UNIVERSIDADE FEDERAL DE CAMPINA GRANDE – UFCG
CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS – CCJS
UNIDADE ACADÊMICA DE DIREITO – UAD

MARIA LUIZA BATISTA FERNANDES

INFILTRAÇÃO VIRTUAL DE AGENTES POLICIAIS NO COMBATE AOS CRIMES CIBERNÉTICOS: Ampliação na proteção da criança e do adolescente à luz da Lei 13.441/17

Sousa – PB
2023

MARIA LUIZA BATISTA FERNANDES

INFILTRAÇÃO VIRTUAL DE AGENTES POLICIAIS NO COMBATE AOS CRIMES CIBERNÉTICOS: Ampliação na proteção da criança e do adolescente à luz da Lei 13.441/17

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande, como exigência parcial para obtenção do título de Bacharela em Ciências Jurídicas e Sociais.

Orientador: Prof.º Dr. Guerrison Araújo Pereira de Andrade

Data da aprovação: 08 / 11 / 2023

Banca Examinadora:

_____

Orientador: Prof.º Dr. Guerrison Araújo Pereira de Andrade

_____

Prof.º Andre Gomes de Sousa Alves

_____

Prof.ª Sabrinna Correia Medeiros Cavalcante

F363i Fernandes, Maria Luiza Batista.
Infiltração virtual de agentes policiais no combate aos crimes cibernéticos: ampliação na proteção da criança / Maria Luiza Batista Fernandes. – Sousa, 2023.
58 f.

Monografia (Bacharelado em Direito) – Universidade Federal de Campina Grande, Centro de Ciências Jurídicas e Sociais, 2023.
"Orientação: Prof. Dr. Guerrison Araújo Pereira de Andrade".
Referências.

1. Crimes Cibernéticos. 2. Agentes Policiais – Investigação – Infiltração Virtual. 3. Lei 13.441/17. 4. Pornografia Infantil. 5. Direito Processual Penal. I. Andrade, Guerrison Araújo Pereira de. II. Título.

CDU 343.63:004.738.5(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

TERMO DE RESPONSABILIDADE AUTORAL

Declaro para os devidos fins que eu **MARIA LUIZA BATISTA FERNANDES**, aluna do Curso de Direito da Universidade Federal de Campina Grande, matrícula 319130803, responsabilizo-me pela Monografia apresentada como Trabalho de Conclusão de Curso de Bacharel em Direito sob o título **INFILTRAÇÃO VIRTUAL DE AGENTES POLICIAIS NO COMBATE AOS CRIMES CIBERNÉTICOS: Ampliação na proteção da criança e do adolescente à luz da Lei 13.441/17**, isentando, mediante o presente termo, a Universidade de qualquer responsabilização, consequência de ações atentatórias à "Propriedade Intelectual", assumindo as responsabilidades civis e criminais decorrentes de tais ações.

Sousa/PB, 7 de novembro de 2023.

MARIA LUIZA BATISTA FERNANDES

Matricula n° 319130803

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer a Deus, por me permitir vivenciar esses cinco anos incríveis, me conceder saúde e forças para continuar, apesar das adversidades. Quando a angústia tomava conta do meu coração, Ele fez abrigo em meus sonhos e ouviu minhas orações. Tudo que sou hoje, é graças a Ele.

Aos amigos de vida, Alyne, Isa Bruna e Kaylane, que estiveram ao lado, desde primeiro rabisco até o B a Ba e até hoje permaneceram, estendendo a mão e colecionando memórias comigo. A minha panelinha da faculdade, Marina, Stefany, Mel, Igor, e Duanny, e colegas de van Duarte, Bianca, Gabriel e Talita, que hoje são como extensão de minha família, os quais criei vínculos, chorei e berrei de rir nos corredores da faculdade. Deixando um agradecimento especial a minha amiga Jade, que foi sinônimo de abrigo durante esses anos, minha dupla e minha melhor amiga.

Ao meu namorado, companheiro e melhor amigo, Antônio Victor, que veio sendo meu ponto de paz nos dias turbulentos, não soltando minha mão nas horas mais difíceis, dividindo comigo todo o peso e alegrias desses últimos meses.

Ao meu ilustre orientador, Dr. Guerrison Andrade, por todos os conselhos e por ter aceitado ser meu mentor. Ao meu amigo, Esdras Albuquerque, que foi sinônimo de paciência durante esses dias e por ter me prestado auxilio mais que necessário para a conclusão desse trabalho.

A toda minha família, que sempre colocaram fé em mim, apoiando todas as minhas decisões, sendo a base de tudo. Minhas avós, padrinhos e tias, que viveram os meus sonhos como se fosse deles.

Ao meu pai e meu irmão, que são motivo e causa de tudo, são por eles que batalho diariamente para trilhar meu futuro, para oferecer a eles tudo que existe de melhor no mundo.

Por fim, a minha Mãe, propulsora de tudo, que me incentivou a entrar na carreira jurídica porque sempre fui muito “respondona”. Ela que me cercou de carinho e amor em todos os momentos, abdicou de muito para que eu vivesse meu sonho. E que, ao me guiar nesses incríveis 22 anos, não se um dia ela soube que a pessoa que eu sempre quis ser, era ela! Obrigada, mãe. Você é o meu maior exemplo.

"É justo que muito custe, aquilo que muito vale." **Santa Teresa D'Ávila**

RESUMO

O trabalho em questão apresenta como tema central a infiltração virtual dos agentes policiais no combate aos crimes cibernéticos à luz da Lei 13.441/17, tendo como objetivo principal tratar da efetividade da lei no ordenamento jurídico ao reprimir os crimes contra dignidade sexual de crianças e adolescentes. Na presente pesquisa foram abordados temas como: A trajetória histórica da internet até o seu consumo massivo na contemporaneidade, o aumento expressivo de crianças e adolescentes em redes sociais, além de abordar as camadas mais profundas da internet, Deep e Dark Web. Ademais, no segundo capítulo, debate-se acerca das infrações penais no meio digital, tratando sua evolução contínua no Brasil e as acepções doutrinárias sobre o assunto e, logo após, uma exposição dos delitos que são alvo da maior quantidade de denúncias, como a pedofilia e a pornografia infantil. A metodologia utilizada foi a método dedutivo, por meio de pesquisa qualitativa e documental, usando sites, doutrinas, a legislação brasileira e artigos científicos que tratam acerca desse conteúdo, bem como a utilização de dados estatísticos visando estabelecer um parâmetro dos crimes mais recorrentes com menores vulneráveis. Por fim, esclarece-se os aspectos procedimentais presentes no instituto, em contrapartida com as lacunas deixadas pelo legislador ao tratar de prazos fiduciários da investigação, bem como o exercício legal do agente sem ultrapassar as barreiras legislativas, abordando ao final a efetividade no ordenamento jurídico buscando o aperfeiçoamento técnico da polícia judiciária.

Palavras-Chave: crimes cibernéticos; agentes policiais; Lei 13.441/17; investigação; pornografia infantil.

ABSTRACT

The work in question presents as its central theme the virtual infiltration of police agents in the fight against cybercrimes in light of Law 13,441/17, with the main objective of addressing the effectiveness of the law in the legal system when repressing crimes against the sexual dignity of children and adolescents. . In this research, topics such as: The historical trajectory of the internet until its massive consumption in contemporary times, the significant increase in children and adolescents on social networks, in addition to addressing the deeper layers of the internet, Deep and Dark Web. Furthermore, in second chapter, debates about criminal offenses in the digital environment, dealing with their continuous evolution in Brazil and the doctrinal meanings on the subject and, soon after, an exposition of the crimes that are the target of the greatest number of complaints, such as pedophilia and child pornography. The methodology used was the deductive method, through qualitative and documentary research, using websites, doctrines, Brazilian legislation and scientific articles that deal with this content, as well as the use of statistical data aiming to establish a parameter of the most recurrent crimes with minors vulnerable. Finally, the procedural aspects present in the institute are clarified, in contrast to the gaps left by the legislator when dealing with fiduciary deadlines for the investigation, as well as the legal exercise of the agent without overcoming legislative barriers, ultimately addressing effectiveness in the legal system seeking the technical improvement of the judicial police.

Keywords: cybercrimes; police officers; Law 13,441/17; investigation; child pornography.

LISTA DE ABREVIAÇÕES E SIGLAS

ART. – Artigo
ANPD - Autoridade Nacional de Proteção de Dados Pessoais
CP – Código Penal

CIA - Agência Central de Inteligência dos Estados Unidos da América

CV – Comando Vermelho

CETIC - Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação

ECA – Estatuto da Criança e do Adolescente

FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo

G-8 - Oito países mais ricos e influentes do mundo: Estados Unidos, Japão, Alemanha, Canadá, França, Itália, Reino Unido e Rússia.

IA – Inteligência Artificial

LGPD – Lei Geral de Proteção de Dados

NSA - Agência de Segurança Nacional dos Estados Unidos

OMS – Organização Mundial de Saúde

ONG – Organização Não Governamental

ONU – Organização das Nações Unidas

PCC – Primeiro Comando da Capital

RNP - Rede Nacional de Pesquisa

STJ - Supremo Tribunal de Justiça

TPS - Transtorno de Preferência Sexual

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

O crescimento exponencial dos diversos meios tecnológicos proporcionou diversos avanços no desenrolar da vida em sociedade. A velocidade na difusão de informações, rompendo com barreiras geográficas nacionais e internacionais, reduziu o processo de comunicação a distância entre o toque e a tela de um aparelho, que é denominado de clique.

Entretanto, o avanço dos meios tecnológicos não trouxeram apenas benefícios, pois, por se tratar de um ambiente sem fronteiras, as práticas de crimes em ambientes virtuais tornaram-se cada vez mais corriqueiros, especialmente em grupos com maior vulnerabilidade, como crianças e adolescentes.

Paralelamente ao avanço de práticas criminosas no ambiente digital, houve, também, um crescimento descomunal de crianças e adolescentes que adentraram nos meios digitais para a realização de atividades comuns, e toram-se assim, vítimas em potencial das ações criminosas nas redes.

Entretanto, a dificuldade de reunir evidências e identificar os indivíduos reverberou na seara das investigações criminais ao ponto de haver uma necessária readaptação às demandas advindas do ambiente virtual.

Sendo assim, na tentativa de obstaculizar as ações criminosas no âmbito do ciberespaço, tendo em vista os altos índices de violações da dignidade humana das crianças e adolescentes, a legislação pátria valendo-se de uma modalidade já existente no ordenamento – a infiltração de agentes de polícia no âmbito da Lei de Drogas e Organizações Criminosas – instituíram por meio da Lei n° 13.441/17, a modalidade de infiltração no ambiente virtual com o intuito de proteger crianças e adolescentes e garantir legitimidade no processo de identificação, colheita de provas e repressão de práticas violadoras da dignidade humana desses grupos vulnerabilizados.

Diante do exposto, surge o questionamento: A infiltração virtual de agentes policiais, criada com a Lei n° 13.441/17, é um instrumento efetivo na repressão de práticas criminosas no ciberespaço perpetradas em desfavor de crianças e adolescentes?

Para responder esse problema, a presente pesquisa objetivou analisar a efetividade do instrumento da infiltração virtual de agentes policiais na repressão de práticas criminosas no ciberespaço contra crianças e adolescentes.

Para alcançar o objetivo geral, foi proposto como objetivos específicos: expor aspectos referentes à evolução das tecnologias e como elas se tornaram um catalizador e/ou facilitador de condutas criminosas denominadas de cibercrimes; Descrever as variedades de crimes perpetrados contra crianças e adolescentes no âmbito do ciberespaço, como também o papel da legislação vigente na proteção da dignidade humana desses indivíduos vulnerabilizados; e por fim, abordar acerca da efetividade do instrumento da infiltração virtual como mecanismo de enfrentamento e repressão de práticas criminosas, identificação dos agentes e comprovação de ilícitos no ciberespaço contra crianças e adolescentes.

Foi neste ínterim, para alcançar os objetivos prepostos, que se desenrolou o presente trabalho tendo como norte compreender se o instrumento da infiltração virtual de agentes de polícia impacta na repressão de práticas criminosas no âmbito do ciberespaço, em especial contra vítimas menores e vulneráveis. Para isso, adotou-se o método de abordagem dedutivo. Quanto à forma de abordagem do problema, trata-se de uma pesquisa de cunho qualitativa. Enquanto técnicas de pesquisa fez-se uso da bibliográfica e documental.

Dessa forma, a presente temática se demonstra de extrema relevância em razão de sua complexidade, como também por se tratar de uma temática atual que assola a sociedade como um todo. Ademais, sob os aspectos jurídicos, a infiltração virtual caracteriza-se como um instrumento de repressão imprescindível para a materialização de condutas desveladas contra crianças e adolescentes no âmbito virtual. Bem como, sob o aspecto social, garante uma maior proteção aos indivíduos vulnerabilizados quando da inserção nos meios cibernéticos, em razão da prevenção e repressão dos cibercrimes.

2 EVOLUÇÃO HISTÓRICA DA PRÁTICA DE CIBERCRIMES NO BRASIL

O ponto de partida emerge em meio a chegada da internet e a banalização do acesso aos meios digitais. De fato, ocorreram mudanças devido as diversas possibilidades ocasionadas por esses recursos digitais, transformando a vida das pessoas que estão conectadas.

Diante da adesão massiva de dispositivos móveis, tais como celulares smartphones, percebe-se a alteração na nossa cultura. O que antes propiciava apenas uma inserção visando a comunicação por meio da web, tornou-se um amplo meio suscetível a prática de crimes.

