Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Felipe Castanha da Silva

Pamela Cristina da Silva

Metodologia e análise utilizadas na solução de crimes sexuais contra crianças e adolescentes na era digital: um estudo de caso baseado no *software* IPED

Americana, SP

2019

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Felipe Castanha da Silva

Pamela Cristina da Silva

Metodologia e análise utilizadas na solução de crimes sexuais contra crianças e adolescentes na era digital: um estudo de caso baseado no *software* IPED

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, para a obtenção do título de Tecnólogo, sob a orientação do Prof. Ms. Benedito Luciano Antunes de França.

Área de concentração: Tecnologia da Informação

Americana, SP.

2019

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

S58m SILVA, Felipe Castanha da; SILVA, Pamela Cristina

Metodologia e análise utilizadas na solução de crimes sexuais contra crianças e adolescentes na era digital: um estudo de caso baseado no software IPED. / Felipe Castanha da Silva, Pamela Cristina da Silva. – Americana, 2019.

82f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Benedito Luciano Antunes de França

1 Segurança em sistemas de informação 2. Perícia computacional 3. Pedofilia I. SILVA, Pamela Cristina da II. FRANÇA, Benedito Luciano Antunes de III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: *681.518.5*

Felipe Castanha da Silva
Pamela Cristina da Silva

Metodologia e análise utilizadas na solução de crimes sexuais contra crianças e adolescentes na era digital: um estudo de caso baseado no software IPED

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação, pelo CEETEPS/Faculdade de Tecnologia - Fatec/ Americana.
Área de concentração: Tecnologia da Informação.

Americana, 07 de agosto de 2019,

Banca Examinadora:

Benedito Luciano Antunes de França (Presidente)
Mestre
Fatec Americana

Edson Roberto Gaseta (Membro)
Mestre
Fatec Americana

Rogério Nunes de Freitas (Membro)
Mestre
Fatec Americana

AGRADECIMENTOS

Gostaríamos de agradecer primeiramente à Deus. Ao perito judicial, Prof. Marcos Monteiro, por iluminar esse trabalho com informações técnicas e precisas nesse delicado tema. Aos nossos familiares, por ser um de nossos pilares no período da faculdade nos acolhendo com carinho e compreensão durante os nossos estudos. Aos nossos amigos, por sempre estarem presentes nesse momento único de nossa vida acadêmica e profissional. Ao Professor Mestre Benedito Luciano Antunes de França, pela paciência, incentivo, apoio, compreensão, amizade e dedicação ao nos instruir nesse trabalho e acreditar em toda a ideia e importância para o desenvolvimento do trabalho.

RESUMO

Este Trabalho de Graduação objetiva apresentar as atividades periciais da Polícia Federal brasileira, no combate à pornografia infanto-juvenil, tomando como ponto de partida, mais especificamente, as práticas desenvolvidas no Estado de São Paulo. Intenciona explorar o cotidiano dos peritos forenses que realizam a coleta, o exame e a análise das evidências do compartilhamento ilegal de imagens e vídeos, que expõem crianças e adolescentes no ambiente virtual, por meio da Rede Mundial de Computadores. Busca oferecer o conhecimento de como as vítimas sexuais, no ambiente virtual, devem proceder para a realização das denúncias, neste Estado, a fim de garantir a confidencialidade, a integridade e a disponibilidade de evidências e, com base nas provas coletadas, a efetivação da instauração de processo judicial. A pesquisa bibliográfica e documental oferece, ainda, uma gama de conhecimento dos recursos técnicos e informáticos desenvolvidos pela Polícia brasileira, mediante os quais são analisadas as diligências dos crimes cibernéticos relacionados aos crimes sexuais contra crianças e adolescentes, graças aos estudos de ferramentas forenses utilizadas para a identificação destes conteúdos. Este Trabalho de Graduação proporciona o entendimento da proteção jurídica e institucional do Estado brasileiro e dos entes federativos, na intenção de preservar as crianças e os adolescentes da propagação ilegal de conteúdos eróticos. E, por último, visa compreender e examinar, por simulação laboratorial, as abordagens dos peritos, através de ferramentas livres disponíveis para testes, por meio do IPED (Indexador e Processador de Evidências Digitais), no intuito de entender as delimitações de seu uso.

Palavras Chave: Perícia forense; Legislação brasileira; Crimes virtuais de natureza sexual contra crianças e adolescentes.

