

**FUNDAÇÃO EDUCACIONAL DE ITUVERAVA  
FACULDADE DR. FRANCISCO MAEDA**

**André Mantovani Neto**

**PEDOFILIA NA INTERNET: A DIFICULDADE EM APLICAR A LEI EM CASOS  
DE CRIMES CIBERNÉTICOS**

**ITUVERAVA  
2021**

**ANDRÉ MANTOVANI NETO**

**PEDOFILIA NA INTERNET: A DIFICULDADE EM APLICAR A LEI  
EM CASOS DE CRIMES CIBERNÉTICOS**

**Trabalho de Conclusão de Curso apresentado  
à Faculdade Dr. Francisco Maeda. Fundação  
Educativa de Ituverava para obtenção do  
título de Bacharel em Direito.**

**Orientador: Prof Dr. Antônio Marco Ventura  
Martins**

**ITUVERAVA  
2021**

**ANDRÉ MANTOVANI NETO**

**PEDOFILIA NA INTERNET: A DIFICULDADE EM APLICAR A LEI EM CASOS  
DE CRIMES CIBERNÉTICOS**

**Trabalho de Conclusão de Curso apresentado à  
Faculdade Dr. Francisco Maeda. Fundação  
Educativa de Ituverava para obtenção do título de  
Bacharel em Direito.**

**Ituverava, \_\_\_\_\_ de \_\_\_\_\_ de 2021.**

**Orientador: \_\_\_\_\_  
Nome do Orientador**

**Examinador: \_\_\_\_\_  
Nome do Examinador**

**Examinador: \_\_\_\_\_  
Nome do Examinador**

## **DEDICATÓRIA**

Dedico este trabalho aos meus pais. Sem eles nada seria possível.

## **AGRADECIMENTOS**

Agradeço a Deus, meus pais, meu irmão e todos meus amigos que acreditaram em mim.  
Agradeço também ao meu orientador, Prof. Dr Antônio Marco, por ter me guiado até aqui.

“A Verdadeira motivação vem de realização, desenvolvimento pessoal, satisfação no trabalho e reconhecimento”.

Frederick Herzberg

## **PEDOFILIA NA INTERNET: A DIFICULDADE EM APLICAR A LEI EM CASOS DE CRIMES CIBERNÉTICOS**

André Mantovani Neto<sup>1</sup>

**RESUMO:** O presente estudo tem como foco abordar a dificuldade em aplicar a lei em casos de crimes contra a criança na internet. Como objetivos específicos, busca-se demonstrar a necessidade de adotar medidas para prevenir a pedofilia na internet, assim como identificar e demonstrar os métodos de ações do criminoso. A prática dos cibercrimes gera um ambiente propício para o criminoso praticar os seus delitos sem a devida punição, gerando uma insegurança virtual. O presente estudo consiste em pesquisa de caráter exploratório, com resultados tratados de maneira qualitativa, a partir da revisão bibliográfica crítica. Com o levantamento de informações e de suas análises, foi possível concluir que ainda se faz necessário mais medidas de prevenção, não somente na lei, mas também na conscientização e o entendimento da tecnologia para que as crianças estejam protegidas.

**Palavras-chave:** Internet, Cibercrime, Pedofilia, Lei, Prevenção.

### **PEDOPHILIA ON THE INTERNET: THE DIFFICULTY IN APPLYING THE LAW IN CASES OF CYBERCRIME**

**SUMMARY:** This study focuses on addressing a difficulty in applying a law in cases of crimes against a child on the internet. As specific objectives, it seeks to demonstrate the need to adopt measures to prevent pedophilia on the internet, as well as to identify and demonstrate the criminal's methods of actions. The practice of cybercrimes creates a favorable environment for criminals to practice their crimes without proper punishment, generating virtual insecurity. The present study consists of an exploratory research, with results treated in a qualitative way, from the collection of secondary sources. With the survey of information and its analyses, it was possible to conclude that more prevention measures are still needed, not only in the law, but also in the awareness and understanding of the technology so that the chosen children are protected.

**Keywords:** internet. cybercrime. pedophilia. law. prevention.

## **1 INTRODUÇÃO**

O presente artigo científico tem como foco principal abordar a dificuldade em aplicar a lei nº 11.829, de 25 de novembro de 2008 para os crimes cibernéticos. Segundo Júnior (2019, p.1), são cibercrimes “os crimes que são praticados por meio cibernéticos, ou seja, atividades que envolvam a prática ilícita por meio de um computador na rede informacional de comunicação tecnológica”. Sendo assim, é imperativo a consciência que esse ciberespaço é uma área relativamente nova e muito propensa para o crime, já que mesmo tendo legislação vigente, muitas vezes é impraticável a aplicação da mesma.