2.1 As consequências do aumento massivo da cultura digital

Atualmente se perpetuou uma cultura digital na sociedade, que surgiu em decorrência da evolução tecnológica constante através dos séculos, ao passo que a modernização dos dispositivos está cada vez maior, no intuito de promover acesso a todas as pessoas.

Dentre os grandes passos na tecnologia, a internet foi um grande marco na evolução, possibilitando melhorias em diversos aspectos da globalização. Esse advento foi propulsor de mecanismos que facilitam as comunicações e transformou, de forma permanente, as relações no contexto social, além de contribuir para o acesso a informações e também na realização de pesquisas e estudos em diversas áreas de conhecimento, como a ciência.

No Brasil, o primeiro contato foi no ano de 1988, pela Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), vinculada a Secretaria Estadual de Ciência e Tecnologia, realizou a primeira conexão. Diante disso, o governo criou a Rede Nacional de Pesquisa (RNP), que propiciou uma gigantesca infraestrutura operando o funcionamento da internet, distribuindo o acesso não só para as instituições de ensino, mas para todo o território nacional (Vieira, 2003).

Em um contexto mais contemporâneo, acredita-se que, em meio ao cenário pandêmico, como consequência do surto de corona vírus, o consumo de mídia em geral aumentou significativamente, não só das redes sociais, mas também de outros meios que permitiam a interação por meio de vídeo conferência, ainda que

de forma desigual numa escala mundial. As plataformas sociais então se tornaram uma forma de diminuir a distância física entre as pessoas, nos períodos entre 2020 até o fim da pandemia, o que trouxe uma revolução na forma de relacionamento interpessoal (Zang, 2023).

Além disso, o uso continuo da internet se torna algo facilmente viciante por ser a alternativa mais viável de recreação de criança e adolescentes tendo em vista o distanciamento social imposto pela OMS (Organização Mundial de Saúde). Deslandes e Coutinho (2020) afirmam que, de uma forma brusca, a transmissão de dados por meio digital se tornou o único meio para que não houvesse a interrupção completa das interações sociais e de trabalho, surgindo assim o home office. Mesmo que de forma desigual, as principais características desse meio virtual é a hiper interatividade entre seus usuários e facilidade de mobilização em que podem ser acessados nos espaços digitais (BC LEÃO, SM DE OLIVEIRA, SSD DANTAS, 2023).

Para Cabette (2018), é notável que a internet foi um grande avanço científico e tecnológico, contudo, ressalta que existem possíveis malefícios, tais como a troca de informações ilegais, vejamos:

> Cada vez mais a internet vem ganhando espaço no mundo todo no que diz respeito a serviços e informações. Neste caso, a Internet é uma grande ferramenta da comunicação e, por isso mesmo ela encontra-se no universo de varias formas e ambientes. As vantagens do mundo digital são extensas e uma em destaque é a navegação com certo anonimato; possibilidade de ser uma pessoa descolada e fluente enquanto na vida analógica é apenas um avesso social. O anonimato, por sinal, é tanto benéfico como maléfico, é o poder de expressar, realizar e trocar informações que podem ser inclusive ilegais. Esta aparente 'liberdade' é como um vício, e muitos indivíduos quando entram dificilmente saem, pois sabem que o local é privilegiado.

Diante do cenário que o Brasil ocupa a 5ª posição no *ranking* no número de usuários de redes sociais mundial, é possível citar algumas problemáticas, principalmente quando se fala em crianças, adolescentes e jovens.

Em suma, não há dúvidas que a internet seja uma porta de entrada para uma ameaça aos direitos basilares e fundamentais, devido ao aumento da

exposição as inúmeras ofensas, tais como pedofilia, incentivo ao suicídio, além da prática de bullying e a abertura para o assédio.

2.2 O uso da rede para a prática de crimes

A rápida e constante evolução acaba sendo um meio para a realização de cibercrimes, contribuindo para o aumento na taxa de criminalidade, e, consequentemente, dificultando o combate por parte das autoridades competentes (Castro, 2022).

A característica que sobressaí nessa prática delituosa é a sua transnacionalidade, também denominada de caráter transfronteiriço, ou extraterritorialidade, termo já utilizado e reconhecido no Direito Penal. Essa característica se consubstancia na falta de um fator distância, mais especificamente na capacidade de tais crimes serem cometidos dentro de um país e afetar uma vítima que está localizada em outro. Aliado a esse fator e a velocidade da disseminação de informações, o agente consegue realizar diversas infrações em fração de segundos (Dias, 2010, p. 13). Seguindo o entendimento do autor mencionado:

> A distância continental entre pessoas, dados e serviços reduz-se a um simples clique. Esta característica leva, assim, a um exponencial agravamento dos danos das condutas criminosas, pois podem atingir um número massivo de pessoas e em qualquer lugar que estas se encontrem (Dias, 2010, p.13).

A grande maioria dos crimes são cometidos por agentes que se omitem por meio de navegadores desconhecidos, usando de redes sociais ou camadas mais profundas da internet para as práticas dos delitos. Diante disso, os sistemas jurídicos mundiais começaram uma corrida para adequar as respectivas legislações de forma que abarcasse os crimes cibernéticos cada vez mais presentes na realidade contemporânea.

Conforme o acesso e a modernização foram progredindo, a natureza dos crimes modificou-se. Inicialmente, crimes patrimoniais eram a prática mais comum,

onde o *modus operandi*[1] do indivíduo se caracteriza na aplicação de golpes e obtenção de vantagem ilícita sob a vítima, que por vezes acaba realizando pagamentos sem ter noção da ação criminosa.

Logo após, a internet não só se tornou palco para crimes contra a honra, mas também passou a permitir que menores vulneráveis (crianças e adolescentes) fossem vítimas constantes de crimes contra a dignidade sexual. Como consequência, a pornografia infantil passou a ser comercializada e até hoje, mesmo com instrumentos legislativos para combate, é algo muito recorrente em razão do aumento a exposição de menores nas redes sociais (Zang, 2023).

Visto os avanços tecnológicos e o compartilhamento constante de informações e ideologias no meio digital, a sociedade atual demanda intervenção governamental para estabelecer regras constitucionais e regulamentos que estendam os princípios fundamentais a todas as áreas onde a democracia busca atender às necessidades básicas da existência.

Somente nas duas últimas décadas, o Brasil passou a se preocupar com o crescimento exponencial dos índices de crimes virtuais, surgindo então a necessidade de regulação, pelo Direito, de tais práticas, trazendo inovações tanto na legislação como na forma de investigação de modo geral, sendo estas uma das maiores dificuldades na estrutura da polícia atualmente. Apesar dos impasses, a justiça brasileira caminha para manter a legalidade e a liberdade do uso da Internet de forma geral, conforme declaração do Ministro Raul Araújo, do Superior Tribunal de Justiça (STJ) depois do lançamento de 65 julgados acerca dos crimes virtuais:

> A internet não é um universo sem lei. Os julgados do STJ retratam o cenário atual no Brasil ao mostrar que a internet é um espaço de liberdade, muito valioso para a busca de informações e o contato entre as pessoas, mas também de responsabilidade", explica o ministro Raul Araújo. "O Judiciário está atento ao direito das pessoas que têm a sua imagem violada. E os agressores, que imaginam estar encobertos pelo anonimato, serão devidamente responsabilizados por suas condutas (CONJUR, 2015).

Aos poucos, o país vem buscando alternativas para sanar a precariedade na conjuntura investigativa, se baseando em formatos internacionais, realizando a

[1] Modus operandi significa o modo de agir e, no mundo jurídico, é a expressão utilizada para caracterizar a forma que um criminoso tem de agir.

colheita de provas virtuais e aos poucos incumbindo aos agentes a infiltração nos meios digitais.

Por fim, importante destacar que existe um paradoxo entre o amplo acesso da população aos meios virtuais e a falta de conscientização sobre a importância de se prevenir as inúmeras possibilidades de crimes na internet. Ou seja, à medida que o número de usuários cresce, a necessidade de orientação sobre os perigos se torna mais indispensável, mas sempre prezando liberdade de expressão e o Estado Democrático.

2.3 Aumento da presença de menores vulneráveis nas redes sociais

Na Constituição Federal de 1988, redação do artigo 227, bem como no Estatuto da Criança e do Adolescente - ECA, no artigo 5º, tratam do dever familiar para com as crianças e os adolescentes:

> Art. 227. 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 colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. (Redação dada Pela Emenda Constitucional nº 65, de 2010) (Brasil, 1988).
> Art. 5º Nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punido na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais (Brasil, 1990).

Nestes respectivos artigos são resguardados direitos básicos e fundamentais para o desenvolvimento saudável e seguro dos menores, tais como 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 do já exposto, estes dispositivos dispõem sobre a proteção de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. Isto é, a proteção integral aos menores (Brasil, 1988).

Com o advento das redes sociais como *Instagram, Tiktok* e outros, estão cada vez mais propensos à aparição de crianças e adolescentes nesses meios. A

principal função das mídias sociais, inicialmente, era ser fonte de entretenimento, destinado principalmente para o lazer. Contudo, sua finalidade ficou paulatinamente mais destinada a fins financeiros por alguns usuários, tendo em alguns casos, uma criança como ‘’estrela’’ no conteúdo produzido. Conforme a Childhood Brasil (2012, p. 15):

> Apesar de chamarmos a internet de “mundo virtual”, ela faz parte do mundo real e como tal também traz alguns perigos: existem sites, pessoas e redes criminosas que podem enganar, seduzir ou induzir crianças e adolescentes a acessar conteúdos inadequados, como pornografia, incluindo a infantojuvenil. Elas podem ser encorajadas a enviar fotos e informações pessoais com propósitos duvidosos.

Não há dúvidas que a internet é um mecanismo útil, que está à disposição das pessoas, e presente atualmente na vida das crianças e dos adolescentes, viabilizando coisas benéficas, como por exemplo, amplo acesso ao conhecimento; rapidez na informação e comunicação; dinamismo; entre outras. Para Bretan (2012, p. 24), o crescimento em uma sociedade em rede significa aprender códigos ao mesmo passo que desenvolvem sua identidade, limites de privacidade e intimidade, bem como as regrais morais de respeito.

Seguindo o raciocínio do autor mencionado anteriormente, a cultura tecnológica permite que a intimidade dos jovens seja exposta, de uma forma tão invasiva que nem mesmo adultos estão as vezes preparados, além de incentivar que se perpetue uma ideia de vaidade e padrão de autoimagem muitas vezes inalcançável.

Nesse ínterim, uma pesquisa realizada pela *TIC Kids Online Brasil*, rede de pesquisa da Cetic.br - Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, em matéria reproduzida pela Agência Brasil constata que nove em cada dez crianças e adolescentes são usuárias de internet, é possível ter um parâmetro da quantidade de menores presentes nas redes, principalmente após a pandemia COVID-19, vejamos:

> Entre crianças e adolescentes no país, o uso de redes sociais é uma das atividades online que mais cresceram. Em 2021, 78% dos usuários de internet com idades de 9 a 17 anos acessaram alguma rede social, um aumento de 10 pontos percentuais em relação a

> 2019 (68%). A proporção de usuários de internet de 9 a 17 anos que têm perfil no Instagram avançou de 45% em 2018 para 62% em 2021 (Tic Kids, 2022).

A exploração constante de crianças nas mídias ou a falta de supervisão pelos seus ascendentes podem torná-las reféns de uma exposição e, em um cenário mais crítico, ter uma intimidade invadida. Existem inúmeros casos relatados de pedófilos que utilizam do anonimato das redes para acessar e divulgar conteúdos impróprios envolvendo menores (Fernandes, 2023).

Por outro lado, a recente utilização de Inteligência Artificial também propicia jovens a serem vítimas de criminosos. Um exemplo bem retratado de como ocorre o contato do agente com o vulnerável é o caso retratado na novela Travessia, exibida na programação da Tv Globo, onde na dramaturgia a personagem Karina fez amizade virtual com um perfil que se dizia ser a Bruna Shuler, mas na realidade era um pedófilo utilizando de IA para se passar por mulher, e no fim a vítima sofreu um estupro virtual após ter fotos intimas vazadas.

Diante da repercussão, a novela trouxe visibilidade para o crime nacionalmente, alertando as pessoas, principalmente os responsáveis, para o recente emprego da IA, que colaborou significativamente para a propagação desses crimes.

Plausível acrescentar que a criança e o adolescente, assim como seus respectivos responsáveis, acham que estão imunes aos crimes virtuais e que, diante do acontecimento, saberão lidar com a situação. Porém, devido a essa mentalidade equivocada que muitos crimes costumam ocorrer, passando despercebidos e de uma forma diversa ao que os filmes ou séries apresenta.

São frequentes os casos em que as próprias vítimas que produzem e enviam o material pornográfico e incitam que outros menores participem dessa rede de exploração sexual, por vezes, em razão da falta de instrução e preocupação no momento de alertar sobre os crimes. Isso ocorre principalmente devido a ideia que a internet é uma terra sem lei, não havendo “responsabilização”, tornando tudo possível e, um exemplo claro é a criação de “perfis fakes”, que possuem a principal finalidade de fingir ser outra pessoa, alguns inclusive apresentando comportamentos hostis e inadequados (Childhood Brasil, 2012, p 16).

Em suma, a conscientização em relação a supervisão e acompanhamento nas redes para evitar que isso ocorra é crucial, pois mesmo o caso citado anteriormente sendo fictício nada impede que venha a ocorrer na realidade. Importante frisar que, apesar desses casos serem resolvidos juridicamente, estes causam danos psicológicos nas vítimas, sendo primordial um acompanhamento psicológico, que é um direito assegurado constitucionalmente em seu artigo 227 (Brasil, 1988).