ABSTRACT

This graduation work aims to present the digital forensics activities of the Brazilian Federal Police in the fight against child pornography, taking as starting point, specifically, the practices developed in the State of São Paulo. It intends to explore the daily activities of forensic experts who carry out the collection, examination and analysis of illegal evidence, sharing of images and videos, which expose children and adolescents on virtual environment through the World Computer Network. It seeks to provide knowledge of how sexual victims, in the virtual environment, should proceed to make complaints in this State in order to ensure the confidentiality, integrity and availability of evidence and, based on the evidence collected, and the execution of legal proceedings. The bibliographical and documentary research also offers a range of knowledge of technical and computer resources developed by the Brazilian Police, through which the efforts of cybercrime related to sexual crimes against children and adolescents are analyzed, thanks to the forensic tool studies used for the identification of these content. This graduation works provides the understanding of the legal and institutional protection of the Brazilian State and federative entities, in order to preserve children and adolescents from the illegal spread of erotic content. Finally, it aims to understand and examine, by laboratory simulation, the approaches of experts, through free tools available for testing, including by IPED (Indexador e Processador de Evidências Digitais), in order to understand the delimitation of their use.

Keywords: Digital Forensic; Brazilian legislation; Virtual crimes of a sexual nature against children and adolescents.

SUMÁRIO

INTRODUÇÃO.....9

CAPÍTULO I – DIMENSÃO TÉCNICO-COMPUTACIONAL..... 111

1.1 Metodologia utilizada para coletar e analisar informações sobre crimes sexuais contra crianças e adolescentes.....11

1.2 Exploração das técnicas aplicadas em prol da Perícia Forense para a captura de informações relacionadas aos crimes sexuais contra crianças e adolescentes efetuadas pela Polícia brasileira..... 16

1.3 Análise da existência de aplicativos utilizados pelo aparato policial (Polícias Federal, Militar, Civil) para a identificação de criminosos que cometem ações civis e penais dessa natureza 25
1.3.1 EspiaMule.....26
1.3.2 Indexador e Processador de Evidências Digitais (IPED).....27
1.3.3 Localizador de Evidências Digitais (LED).....31
1.3.4 NuDetective.....34

1.4 (IN)Eficácia dos *softwares* Forenses utilizados pela polícia técnica para a identificação de crimes contra a Infância e Juventude 37

1.5 Delegacias especializadas de combate aos crimes sexuais de menores no ambiente virtual no Estado de São Paulo 41

CAPÍTULO II – DIMENSÃO TÉCNICO-JURÍDICA DA CLASSIFICAÇÃO E DA PENALIZAÇÃO DOS CRIMES SEXUAIS CONTRA A INFÂNCIA E A JUVENTUDE.....48

2.1 Pressupostos de crimes contra a Infância e Juventude no Código Civil e no Estatuto da Criança e do Adolescente 48

2.2 Código Penal.....51

2.3 Estatuto da Criança e do Adolescente.....55

2.4 Legislação referente à área de Informática e de Computação no combate ao crime de natureza sexual, na dimensão virtual 57

CAPÍTULO III – ESTUDO DE CASO: ANÁLISE LABORATORIAL BASEADA NA FUNCIONALIDADE DO PROGRAMA IPED..... 61

3.1 Análise e verificação da funcionalidade do Programa IPED..... 62

3.2 Análise dos resultados da funcionalidade do Programa IPED..... 68

CONSIDERAÇÕES FINAIS.....70
REFERÊNCIAS...... 72
ANEXOS.....
78

LISTA DE FIGURAS

Figura 1 - Etapas do processo de computação forense 15
Figura 2 - Balanço da Operação Darknet II 21
Figura 3 - O funcionamento Tor 23
Figura 4 - Processo geral para análise com base em NetFlow contra o Tor 24
Figura 5 - Proporção de usuários da rede Tor no mundo em 2014 25
Figura 6 - Interface inicial do aplicativo EspiaMule 27
Figura 7 - Tela de processamento IPED – Versão 3.9 31
Figura 8 - Tela inicial do aplicativo LED 32
Figura 9 - Abordagem de detecção via Talon 37
Figura 10 - Resposta do Youtube às denúncias de M. Watson 40
Figura 11 - Ranking de páginas removidas com pornografia infantil, em 2018 44
Figura 12 - Índice de denúncia da pornografia infantil processada pelo Hotline/SaferNet entre os aos de 2006 e 2018 44
Figura 13 - Fluxo de Denúncia SaferNet 46
Figura 14 - Verificando a versão do java no dispositivo utilizado 61
Figura 15 - Definindo a quantidade de memória RAM em MB (megabytes) 62
Figura 16 - Definido um caminho para indexação 63
Figura 17 - Alterando parâmetro para reduzir tempo de processamento 63
Figura 18 - Alterando parâmetro para diminuir requisito de espaço livre no “temp”.....63
Figura 19 - Iniciando a execução do IPED 64
Figura 20 - Parâmetros definidos e execução do IPED 64
Figura 21 - Tela de inicialização do IPED 65
Figura 22 – Tela de processamento do IPED 66
Figura 23 - Mensagem de conclusão do processamento do IPED 66
Figura 24 - IPED indexado 67
Figura 25 Resultado de pesquisa no IPED (Inserção de palavra-chave) 67
Figura 26 Resultado da pesquisa no IPED 67
Figura 27 - Visualização de miniaturas de imagens 68