A internet é uma das invenções mais revolucionárias na história da humanidade. Ela possibilitou a mensagem instantânea com qualquer pessoa, acesso à informação de forma prática, a democratização do conhecimento, entre várias outras facilidades. Porém, a própria

---

<sup>1</sup> Graduando em Direito pela Faculdade Dr. Francisco Maeda. E-mail: andre.neto@sou.fafam.com.br.

dinâmica da internet, bem como as suas ferramentas de criptografia, possibilitou uma facilidade maior para cometer crimes e, com isso, tais delitos aumentaram de forma considerável. Os crimes de pedofilia, segundo uma nota feita pela Polícia Federal Brasileira em 2020, cresceram mais de 190% durante a pandemia do Corona Vírus. Esse aumento é devido ao fato de que as crianças passaram mais tempo em casa tendo aulas online e, conseqüentemente, passando mais tempo na internet. Isso evidencia claramente que a internet é uma terra fértil para tais crimes (BASTOS, 2021)

Sendo assim, é imprescindível discutir sobre as dificuldades na aplicação do direito para os crimes de pedofilia na internet e de como isso impacta na dinâmica social, além disso, esse padrão de uso da tecnologia projeta uma “terra de ninguém”, em que o criminoso utiliza meios de criptografia para se esconder e aliciar crianças que não tem aptidão necessária para navegar na web, tornando, assim, mais dificultoso a aplicação da lei.

Atualmente há centenas de programas que criptografam o IP do computador e, por consequência de tais programas, muitos criminosos a utilizam, principalmente na “*Deep Web*”, para tornar a internet em um verdadeiro mercado negro de produção e distribuição de pornografia infantil. Dito isso, é possível notar que a pedofilia na internet pode impactar diretamente nas próprias crianças, bem como os pais, através do aliciamento de menores e como os criminosos manipulam a vítima para produzir conteúdo impróprio.

Para tanto, se faz necessário o entendimento da Internet como um todo para que se possa identificar maneiras de como os pais possam de fato supervisionar os seus filhos na rede, bem como apontar a dificuldade em rastrear o criminoso e, com isso, a própria atribuição do delito, fazendo com que o crime aumente de forma considerável. Há de se notar que o direito se molda conforme a realidade.

O presente artigo estabeleceu como problema de pesquisa a seguinte questão: Quais são as principais dificuldades na aplicação da lei federal nº 11.829, de novembro de 2008, para os crimes cibernéticos de pedofilia? Já o objetivo geral é entender como o criminoso age, identificar as principais causas que impedem a aplicação da lei, e também obter um panorama geral do funcionamento da internet para compreender de fato como o criminoso opera nas redes. Para alcançar o objetivo geral, os objetivos específicos serão

- A) Conceituar a pedofilia na internet.
- B) Demonstrar a necessidade de adotar medidas para prevenir a pedofilia na internet.
- C) Discutir os motivos que dificultam a aplicação da lei



O presente estudo consiste em pesquisa aplicada, de caráter exploratório, que, segundo Gil (2002, p.41), “[...] tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito. Geralmente, assume a forma de pesquisa bibliográfica e estudo de caso”. O estudo visa identificar quais são as maiores dificuldades na hora de punir o criminoso que comete delitos na internet, com enfoque na pedofilia. Nesse sentido, os resultados serão apresentados de forma qualitativa, a partir da coleta de informações de fontes secundárias, incluindo pesquisa documental, bibliográfica e revisão de autores significativos.

## **2 PEDOFILIA NA INTERNET**

Para entender esse mal crescente na atualidade, se faz necessário uma contextualização, entendendo o surgimento da internet, o seu crescimento, os crimes virtuais e seus desdobramentos e avanços.

### **2.1 História da internet**

Hoje em dia a internet é uma ferramenta de uso corriqueiro na vida de muitas pessoas. Uma pesquisa feita pelo IBGE (2017) afirma que 82,7% dos domicílios brasileiros têm acesso à internet e essa realidade só tende a aumentar. Mas apesar de hoje o ser humano estar tão dependente dessa ferramenta, a tecnologia começou a ficar popular no meio da década de 1990, com a introdução do “*World Wide Web*”, criada por Timothy Berns-Lee.

O “WWW”, como é popularmente conhecido, possibilitou uma interface sofisticada e acessível para usuários comuns, fazendo com que a internet se popularizasse exponencialmente (LEE, 2015). Entretanto, apesar de ter-se tornado acessível para a massa na última década do século XX, a história da internet é bem mais antiga.

Apesar de a guerra ter ceifado a vida de milhões de pessoas, é inegável que a mesma contribuiu, de certa forma, para o desenvolvimento de algumas tecnologias. A título de exemplo, a Segunda Guerra Mundial contribuiu com o surgimento dos computadores para decodificar e ajudar em cálculos matemáticos para aprimorar as estratégias de batalha (CARVALHO, 2006).

Alan Turing, por exemplo, foi um dos pioneiros da ciência da computação durante a Segunda Guerra Mundial (Hodges, 2012), ajudando o governo britânico a decifrar códigos que a Alemanha nazista utilizava para se comunicar. Se na Segunda Guerra o computador

teve sua origem, foi na Guerra Fria que a comunicação e o controle de informações surgiram e consolidaram (EDWARDS, 1996). Sendo assim, “as principais armas da Guerra Fria foram ideológicas, alianças, propagandas, ajuda estrangeira, prestígio nacional e, acima e por trás de todos eles, o rolo compressor da alta tecnologia”. (EDWARDS, 1996, p. 9).

De modo geral, a Guerra Fria, nome esse cunhado por Bernard Baruch (Sotana, 2014), foi um conflito entre os Estados Unidos e a União Soviética iniciado no pós-guerra até o início da década de 1990, em que ambas as potências procuravam a soberania mundial, tanto no âmbito armamentista quanto no âmbito tecnológico com a corrida espacial (SILVA, s.d.).