Ademais, as práticas desses crimes se intensificaram com a criação das redes mais obscuras da internet, que possibilitam o anonimato dos agentes, bem como a facilidade no emprego de golpes e impunidade perante ao sistema judiciário brasileiro.

2.4 A internet Deep e Dark Web

Atualmente, estas camadas mais obscuras da internet possuem links próprios dificultando o acesso de seu conteúdo para os leigos, diferentemente da *Surface Web*[2], utilizada por boa parte dos usuários para realizar suas atividades cotidianas, tendo como exemplos mais famosos de softwares que facilitam a entrada nesse submundo da internet são: o *Tor*, i2P e o *FreeNet* (Barreto; Santos, 2019).

No que diz respeito ao tamanho desse mundo virtual, com relação mencionada, Michael Bergman, autor do termo tratado nesse tópico, afirma que:

> (...) informações públicas na Deep Web são comumente de 400 a 500 vezes maior que as definidas da World Wide Web. A Deep Web contém 7.500 terabytes de informações comparadas a 19 terabytes de informação da Surface Web. A Deep Web contém aproximadamente 550 bilhões de documentos individuais comparados com 1 bilhão da Surface Web. Existem mais de duzentos mil sites atualmente na Deep Web. Seis das maiores enciclopédias da Deep Web contém cerca de 750 terabytes de informação, suficiente para exceder o tamanho da Surface Web quatro vezes. Em média, os sites da Deep Web recebem 50% mais tráfego mensal, ainda que não sejam conhecidos pelo público em geral. A Deep Web é a categoria que mais cresce no número de

[2] Pompéo, Wagner Augusto; Seefeldt, João Pedro. Nem tudo está no Google: deep web e o perigo da invisibilidade. In: Congresso Internacional de Direito e Contemporaneidade. Santa Maria: UFSM, 2013, p. 439. Surface web: conteúdo indexado. Pode ser encontrado através de mecanismos de pesquisas tradicionais, como Google, e acessado através de navegadores padrões.

> novas informações sobre a Internet. Deep Web tende a ser mais estrita, com conteúdo mais profundo, do que sites convencionais. A profundidade de conteúdo de qualidade total da Deep Web é de 1.000 a 2.000 mil vezes maior que a da superfície. O conteúdo da Deep Web é altamente relevante para todas as necessidades de informação, mercado e domínio. Mais da metade do conteúdo da Deep Web reside em tópicos específicos em bancos de dados. Um total de 95% da Deep Web é informação acessível ao público não sujeita a taxas ou assinaturas (...) (Bergman, 2001).

Tal conceito também foi abordado por Shimabukuro e Silva (2017), relatando que a internet profunda, mais conhecida por *Deep Web*, é uma parte restrita da rede, que possui uma dimensão semelhante e crescimento semelhante ao da Internet que conhecemos, utilizada como meio subsidiário quando alguns conteúdos não se encontram disponíveis nos principais navegadores, como *Yahoo e Google*.

Outros pesquisadores do meio trouxeram características relevantes acerca da *Deep Web*, Barreto; Santos (2019) expõe que:

> a) Anonimato: O principal objetivo da utilização de redes cujo conteúdo não é indexado na surface web é proporcionar anonimato a seus usuários. Nesse cenário podemos destacar: pessoas comuns na busca de conteúdo com garantia de privacidade; blogueiros, ativistas e jornalistas, para a publicação de suas opiniões, ideias e críticas e denúncias, principalmente em regiões do globo onde a censura governamental, política e de grupos extremistas não permite que certos conteúdos sejam levados ao conhecimento das pessoas de outros países, além de criminosos que buscam meios para não serem alcançados pela aplicação da lei penal.
> b) Segurança: essa peculiaridade decorre da conexão criptografada entre os nós componentes de rede[...]
> c) código aberto: [...] um software de código aberto ou open source é aquele que pode ser manipulado por um usuário/ programador de forma a eliminar suas vulnerabilidades e/ou problemas e propor novas funcionalidades e melhoramentos, a fim de beneficiar a comunidade de usuários.

Pode-se dizer que, qualquer pessoa que se proponha a buscar esse termo irá encontrar como resultado imagens macabras e horripilantes, textos com conteúdo deturbado, arquivos de origem duvidosa e todo o tipo de conteúdo que desafiam a imaginações mais férteis (Andrade, 2015).

Sob a mesma ótica do autor, na *Deep Web* encontra-se tudo, sendo possível citar diversos crimes, dos mais “simples”, como comprar cartões de crédito

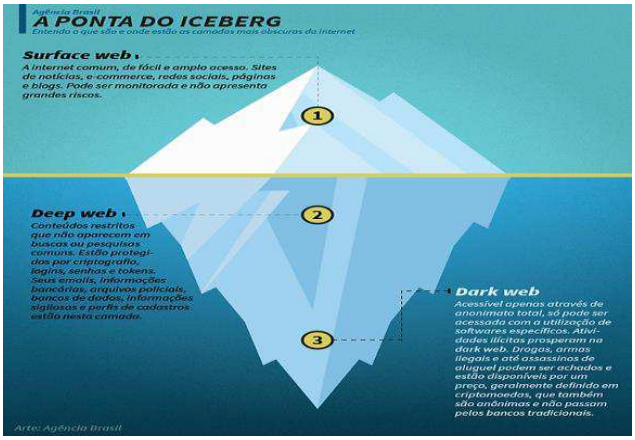
furtados, até crimes mais perversos, como venda de órgãos humanos, assassinos de aluguel, comércio de armas e drogas. E, dentro desse meio, encontra-se os maiores exploradores de pornografia infantil, que costumam comercializar, produzir e, em alguns casos, fornecer crianças ao mercado de tráfico de pessoas, para fins de exploração sexual e prostituição.

Diante dessa restrição, ao longo dos anos, se proliferaram cada vez mais informações sobre a existência de uma rede ainda mais profunda, ocasionando o crescimento de usuários acerca do assunto, por consequência, surgiu uma rede mais anônima, conhecida como *Dark Web*, que nos dias de hoje é o principal palco para os crimes (Shimabukuru; Silva, 2017).

Destarte, os mesmos autores postulam que, por seu grande obstáculo criptográfico, a *Dark Web* ganha destaque entre os agentes e se torna uma grande preocupação das autoridades que são responsáveis pelo combate aos crimes cibernéticos. Nessa rede, o anonimato possui um papel imprescindível para a prática das condutas criminosas. Diante dos avanços, também foi desenvolvida uma moeda virtual, a *bitcoin*, possibilitando que muitos agentes não sejam rastreados pelas suas transações financeiras.

Em diversas matérias acerca desse conteúdo, pesquisadores utilizaram de uma metáfora do iceberg no mar para ilustrar como funcionaria as camadas virtuais, sendo a Surface Web a camada mais exposta, composta pelas redes monitoradas e de fácil acesso; a *Deep Web*, que está um pouco abaixo da superfície, sendo uma camada mais restrita que possui dados sigilosos; e, por fim, a *Dark Web*, utilizada principalmente para fins ilícitos, a qual só é possível o acesso através de softwares específicos, elencada na parte mais inferior da imagem a seguir (Agência Brasil, 2020).

Figura 1 - ENTENDA A DEEP WEB E A DARK WEB



FONTE: AGÊNCIA BRASIL, 2020.

Visto a dificuldade de identificação dos autores dos crimes virtuais, principalmente ocorridos na *Dark Web*, e a consequente falta de punição, resultou em uma preocupação mundial. Desse modo. a Convenção de Budapeste, resultado de um trabalho desenvolvido pelo Conselho da Europa, surge como forma de tentativa de solucionar esses crimes ao priorizar a proteção da sociedade contra os avanços da criminalidade. Durante a Convenção, foi proposta a escolha de uma legislação comum com objetivo de promover a cooperação entre os Estados da União Europeia.

Com a concretização da Convenção de Budapeste, que entrou em vigor em 1º de julho de 2004, e a abertura à assinatura por todos os países que desejassem, comprovou-se a necessidade de combate aos crimes cibernéticos por toda a sociedade mundial, tendo os seguintes crimes tipificados:

> 1) Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos:
> a) acesso doloso e ilegal a um sistema de informática;
> b) interceptação ilegal de dados ou comunicações telemáticas;
> c) atentado à integridade dos dados (conduta própria de um subgrupo hacker, conhecido como cracker);
> d) atentado à integridade de um sistema;
> e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados.
> 2) Infrações informáticas:
> a) falsificação de dados;
> b) estelionatos eletrônicos (v.g., os phishing scams).

> 3) Infrações relativas ao conteúdo:
> **a) pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito);**
> b) racismo e xenofobia (difusão de imagens, ideias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e ameaças qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade);
> 4) Atentado à propriedade intelectual e aos direitos que lhe são conexos.

Cabe salientar que as pesquisas realizadas pelo CORREIO BRAZILIENSE em 2018 apontam que os conteúdos que mais são acessados na *Dark Web* são os de pornografia infantil, apologia e incitação aos crimes contra a vida, dentre outros. Notável também o aumento considerável do número de visualizações também em páginas que divulgam dados restritos do governo como o *WikiLeaks*, os de troca de moedas como *bitcoins*[3] e de tutoriais para fraude virtual.

Dessa forma, com o universo da *Deep Web e Dark Web*, fica de fato evidenciado, o grande avanço tecnológico frente ao Direito Pátrio e que, principalmente, os criminosos utilizam-se desses mecanismos para evadir-se e dificultar as investigações, mostrando conhecimento técnico na área, evitando as sanções penais diante dos crimes praticados na internet.

[3] O Bitcoin (BTC) é um tipo de moeda virtual também chamado de criptomoeda.

3 DOS CRIMES CIBERNÉTICOS

Para melhor elucidação, é necessário explanar os aspectos dos crimes cibernéticos, bem como os debates doutrinários acerca do conteúdo, definindo seus conceitos, natureza jurídica, dentre outros. Além de abordar os crimes mais recorrentes contra menores vulneráveis na atualidade.

Ademais, realizar uma trajetória na legislação brasileira, mostrando as motivações do legislador e seus objetivos ao instituir as diretrizes que regulam o tema, seus devidos princípios e deveres estabelecidos e respectivas sanções penais.

3.1 Surgimentos e seus respectivos conceitos

Crimes cibernéticos, ou virtuais como também são conhecidos, podem ser conceituados como crimes no qual a ferramenta utilizada para praticá-los é a internet, o que, por sua vez, causa bastante divergência doutrinária acerca de sua definição. Essa espécie de infração começou a dar seus primeiros indícios durante a década de 1960, contudo, seu termo surgiu apenas em 1990, a partir de uma reunião do G-8, que corresponde ao grupo dos países mais ricos e influentes (Estados Unidos, Japão, Alemanha, Canadá, França, Itália, Reino Unido e Rússia) (Senado Federal).

Ademais, diante do extenso conceito de crimes cibernéticos, existem alguns doutrinadores que são pertinentes para melhor elucidação acerca desse conteúdo. Em primeiro plano, para Sérgio Marcos Roque (2007, p. 26), o conceito de crime cibernético é “toda conduta definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material.”

Para Augusto Rossini:

> O conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva omissiva, praticada por pessoa física ou jurídica, com o uso a informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que

> tem por elementos a integridade, a disponibilidade a confidencialidade (Rossini, 2004, p.123).

Na mesma linha de raciocínio, Rossini sugere que esses crimes em particular atingem não somente condutas praticadas no âmbito da internet, mas também abarca toda aquela que haja relação direta com os sistemas virtuais, abrangendo delitos em que o computador seria apenas um meio sem a imprescindível conexão à rede mundial de computadores, ou a qualquer outro ambiente telemático. Sendo assim, tem-se como exemplo uma fraude que ocorre fora da internet, onde o computador é apenas um instrumento do crime, atingindo a denominação de delito informático.

Guilherme Guimarães Feliciano expõe que existe um conceito bem amplo de criminalidade informática, caracterizado como um recente fenômeno histórico-sociocultural, tendo como principal traço a elevada incidência de ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware, software, redes, etc.) (Feliciano, 2000).

Na legislação brasileira, não existe um conceito do que seja cibercrime, entretanto, o Código Penal Brasileiro, o Estatuto da Criança e do Adolescente, as leis de nº 12.850/13, 12.735 e 12.739 de 2012, trazem algumas condutas relacionadas aos crimes informáticos, sendo a pedofilia a mais recorrente quando as vítimas são crianças e adolescentes.

3.2 Acepções doutrinárias

Ao passo que esses delitos tomaram visibilidade em razão da recorrência na sociedade atual, muitos doutrinadores se propuseram a estudar afundo, formulando teorias acerca da natureza jurídica e as respectivas classificações, a exemplo de Jesus e Milare, no livro Manual de Crimes Informáticos.

Os referidos autores trazem consigo a classificação mais precisa de delito informático, dividindo o delito em quatro tipos, crimes de informática próprios, crimes de informática impróprios, crimes de informática mistos e crimes de informática mediato ou indireto.

> 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 tipo penal;
> c) crimes informáticos mistos: são crimes complexos em que, além de proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre à existência de dois tipos penais distintos, cada qual protege um bem jurídico;
> d) crime informático mediato ou indireto: trata-se delito informático praticado para a ocorrência de um delito não informático consumando ao final. Em Direito Informático, comumente um delito informático é cometido como meio para a prática de um delito-fim ordem patrimonial. Como, por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vitima. Pelo principio da consunção, o agente só será punido pelo delito-fim (furto) (Jesus; Milare, 2016, p. 49).