LISTA DE TABELAS

Tabela 1 - Processamento de 200 fotos usando o NuDetective.....36

INTRODUÇÃO

Com o decorrer dos anos, a criminalidade pôde se adaptar, fazendo o uso das ferramentas disponíveis na Rede Mundial de Computadores, no intuito de dar continuidade as práticas criminosas desenvolvidas no mundo *off-line*, agora implementadas e sofisticadas no ambiente virtual. A propagação da Rede mundial de computadores (Internet) ocasionou a maior comunicação entre a população e, em contrapartida, possibilitou a exploração de seus recursos por mentes mal-intencionadas, as quais fazem uso de múltiplas tecnologias para desenvolver atividades ilegais.

Este estudo bibliográfico e documental, assentado em simulação laboratorial, retrata o desempenho da Polícia Federal brasileira ao interceptar, rastrear e analisar os conteúdos ilegais de conteúdos sexuais contra crianças e adolescentes circulantes no ambiente virtual. O conhecimento das abordagens policiais, em diferentes esferas, a aplicação e o contínuo desenvolvimento de ferramentas forenses empregadas, auxiliam na descoberta destas práticas nocivas ao mundo infanto-juvenil.

Por meio das pesquisas realizadas aos Portais de comunicação da Polícia Federal brasileira, da realização de entrevista presencial com perito judicial, prof. Marcos Monteiro, que atua diretamente neste tipo de investigação no país, pudemos erigir as bases teóricas e empíricas deste Trabalho de Graduação.

Alicerçado em três capítulo, este Trabalho de Graduação visa promover o conhecimento técnico instrumentalizado pelas polícias atuantes no Brasil e de modo particular, no Estado de São Paulo, expondo, primeiramente, o uso de tecnologias já existentes, além do aprimoramento e criação de novas tecnologias no combate aos crimes de ordem sexual. A fim de entendermos a natureza técnica da criação destas ferramentas tecnológicas, no Primeiro capítulo, sucintamente, apresentaremos alguns conceitos vinculados à área banco e análise de dados, conceito e utilização de *hashes*, conceitos de *internet* por meio da rede ponto-a-ponto e, por fim, os procedimentos técnicos empregados pela Perícia forense à luz da investigação policial no solo brasileiro, por meio de relatos obtidos na pesquisa documental.

No Segundo Capítulo, serão explorados elementos constituintes da dimensão técnica e jurídica, à luz da Legislação brasileira, de modo particular, a Constituição

Federal de 1988, o Código Penal, o Código Civil e, especialmente, o Estatuto da Criança e do Adolescente (ECA), de 1990, além de explanarmos sobre a criação de novas leis para validar a criminalização dos delitos cibernéticos, o processo de investigação até a instauração de processo criminal, sob a intenção de remediar os danos causados, contrários à dignidade de crianças e adolescentes, no Brasil.

E, por último, no Capítulo Terceiro, nós fizemos um estudo de caso, efetuando uma análise técnica e informática do Aplicativo IPED (Indexador e Processador de Evidências Digitais), importante ferramenta criada e usada pela Polícia Federal, no intuito de captar evidências presentes em dispositivos eletrônicos.

CAPÍTULO I – DIMENSÃO TÉCNICO-COMPUTACIONAL

Neste Capítulo, cinco seções ajudarão a compreender a dimensão técnico-computacional, na intenção de demonstrar como um dado ou uma informação técnica é obtida, gerada, armazenada, documentada, em fontes eletrônicas e similares, as quais, eventualmente, podem se tornar dados para pesquisas, inclusive as de ordem forense. Destacamos alguma delas: Metodologia utilizada para coletar e analisar informações sobre crimes sexuais contra crianças e adolescentes; exploração das técnicas aplicadas em prol da Perícia Forense para a captura de informações relacionadas aos crimes sexuais contra crianças e adolescentes efetuadas pela polícia brasileira; análise da existência de aplicativos utilizados pelo aparato policial (Polícias Federal, Militar, Civil) para a identificação de criminosos que cometem ações civis e penais desta natureza; (in) eficácia dos *softwares* forenses utilizados pela polícia técnica para a identificação de crimes contra a Infância e Juventude; delegacias especializadas de combate aos crimes sexuais de menores no ambiente virtual no Estado de São Paulo.