Em resposta à União Soviética, que nessa corrida ao espaço lançou o satélite Sputnik I, os Estados Unidos criaram a *Advanced Research Projects Agency* (ARPA), uma agência cujo o foco principal era incentivar a pesquisa e ciências nas universidades (ADABO, 2014), idealizada para prever acontecimentos tecnológicos como a Sputnik I e avançar a tecnologia dos EUA em busca da vitória na Guerra Fria (CARVALHO, 2006).

Nesse viés, a ARPA investiu milhões de dólares em pesquisa para criar uma rede que facilitasse a comunicação entre computadores em diferentes locais. Em 1969, essa agência passou a chamar “ARPANET” que, a princípio, seria uma importante ferramenta bélica.

Um elemento essencial de sua razão de ser era que a rede pudesse sobreviver à retirada ou destruição de qualquer computador ligado a ela, e, na realidade, até à destruição nuclear de toda a “infra-estrutura” de comunicações (“infra-estrutura” era outra palavra nova). Essa era a visão do Pentágono. A visão das universidades era que a Net oferecia “acesso livre” aos usuários professores e pesquisadores.” (BRIGGS;BURK. 2006, p.301).

O projeto foi originalmente criado para objetivos bélicos. Entretanto, em 1980, o ARPANET foi desvinculado dos militares e passou a integrar à outras redes universitárias. Essa desvinculação foi um atrativo para outros visionários que percebiam que a Internet poderia ser muito maior do que realmente era. Assim, como evidenciado anteriormente, Tim Berners-Lee criou outro mecanismo (WWW) para deixar a Internet mais viável e fácil à população geral e, com isso, atraiu empresas como *Yahoo* e *Amazon*, consolidando a Internet de vez no mundo.

Em pouco tempo, a internet tornou-se um atrativo não só para as grandes empresas, mas também para as massas, que a perceberam como uma fonte rica de informações e compartilhamento de conhecimento. Por conseguinte, tem-se que a informação obtida por meio da internet é constituída de dados que foram organizados de modo que tenham um significado e um valor para o destinatário.

Corroborando tal tese, tem-se que:

A informação é um recurso que tem valor para a organização e deve ser bem gerenciado e utilizado [...] é necessário garantir que ela esteja sendo disponibilizada apenas para as pessoas que precisam dela para o desempenho de suas atividades profissionais. (FONTES, 2006, p. 2)

No entanto, é possível destacar também que essa tecnologia atrairia infratores e transgressores das regras e leis, desde o início de seu desenvolvimento, como será visto a seguir.

## **2.2 Definição e primeiros crimes na internet**

Foi abordado, anteriormente, a origem da Internet e, sua importância para o desenvolvimento do processo histórico. Nessa perspectiva, com o advento da internet, tem-se uma transformação das relações interpessoais com a criação de um ciberespaço, em que “a interconexão condiciona a comunidade virtual, que é uma inteligência coletiva em potencial” (LÉVY, 1999, p. 138).

Entretanto, com seu avanço e popularização, muitas pessoas passaram a utilizar a tecnologia como um modo de perpetrar os seus crimes. Hoje uma pessoa má intencionada consegue, facilmente, praticar vários atos, desde a compra ilegal de armas, até o tráfico humano.

Esses crimes podem ser definidos, à luz jurídica, como uma conduta típica, culpável e ilícita, praticada pelo homem (CARVALHO, 2011). Condutas antijurídicas na Internet definem-se como:

[...] qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, tenha facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o autor ou que, pelo contrário, produza um benefício ilícito a seu autor embora não prejudique de forma direta ou indireta à vítima. (LIMA, 2012, p. 13).

Com base nesta definição, é possível dizer que os crimes digitais começaram bem antes da popularização da Internet como um todo. Sendo uma ferramenta bélica, haviam esforços para prejudicar e sabotar a segurança nacional. Para Albuquerque (2006, p. 35):

[...] os primeiros casos de crimes cibernéticos foram na década de sessenta. Eram utilizados computadores como forma de cometimento do crime virtual, como o estelionato. Na referida década foi que começou a ser relatados pela imprensa os primeiros casos de crimes cibernéticos. A partir da década de setenta, começaram os primeiros estudos empíricos sobre a criminalidade cibernética.

É possível notar, de acordo com a pesquisa realizada, que o crime digital se diferenciava do crime cibernético praticado hoje em dia. Porém, com a sofisticação dessa

tecnologia, começou a ser praticado mais crimes, como por exemplo, o caso da atriz Carolina Dieckmann, em que fotos íntimas foram vazadas e os criminosos fizeram chantagem contra a vítima, assim como os crimes de pedofilia na internet (FMP, 2021).

Em resumo, tal análise é fundamental para um melhor entendimento da trajetória do crime digital.

### 2.3 Conceito de pedofilia.

Segundo o relatório “*Out of the Shadows*” (*The Economist*, 2020), o Brasil é o 11º no ranking de abuso e exploração sexual infantil. Apesar de grande parte da população brasileira ter conhecimento sobre o problema, ainda há muita divergência no tocante ao termo pedofilia.