Ademais, seguindo o fio dos autores já mencionados, é de conhecimento que a informática de fato trouxe novas formas de realizar velhos crimes, pouco importando em qual intermédio estas são praticadas, pois continuam a ameaçar os bens jurídicos.

Dando continuidade, é plausível mencionar, além dos conceitos já abordados, as respectivas falhas no poder punitivo do Estado Democrático de Direito, o qual ainda carece de dispositivos que consigam tanto pôr em prática sua legislação vigente como também propor iniciativas que colaborem com as investigações e ampliem os meios utilizados pelas autoridades.

A constatação de um crime digital é de fato um dos maiores impasses, mas devido a sua classificação, posto que ainda é uma pequena parcela de conclusões a respeito, levando em consideração que a tecnologia nos dias de hoje evolui a passos largos, é de suma importância que as perspectivas se modifiquem na mesma proporção, em razão das diversas situações complexas encontradas no meio virtual (Jusbrasil, 2019).

Não obstante, existe uma discussão que se assenta no princípio basilar do Direito Penal, o princípio da Legalidade, importando a grande dúvida: Como punir os devidos infratores desses crimes sem que haja dispositivos legais que descrevam

tais condutas criminosas? Afinal, tal princípio carrega em seu teor a ideia que uma pessoa não pode ser punida sem que haja uma lei que defina a conduta.

Ainda nessa linha, Rogério Greco preceitua que, sem dúvidas, o princípio da legalidade é o mais importante para tratar dessa questão. Conforme se extrai do art. 1º do Código Penal, bem como do inciso XXXIX do art. 5º da Constituição Federal, a lei é a única fonte do Direito Penal quando se quer tutelar um bem jurídico, proibindo e impondo condutas sob a ameaça de uma sanção. Tudo o que não for expressamente proibido é lícito em Direito Penal (Greco, 2018, p. 215).

Ou seja, é nesse diapasão que se discute a atipicidade de algumas condutas, brechas na legislação e consequente isenção de punição dos indivíduos. Nesse contexto normativo, o *jus puniendi* do Estado está vinculado ao que preceitua a lei, não podendo aplicar sanções ao arrepio de sua vontade, sendo imprescindível que haja expressamente previsão normativa para tal.

3.3 Crimes recorrentes contra Crianças e Adolescentes no meio digital

3.3.1 Pedofilia

Inicialmente, a pedofilia é considerada pela OMS (Organização Mundial de Saúde) como uma doença, mais especificamente, um Transtorno de Preferência Sexual (TPS) segundo a Classificação Internacional de Doenças (CID-10), que consiste na atração de um indivíduo por crianças e adolescentes, em fase de puberdade ou não. Tal prática por muitos anos foi algo normalizado e até nos dias de hoje, em algumas culturas, é comum ver casamentos e uniões entre crianças e adultos.

Importante salientar que, em nosso ordenamento jurídico, nenhuma pessoa será punida em razão de doença, principalmente quando esta não fere bens tutelados, tendo por base o Princípio da Alteridade. Contudo, a partir do momento que o pedófilo passa a exteriorizar suas vontades e desejos, a sua conduta imediatamente se molda ao estabelecido em lei, caracterizando um crime.

No Brasil, o crime de pedofilia está tipificado nos Crimes Contra Dignidade Sexual, no artigo 217-A: “Ter conjunção carnal ou praticar outro ato

libidinoso com menor de 14 (catorze) anos: (Incluído pela Lei nº 12.015, de 2009)". Para tanto, nosso Código ainda não se aperfeiçoou quanto as práticas realizadas virtualmente (Silveira, 2020).

Somente com a alteração no artigo 241 do Estatuto da Criança e do Adolescente (ECA), por meio da edição proposta pela Lei 11.829/2008, que o legislador direcionou a sua atenção para a proteção desse público que é extremamente vulnerável e criou novos dispositivos penais, ou seja, práticas como aliciamento sexual e divulgação de imagens, ocorridos em meio virtual, passam a ser considerados crimes, vejamos:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: (Incluído pela Lei nº 11.829, de 2008)
> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: (Incluído pela Lei nº 11.829, de 2008)
> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais. (Incluído pela Lei nº 11.829, de 2008)

Nesse universo virtual amplo existente, com o advento das redes sociais e as facilidades de estabelecer conversas e entrar em salas de bate papo, portas de entrada para indivíduos mal-intencionados foram criadas, abrindo a possibilidade de atrair vítimas. Atualmente, é muito fácil criar um perfil em qualquer rede social, inclusive utilizando dados falsos, e, consequentemente, possibilitando a criação de uma identidade falsa, ocultado a verdadeira face dos pedófilos.

Perfis "*fakes*" são uma forma muito usual dos criminosos agirem, passando despercebidos pelas autoridades e pelo monitoramento dos responsáveis.

Ao se passar por um amigo, “coleguinha” de jogo, ganha a confiança de suas vítimas e é nesse momento que elas, em grande maioria das vezes, compartilham fotos íntimas ou de cunho sexual (Silveira, 2020).

Ademais, com o advento da Inteligência Artificial, muitos pedófilos conseguem construir melhor uma identidade visual que seja capaz de enganar, utilizando de atores/atrizes, cantores etc do meio *teen,* para convencer crianças a produzirem material pornográfico, que posteriormente usaria para obter vantagens por meio de chantagem.

Uma operação que ficou conhecida no Brasil pelo indivíduo utilizar exatamente das “ferramentas” anteriormente mencionadas foi a Mil Faces, deflagrada pelas Policia Federal, no Estado do Espírito Santo, noticiada pela G1, onde a polícia chegou aos suspeitos através de uma Ong (Organização Não Governamental) dos Estados Unidos, que centralizou todas as denúncias que foram recebidas pelas redes sociais.

Contudo, mesmo com todos os avanços legislativos e tecnológicos, ainda é de extrema dificuldade a identificação desses criminosos. Por isso, algumas empresas ligadas a área, começaram a desenvolver ferramentas para auxiliar no combate à propagação de crimes ligados a pedofilia infantil.

No ano de 2018, o Google lançou uma inteligência artificial que acelerou a identificação de materiais relacionados a pedofilia na internet. Tal tecnologia utiliza redes neurais para reconhecer imagens e vídeos com crianças que estão em situação de abuso e, consequentemente, agilizando o trabalho das pessoas que revisam as páginas, tornando o trabalho mais simples e eficaz. Essa ferramenta visa ampliar os conteúdos nunca vistos e que estejam relacionados a um padrão de abuso sexual de menores.

Em suma, mesmo com diversos institutos desenvolvidos exclusivamente para o combate a pedofilia, a ameaça oculta ainda é presente na rede. Existem diversos criminosos dispostos para seduzir crianças e adolescentes, independente se for para satisfazer sua própria lascívia ou para obter alguma espécie de vantagem ou lucro com a venda de imagens. Ou seja, é necessário que haja um acompanhamento dos responsáveis em relação as atividades dos menores na internet.

3.3.2 Estupro Virtual

A priori, importante destacar que o crime de estupro está tipificado em nosso Código Penal, em seu artigo 213: Constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso. Bem como também existe a previsão do estupro cometido contra vulnerável no artigo 217-A (Brasil, 1940).

Contudo, por muito tempo, o código não recepcionava a ideia que para o estupro consumar-se não haveria a necessidade de conjunção carnal. Somente em 2016, o Supremo Tribunal de Justiça no julgamento do RHC 70976/MS, sustentaram a ideia da prescindibilidade do contato físico entre o autor e a vítima, vejamos a ementa:

> RECURSO EM HABEAS CORPUS. ESTUPRO DE VULNERÁVEL EM CONTINUIDADE DELITIVA. TRANCAMENTO DA AÇÃO PENAL. AUSÊNCIA DE JUSTA CAUSA E ATIPICIDADE DA CONDUTA. CONTEMPLAÇÃO LASCIVA DE MENOR DESNUDA. ATO LIBIDINOSO CARACTERIZADO. TESE RECURSAL QUE DEMANDA REEXAME FÁTICO-PROBATÓRIO. AUSÊNCIA DE FLAGRANTE ILEGALIDADE. RECURSO DESPROVIDO. O Parquet classificou a conduta do recorrente como ato libidinoso diverso da conjunção carnal, praticado contra vítima de 10 anos de idade. Extrai-se da peça acusatória que as corrés teriam atraído e levado a ofendida até um motel, onde, mediante pagamento, o acusado teria incorrido na contemplação lasciva da menor de idade desnuda. **Discute-se se a inocorrência de efetivo contato físico entre o recorrente e a vítima autorizaria a desclassificação do delito ou mesmo a absolvição sumária do acusado. A maior parte da doutrina penalista pátria orienta no sentido de que a contemplação lasciva configura o ato libidinoso constitutivo dos tipos dos arts. 213 e 217-A do Código Penal - CP, sendo irrelavante, para a consumação dos delitos, que haja contato físico entre ofensor e ofendido.** O delito imputado ao recorrente se encontra em capítulo inserto no Título VI do CP, que tutela a dignidade sexual. Cuidando-se de vítima de dez anos de idade, conduzida, ao menos em tese, a motel e obrigada a despir-se diante de adulto que efetuara pagamento para contemplar a menor em sua nudez, parece dispensável a ocorrência de efetivo contato físico para que se tenha por consumado o ato lascivo que configura ofensa à dignidade sexual da menor. Com efeito, a dignidade sexual não se ofende somente com lesões de natureza física. (...)
> Assim, não há amparo para a pretendida absolvição sumária ou mesmo o reconhecimento de ausência de justa causa para o prosseguimento da ação penal para apuração do delito. Recurso desprovido.

> (...)
> Decisão
> Vistos, relatados e discutidos os autos em que são partes as acima indicadas, acordam os Ministros da Quinta Turma do Superior Tribunal de Justiça, por unanimidade, negar provimento ao recurso e julgar prejudicado o exame do pedido liminar. Os Srs. Ministros Felix Fischer, Jorge Mussi, Reynaldo Soares da Fonseca e Ribeiro Dantas votaram com o Sr. Ministro Relator. SUSTENTARAM ORALMENTE: DR. JOSÉ BELGA ASSIS TRAD (P/RECTE) E MINISTÉRIO PÚBLICO FEDERAL.

Em reforço, importante salientar que vítima menor de 14 anos, a proteção integral á criança e ao adolescente, especialmente no que se refere à violações de natureza sexual, é uma preocupação constante do Estado (art. 227, caput, c/c o § 4º, da Constituição da República) e de instrumentos internacionais (art. 34, "b", da Convenção Internacional sobre os Direitos da Criança, aprovada pela Resolução n. 44/25 da ONU, em 20/11/1989, e internalizada no ordenamento jurídico nacional, mediante o Decreto Legislativo n. 28/1990).

Seguindo essa nova ótica, constranger uma pessoa para que ela pratique ato libidinoso por meio da internet também configura os crimes previstos nos artigos 213 e 217-A, pode ocorrer por qualquer mídia social ou meio de transmissão de informações. Em maioria dos casos, é possível traçar uma forma de atuação dos indivíduos. Majoritariamente, ocorre com pré-adolescentes, que se tornam refém de seu agressor pelo medo de ter suas fotos intimas vazadas.

Grande parcela dos doutrinadores adota também o termo de sextorsão ou *sextorsion,* que surgiu propriamente a partir de investigações promovidas pelo *Federal Bureau of Investigation* (FBI), no ano de 2010, quando da análise de um caso envolvendo um hacker que controlava a webcam e conversas de suas vítimas para, posteriormente, as extorquir sexualmente (Jusbrasil, 2023).

3.3.3 Pornografia Infantil

Inicialmente, é necessário esclarecer que essa prática se perpetua desde tempos mais antigos. À primeira vista, era muito recorrente em artes, quadros e esculturas. No decorrer dos tempos, com o advento das revistas, surgiu um novo

contexto de pornografia, se disseminando de uma forma mais fácil na sociedade (Muller, 2002).

Com o advento da internet, assim como o mundo, a pornografia se modificou, evoluindo de imagens para filmagens que são facilmente acessadas com um clique. Em razão dessa revolução, a indústria pornográfica gera bilhões de dólares por ano (Jesus; Milare, 2016).

Porquanto, a dita indústria tem vendido diariamente uma gama de abusos infantis, sendo estes números alarmantes e um dos maiores problemas no que tange aos crimes informáticos, corroborando com outros crimes, como a pedofilia.

Ademais, cumpre salientar que a pornografia pode comprometer a forma de desenvolvimento físico e psicológico da criança. Podendo citar que uma das consequências que se manifesta com maior recorrência são as dificuldades de readaptação e o sentimento de culpa da criança, em conjunto com pensamentos suicidas, autoestima baixa e outros.

Importante mencionar que além dos dispositivos previstos no ECA, o Código Penal Brasileiro também versa sobre a temática da pornografia, tipificando além do estupro de vulnerável e corrupção de menores, a divulgação de cena de estupro ou qualquer material de teor sexual, incluindo o de crianças e adolescentes, na redação do artigo 218-C:

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia;

Mesmo com todos os dispositivos legais que possuem a finalidade evitar e punir os indivíduos que praticam esses crimes, a incidência desses casos continua crescendo exponencialmente. Em uma pesquisa de dados levantados pela Childhood – Pela proteção da Infância (2019), a central de crimes cibernéticos recebeu 75.671 mil denúncias, onde 61% deles eram referentes a pornografia infantil.

