Vade Mecum* Compacto / obra coletiva de autoria da Editora Saraiva com a colaboração de Livia Céspedes e Fabiana Dias da Rocha. 17. ed. São Paulo: Saraiva, 2017.

_____. **Lei n. 12.735, de 30 de novembro de 2012**. A referida Lei altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – O Código Penal, o Decreto-Lei n. 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei n. 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: <http://www.planalto.gov.br/_ato2011-2014>. Acesso em: 26 abr. 2017.

_____. **Lei n. 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/_ato2011-2014>. Acesso em: 26 abr. 2017.

_____. **Lei n. 12.965, de 23 de abril de 2014.** Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Vade Mecum* Compacto / obra coletiva de autoria da Editora Saraiva com a colaboração de Livia Céspedes e Fabiana Dias da Rocha. 17. ed. São Paulo: Saraiva, 2017.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

FELIPE, Jane. **Afinal, que é mesmo pedófilo?** Cadernos Pagu. n. 26, p. 212,213. Jan./jun. 2006. Disponível em <http://scielo.br/pdf/cpa/n26/30391.pdf > Acesso em: 21 nov. 2016.

FERREIRA, Aurélio Buarque de Holanda. **Mini Aurélio**: o dicionário da língua portuguesa. Coord. de edição Marina Baird Ferreira. 8. ed. Curitiba: Positivo, 2010.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

OPERAÇÃO MEFISTO NO RN. Disponível em: <http://www.pf.gov.br/agencia/noticias/2016/12/pf-combate-crime-de-pornografia-infantil-no-rio-grande-do-norte>. Acesso em: 28 set. 2017.

PEREIRA, Liedna do Nascimento Silva. Licenciada em Letras/Língua Inglesa pela Universidade Federal do Rio Grande do Norte. Tradução para a Língua Inglesa do ‘Abstract’ do Trabalho em epígrafe.

PINHEIRO, Patrícia Peck. **Direito digital**. 5. ed. São Paulo: Saraiva, 2014.

ROSSATO, Luciano Alves; LÉPORE, Paulo Eduardo; CUNHA, Rogério Sanches. **Estatuto da Criança e do Adolescente comentado**: Lei nº 8.069/1990: artigo por artigo. 3. ed. São Paulo: RT, 2012.

SILVA, Lillian Ponchio et al. **Pedofilia e abuso sexual de crianças e adolescentes**. In: Coleção Saberes Monográficos. São Paulo: Saraiva, 2013.

SYDOW, Spencer Toth. **Crimes Informáticos e suas vítimas**. 2. ed. São Paulo: Saraiva, 2015. In: Coleção saberes monográficos. Coord. Alice Bianchini e Luiz Flávio Gomes.

ANEXOS

ANEXO A – ENTENDIMENTO DO SUPERIOR TRIBUNAL DE JUSTIÇA COMPETÊNCIA PARA PROCESSO E JULGAMENTO

Voto da Ministra Maria Thereza de Assis Moura

> CONFLITO NEGATIVO DE COMPETÊNCIA. PROCESSUAL PENAL. PUBLICAÇÃO DE PORNOGRAFIA ENVOLVENDO CRIANÇA OU ADOLESCENTE ATRAVÉS DA REDE MUNDIAL DE COMPUTADORES. ART. 241 DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE. COMPETÊNCIA TERRITORIAL. CONSUMAÇÃO DO ILÍCITO. LOCAL DE ONDE EMANARAM AS IMAGENS PEDÓFILO-PORNOGRÁFICAS. 1 – A consumação do ilícito previsto no art. 241 do Estatuto da Criança e do Adolescente ocorre no ato de publicação das imagens pedófilo-pornográficas, sendo indiferente a localização do provedor de acesso à rede mundial de computadores onde tais imagens encontram-se armazenadas, ou a sua efetiva visualização pelos usuários. 2 – Conflito conhecido para declarar competente o Juízo da Vara Federal Criminal da Seção Judiciária de Santa Catarina.
>
> (...). As condutas típicas investigadas se assemelham àquela descrita no art. 241 do Estatuto da Criança e do Adolescente, bem como a definida no art. 218 do Código Penal, tendo em vista que o segundo investigado, além de divulgar fotos contendo pornografia infantil, despertava em menores a concupiscência, por meio de mensagens enviadas através de correio eletrônico.
>
> Apesar das condutas encontrarem-se devidamente tipificadas, sendo, portanto, viável o exercício da pretensão punitiva estatal, não existe na doutrina nenhum consenso acerca da competência para a instrução e julgamento dos crimes cometidos através da Internet.
>
> A competência territorial é definida no art. 70 do Código de Processo penal, estabelecendo-se que, em regra, esta será determinada pelo lugar da consumação delitiva. Todavia, no caso em apreço, urge enfrentar questão espinhosa: onde ocorre a consumação em se tratando de crime cometido por meio da rede mundial de computadores?
>
> Verifica-se que o ilícito em questão prevê a conduta típica representada pelo verbo 'publicar', ou seja, tornar público material que envolva criança ou adolescente em cenas de sexo explícito.
>
> Nos dias atuais, é cediço que a rede mundial de computadores mostra-se como meio eficaz, se não o mais, a tornar públicas informações de quaisquer gêneros, e, inclusive, aquelas que a lei penal tipifica como ilícitas, ao aplicar-lhes as respectivas sanções, como é o caso do art. 241 do Estatuto da Criança e do Adolescente. É certo, ainda, que tais informações são acessíveis em qualquer parte do mundo em que se disponha de um terminal de computador conectado à referida rede. E é justamente esta diversidade de locais em que a informação pode ser acessada que revela o engessamento das normas de direito processual