Embora muito erroneamente divulgado como “crime de pedofilia”, a pedofilia em si não é crime. Segundo a Organização Mundial da Saúde, a pedofilia é um transtorno da preferência sexual classificado no Código Internacional de Doenças no grupo 10. Nesse CID10, estão descritos vários transtornos em torno da preferência sexual, dentre eles: Fetichismo, Exibicionismo, Voyeurismo, Sadomasoquismo, Pedofilia, entre outros. Ainda segundo a OMS, a pedofilia é

... uma preferência sexual por crianças, usualmente de idade pré-puberal ou no início da puberdade. Alguns pedófilos são atraídos apenas por meninas, outros apenas por meninos e outros ainda estão interessados em ambos os sexos. A pedofilia raramente é identificada em mulheres. Contatos entre adultos e adolescentes sexualmente maduros são socialmente reprovados, sobretudo se os participantes são do mesmo sexo, mas não estão necessariamente associados à pedofilia. Um incidente isolado, especialmente se quem o comete é ele próprio um adolescente, não estabelece a presença da tendência persistente ou predominante requerida para o diagnóstico. Incluídos entre os pedófilos, entretanto, estão homens que mantêm uma preferência por parceiros sexuais adultos, mas que, por serem cronicamente frustrados em conseguir contatos apropriados, habitualmente voltam-se para crianças como substitutos. Homens que molestam sexualmente seus próprios filhos pré-púberes, ocasionalmente seduzem outras crianças também, mas em qualquer caso seu comportamento é indicativo de pedofilia. (OMS, 1993, p. 215)

A pedofilia é, portanto, um impulso, um desejo por crianças pré-púberes que possui, em geral, segundo a Associação Americana de Psiquiatria, 13 anos ou menos. Agora, quando esse desejo é consumado na forma de abuso sexual, o perpetrador adentra no âmbito jurídico. Logo, o termo que chega próximo ao correto para classificar esses criminosos seria agressor sexual (Rodrigues, 2008), já que pedofilia é a doença.

Para embasar essa tese, “a pedofilia é vista como um ato cometido por pessoas sem-vergonhas, quando, na verdade, é uma doença que precisa ser tratada” (SERAFIM, 2009, p. 109). Sendo assim, a preocupação quanto ao conceito preciso de pedofilia se faz necessário

para endereçar corretamente aquele que comete ato infracional daquele que possui o transtorno propriamente dito.

## 2.4 Perfil do criminoso

O presente tópico tem como objetivo afunilar e evidenciar ainda mais o perfil do criminoso, bem como sinais de alertas e como identifica-los.

Segundo o Manual de Diagnóstico e Estatística das Perturbações Mentais (2014, p. 743) “A prevalência mais alta possível para o transtorno entre os indivíduos do sexo masculino é de cerca de 3 a 5%”. Já para a população feminina, esse número ainda é nebuloso, já que o índice de mulheres com esse distúrbio é bem baixo.

Para ser diagnosticado com Transtorno Pedofílico, o paciente necessita ter uma idade mínima de 16 anos e ser, pelo menos, cinco anos mais velho que a menina ou menino pelo qual o indivíduo sente o impulso sexual (DSM-5, 2013).

Tendo isso como base, ainda há muita discussão a respeito da forma com a qual o distúrbio acomete uma pessoa. Para Serafim *et al.* (2009) o pedófilo pode ter, dentre outras características, altos níveis de testosterona, retardo mental, abuso de álcool e substâncias psicoativas. Já para Spizirri (2008), a maioria dos portadores desse distúrbio sofreram abuso quando criança, seja sexual ou então familiar originado por uma estrutura familiar abusiva. Araújo (2004) diz que o problema pode ser cultural, psicológicos ou econômicos.

Sendo assim, é possível notar que há muitas divergências sobre o que causa essa doença, bem como um possível tratamento, e há pouco estudo com validação científica, sendo todos os dados tirados de forma empírica (SERAFIM *et al.* 2009). Desse modo, é uma tarefa árdua identificar possíveis agressores antes de consumado o crime. Até mesmo os sinais que os agressores podem demonstrar são variados dependendo do perfil do indivíduo. Um exemplo disso são as duas categorias principais de pedófilo: o pedófilo abusador e o pedófilo molestatador (SERAFIM *et al.* 2009).

O primeiro é um indivíduo imaturo, com pouca habilidade social e que tem um comportamento menos invasivo. A análise desse trabalho é focada principalmente nesse grupo, já que o mesmo tende a procurar satisfazer a sua lasciva através da pornografia infantil ou então tentar seduzir o menor utilizando perfis falsos na internet.

Já os pedófilos molestatadores, que podem ser divididos em duas classes, os situacionais e os preferenciais, podem ser pessoas com uma inteligência superior, uma situação econômica vantajada e compulsiva (Molestatador Preferencial), ou então um indivíduo da baixa classe

socioeconômica, antissocial, narcisista e impulsiva (Molestador Situacionais) (SERAFIM et al. 2009).

### 3. MEDIDAS PARA PREVINIR OS CRIMES NA INTERNET

Sendo a internet uma ferramenta de fácil acesso à pessoas de várias idades, se faz necessário adotar algumas medidas para tentar reduzir o dano que possíveis criminosos podem cometer contra crianças. O direito se adequa às necessidades sociais e, como a internet é uma tecnologia que moldou e molda a forma de como as pessoas veem a sociedade, se tornou imprescindível que a legislação também mudasse nesse sentido. Sendo assim, será exposto no tópico a seguir algumas medidas para tentar combater a pedofilia na internet.