1.1 Metodologia utilizada para coletar e analisar informações sobre crimes sexuais contra crianças e adolescentes

Antes de explicar a metodologia utilizada nas coletas, nas análises e no armazenamento de dados, realizada pela Polícia Federal brasileira em investigações sobre pornografia infantil na internet, foram tomadas algumas definições de natureza da tecnologia da informação, tais como, dados, informação, banco de dados, metadados, armazenamento de dados, indexação de documentos, *hash*, redes de comunicação virtual (Internet) e Perícia Forense.

A palavra “Dados”, de acordo com o Portal Conceito de, tem origem no Latim, *datum* que significa “aquilo que se dá”, desta forma, o dado é um documento compilado da informação, por exemplo, um testemunho (CONCEITO DE, 2010-2019). Na área da tecnologia, os dados são expressões gerais que devem ser apresentadas ao sistema na qual, possibilitam a descrição de características das entidades que operam os algoritmos. Entretanto, os dados normalmente são fornecidos em sua forma bruta, a qual pode dificultar a compreensão, por exemplo, em casos isolados.

Sendo assim, ainda de acordo com o mesmo Portal, entendemos que “Informação” é o conjunto de dados brutos que, de forma organizada, possibilitam a compreensão e análise dos conjuntos, em prol da geração de conhecimento sobre um determinado fenômeno ou evento, pois em posse de uma informação é possível tomar decisões e resolver problemas, isto é, ela gera sentido aos dados (CONCEITO DE, 2010-2019). O termo definição de “conhecimento”, por sua vez, ainda segundo o mesmo Portal, é o conjunto de informações armazenadas, mediante uma experiência ou aprendizagem (CONCEITO DE, 2010-2019).

Tendo em vista a união conceitual de dados e de informação, obtemos os conhecidos de “bancos de dados”, os quais estão presentes em quase cem por cento dos ambientes virtuais, e, por definição, segundo Korth (*Apud* DEVMEDIA, 2006), um banco de dados “é uma coleção de dados inter-relacionados, representando informações sobre um domínio específico”. Isto é, quando existe uma correlação de dados similares, reunidos e estruturados, podemos assim chamá-los de banco de dados.

No intuito de incrementar as informações relacionadas aos dados, os bancos de dados são complementados com Metadados, que, de acordo com o Portal Devmedia (2006), este conceito institui-se de tecnologia para o conhecimento. Dessa forma, as informações contidas nos Metadados descrevem os dados de um sistema, que podem ser documentados, através de uma coleção de documentos, gráficos, tabelas, imagens, vídeos, etc., inclusive, por exemplo, informações de indexação de imagem nos *softwares* de Perícia Forense.

Ao longo do tempo, as formas de armazenamento de dados e informações sofreram diversas mudanças em decorrência das atualizações de ambiente e necessidades pontuais. Na Idade Média, por exemplo, os patrimônios intelectuais encontravam-se em mosteiros com bibliotecas; na Idade Moderna, institui-se a imprensa, o que gerou a publicação de livros fabricados em série, seguido do surgimento dos jornais. Entretanto, no século XX, foram inseridos no contexto os meios de comunicação em massa (Rádio, TV) e, em seguida, as ferramentas digitais que conhecemos atualmente. Quando falamos de armazenamento, precisamos entender que contamos com dispositivos que englobam duas noções: primeiramente, esses dispositivos são máquinas capazes de satisfazer objetivos para as quais foram desenvolvidas; segundo, o objetivo do armazenamento é a ação e o efeito de

armazenar (reunir ou guardar coisas, registar) informações (CONCEITO DE, 2010-2019).

Por meio dessas definições compreendemos que esses dispositivos escrevem ou leem dados de um suporte, em sistemas informáticos, de forma lógica e física. Esses dispositivos utilizam de qualquer forma de energia, desde força manual humana, como, por exemplo, a escrita, incluindo vibrações acústicas em gravações fonográficas, ou até mesmo modulação de energia eletromagnética. Alguns dispositivos físicos, que têm como característica o armazenamento, são por meio magnéticos, disco rígido, meios ópticos, unidades de *CD-ROM* ou *DVD-ROM*, meios eletrônicos, *SSDs* (*chips*, cartões de memória, *pen drives*). A maneira como os dados são coletados e manipulados são determinantes para o caso ser bem-sucedido, os registros permanentes são armazenados em vários arquivos, o que requer o desenvolvimento de diversos programas de aplicação para extrair e gravar registros nos arquivos apropriados, os quais são chamados de sistemas de armazenamento típico, e podem ser aceitos pelos sistemas operacionais convencionais, tais como *Windows*, ambiente *Unix*, *IOS* (CONCEITO DE, 2010-2019).