Diante do exposto, fica claro o consumo massivo de pornografia infantil na internet, que contribui para o aumento de abusos e explorações sexuais cometidos, os quais se disseminam facilmente no âmbito virtual, colaborando não só com os crimes anteriormente mencionados, mas também com tráfico de crianças. Onde os agentes possuem a finalidade de prostituir, ou vender ilegalmente seus corpos em redes mais obscuras, ou comercializar imagens/vídeos que satisfazem uma quantidade abundante de pedófilos.

3.4 Legislação vigente e seu papel na repressão dos crimes

3.4.1 Marco Civil da Internet

Para Ronaldo Lemos (2016), o Marco Civil da internet surge posteriormente as declarações realizadas por Edward Snowden, um analista de sistemas, ex-administrador de sistemas da Agência Central de Inteligência dos Estados Unidos da América (CIA) e ex-contratado da Agência de Segurança Nacional dos Estados Unidos (NSA), o qual revelou informações que repercutiram em todo Brasil, constatando que o governo brasileiro teria sido espionado.

Neste contexto, houveram muitas propostas como forma de reagir a situação que o governo se encontrava, sendo a mais viável a reabertura do debate acerca do Marco Civil Da Internet, promovida pela própria sociedade que buscava uma resposta quanto a regulação desta no Brasil. Em razão do cenário caótico, o Congresso Nacional e o Governo ouviram todas as mobilizações, que promoveu um forte impacto no território nacional e internacional, a tutelar o âmbito criminal virtual. Juntamente com Souza, Lemos também traz uma visão diante da aprovação da lei, vejamos:

> Uma vez aprovado em 2014, o Marco Civil serviu de inspiração para um processo de construção colaborativa de uma Declaração de Direitos para Internet, realizada pelo governo italiano. Citando expressamente a experiência brasileira e convidando diversos atores envolvidos com o Marco Civil para apresentar as suas contribuições ao Parlamento Italiano, a cooperação entre os dois países demonstra o rápido impacto que a aprovação do texto brasileiro desencadeou (Souza; Lemos, 2016, p. 33).

Desta forma, o Marco Civil criou forças, pois foi o pioneiro na construção de direitos civis na internet. Sendo assim, ao invés de instituir punições, criou-se uma moldura de direitos e liberdades, de forma que traduzisse os princípios presentes na Constituição Federal para o mundo virtual.

Em suma, houve uma série de estudos e procedimentos, que no fim das contas constituiu uma lei tecnicamente sólida e abrangente, que despertou o interesse internacional. Após concluída a redação final de seu texto e passada pela análise do governo, foi encaminhada para o Congresso em 24 de agosto de 2011, com a assinatura da Presidenta Dilma Rousseff e outros quatro ministros, conhecida por Lei nº 12.965/2014 (Viese Buturi, 2021).

No artigo 3º desta lei, são elencados de forma objetiva todos os princípios e respectivas garantias, direitos e deveres para o uso da Internet no Brasil:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte (Brasil, 2009).

Desta forma, o judiciário visa estabelecer uma base legal para o advento de novos conflitos meios tecnológicos, além de servir como amparo para instituir outras diretrizes acerca desse tema.

3.4.2 LEI 12.737/2012 – “Lei Carolina Dieckmann”

Antes da existência dessa referida Lei, o sistema judiciário carecia de uma legislação que tratasse dos crimes virtuais. Esta foi sancionada em novembro de 2012, entrando em vigor em abril de 2013. A mesma objetiva padronizar o entendimento que a internet é um meio para consumação de delitos que ferem bens jurídicos tutelados pelo Direito Penal (Viese Buturi, 2021).

O dispositivo em questão foi denominado “Lei Carolina Dieckmann”, nome de uma atriz de televisão conhecida nacionalmente que teve sua intimidade exposta depois de fotos íntimas terem sido vazadas e espalhadas na internet.

Situações como a desta atriz, passaram a ser foco da referida Lei, em razão da impunibilidade dos agentes, que a partir de seu sancionamento se enquadrariam no ilícito penal. Portanto, para que se enquadre no caso, é necessário a invasão a computadores, e demais aparelhos de cunho pessoal, com a finalidade de obter, adulterar ou destruir dados ou informações.

A partir deste acontecimento, as infrações passaram a ser legisladas pelos artigos 154-A e 154-B do Código Penal e suas respectivas causas de aumento de pena, procedendo-se mediante representação.

Esta lei provocou inovações no Código Penal brasileiro. Um exemplo foram os artigos 266 e 298, os quais tiveram seu texto legal alterado para uma adequação à época da inclusão no mundo virtual. Além deles, em 2017, os crimes definidos no artigo 154-A, entrou para o rol de crimes que permitem a infiltração de agentes policiais. Tendo isso em mente, esta lei veio para trazer inovações e melhorias para as punições dos delitos de invasão de dispositivos informáticos com pena de detenção de três meses a um ano e multa.

3.4.3 Lei Geral de Proteção de Dados Pessoais

Uma outra importante inovação no campo jurídico diz respeito à Lei Geral de Proteção de Dados (LGPD), que foi aprovada em 2018 durante o mandato do ex-presidente Michel Temer e promulgada em 19 de setembro de 2020. Essa legislação tem como principal objetivo proporcionar maior segurança jurídica aos cidadãos, assegurando a proteção de seus dados pessoais tanto no âmbito nacional quanto no internacional. A presente legislação visa resguardar as informações que possam

identificar um indivíduo, abrangendo assim todas as pessoas que tenham seus dados tratados em território brasileiro (Brasil, 2018).

Importante destacar que, além do que se refere aos dados já mencionados, ainda existem aqueles chamados dados sensíveis, que são os pertencentes às crianças e adolescentes, os quais precisam de uma atenção especial e diferente, utilizando de uma maior cautela.

É crucial destacar que a LGPD deve ser observada por qualquer indivíduo presente em território brasileiro, independentemente de sua nacionalidade. Quando se trata do compartilhamento de dados em nível internacional, é imperativo estabelecer protocolos que assegurem tanto a segurança quanto o pleno cumprimento da legislação (Molina, 2021).

Por fim, ela desempenha o papel fundamental de gerenciar riscos e prevenir falhas. Ela exige que aqueles que detêm dados pessoais elaborem normas de administração, implementem medidas de segurança e, em caso de vazamento de dados, notifiquem imediatamente a ANPD (Autoridade Nacional de Proteção de Dados Pessoais), o órgão encarregado de fiscalizar a conformidade com a Lei, bem como as partes envolvidas.

4 INFILTRAÇÃO POLICIAL DE AGENTES

No capítulo em questão, será realizada uma trajetória do instituto da investigação, desde suas primeiras discussões até o instituto no meio virtual dos dias atuais. Além disso, trata-se todos os aspectos procedimentais legais ressalvados em lei, bem como sua efetividade na tutela dos bens jurídicos em meios as lacunas legislativas.

4.1 Aspectos Gerais e Evolução

Com a queda da Ditadura Militar no Brasil, juntamente com o advento da Constituição Federal de 1988, dando inicio a era democrática, houve uma abertura nas fronteiras do país que possibilitou avanços na globalização. Com o surgimento da interação digital e avanços nas comunicações, nasceu uma visão mais crítica por parte do cidadão, passando a exigir participação mais ativa na política nacional (Reschke;Wendt; Matsubayaci, 2021).

Em meados de 80 e 90, surgiram organizações criminosas diante das falhas presentes no sistema penitenciário. Duas, em ocasião, tomaram maior destaque nacionalmente logo após a criação, são estas o Primeiro Comando da Capital (PCC) e o Comando Vermelho (CV). Estas ampliaram sua forma de atuação, tipologias de crimes e áreas de atuação, incluindo rotas dentro e fora do país, causando preocupação no governo (Reschke;Wendt; Matsubayaci, 2021).

Diante da complexidade no combate ao crime organizado foi necessário tomar uma atitude por parte do Estado em estabelecer medidas especiais para o enfrentamento, tratando o assunto de forma mais profunda e especifica, sem violar os valores do Estado Democrático de Direito.

Nesse contexto, Michel Temer, ex-presidente e na época então deputado federal, propôs um projeto de Lei nº 3.516 de 1989, objetivando tratar os meios operacionais para combater e prevenir os crimes cometidos pelas organizações criminosas, que posteriormente foi convertido na Lei nº 9.034 de 1995 dando inicio a discussão do legislativo acerca da infiltração de agentes, pois em seu artigo 2º previa o instituto mencionado, com a seguinte redação:

> Art. 2º Em qualquer fase de persecução criminal são permitidos, sem prejuízo dos já previstos em lei, os seguintes procedimentos de investigação e formação de provas:
> (...)
> **V – infiltração por agentes de polícia ou de inteligência, em tarefas de investigação, constituída pelos órgãos especializados pertinentes, mediante circunstanciada autorização judicial. (Inciso incluído pela Lei nº 10.217, de 11.4.2001)** (Brasil, 1995).

Contudo, o texto foi vetado pelo Presidente, por não condicionar a infiltração à autorização do Poder Judiciário, o que contrariava o interesse público, tendo em vista que o agente poderia agir sem permissão.

Alguns anos depois, foi sancionada a Lei de Drogas (Brasil, 2006), que dispunha em sua redação, no seu artigo 53 inc. I, a infiltração de agentes no momento da investigação, mediante autorização judicial e ouvido o Ministério Público. Mas tão somente em 2013, sete anos depois a Lei de Crimes Organizado foi recepcionada, trazendo em seu seio novas técnicas de investigação, especialmente o instituto então abordado como forma de obtenção de provas:

> Art. 3º Em qualquer fase da persecução penal, serão permitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção da prova:
> I - colaboração premiada;
> II - captação ambiental de sinais eletromagnéticos, ópticos ou acústicos;
> III - ação controlada;
> IV - acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais;
> V - interceptação de comunicações telefônicas e telemáticas, nos termos da legislação específica;
> VI - afastamento dos sigilos financeiro, bancário e fiscal, nos termos da legislação específica;
> **VII - infiltração, por policiais, em atividade de investigação, na forma do art. 11;**
> VIII - cooperação entre instituições e órgãos federais, distritais, estaduais e municipais na busca de provas e informações de interesse da investigação ou da instrução criminal (Brasil, 2013).

Partindo para a abordagem principal, em 2017, em um contexto onde a modernização já tinha avançado e os meios virtuais já eram uma realidade presente no dia a dia da população, surgiu o instituto da infiltração nos meios virtuais,

mediante o sancionamento da Lei 13.441/17, um marco no avanço da polícia judiciária (Reschke;Wendt; Matsubayaci, 2021).

Ainda de acordo com o disposto pelos autores, apesar da referida ser mais recente, a Lei 12.850/2013 apresenta também dispositivos importantes sobre a infiltração e questões necessárias acerca do tema, sendo vista como a norma procedimental geral da técnica, sendo também um importante passo procedimental, servindo de norte para os demais textos legais que passam a prever a tal ferramenta da investigação, servindo como norte naquilo que forem omissos.

No mais, a Lei 13.441, principal instituto abordado nesse trabalho, traz um rol taxativo de crimes previstos no Estatuto da Criança e do Adolescente, já abordados anteriormente, que visam combater crimes contra a dignidade sexual, além da modalidade presente no artigo 154-A do Código Penal Brasileiro, instituto que surgiu com a Lei Carolina Dieckman. (Brasil, 2017). Ademais, a lei carrega consigo detalhes acerca da investigação, tais como prazos, competências, dentre outros.

4.2 Aspectos Procedimentais

4.2.1 Legitimados

De acordo com a Lei 12.850/13, na redação do seu artigo 10, reza que:

> Art. 10. A infiltração de agentes de polícia em tarefas de investigação, representada pelo delegado de polícia ou requerida pelo Ministério Público, após manifestação técnica do delegado de polícia quando solicitada no curso de inquérito policial, será precedida de circunstanciada, motivada e sigilosa autorização judicial, que estabelecerá seus limites (Brasil, 2013).

Esse instituto em questão possibilitou o preenchimento de várias lacunas existentes na Lei nº 9.034/1995, inovando o ordenamento ao dispor desse importante meio de obtenção de prova.

Desta forma, pode-se destacar alguns pontos importantes. Inicialmente, a infiltração só poderá ocorrer mediante a representação da autoridade policial, nestes termos, o delegado de polícia, ou a requerimento do Ministério Público. Não

obstante, o juiz competente antes de decidir pelo deferimento, ouvirá o MP, em conformidade com o sistema acusatório postulado em nosso Código de Processo Penal.

Ainda neste seguimento, é necessário o posicionamento do Ministério Público, para que não haja maculação do sistema vigente, e desta forma, o magistrado não comprometeria sua imparcialidade ao decretar a infiltração de ofício, respeitando a igualdade das partes. Contudo, diante da determinação, o juiz estaria impedido de analisar os eventuais pedidos e de participar da instrução criminal (Reschke;Wendt; Matsubayaci, 2021).

Entretanto, é imprescindível, mesmo diante do requerimento do MP, que haja a manifestação da autoridade policial, dispondo de seu pronunciamento acerca da adequação da infiltração no caso em questão. Sendo assim, essa exigência reforça que o critério deve ser primordialmente policial, levando como prioridade a segurança do agente infiltrado (Reschke;Wendt; Matsubayaci, 2021).

Nesse ponto valem as lições de Roque, Távora E Alencar (2016, p. 626) ao comentar a Lei das Organizações Criminosas:

> (...) andou muito bem o legislador em estabelecer tal requisito, pois, estando o delegado na condução do inquérito e à frente da investigação, tem maiores condições de aquilatar a viabilidade de uma medida desta natureza. Com efeito, de nada adiantaria as boas intenções ministeriais no sentido da autorização judicial se o delegado demonstra, por exemplo, que a possibilidade de o agente vir a ser descoberto é muito grande.