#### 3.1 Legislação

Com o avanço sistemático da internet, tornou-se uma necessidade a criação de novas leis para que fosse possível enquadrar os diversos crimes cometidos online e tipifica-las no código penal. Como visto anteriormente, não há tipificação legal no código penal acerca do “crime” de pedofilia. Quando há casos em que ocorre abuso sexual de menores, será recorrido às leis encontradas no “CAPÍTULO II – DOS CRIMES SEXUAIS CONTRA VULNERÁVEL”, como, por exemplo

Art. 217-A. Ter conjunção carnal ou praticar outro ato libidinoso com menor de 14 (catorze) anos:

Pena - reclusão, de 8 (oito) a 15 (quinze) anos.

Art. 218. Induzir alguém menor de 14 (catorze) anos a satisfazer a lascívia de outrem:

Pena - reclusão, de 2 (dois) a 5 (cinco) anos.

Entretanto, como pode ser observado, utilizar somente as leis do direito penal pode provocar uma insegurança jurídica para os crimes contra a criança na internet. Por esse motivo, deve-se recorrer ao Estatuto da Criança e do Adolescente, em que a Lei nº 11.829, de novembro de 2008 qualificou as diversas possibilidades de crimes contra a criança na internet, como por exemplo o artigo 241-E, que definiu o que é cenas de sexo explícito ou pornográfica.

Sendo assim, essa lei gerou um respaldo maior para imputar o delito, bem como tornou *novatio legis in pejus*, já que a lei nova ficou mais severa. Há de se notar a constante mudança no tocante a letra da lei. Segundo o Estatuto da Criança e do Adolescente, a lei nº 8.069/90, de 13 de julho de 1990, eram condutas puníveis apenas fotografar e publicar.

Observa-se que essa lei ficou em vigor até 2003. Com a lei nº 11.829/08, de 25 de novembro de 2008, a letra da lei incorporou outros verbos, sendo eles:

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:  
Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.  
(BRASIL, 2008)

Para efeito direto no combate ao crime contra a criança e o adolescente na rede mundial de computadores, os legisladores tipificaram como cyber crimes nos artigos 241, 241-A, 241-B, 241-C, 241-D e 241-E, onde houve uma preocupação em definir e coibir a prática da pornografia na internet.

Entretanto, somente a lei não é eficaz no combate ao crime na internet contra a criança. Os criminosos utilizam vários métodos de camuflagem, o que impede a aplicação da lei de forma eficaz. Sendo assim, além da preocupação jurídica para proteger os mais vulneráveis, se faz necessário medidas preventivas e de conscientização, como será visto a seguir.

### **3.2 Medidas preventivas**

Apesar das leis e da responsabilidade que o Poder Legislativo tem para resolver as questões dos crimes virtuais (PEREIRA, 2006), ainda assim é de suma importância a incumbência que os pais têm na hora de educar os seus filhos para navegar na internet, visto que a legislação nem sempre é cumprida, seja por falta de pessoas qualificadas para realizar as investigações, déficit de equipamentos ou uma infraestrutura precária para realizar as operações (KALB, 2008).

Nesse sentido, é necessário a mobilização da sociedade para combater esse mal, desde os pais até os professores ou ONGs para divulgar informações.

Com base nisso, para ajudar a combater os crimes contra a criança, foi assinada em 2005 um termo de compromisso e responsabilidade entre alguns provedores de internet no intuito de “unir esforços para prevenir e combater a pornografia infantil, o racismo e outras formas de discriminação na rede mundial de computadores” (KALB, 2008, p. 368).

No âmbito familiar, os pais devem entender que há criminosos na internet e orientar as crianças nesse sentido. Segundo Kalb (2008), há vários métodos para deixar as crianças um

pouco mais seguras na internet, como, por exemplo, utilizar programas que restringe o acesso à alguns sites; sempre acompanhar a trajetória que a criança faz na internet, seja pelo acesso ao histórico ou então conversar com a criança e pedir para que ela mostre por onde anda navegando; informar a criança a nunca expor nenhuma informação pessoal ou número de telefone em chats com estranhos; instruí-las a nunca postarem fotos delas em algum site; conhecer as pessoas que a criança conversa na internet; orientá-las a nunca marcar encontros com qualquer pessoa na internet sem antes consultar os pais.

Desse modo, considerando que o conhecimento “[...] é a base para a formação crítica de um cidadão a respeito de tudo que interfere em seu bem-estar” (ALVES; ANDRELO; CABRAL, 2016, p. 49), zelar pelo conhecimento e direito à informação para com as crianças e adolescentes acerca dos perigos por trás das telas é fundamental em um país que se constitui como Estado Democrático de Direito.

Como pode ser observado, os pais têm grande responsabilidade nesse quesito, assim como a sociedade como um todo. É a união de esforços, tanto com os órgãos públicos quanto no âmbito familiar, que surtirá efeito no combate a esse mal. Entretanto, mesmo com todo esse empenho, é muito difícil eliminar completamente esse conteúdo da internet, como será visto posteriormente.