Para analisar os dados é preciso que esses estejam disponíveis de maneira organizada. Para Sousa (2016) no estudo denominado “Etapas do processo de Computação Forense: uma revisão”, publicado na Revista Acta de Ciências & Saúde, uma das técnicas presente nas Perícias computacionais ocorre por meio da indexação de dados, a qual podemos definir como arrumação de dados (SOUSA, 2016, p. 106). Essa técnica envolve a criação de estruturas de dados associados aos documentos de um determinado subconjunto, para que seja acessado posteriormente através de índices, o que, consequentemente, traz velocidade as pesquisas dos dados. Existem vários tipos de índices, cada qual composto por uma estrutura particular de dados, qualquer campo de um arquivo pode ser utilizado para a criação de índice, assim como o mesmo arquivo pode conter vários índices (SOUSA, 2016).

A metodologia utilizada nas análises policiais aborda conteúdo baseados em *hash*, sendo que as funções existentes calculam um número de tamanho limitado, normalmente de 128 *bits* a 2.048 bits (16 a 256 *bytes*), de qualquer arquivo. É uma função unidirecional, a qual não permite dedução de conteúdo, apenas de assinatura, e dentro do contexto de Perícia computacional é usada para fazer

rápidas comparações de arquivos, verificar se são os mesmos. A autenticação por meio de *hash* pode verificar cópias de arquivos. Entretanto, qualquer alteração no arquivo compromete drasticamente o valor de *hash*. Os *hashes* são criados através de algoritmos matemáticos e suas funções facilitam a verificação da integridade dos arquivos, armazenamento de senhas ou pesquisar determinado arquivo em uma base de dados muito grande, como, por exemplo, em redes de comunicação virtual (BRASIL, 2017).

Em seguida, usaremos o conceito de rede de internet, de modo especial verificaremos onde são analisados os *hashes* pela Polícia Federal brasileira, na Rede *peer-to-peer*.

As redes de comunicação virtual são muitas e em cada uma delas atua de acordo com algumas particularidades, em busca de um objetivo final similar. Em outras palavras, o compartilhamento de dados e informações tornam-se possíveis através de usuários conectados. Para compreendermos as análises de *hashes* realizadas pela Polícia Federal brasileira em busca de assinaturas previamente conhecidas e relacionadas à pornografia infantil, abordaremos a comunicação virtual possibilitada pela Rede de conexão *peer-to-peer*, que significa uma conexão estabelecida de ponta a ponta, visto que busca isentar-se de uma rede tradicional vinculada através de um servidor central e cliente, e possibilitar que, cada cliente da rede, também seja capaz de atuar como servidor de distribuição de dados (DALPIAN; BENITES, 2007).

De acordo com os peritos criminais federais Guilherme M. Dalpian e Carlos A. A. Benites, participantes do “Second International Conference on Forensic Computer Science” (ICoFCS, 2007), organizado pela “The International Conference on Cyber Crime Investigation” com o suporte técnico e pedagógico da Universidade de Brasília e da Associação Brasileira de Especialistas em Alta Tecnologia (ABEAT), autores do artigo “Ferramenta para monitoramento de redes P2P: EspiaMule”:

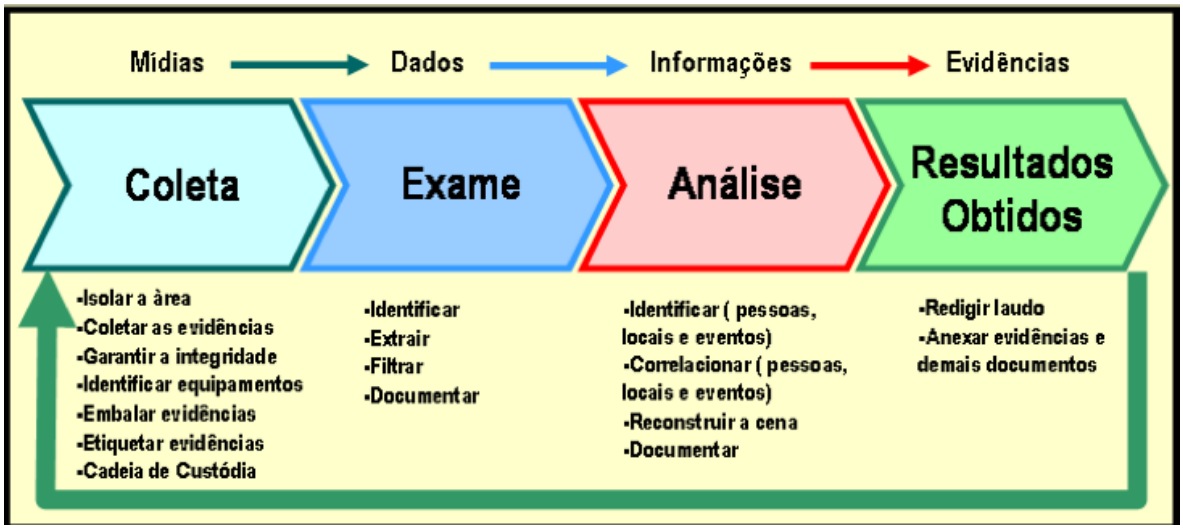
> Da mesma forma que essas redes podem ser utilizadas de forma benéfica, para a troca de arquivos e de conhecimento, elas também são amplamente utilizadas para fins ilegais, como a troca de arquivos com conteúdo pedófilo ou mesmo para a troca de conteúdos protegidos por direitos autorais (DALPIAN; BENITES, 2007, p. 1).

Como contraponto da Rede *peer-to-peer*, algumas redes não atendem cem por cento os requisitos de Cliente-Servidor, como, por exemplo, a rede *eDonkey*, utilizada pelo aplicativo *eMule* para o compartilhamento de arquivos. Nessa rede há

uma dinâmica de servidores, os quais os endereços acompanham a instalação dos aplicativos e se conectam com os clientes para conexões específicas. Em contrapartida o aplicativo *eMule* também compartilha da rede *Kad* a qual atente fielmente os requisitos de *peer-to-peer*, sendo que cada conexão dentro desta rede se comporta tanto como servidor, quanto como cliente, causando uma completa descentralização dos dados compartilhados, facilitando o suposto anonimato da rede (DALPIAN; BENITES, 2007, p. 1).

Por fim, abordando todos os conceitos citados anteriormente, a metodologia utilizada pela Polícia Federal brasileira trata-se da Perícia Forense dos dados, a qual é dividida em coleta, em exame, em análise e em resultados obtidos, conforme ilustra a Figura1.

Figura 1 - Etapas do processo de computação forense



Fonte: (KENT; CHEVALIER; GRANCE; DANG, 2006, p. 3.1.1, *Apud* SOUSA, 2016, p. 101)

As etapas do processo forense iniciam-se na coleta, cujo objetivo é estabelecer a integridade das evidências, enquanto identifica, isola, etiqueta e registra os dados relacionados à investigação, seguida pela etapa de exame, a qual permite extrair e identificar os dados, por meio de ferramentas forenses e técnicas adequadas, e, na etapa de análise, os resultados do exame são analisados de forma criteriosa para que possibilite a criação de respostas para as questões relacionadas as etapas anteriores, e por fim, os relatórios ou resultados, os quais se instituem em encontrar a relevância da investigação; nesta etapa se inclui a redação dos laudos periciais, os quais obrigatoriamente devem conter conclusões imparciais, claras e objetivas, de

fácil compreensão e interpretação por uma pessoa de conhecimento médio (SOUSA, 2016, p. 101).

A partir das mídias eletrônicas, as informações geradas pelos dados são analisadas, e o perito é responsável por preservar e analisar as evidências comprobatórias de crimes virtuais relacionados à pornografia infantil e, por último, prosseguir com o processo judicial.

1.2 Exploração das técnicas aplicadas em prol da Perícia Forense para a captura de informações relacionadas aos crimes sexuais contra crianças e adolescentes efetuadas pela Polícia brasileira

Conforme mencionado anteriormente, a metodologia utilizada pela polícia brasileira para coletar e analisar informações sobre crimes sexuais contra crianças e adolescente, se baseia em Perícia Forense, também conhecida como Computação Forense e/ou Investigação Forense. Para compreendermos a técnica forense, o presente item explora os conceitos de definição de Computação Forense, técnicas aplicadas na etapa de coleta de dados, técnicas utilizadas na etapa de extração de dados, etapa de análise, cadeia de custódia de evidencias e, por fim, exemplo de abordagem sofisticada para extração de dados, a denominada “Operação *Darknet*”, a qual permite entender as etapas e procedimentos para coleta, análise e relatório de dados, os quais, fundamentam um processo judicial de combate à exploração sexual de crianças e adolescentes.