Salienta-se que a figura do delegado de polícia, como líder da Policia Judiciária, é a autoridade com capacidade para verificar as qualidades técnicas e estruturais para a realização desse instrumento investigativo. Destarte, o instituto determina que as atividades serão realizadas por “agente de policia em atividade de investigação”, o que compreende inegavelmente estes compõem o corpo da Policia Civil e a Federal. Em síntese, os agentes das corporações mencionadas, estão elencados no artigo 144, inc. I e §4º da Constituição Federal (Brasil, 2013; Santos, Awuino, 2019).

No mais, Francisco Sannini Neto (2017) ressalta que para a infiltração ser executada de maneira correta, exige-se uma preparação adequada por parte do

agente, especialmente quando se trata em meios virtuais, sendo essencial o conhecimento acerca de *softwares* e um conhecimento mais aprofundado de outras técnicas para o êxito da investigação.

Em suma, o mesmo autor destaca que, caso não exista agentes da policia aptos para a realização da tarefa, o procedimento não deve ser dado prosseguimento, em virtude da possibilidade de comprometer a produção de informações objetivando o correto uso do *jus puniende* do Estado.

4.2.2 Requisitos para a infiltração

A priori, no próprio corpo da Lei nº 13.441/17 e no artigo 190-A do Estatuto da Criança e do Adolescente, traz um rol taxativo de crimes que permitem a infiltração virtual de agentes.

Na redação do texto legal, não existe exigência a demonstração de indícios de autoria em relação aos crimes elencados, contudo, analisando o artigo do ECA anteriormente citado, em seu inc. II e §3º é possível concluir que este meio investigatório depende da existência de autoria, sendo esta uma excepcionalidade quando os demais meios de obtenção de provas não forem suficientes. Ademais, o próprio Código de Processo de Penal determina em seu artigo 4º que a abertura do inquérito “tem por fim a apuração das infrações penais e sua autoria” (Brasil, 1990; Brasil, 1941).

Diante da representação da autoridade policial e requerimento do Ministério Público, o juiz autorizará o ingresso ou não de agentes, com um prazo previsto em lei de 90 dias, suscetível a prorrogação, contudo, esta não poderá ultrapassar o prazo máximo de 720 dias, dentro dos quesitos já estipulados: ser uma prova subsidiária; seguir um procedimento sigiloso; obedecendo ao rol taxativo e técnica especial (Melo, 2021).

Importante salientar que a infiltração em crimes virtuais contra a dignidade sexual da criança e do adolescente é imprescindível, em grande maioria dos casos, para a deflagração das infrações. Como já abordado anteriormente, os investigados costumam seduzir os menores de alguma maneira, sendo assim, é necessário a presença do agente para desvendar os perfis que costumam praticar esses crimes,

encontrando os pedófilos e abusadores que estão por trás do anonimato (Melo, 2021).

Nestes casos, o policial irá interagir com outros criminosos, utilizando de meios necessários para conseguir se disfarçar no meio dos investigados, podendo demonstrar interesse em manter relação sexual com crianças, e também interagir por meio de sala de bate papo, ou redes sociais que são alvos da investigação, no final, toda prova e documentação obtida será encaminhada para análise ao judiciário (Neto, 2017). Sobre essa temática, Jorge (2018, p. 208) aponta o seguinte:

> Como estabelecido na Lei todos os atos eletrônicos praticados durante operação serão registrados, gravados, armazenados e encaminhados para Vossa Excelência e para o Ministério Público, juntamente com o relatório circunstanciado.

Condizente com que afirma Jorge (2018), o autor esclarece que o agente, após a autorização judicial, irá se infiltrar, adentrando em grupos que tenham por finalidade a prática de crimes contra dignidade sexual de menores, interagindo diretamente com os criminosos buscando descobrir sua identidade bem como os crimes praticados.

No mais, importante destacar que, diferentemente da Lei 12.850/13 (art. 14, I), a Lei 13.441/17 não exige a concordância do agente infiltrado para a sua realização. Nesse ponto, o legislador estabeleceu de forma coerente, tendo em vista que esse procedimento investigatório não põe em risco a integridade física do agente (Neto, 2017).

Em suma, podemos arrolar que os requisitos estabelecidos para a infiltração virtual são: a) indícios de autoria ou participação nos crimes previstos na Lei 13.441/17; b) o esgotamento de outros meios de obtenção de provas; c) e, por fim, a autorização judicial.

4.2.3 Prazo de duração

Tendo como comparativo a Lei de Organização Criminosa, é plausível mencionar algumas diferenças. Primeiramente, o legislador impôs um limite na redação da lei para a duração da infiltração de agentes, impondo um prazo

determinado para que esta chegue ao fim. No artigo 10, §3º da referida Lei, encontra-se a seguinte redação: “A infiltração será autorizada pelo prazo de até 6 (seis) meses, sem prejuízo de eventuais renovações, desde que comprovada sua necessidade.” Desta forma, ressalta-se que há a possibilidade de prorrogação, não havendo limites para renovações, contanto que seja demonstrada a necessidade para tal feito (Brasil, 2013).

Entretanto, a Lei de 13.441/17 que trata da infiltração virtual, trouxe em seu corpo um prazo diverso ao estabelecido pela Lei de Organizações Criminosas, a qual dispõe no artigo 190-A, inciso III, que o prazo não poderá exceder noventa dias, podendo ser renovado desde que não ultrapasse 720 dias, demonstrando o estado de necessidade e mediante autorização judicial”. Ou seja, este mesmo dispositivo, ao contrário do disposto na Lei de Organizações Criminosas, estabeleceu um termo para que a operação chegue ao fim.

Para Henrique Hoffmann (2017), Delegado de Polícia Civil do Paraná, estabelecer um limite de renovações não é eficaz:

> Andou mal o legislador ao estabelecer um limite de renovações, pois se demanda tempo para obter confiança do interlocutor e com isso coletar os elementos suficientes e identificar todos os criminosos. A imposição arbitrária de um prazo máximo pode colimar na interrupção forçada da operação e a colocação de vítimas em situação de risco. Por isso mesmo, sequer a infiltração presencial (mais gravosa e arriscada) prevê limite para o número de renovações, e a jurisprudência admite sucessivas renovações de medidas como a interceptação telefônica.

Em comentários acerca deste instituto, Márcio André Lopes Cavalcante (2017) através do Dizer o Direito, afirma que a finalidade principal dos limites que o legislador impôs era principalmente evitar que, bem como na interceptação telefônica, as investigações excedessem o limite de tempo, prejudicando a celeridade ao durar muitos anos.

Seguindo a linha de raciocínio do mesmo autor, ele também expõe algumas críticas a instituição de prazo limite de renovações. De início, ele relata a dificuldade de acesso as redes que envolvam a pedofilia, tendo em vista que são muito fechadas e restritas, desta forma, é certo que o agente encontrará dificuldades para adquirir confiança e efetivamente se infiltrar. Portanto, significa dizer que, em

alguns casos, talvez a investigação seja interrompida no momento mais propicio para o agente lograr êxito e conseguir colher informações que fossem determinantes para a conclusão do caso.

Como segunda motivação, o autor trata dos direitos humanos do investigado. Ao realizar um comparativo, como com a interceptação telefônica, é perceptível que não existe uma violação tão intensa do investigado, não violando profundamente sua intimidade, afinal, as informações colhidas acerca do caso serão fornecidas pelo próprio investigado.

Em síntese, grande maioria das doutrinas se posicionam acerca desse prazo, chegando à conclusão que o prazo estabelecido pelo legislador, bem como o máximo de renovações para que haja a continuidade da operação foi um erro.

4.2.4 Sigilo

É de conhecimento que o próprio Código Penal, na redação do artigo 234-B, que os processos presentes no Título VI – Dos Crimes Contra Dignidade Sexual correrão em segredo de justiça, preservando a integridade do ofendido, bem como as informações que possam ofender sua integridade.

Ademais, o legislador se preocupou em estabelecer e reafirmar acerca desse sigilo na lei. No artigo 190-B, da Lei 13.441/17, prevê que todas as informações obtidas resultantes da investigação devem ser encaminhadas ao magistrado responsável pela autorização, que terá de zelar pelo sigilo. Outrossim, para que haja a eficácia do procedimento, a sigilosidade da investigação deve se manter até o final das diligências. Desta forma, as únicas pessoas que poderão ter acesso aos autos são as figuras do Magistrado, o Ministério Público e o Delegado de Polícia (Neto, 2017).

Desta forma, pode-se concluir que o sigilo é indispensável em razão das características do procedimento que, por sua vez, perderia uma de suas principais finalidades caso fosse realizada com conhecimento dos respectivos acusados e advogados, estando fadada ao fracasso (Mendroni, 2016).

4.2.5 Responsabilidades e direitos do agente infiltrado

Ao tratar da responsabilidade do agente infiltrado no meio virtual, o artigo 190-C, trazido pela Lei 13.441/17 ao Estatuto, exclui o policial da ilicitude do ato de ocultar sua identidade para realizar as investigações pertinentes.

Para Cunha e Pinto (2018), este dispositivo foi criado no intuito de evitar que o agente fosse punido pelo constante no artigo 190-A do mesmo dispositivo, contudo, o legislador não se atentou ao fato que, o anonimato por si não constitui fato típico, muito menos a ocultação da identidade, tendo em vista que a concretização de uma infração só ocorreria se o agente obtivesse vantagem ilícita causando dano a outrem. Os autores ainda complementam:

> É certo que no caso da infiltração virtual não é fácil vislumbrar hipóteses em que o agente policial pudesse ser colocado em uma situação na qual lhe seria inexigível outra conduta a não ser a criminosa, pois, pelas próprias características dessa forma de infiltração, não deve haver contato pessoal entre ele e os autores dos crimes sob investigação.

Dessa forma, é notório que o legislador deixou uma lacuna quando se trata da responsabilidade do agente. Outro ponto a ser colocado em exposição seria a posse de materiais pode vir a receber ao colher informações acerca dos delitos, bem como seu armazenamento e transmissão. Além do já exposto, o servidor ainda pode estar em constante comunicação com as vítimas e com os autores dos crimes, o que poderia incorrer em assédio.

Cunha e Pinto entendem que a atipicidade também deve abarcar as condutas que derivam ou as circunstâncias que o agente se coloca para tratar da investigação desses crimes, como armazenar imagens de cunho pornográfico-infantil observando o artigo 241-B, §2º do ECA:

> Art. 241-B. [...] §2o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241-A e 241-C desta Lei, quando a comunicação for feita por:
> **I – agente público no exercício de suas funções;**
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o

> recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.

Ademais, o parágrafo único do artigo 190-C do ECA dita que o agente estar suscetível a responder pelos seus excessos, o que pressupõe a proporcionalidade da investigação. Mas quanto a este ponto ainda existe debates pertinentes por parte dos doutrinadores, pois de fato, o que configuraria um excesso? Os autores anteriormente citados citam como exemplo a situação em que um agente, além de portar as imagens, decide encontrar uma criança ou adolescente com finalidade de praticar atos libidinosos, utilizando a investigação como desculpa o que acarretaria uma sanção criminal e disciplinar (Cunha; Pinto, 2018).

Em contraponto, a legislação em si não traz em seu corpo os direitos do infiltrado, contudo, a Lei de Organizações Criminosas que foi criada anteriormente, em seu artigo 14, sendo estes:

> Art. 14. São direitos do agente:
> I - recusar ou fazer cessar a atuação infiltrada;
> II - ter sua identidade alterada, aplicando-se, no que couber, o disposto no art. 9º da Lei nº 9.807, de 13 de julho de 1999, bem como usufruir das medidas de proteção a testemunhas;
> III - ter seu nome, sua qualificação, sua imagem, sua voz e demais informações pessoais preservadas durante a investigação e o processo criminal, salvo se houver decisão judicial em contrário;
> IV - não ter sua identidade revelada, nem ser fotografado ou filmado pelos meios de comunicação, sem sua prévia autorização por escrito.

Tendo em mente isso, é plausível realizar uma analogia com o referido artigo, perante dois argumentos. O primeiro seria em razão da proteção por parte do Estado para com o seu servidor, o segundo seria que, em maior parte dos casos, os crimes contra a dignidade sexual de crianças e adolescentes são praticados por organizações. Podendo concluir que é perfeitamente cabível a aplicação do artigo 14 da Lei 12.850/13 para o instituto da investigação virtual (Cunha; Pinto, 2018).

4.3 Efetividade da norma para o ordenamento jurídico

Abordados os aspectos relevantes acerca do instituto no tópico anterior, há ressalvas importantes acerca da infiltração. Tratando inicialmente das responsabilidades do agente, é permitido que este pratique crimes desde que obedeça a devida proporcionalidade, o que, por conseguinte, configuraria de fato a inexigibilidade de conduta diversa, não sendo mais culpável e ocorrendo a isenção da pena. Devido a gama diversa de crimes, não se pode constatar que efetivamente a lei abarcará todas as possíveis condutas que podem prejudicar o agente.

Desta forma, não é plausível que o Poder Judiciário, bem como também a figura do Estado, que o agente pratique atos heroicos e totalmente coerentes, restando apenas a possibilidade de agir com cautela, visando sempre evitar o evento mais danoso de suas condutas. Afinal, para que haja uma investigação mais afundo, é necessário que este conquiste a confiança dos investigados e haja de acordo com os ilícitos, e, talvez dessa forma, consiga colher provas (Nicci, 2013).