#### **4. MOTIVOS QUE DIFICULTAM A APLICAÇÃO DA LEI**

Como evidenciado ao longo desse artigo, existem vários fatores que contribuem para dificultar a aplicação da lei. É complexo aplicar a lei até mesmo fora da internet, já que, como exposto, a pessoa portadora do distúrbio pedofílico é muito difícil de ser identificado, visto que grande parte pode se passar por uma pessoa comum.

Dentro da internet se torna uma tarefa ainda mais complexa rastrear e identificar o infrator, dado que o mesmo pode utilizar ferramentas para se esconder e satisfazer a sua lasciva através da pornografia ou então conversando com crianças em sala de bate papo.

Sendo assim, será exposto ao longo do próximo tópico algumas ferramentas que os criminosos utilizam para praticar seus crimes, deixando inevitável a impunidade para esses transgressores.



#### 4.1 *Modus operandi* do pedófilo na internet

Antes de tudo, é importante ressaltar o *modus operandi* do criminoso na internet para, assim, ter um contexto maior das ferramentas utilizadas por eles.

Segundo o delegado-chefe da Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC), Giancarlo Zuliani, muitos criminosos utilizam jogos *on-line* para conhecer as suas vítimas. Os mesmos criam perfis infantis e tentam conversar e manipular as vítimas e, com o passar do tempo, o criminoso tenta adquirir o *e-mail* ou *Whatsapp* da criança. É nesse estágio em que o infrator tenta persuadir a vítima a mandar fotos pornográficas ou marcar um encontro, onde possivelmente ocorrerá a agressão sexual.

Com isso, no âmbito da internet, o infrator tende a adotar um comportamento mais manipulativo. Entretanto, a estratégia utilizada pelo criminoso (se ele utilizará uma estratégia coercitiva ou manipulativa) tende a variar de acordo com a idade da vítima. Na estratégia manipulativa, agressor tende a utilizar esse comportamento em crianças mais velhas, já a estratégia coercitiva é utilizada em crianças mais novas (LECLERC *et al.*, 2009).

Aplicando esse método manipulativo no âmbito da internet, é possível dizer que o agressor utiliza jogos eletrônicos ou chats de bate-papo para ter o primeiro contato com a vítima e, quando ele consegue conquistar a confiança da criança, o infrator tenta conseguir algum meio de comunicação mais intimista, como *Whatsapp* ou uma rede social pessoal.

Depois, o *modus operandi* da maioria dos criminosos seria adotar uma estratégia de dar presentes, amor e atenção para conquistar ainda mais a confiança da criança e, depois, ameaçar a cortar os benefícios para manter a vítima calada (KAUFMAN, *et al.*, 1996). Sendo assim, a criança cria um vínculo com o pedófilo, primeiro confiando e depois se sentindo culpada e com medo de denuncia-lo.

Como exposto, o sexo e a idade da vítima influenciam na abordagem do criminoso. Como o presente artigo propõe evidenciar o *modus operandi* apenas dos criminosos que agem na internet, serão deixadas as estratégias utilizadas pelos agressores fora da internet.

Nesse diapasão, pode-se concluir que o *modus operandi* do pedófilo na internet é adotar uma conduta manipulativa para conquistar a vítima e, depois, faz-la se sentir presa e com medo de denuncia-lo.

## 4.2 Programas de VPN

Além da dificuldade em identificar um possível pedófilo no cotidiano, na internet há um acréscimo ainda maior pelas ferramentas disponíveis para o uso de criminosos. Apesar de ser uma ferramenta completamente legal, o indivíduo pode utilizar a VPN para ficar sem possibilidade de rastrear, mascarando o seu endereço de IP e dificultando o trabalho das autoridades.

O *Virtual Private Network* (VPN) é uma ferramenta para navegação na internet, onde é criado um canal público no qual é transmitido os dados de forma criptografado (SILVA, 2012). Sendo assim, muitas pessoas utilizam essa ferramenta para tornar a navegação na internet um pouco mais segura, protegendo os seus dados contra possíveis ataques. *A priori*, VPN é um mecanismo da Segurança da Informação, essa que “protege a informação de diversos tipos de ataques [...] garante a continuidade dos negócios, reduz as perdas e maximiza o retorno dos investimentos e das oportunidades” (FERREIRA, 2003, pg. 162).

Nesse sentido, o *Internet Protocol* (IP) é o único dado para rastreamento de um indivíduo na internet (SILVA, 2012) e o VPN foi criado como uma forma de criptografar esse dado. Entretanto, como essa ferramenta é feita para criptografar esses dados, algumas pessoas podem utilizar para ocultar qualquer forma de rastreamento e, assim, podendo aliciar menores para a produção de pornografia infantil ou satisfazer a sua lasciva em conversas com teor sexual em salas de bate papo com maior facilidade e tranquilidade, sem se preocupar em ser encontrado.

Para compreender a magnitude do problema, o Zuliani (2020) diz:

As Investigações de crimes de pornografia infantil pela internet, em geral, têm como ápice a apreensão dos Hard Discs (HDs) dos computadores dos suspeitos. O procedimento ocorre da seguinte maneira: identificado e localizado o provável autor do fato, o delegado representa à autoridade judiciária pela busca e apreensão de prováveis instrumentos utilizados na prática do crime no domicílio do investigado, por exemplo. Autorizada a busca e apreensão, uma equipe de policiais comparece ao local para cumprir a referida diligência.