A Computação Forense se dispõe da necessidade de investigar crimes cometidos no âmbito digital, conforme o Artigo 158 do Código de Processo Penal Brasileiro (CPP), Decreto Lei nº 3.689, de 3 de outubro de 1941, que diz que: “Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado”. Em outras palavras, para o ambiente virtual, significa seguir vestígios digitais, através de rastreamentos de informações lógicas relacionadas aos *bits* e de Metadados das informações obtidas. Neste sentido, toda a documentação obtida por meio da investigação dos vestígios digitais deve ser preservada e armazenada, conforme sugerem Eleutério e Machado, em dispositivos de armazenamento digital, a fim de garantir a integridade das evidências digitais (ELEUTÉRIO; MACHADO, 2011, p. 28).

A utilidade de técnicas de imagem e de espelhamento possibilitam os exames Forenses através de duplicatas idênticas dos dados, os quais são efetuados por meio de softwares e equipamentos forenses. A cópia fiel dos dados e correta

preservação de material apreendido são possibilitadas nessa etapa, há muitas ferramentas de hardware que ajudam nas técnicas de imagem e de espelhamento, como, por exemplo, duplicadores Forenses e bloqueadores de escrita (ELEUTÉRIO; MACHADO, 2011). Os sistemas operacionais, por sua vez, apesar de compartilharem do objetivo comum de manipulação de dados, possuem particularidades para atuar em certos sistemas operacionais mais conhecidos, nesse caso, há softwares Forenses que atuam de forma coerente. De acordo com Eleutério e Machado (2011), alguns exemplos de software são: para o sistema operacional Windows, *Forensic ToolKit* (FTK) e Encase (ELEUTÉRIO; MACHADO, 2011, p. 68). Entretanto, há sistemas operacionais desenvolvidos exclusivamente com o propósito Forense, tais como “Knoppix” e o “Helix” (ELEUTÉRIO; MACHADO, 2011, p. 28).

Para ilustrar a coleta de evidências digitais para dados, abordaremos a divisão em dois grupos que, segundo Lillard *et al* (2010), são as divisões de Perícia Forense computacional, grupo *post-mortem* e coleta *Live*. O primeiro grupo, *post-mortem*, realiza a coleta em fontes de dados não voláteis, ou seja, aqueles que independem de energia para armazenamento, como, por exemplo, *CDs*, *DVDs*, cartões de memória, mídias de armazenamento, discos rígidos (*HD)* (ELEUTÉRIO; MACHADO, 2011, p. 29-35). Já o segundo grupo, *live* ou grupo em vida, realiza a coleta em fonte de dados voláteis, ou seja, armazenamento temporário de dados, como, por exemplo, memória *RAM* ou dados presentes em uma rede de computadores (ELEUTÉRIO; MACHADO, 2011, p. 27).

Após o fim da coleta de evidências, o próximo passo é a extração de dados, cujo objetivo é selecionar informações relevantes para análise do próximo passo. Em alguns casos na etapa de extração de dados, o perito se depara com alguns entraves, por exemplo, evidências inacessíveis, seja por proteção de senha, criptografias ou até mesmo exclusão dos dados, tornando assim necessário aplicar algumas técnicas de recuperação como, por exemplo, *Data Carving*, Engenharia reversa, Engenharia social e ataques de força bruta (ELEUTÉRIO; MACHADO, 2011, p. 80-84). A técnica denominada *Data Carving*, se dispõe à recuperação de arquivos deletados por meio de softwares como, *Photorec* e *Ontrack Recovery* (ELEUTÉRIO; MACHADO, 2011, p. 65). A Engenharia Reversa propõe que, através de um produto, seja possível conhecer o modelo virtual, ou seja, com o modelo virtual obtido do modelo físico, realiza-se a análise de forma a conhecer a estrutura de desenvolvimento (ELEUTÉRIO; MACHADO, 2011, p. 83-84).

A Engenharia Social, por sua vez, usa-se da persuasão do usuário para obter informações com ou sem o uso de tecnologia, segundo Mitnick (2003, p. 6). Os ataques de força bruta são aqueles que se dispõem a acessar um sistema com inúmeras tentativas até obter sucesso, o qual, muitas vezes, conta com suporte de softwares que usam de um dicionário de senhas, como, por exemplo, *Advanced Password Recovery Kit* (ELEUTÉRIO; MACHADO, 2011, p.82).