> penal frente às inovações tecnológicas perpetradas pelo homem, ante a dificuldade de identificação do local da consumação do ilícito, como exige a regra geral contida no art. 70 do Código de Processo penal, para fixação da competência.
> Todavia, a melhor técnica de interpretação das normas não permite ao exegeta o distanciamento das intenções do legislador ordinário ao introduzir no ordenamento jurídico o comando normativo (...).
> Diante disso, e das informações constantes dos autos, verifica-se que, ainda que as imagens de conteúdo pedófilo-pornográfico estejam armazenadas no provedor de acesso à rede mundial de computadores, localizado na cidade de São Paulo, sabe-se, é certo, que o responsável pela veiculação de tais imagens, o qual possui autonomia no gerenciamento das informações disponibilizadas no espaço virtual fornecido pelo provedor, encontra-se na cidade de Florianópolis/SC, devendo ali serem praticados os ulteriores atos de investigação e eventual persecução penal, pois nesta localidade é que ocorreu a publicação vedada pelo tipo em apreço (...) (CC 29.886/SP – rel. Min. Maria Thereza de Assis Moura - 3ª Seção – julgamento em 12-12-2007).

SUPERIOR TRIBUNAL DE JUSTIÇA apud SILVA, Lillian Ponchio; et al. **Pedofilia e abuso sexual de crianças e adolescentes**. *In*: Coleção Saberes Monográficos. São Paulo: Saraiva, 2013, p. 154-156.

ANEXOS

ANEXO B - OPERAÇÃO MEFISTO NO RIO GRANDE DO NORTE

Agência de Notícias

PF combate crime de pornografia infantil no Rio Grande do Norte

16/12/2016

Natal/RN – A Polícia Federal deflagrou hoje (16/12), nas cidades de Natal, Tiba do Sul, Caicó e Mossoró, a **Operação Mefisto**, visando identificar suspeitos e levantar dados que confirmem as provas já existentes dos crimes de exploração sexual praticados contra crianças e adolescentes através do assédio, armazenamento, produção e compartilhamento de material contendo cenas de pornografia infanto-juvenil.

Cerca de 52 policiais federais estão cumprindo 12 mandados judiciais de busca e apreensão nos endereços residenciais de 10 pessoas investigadas, sendo 7 delas, na capital.

As investigações iniciaram em agosto, por iniciativa da Polícia Federal, devido à constatação do crescimento exponencial de crimes relacionados à exploração sexual de crianças e adolescentes por meio da internet, inclusive, com a utilização de redes sociais.

Neste trabalho investigativo, a PF conta com a colaboração da INTERPOL, cujo intercâmbio de informações foi fundamental para a identificação de um dos principais alvos da operação.

O nome da operação vem de Mefistófeles, uma entidade satânica da Idade Média, conhecida como uma das encarnações do mal, aliado de Lúcifer na captura de almas inocentes, através da sedução e encanto.

Mais informações serão repassadas durante a entrevista coletiva, que será concedida, às 10h30, na sede da Superintendência Regional da PF (Rua Dr. Lauro Pinto, 155 – Lagoa Nova - Nesta).

Comunicação Social da Polícia Federal no Rio Grande do Norte

Contato: (84) 3204.5588

Operação Mefisto no RN. Disponível em: <http://www.pf.gov.br/agencia/noticias/2016/12/pf-combate-crime-de-pornografia-infantil-no-rio-grande-do-norte>. Acesso em: 28 set. 2017.