Assim, fica claro que a participação da polícia nesses crimes se dá quando já é identificado o suspeito. Entretanto, até chegar nessa fase da investigação, primeiro é necessário rastrear o indivíduo, algo que chega a ser impossível se o criminoso utilizar ferramentas como a VPN em conjunto com outros softwares para se tornar completamente anônimo na internet.

### 4.3 Rede aberta

Além do criminoso utilizar softwares que possam mascarar o seu endereço de IP, o indivíduo pode acessar redes abertas para praticar os seus crimes, seja em *Lan House*, *Shopping*, praças públicas com internet aberta, etc. Sendo esses lugares com grande volume de tráfego de pessoas, mesmo que a polícia identifique o IP e consiga rastrear o local exato do crime, torna-se uma tarefa árdua para achar o autor do crime, já que centenas de aparelhos podem estar conectados.

Sendo assim, Vladimir Aras (2002) diz:

O único método realmente seguro de atribuição de autoria em crimes informáticos é o que se funda no exame da atuação do responsável penal, quando este se tenha valido de elementos corporais para obter acesso a redes ou computadores. Há mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. As formas mais comuns são a análise do fundo do olho do usuário ou a leitura eletrônica de impressão digital, ou ainda, a análise da voz do usuário.

Um combate eficaz no âmbito das redes públicas seria aderir algum sistema de validação antes de entrar na rede, contendo os dados do usuário e alguma forma de identificação. Alguns *Shoppings Centers* pedem para o usuário fazer o cadastro antes de utilizar a rede. Entretanto, somente esse mecanismo é ineficaz, já que o usuário pode cadastrar utilizando dados falsos.

Não é somente em lugares públicos que o autor pode acessar a internet para cometer os crimes. Muitos roteadores de internet pessoais possuem uma senha padrão que muitos usuários não mudam, seja por desconhecimento ou por não ter a perícia necessária para alterá-la. Sabendo disso, o criminoso consegue facilmente acessar o roteador pela senha padrão e utilizar o endereço de IP de uma pessoa inocente.

Por conseguinte, caso a polícia venha a rastrear o IP, será apontado para uma pessoa que nada fez. Nesse viés, tal temática se relaciona, também, com a Lei Geral de Proteção de Dados, uma vez que referida legislação se destina à proteção dos dados de usuários, desde sua coleta a seu processamento – devendo sua aplicação ser observada pelas investigações policiais ligadas aos crimes cibernéticos.

## 5. CONSIDERAÇÕES FINAIS

Conforme apresentado ao longo do artigo, é possível reforçar a importância do assunto abordado, visto que o mesmo pode impactar fortemente na maneira de como a sociedade se relaciona com a Internet e de como as pessoas, mais especificamente, os familiares, devem se manter observantes aos riscos que as crianças se expõem diante de pessoas transgressoras que usam a tecnologia, por meio do ambiente cibernético, para cometerem seus crimes.

Existe uma necessidade de se atentar para a facilidade com que o crime na internet possa ser cometido, já que a investigação é uma tarefa árdua devido a dificuldade em rastrear o indivíduo e imputar o crime. Desse modo, as informações e dados apresentados neste trabalho objetivaram contribuir para esse campo de estudo, visto que, mesmo com informações alarmantes sobre o crescimento do crime na internet, ainda há poucos trabalhos difundidos o que impacta em poucas ações para combater esse mal.

É preciso salientar que existem vários softwares para deixar o indivíduo anônimo, ou então, estratégias que o criminoso utiliza, como a de redes abertas para cometer o crime. É extremamente importante demonstrar que a internet pode ser um ambiente propício para cometer crimes contra as crianças, seja manipulando o menor para gravar vídeos pornográficos ou utilizando de chat de bate-papo para marcar encontros, onde ocorre o possível crime.

Os conteúdos aqui apresentados demonstram que muitas outras pesquisas ainda podem ser realizadas sobre a pedofilia na internet. Para futuras pesquisas, é importante buscar evidenciar meios para combater esse crime, seja por divulgação do problema, ação social ou até mesmo um estudo aprofundado sobre o Marco Civil da Internet, trazendo um debate se regulamentar a internet é uma boa alternativa para combater o crime ou se possivelmente fere princípios básicos do homem como a liberdade de expressão.

## REFERÊNCIAS

ADABO, Gabrielle. **Ciência e guerra**: era uma vez a internet. ComCiência, 2014

ALVES; Mariana Carareto; CABRAL, Raquel; ANDRELO, Roseane. Reputação e direito à informação: a comunicado da mineradora Samarco no caso do acidente ambiental em Mariana (Minas Gerais, Brasil). **Revista Internacional de relaciones publicas**, Málaga, v. 6, n. 12, p. 43-64, 2016. Disponível em: <http://revistarelacionespublicas.uma.es/index.php/revrrpp/article/view/416>. Acesso em: 14 ago. 2021.

AMERICAN PSYCHIATRIC ASSOCIATION et al. **DSM-5: Manual diagnóstico e estatístico de transtornos mentais**. Artmed Editora, 2014.

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 6, n. 51, 2001.

ARAÚJO, Naira (org). **Abuso e exploração sexual contra crianças e adolescentes: Manual de orientação para educadores**. Manaus: Agência Uga-Uga de Comunicação, 2004.