Além disso, deve-se compreender que a infiltração exige um estudo aprofundado, como já exposto, o que contradita o imposto pelo legislador acerca dos prazos, os quais não são suscetíveis a renovação, diferentemente ao que ocorre nas investigações das organizações. Como já explanado no corpo do trabalho, a infiltração nas camadas mais profunda da internet são atualmente uma das maiores dificuldades, ademais, aliada ao fato dos próprios investigados serem anônimos ou de difícil acesso, torna o trabalho árduo e dificultoso.

A Polícia Judiciária por si já possui um grande déficit quando se trata de estrutura e amparo tecnológico, o que, consequentemente interfere na celeridade das investigações, necessitando de uma atenção maior por parte do Ministério da Justiça e da Segurança Pública. Essa inovação legislativa surgiu sem que houvesse anteriormente ferramentas mais modernas, além de cursos preparatórios que tratam da coleta de vestígios e técnicas de interrogatório, dentre outras etapas importantes no procedimento (Brasil, 2022).

É primordial também o auxilio técnico de outros países tendo em vista os diversos tratados que visam combater esses crimes, a exemplo, os Estados Unidos. O país em questão é um dos mais avançados tecnologicamente, estando a frente no quesito de investigações, as quais ocorrem por meio de agências americanas, como FBI e o Serviço Secreto. Afinal, a existência de tratados internacionais, como a

Convenção de Budapeste, visa a colaboração entre os países, ampliando a tutela dos bens em questão (Brasil, 2023).

Diante dos argumentos expostos, há de se exigir que o Poder Legislativo entenda a tamanha importância ao tratar da lesividade desses direitos de crianças e adolescentes, principalmente em crimes de tamanha perversidade, que causam traumas irreversíveis no desenvolvimento. Nesse contexto, fica clara a necessidade de uma revisão legislativa a fim de sanar lacunas, possibilitando a inserção do agente até a conclusão da investigação e da junta de todos os elementos probatórios colhidos no momento da infiltração. Outrossim, o Estado deve direcionar investimentos específicos a segurança, colaborando diretamente com a formação do agente, desta forma, seria mais propício o sucesso investigativo.

Imperioso destacar que, quanto aos direitos e deveres do agente, sempre haverá diversas possibilidades que perpassem a linha tênue entre o efetivo exercício de suas atividades e a consumação do crime. A norma jurídica por si deve contemplar sua forma genérica, tentando abranger a maior quantidade de ilícitos, contudo, o legislador tem o papel fundamental de analisar e propor novidades nos institutos, adequando as inúmeras situações que podem ocorrer.

Em suma, não há o que se falar em prazo sem renovações na legislação, isso pode caminhar para o fracasso da operação, apenas dificultando o colhimento de provas que são necessárias para efetiva proteção dos bens tutelados e punição dos acusados.

CONSIDERAÇÕES FINAIS

A temática abordada nessa pesquisa é extremamente complexa, tendo em vista esta tratar-se da proteção de crianças e adolescentes vítimas de crimes no ambiente virtual. O ambiente virtual se difundiu com o avanço das tecnologias, principalmente por oportunizar uma maior facilidade aos usuários. Entretanto, tal facilidade foi utilizada como mecanismo de práticas criminosas, em especial, contra menores vulneráveis.

A discussão acerca dos crimes virtuais não se tratou de algo novo no cenário nacional. Constatou-se a estruturação de uma cultura digital responsável por manter boa parte das ações humanas dentro das telas, principalmente de crianças e adolescentes, público preferencialmente escolhidos pelos criminosos.

Nesse sentido, a internet como meio propagador de crimes, foi um problema a ser enfrentado pelo sistema jurídico, pois as violações lá cometidas tinha uma característica própria dessas condutas: o desconhecimento do autor das práticas violentas.

Paralelamente ao exposto, com o advento das redes sociais, houve uma explosão na aparição de grupos vulneráveis nesses ambientes. Observou-se no decurso da pesquisa que, 78% dos usuários de internet continham a idade de 9 (nove) a 17(dezessete) anos, como também, 62% desses usuários tinham perfis nas redes. Sendo assim, aliada a falta de supervisão dos pais, esse grupo tornou-se alvo de crimes contra a dignidade sexual.

Outrossim, concomitantemente ao crescimento da internet, foi constatado o avanço da parte mais restrita desta, conhecida como *Dark Web*. Nesse ambiente, o cometimento de crimes são práticas rotineiras. Foi possível constatar condutas como venda de cartões de créditos furtados a prática de venda de órgãos humanos, como também, exploração de pornografia infantil.

Observou-se também que, diante desse cenário, a legislação brasileira buscou tratar sobre os meandros dos crimes informáticos, especialmente no Código Penal e no Estatuto da Criança e do Adolescente (ECA). Entretanto, muitas condutas foram consideradas atípicas pela falta de uma tipificação legal específica que comportasse as necessidades impostas pelo princípio da legalidade.

Ademais, pode-se observar também que, mesmo com a evolução legislativa, crimes de pedofilia, por exemplo, ainda não comportavam sua reprimenda em âmbito virtual. Foi apenas com a lei n° 11.829/08 que o legislador instituiu no dispositivo penal as condutas de aliciamento sexual e divulgação de imagens ocorridas no meio virtual. Outrossim, com a lei n° 12.015/09, que alterou o Código Penal, a conduta de estupro foi ampliada, podendo alcançar o ambiente virtual e ter como sujeitos, menores vulneráveis, pela prática de sextorsão ou *sextorsion*.

Igualmente relevante, o Código Penal e o ECA trataram de tipificar condutas como pornografia infantil, corrupção de menores e divulgação de cenas de estupro ou qualquer material com teor sexual que incluam crianças e adolescentes. Entretanto, não se constatou redução dessas condutas.

Ainda com o intuito de reduzir as práticas criminosas no ciberespaço, pode-se constatar durante a pesquisa que o legislador buscou diversos mecanismos legais com vistas a repressão dessas práticas, como: o marco civil da internet, a Lei n° 12.737/12 (Lei Carolina Dieckmann) e a Lei geral de proteção de dados pessoais.

Cumpre destacar que, mesmo com todo o aparato legislativo vigente, havia dificuldades existentes em razão do avanço dos meios cibernéticos, principalmente no que tange a constatação da autoria dos agentes. Sendo assim, em 2017, foi sancionada a Lei n° 13.441/17, que disciplinou acerca da infiltração policial em âmbito virtual, especificando um rol taxativo de crimes, objetivando combater as condutas contra a dignidade sexual, como também estabeleceu aspectos relacionados a investigação, competências, prazos e responsabilidades dos agentes infiltrados.

Entretanto, foi possível perceber a existência de alguns equívocos pelo legislador na descrição normativa da atuação do agente infiltrado. O prazo estabelecido, como também o quantitativo máximo de renovações, por exemplo, foi um equivoco, tendo em vista a dificuldade natural de adentrar nos ambientes virtuais onde as práticas de crimes contra crianças e adolescentes se desenvolvem, em razão da vastidão das redes, como também, pelo risco existente de impossibilitar uma investigação em desenvolvimento em razão da extinção do prazo.

Por essa razão, restou imprescindível expor que, mesmo se tratando de uma evolução tão necessária para constatar a autoria e materialidade de condutas

no âmbito do ciberespaço, ainda havia muito que progredir. Por mais que o agente infiltrado possa utilizar-se de condutas tidas como reprováveis no ordenamento jurídico com o intuito de criar uma ligação com os criminosos sem ser punido, a norma ainda não pode garantir esse tratamento para todas as condutas. Outrossim, para que a infiltração seja efetiva é indispensável um planejamento aprofundado, o que restou dificultoso, principalmente, pela restrição do tempo de atuação do agente.

Paralelamente, aos problemas descritos, pode-se perceber que, há um distanciamento da norma com a realidade da própria polícia, tendo em vista que, uma investigação desse porte requer uma estrutura capaz de dar suporte aos agentes, com vistas a evitar danos para vítimas e investigador.

Por fim, é imperioso destacar que, o presente trabalho não teve o intuito de esgotar a temática, sendo necessário o desenvolvimento de outras pesquisas para o devido aprimoramento do instituto.

REFERÊNCIAS

AGÊNCIA BRASIL. **Agência Brasil explica: entenda a deep web e a dark web Camadas profundas da internet são indisponíveis para usuários comuns**. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-09/agencia-brasil-explica-entenda-deep-web-e-dark-web (figura 1). Acesso em: 05 set. 2023.

AGÊNCIA BRASIL. **Nove em cada dez crianças e adolescentes são usuários de internet.** 2022. Disponível em: https://agenciabrasil.ebc.com.br/educacao/noticia/2022-08/nove-em-cada-dez-criancas-e-adolescentes-sao-usuarias-de-internet. Acesso em: 29 de ago. 2023.

AGRELA, L.. **WhatsApp cresce até 76% por causa do coronavírus**. 2020. Disponível em: https://exame.com/tecnologia/whatsapp-cresce-ate-76-por-causa-do-coronavirus/. Acesso em: 26 jul. 2020.

ALVES, N.. **Delitos cibernéticos**. Disponível em: https://www.jusbrasil.com.br/artigos/delitos-ciberneticos/1481249006. Acesso em: 01 out. 2023.

ALVES, P.. **Google lança ferramenta para combater pedofilia na internet**. 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/09/google-lanca-ferramenta-para-combater-pedofilia-na-internet.ghtml. Acesso em: 05 out. 2023.

ANDRADE, L.. Cybercrimes na deep web: as dificuldades de determinação de autoria nos crimes virtuais. **Jus.com.br**, 2015. Disponível em: jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicasdedeterminacao-de-autoria-nos-crimes-virtuais/2. Acesso em: 24 set. 2023.

BARBOSA, M. I. A. C.. **Crimes virtuais: a evolução dos crimes cibernéticos e os desafios no combate**. 2020. Trabalho de conclusão de curso (Graduação em Direito) – Pontifícia Universidade Católica, Goiás, 2020.

BARRETO, A. G.; SANTOS, H. dos. **DEEP WEB:** investigação no submundo da internet. Rio de Janeiro: Brasport, 2019.

BERGMAN, M. K. White paper: the deep web surfacing Hidden value. **Journal of Eletronic Publishing**, v. 7, n. 1, 2001. http:// dx.doi.org/10.3998/3336451.0007.104.

BRASIL ESCOLA. **G-8**. Disponível em: https://brasilescola.uol.com.br/geografia/g8.htm. Acesso em: 28 ago. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil.** Brasília: Presidência da república, 1988. Disponível em: Constituição (planalto.gov.br). Acesso em: 01 out. 2023.

BRASIL. **Código penal**. Disponível em: DEL2848compilado (planalto.gov.br). Acesso em: 22 ago. 2023.

BRASIL. **Código de processo penal**. Disponível em: Del3689 (planalto.gov.br). Acesso em: 22 ago. 2023.

BRASIL. **Lei n° 8.069**, de 13 de julho de 1990. Dispõe dobre o Estatuto da Criança e do Adolescente e da outras providências. Disponível em: L8069 (planalto.gov.br). Acesso em: 22 ago. 2023.

BRASIL. **Lei n° 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: L12737 (planalto.gov.br). Acesso em: 21 ago. 2023.

BRASIL. **Lei n° 12.850**, de 02 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: L12850 (planalto.gov.br). Acesso em: 22 ago. 2023.

BRASIL. **Lei n° 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: L12965 (planalto.gov.br). Acesso em: 22 ago. 2023.

BRASIL. **Lei n° 13.441**, de 8 de maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Disponível em: L13441 (planalto.gov.br). Acesso em: 22 ago. 2023.

BRASIL. **Lei n° 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019) Vigência. Disponível em: L13709 (planalto.gov.br). Acesso em: 20 ago. 2023.

BRASIL. Ministério da Justiça. **Brasil e Estados Unidos atualizam método de investigação de crimes cibernéticos e moeda digital**. 2023. Disponível em: Notícias — Ministério da Justiça e Segurança Pública (www.gov.br). Acesso em: 21 out. 2023.

BRASIL. Ministério Público Federal. **Crimes cibernéticos** / 2ª Câmara de Coordenação e Revisão, Criminal. Coletânea de artigos, v. 3. Brasília: MPF, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 10 set. 2023.

BRASIL. Ministério Público Federal. **Crimes cibernéticos: manual prático de investigação.** São Paulo: Procuradoria da República de São Paulo: 2006, p. 79 a 100.

BRASIL. Supremo Tribunal Federal (2° grau). **HC 1.331.48**, Habeas corpus. Processual penal e penal. Writ substituto de recurso extraordinário: admissibilidade. Delatio criminis: diligências prévias. Possibilidade. Licitude da interceptação telefônica determinada pelo juízo natural da causa. Factível a razoável prorrogação da medida. O indeferimento de diligência pelo magistrado não configura cerceamento de defesa. Dilação probatória em habeas corpus: inadmissibilidade. Ordem denegada. Relator: Min. Ricardo Lewandowski, DJ 21/02/2017. Disponível em: downloadPeca.asp (stf.jus.br). Acesso em: 25 set. 2023.

BRASIL. Superior Tribunal de Justiça (6° Turma). **REsp 1767902/RJ**. Recurso especial. Penal. Estupro de vulnerável e estupro. Arts. 217-a e 213, ambos c/c o 226, ii, todos do cp. Continuidade delitiva. Crimes da mesma espécie. Requisitos objetivos e subjetivos. Lapso temporal. Período superior a 2 anos. Recorrente: Ministério Público do Estado do Rio de Janeiro. Relator: Ministro Sebastião Reis Júnior, sexta turma, julgado em 13/12/2018, dje 04/02/2019). Disponível em: Revista Eletrônica (stj.jus.br). Acesso em: 15 out. 2023.