BASTOS, Ângela. **Pedofilia na internet: denúncias aumentam durante a pandemia**. nsctotal. 2021. Disponível em: <https://www.nsctotal.com.br/noticias/pedofilia-na-internet-denuncias-aumentam-durante-a-pandemia>. Acesso em: 7 ago. 2021.

BRIGGS, Asa; BURKE, Peter. **Uma história social da mídia: de Gutenberg à Internet**. Schwarcz-Companhia das Letras, 2016

CARVALHO, Américo Taipa de. **Direito Penal – Parte Geral: Questões Fundamentais. Teoria Geral do Crime**. 2. Ed. Coimbra, 2011.

CARVALHO, M. S. R. M. **A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança**. 2006. Unpublished Estudos de Ciência e Tecnologia no Brasil, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

DA SILVA, Camila Cortellete Pereira; PINTO, Daniela Devico Martins; MILANI, Rute Grossi. **Pedofilia, quem a comete?** Um estudo bibliográfico do perfil do agressor. 2013.

EDWARDS, Paul N. **The closed world: Computers and the politics of discourse in Cold War America**. MIT Press, 1996.

FERREIRA, Fernando N. F. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna. 2003.

FONTES, Edson. **Segurança da Informação: o usuário faz a diferença**. São Paulo: Saraiva, 2006.

FUNDAÇÃO ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO. Lei Carolina Dieckmann: Você sabe o que essa lei representa?. fmp. 2021. Disponível em: <https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/>. Acesso em: 10 set. 2021.

HODGES, Andrew. **Alan Turing: uma biografia introdutória**. Boletim da Sociedade Portuguesa, 2012.

KALB, Christiane Heloisa. Pedofilia na internet: legislação aplicável e sua eficácia na realidade brasileira. **Revista Jurídica**, Porto Alegre, v. 56, n. 368, p. 105-124, jun. 2008.

LEE, Timothy B. **The internet, explained**. vox. 2015. Disponível em: <https://www.vox.com/2014/6/16/18076282/the-internet>. Acesso em: 9 ago. 2021.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34 Ltda, 1999. Disponível em: <https://mundonativodigital.files.wordpress.com/2016/03/cibercultura-pierre-levy.pdf>. Acesso em: 14 ago. 2021.

LIMA, Paulo Marco Ferreira. Crimes de Computador e Segurança Computacional. 2 ed.

**Editora Atlas.** São Paulo, 2011. p. 13.

LUCCHESI, Ângela Tereza; HERNANDEZ, Erika Fernanda Tangerino. CRIMES VIRTUAIS: cyberbullying, revenge porn, sextortion, estupro virtual. **Revista Officium: estudos de direito**, v. 1, n. 1, p. 2, 2018.

METRÓPOLES. Distrito Federal, ano 2020, 6 dez. 2020. Disponível em: <https://www.metropoles.com/distrito-federal/pais-denunciam-pedofilos-que-se-infiltram-em-jogos-on-line-para-aliciar-criancas-do-df>. Acesso em: 10 set. 2021.

MITANI, Amanda Wendt. A imprecisão da linguagem da lei e a dificuldade de comunicação entre delegados e peritos nos crimes de pornografia infantil pela Internet. **Revista Brasileira de Segurança Pública**, v. 6, n. 1, 2012.

RODRIGUES, Willian Thiago de Souza. A pedofilia como tipo específico na legislação penal brasileira. **Âmbito Jurídico**, v. 9, p. 59, 2008.

SERAFIM, Antonio de Pádua et al. Perfil psicológico e comportamental de agressores sexuais de crianças. **Archives of Clinical Psychiatry**, São Paulo, v. 36, p. 101-111, 2009.

SERAFIM, Antonio de Pádua, SAFFI, Fabiana; RIGONATTI, Sérgio Paulo; CASOY, Ilana; BARROS, Daniel Martin de. Perfil psicológico e comportamental de agressores sexuais de crianças. **Psiquiatria Clínica**, 101-11, 2009.

SILVA, Daniel Neves. "Guerra Fria"; **Brasil Escola**. Disponível em: <https://brasilecola.uol.com.br/guerras/guerra-fria.htm>. Acesso em 19 jul 2021.

SILVA, Deidigley Menezes Pires da. Introdução à criminalística. **DireitoNet**, jan. 2015. Disponível em: <https://www.direitonet.com.br/artigos/exibir/8756/Introducao-a-criminalistica>. Acesso em: 14 ago. 2021.

SILVA, Edelberto Franco. **Anonimato na Internet**.

SOTANA, Edvaldo Correa. O início da Guerra Fria nas páginas da imprensa escrita brasileira (1946-1949). **Diálogos-Revista do Departamento de História e do Programa de Pós-Graduação em História**, v. 18, n. 1, p. 325-359, 2014.

SPIZZIRRI, Giancarlo. **Pedofilia** – considerações atuais. Diagnóstico e tratamento. **Diagn. tratamento**, v.15, n. 1, jan-mar, 2010.

UNIT, Economist Intelligence. **Shining light on the response to child sexual abuse and exploitation**. World Childhood Foundation, Oak Foundation, and Carlson Family Foundation. Disponível em: <http://outoftheshadows.eiu.com>. Acesso em: 05 jul 2021.