BRASIL. Superior Tribunal de Justiça (6° turma). **Informativo n° 685 de 22 de fevereiro de 2021.** Estupro de vulnerável. Contato físico direto. Prescindibilidade. Qualquer ato de libidinagem. Contemplação lasciva por meio virtual. Suficiência. HC 478.310/PA, Rel. Min. Rogério Schietti, Sexta Turma, por unanimidade, 09/02/2021. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?aplicacao=informativo&acao=pesquisar&livre=@CNOT=%27018011%27. Acesso em: 04 out. 2023.

BRASIL. Tribunal Regional Federal da 3ª Região. **Escola de Magistrados Investigação e prova nos crimes cibernéticos.** São Paulo: EMAG, 2017. p. 352.

CABETTE. E. L. S.. **A pedofilia na era digital à luz do Estatuto da Criança e do Adolescente.** Disponível em: https://www.jusbrasil.com.br/artigos/a-pedofilia-na-era-digital-a-luz-do-estatuto-da-crianca-e-do-adolescente-por-caio-tacito-griecco-de-andrade-siqueira/239700073. Acesso em: 02 out. 2023.

CASTRO, H. H. M. de. Lei 13.441/17 instituiu a infiltração policial virtual. **Revista Consultor Jurídico**, mai. 2017. Disponível em: https://www.conjur.com.br/2017-mai16/academia-policia-lei-1344117-instituiu-infiltracao-policial-virtual. Acesso em: 10 de out de 2023.

CASTRO, T. C. de. Crimes virtuais: crimes cibernéticos e as considerações sobre a criminalidade na internet. **Conteudo Juridico**, Brasilia-DF, jun. 2022. Disponível em: https://www.conteudojuridico.com.br/consulta/artigos/58585/crimes-virtuais-crimes-cibernticos-e-as-consideraes-sobre-a-criminalidade-na-internet. Acesso em: 12 ago. 2023.

CAVALCANTE, M. A. L.. Comentários à infiltração de agentes de polícia na internet para investigar crimes contra a dignidade sexual de criança e de adolescente. 2017. **Dizer Direito.** Disponível em: https://www.dizerodireito.com.br/2017/05/comentarios-infiltracao-de-agentesde.html. Acesso em: 10 out. 2023.

CECÍLIO, T.; MOREIRA, T. C.; SANTOS, A.. A proteção dos menores na sociedade da informação: desafios criados pelas redes sociais, Braga: **Scientia Ivridica**, Universidade do Minho, Tomo LXV, N.º 341 (2016). p. 260.

CHILDHOOD BRASIL. **Navegar com segurança: por uma infância conectada e livre de violência sexual.** 3. ed. São Paulo: CENPEC: Childhood Instituto. WCF Brasil, 2012. Livro eletrônico. Disponível em: https://www.childhood.org.br/app/uploads/2022/12/navegar-com-seguranca.pdf. Acesso em: 23 set. 2023.

COLAB. **Infância vigiada: cresce exposição de crianças em plataformas digitais.** Disponível em: https://blogfca.pucminas.br/colab/infancia-vigiada-cresce-exposicao-de-criancas-em-plataformas-digitais/. Acesso em: 22 set. 2023.

CRISTINA BORGES, D.; PIONER SARTORI, L.; Sebastião de Barros, M.;. (2015). A Deep Webe a Relação com a Criminalidade na Internet. **Revista Eletrônica Direito & TI**, 1(3), 6. Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/32. Acesso em: 07 out. 2023.

CUNHA, R. S.; PINTO, R. B.. Infiltração de agentes de polícia na internet. **Migalhas**, 2017. Disponível em: https://www.migalhas.com.br/dePeso/16,MI258738,101048-Infiltracao+de+agentes+de+policia+na+internet. Acesso em 24 set. 2023.

DIAS, V. E. M. **A Problemática da Investigação do Cibercrime**. 2010. Disponível em: www.verbojuridico.net/doutrina/2011/veradias_investigacaocibercrime.pdf. Acesso em: 06 out. 2023.

FELICIANO, G. G.. **Informática e Criminalidade**: Primeiras Linhas. Ribeirão Preto: Nacional de Direito, 2001. p. 137.

FERNANDES, M. A. D.; LIMA, F. Z. S; PEDROZA, E. S. F. O de. **A prática dos crimes cibernéticos como violação dos direitos da criança e do adolescente.** 2023. Disponível em: Microsoft Word - PROJETO ALUNO (MODELO) (animaeducacao.com.br). Acesso em: 23 set. 2023.

G1. **Homem é preso no ES em operação da PF contra pedofilia**. Disponível em: https://g1.globo.com/es/espirito-santo/noticia/2019/01/24/homem-e-preso-no-es-em-operacao-da-pf-contra-exploracao-sexual-de-criancas-e-adolescentes.ghtml https://www.lexml.gov.br/urn/urn:lex:br:superior.tribunal.justica;turma.5:acordao;rhc:2016-08-02;70976-1550478. Acesso em: 27 set. 2023.

GUERRA, G. G. A.. **Infiltração virtual dos agentes policiais:** Como meio de investigação de prova na persecução penal. 2019. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Evangélica, Anápolis, 2019.

GRECO FILHO, V.. Algumas observações sobre o direito penal e a internet. **Boletim do IBCCrim**. São Paulo,v. 1, ano. 8, n. 95, p. 3, out. 2000. Disponível em: Vista do Algumas observações sobre o Direito penal e internet (mackenzie.br). Acesso em: 27 ago. 2023.

IZIDRO, A.. **Crimes Cibernéticos**. 2023. Trabalho de conclusão de curso (Graduação em Direito) – Universidade São Judas Tadeu, São Paulo, 2023.

JORGE, H. V. N.. **Investigação criminal tecnológicas:** contém modelos de representações e requisições, além de procedimentos para investigação em fontes abertas – Volume 1. 1° ed. Rio de Janeiro: Brasport, 2018.

JUSBRASIL. **Crimes virtuais:** conceito e seus tipos. Disponível em: https://carmo311.jusbrasil.com.br/artigos/307607071/crimes-virtuais-conceito-e-seus tipos. Acesso em: 02 out. 2023.

KENSKI, V. M.. Dicionário crítico de educação e tecnologias e de educação a distância. **Cultura digital**, Campinas: Papirus, p. 139-144, 2018.

LUCCHESI, Â. T.; HERNANDEZ, E. F. T.. Crimes virtuais: ciberbullying, revenge porn, sextortion, estupro virtual. **Revista Officium: estudos de direito**, v. 1, n. 1, p. 2, 2018.

MASSON, C.. **Direito penal esquematizado – Parte geral** – . 9. ed. Rio de Janeiro: Forense; São Paulo: Método, 2015.

MARTINELLI, J. P. O.. **Aspectos relevantes da criminalidade na internet**. Disponível em: http://jus.com.br/artigos/1829/aspectos-relevantes-da-criminalidade-na-internet. Acesso em: 09 out. 2023.

MELO, M. P. P. T. de. **Infiltração policial virtual no âmbito dos crimes contra dignidade sexual de crianças e adolescentes: reflexões sobre a constitucionalidade da Lei 13.441/2017.** 2021. Trabalho de Conclusão de Curso (Graduação em Direito) – Escola de Direito de Brasília, Brasília, 2021.

MENDRONI, M. B.. **Crime organizado:** aspectos gerais e mecanismos legais. São Paulo: Atlas, 2015.Livro eletrônico. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2016/Bol16_02.pdf. Acesso em: 14 out. 2023.

MULLER, M. A.. O problema da pedofilia. **Cultura e Fé –Revista**, PortoAlegre: Instituto de Desenvolvimento, v.25, 2002.

NETO, F. S.. **Infiltração de agentes é um avanço nas técnicas especiais de investigação criminal.** 2017. Disponível em: https://www.jusbrasil.com.br/artigos/infiltracao-virtual-de-agentes-e-um-avanco-nas-tecnicas-especiais-de-investigacao-criminal/457258991. Acesso em: 15 out. 2023.

NUCCI, G. S. de. **Código penal comentado**. 2. ed. São Paulo: Revista dos Tribunais, 2003.

NÚCLEO DA INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil**: TIC Kids Online Brasil. 2018. Disponível em: Cetic.br - TIC Kids Online Brasil. Acesso em: 09 ago. 2023.

OLIVEIRA, C. L. ; VIEIRA, G. S.. Pornografia infantil: a pedofilia no mundo virtual. **CIPEEX –Congresso Internacional de Pesquisa, Ensino e Extensão**,Goiás, v.3, 2022, ISSN: 2596-1578. Disponível em: http://anais.unievangelica.edu.br/index.php/CIPEEX/article/view/8957/4429. Acesso em: 15 set. 2023.

PAIXÃO, K. M.. Etiologia da pornografia infantil: um olhar crítico sobre a (cyber)pedofilia. **Revista direito e sexualidade**, Bahia, n. 1, p. 03-22, mai. 2022. Disponível em: https://periodicos.ufba.br/index.php/revdirsex/article/view/36861/21119 https://www.childhood.org.br/nossa-causa/. Acesso em: 08 set. 2023.

PIRES, L. M.. A infiltração policial virtual nos crimes contra a dignidade sexual da criança e do adolescente: análise da infiltração sob a ótica da lei 13.441/17. **Intertem@s**, São Paulo, v. 36, n. 36, 2018. ISSN 1677-1281.

POMPÉO, W. A.; SEEFELDT, J. P.. **Nem tudo está no Google: deep web e o perigo da invisibilidade.** *In*: Congresso Internacional de Direito e Contemporaneidade. Santa Maria: UFSM, 2013.

RESCHKE, C.; WENDT, E.; MATSUBAYACI, M.. **Infiltração Policial: da tradicional à virtual.** 1° ed. Rio de Janeiro: Brasfort, 2021.

ROSSINI, A. E. S. de. Informática, Telemática e Direito Penal. **Memória Jurídica**, São Paulo, p. 123, 2004.

ROQUE, F.; TÁVORA, N.; ALENCAR, R. R.. **Legislação Criminal para concursos.** Salvador: Juspodivm, 2016.

ROQUE, S. M.. **Criminalidade Informática: crimes e criminosos do computador**. São Paulo: ADPESP Cultural, 2007. p. 25.

SANTOS, A. P. T. R.. **A infiltração policial virtual como meio de investigação de crimes cibernéticos:** os limites para a obtenção de provas válidas. 2021. Trabalho de Conclusão de Curso (Graduação em Direito) – Centro Universitário de Brasília, Brasília, 2021.

SANTOS, L. G.. **A infiltração policial em organizações criminais como meio de prova.** 2019. Disponível em: https://www.conteudojuridico.com.br/consulta/Artigos/52710/a-infiltracao-policial-em-organizacoes-criminosas-como-meio-de-prova. Acesso em: 27 set. 2023.

SERIBELI, E.. Crime cibernético: estupro virtual e embasamento à infiltração virtual com o advento da lei 13.441/17. **Intertem@ s**, ISSN 1677-1281, v. 36, n. 36, 2018.

SILVEIRA, S. L.. Pedofilia na Internet. **Inova+ Cadernos da Graduação da Faculdade da Indústria**, v. 1, n. 2, 2020.

SOUZA, C. A.; LEMOS, R.. **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar Editora Associada Ltda, 2016. Livro digital. Disponível em: capa Frente marco civil da internet copiar.tif (itsrio.org). Acesso em: 22 set. 2023.

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

STATISTA. **Número de usuários de redes sociais em países selecionados em 2022 e 2027.** Disponível em: https://www.statista.com/statistics/278341/number-of-social-network-users-in-selected-countries/. Acesso em: 05 set. 2023.

TIMACHI, K. B.. **Sextorsão.** 2023. Disponível em: https://www.jusbrasil.com.br/artigos/sextorsao/1738968750. Acesso em: 04 out. 2023.

VENTURA, D. C.. Organização Mundial da Saúde. Vamos falar (corretamente) sobrePedofilia? **Jusbrasil.** Disponível em: https://deniscaramigo.jusbrasil.com.br/artigos/406255800/vamosfalar-corretamente-sobre pedofilia. Acesso em: 05 set. 2023.

VERSI, R.. **Estupro virtual: crime que ganhou evidência após cenas em "Travessia".** Disponível em: http://jornalcobaia.com.br/estupro-virtual-crime-que-ganhou-evidencia-apos-cenas-em-travessia/. Acesso em: 30 set. 2023.

VIEIRA, E.. **Os bastidores da Internet no Brasil**. Editora Manole Ltda, 2003.

VIESE BUTURI, L.; PANZA, L. O. M.. **Direito penal: internet x estupro virtual e pedofilia virtual.** 2021. Disponível em: ARTIGO CIENTIFICO LEONARDO VIESE BUTURI - 9MC - 2017101307.pdf (animaeducacao.com.br). Acesso em: 02 out. 2023.

VIGNOLI, R. G.; MONTEIRO, S. D. Deep Web e Dark Weeb similaridades e dissiparidades no contexto da Ciência da Informação. **Transinformação**, v. 32, e190052, 2020. https://doi.org/10.1590/2318-0889202032e190052.

ZANG, A. K. A.. **Conflito entre responsabilidade parental e a autodeterminação das crianças face aos perigos da utilização das redes sociais.** 2023. 83f. Dissertação (Mestrado em Direito Forense e Arbitragem) – Nova School of Law, Portugal, 2022.