No caso da identificação de materiais que contem pornografia infantil, a extração de dados ocorre ao selecionar os arquivos que possuem *hashes* e palavras-chave previamente conhecidos como ilegais e faz parte da etapa de análise, realiza-se, ainda, uma comparação com um conjunto de dados pertencentes à Polícia Federal, como, por exemplo, o *Known File Filter* (KFF), visto que, quando os dados extraídos são compatíveis ao banco de dados com valores de *hashes* conhecidos, o relatório de evidências começa a ser desenvolvido (ELEUTÉRIO; MACHADO, 2011, p.66).

Em alguns casos, na etapa de análise é viável utilizar técnicas de virtualização para simular e entender as abordagens do usuário, recriando seus passos (ELEUTÉRIO; MACHADO, 2011). Nessa etapa também é possível realizar análise em tráfego de redes, o qual permite a análise em tempo real ou a partir de captura anterior, por meio da captura de um pacote, e independe de como foi capturado; o pacote de dados é importante para conhecer a origem e o destino das informações, além de oferecer o conhecimento das portas utilizadas para entrada e saída e, principalmente, o conteúdo completo de pacotes suspeitos (GALVÃO, 2013).

A Secretaria Nacional de Segurança Pública (SNSP), vinculada ao Ministério da Justiça, por meio da Portaria nº 82, de 16 de julho de 2014, estabelece algumas diretrizes sobre os procedimentos a serem observados no tocante à cadeia de custódia de vestígios, cujas etapas descreveremos logo abaixo (BRASIL, 2014).

As etapas de coleta, de extração e de análise de dados são seguidas pela etapa de relatórios, os quais fazem parte da cadeia de custódia, que consiste em obter registros detalhados de como as evidências foram tratadas em todas as fases; os registros devem conter informações sobre quem teve acesso as evidências e são extremamente relevantes durante o processo judicial para garantir a integridade das evidências obtidas, haja vista que cada evidência coletada deve ter um registro de custódia compatível.

Um registro de custódia deve conter data e hora da coleta, dono da evidência apreendida, informações sobre o *hardware* analisado, nome de quem coletou os

dados, descrição detalhada da evidência, nome e assinatura das pessoas envolvidas, identificação das evidências (como *tags*, ou indexação), se possível, ainda, assinaturas únicas, e todas as informações técnicas pertinentes (BRASIL, 2014).

O presente registro das evidências colhidas dará subsídio para a apuração do delito, conforme estabelece os *caputs* dos artigos 159 e 160, respectivamente, do Código de Processo Penal:

“O exame de corpo de delito e outras Perícias serão realizados por perito oficial, portador de diploma de curso superior” e “os peritos elaborarão o laudo pericial, onde descreverão minuciosamente o que examinarem, e responderão aos quesitos formulados” (BRASIL, 1941b).

Para ilustrar as fases mencionadas, observamos um exemplo de abordagem fundada em extração de dados, como ocorreu com a “Operação *DarkNet”,* realizada pela Polícia Federal, em duas fases distintas, nos anos de 2014 e 2016. Podemos justificar o exemplo aludido, pois observaremos a existência de dois elementos fundamentais: 1) a extração de dados; 2) a análise dos dados obtidos pela operação da Polícia Federal.

A operação policial se desenvolveu em duas fases. A primeira ocorreu em 2014, contou com a participação de mais de quinhentos policiais federais, isso foi possível graças a infiltração de policiais na *Deep Web*, que utilizaram o *malwares*, assim, facilitou o rastreamento, para a comprovação da existência de delitos virtuais, e, ao mesmo tempo, os policiais criaram um fórum para discutirem a pedofilia, sob o controle da Polícia Federal, a fim de rastrear suspeitos. Através dessas informações obtidas pela Polícia Federal, foi possível realizar cinquenta e uma prisões, das quais, cinquenta delas em flagrantes, além do cumprimento de cem mandados de múltiplas naturezas, como, busca, apreensão, prisão e condução coercitiva, propagadas em dezoito Estados e no Distrito Federal.

“A Operação *DarkNet* foi deflagrada simultaneamente por quarenta e quatro unidades da Polícia Federal nos estados do Amazonas, do Amapá, da Bahia, do Ceará, do Espírito Santo, de Goiás, de Minas Gerais, do Pará, de Pernambuco, do Piauí, do Paraná, do Rio de Janeiro, do Rio Grande do Norte, do Rio Grande do Sul, de Rondônia, de Santa Catarina, de São Paulo, do Mato Grosso do Sul e no Distrito Federal. As informações obtidas durante as investigações que envolvem suspeitos

de outros países foram repassadas para autoridades de Portugal, da Itália, da Colômbia, do México, da Venezuela” (POLÍCIA FEDERAL, 2014).

A infiltração dos servidores na *Deep Web* visava confirmar a identidade dos suspeitos e buscar elementos comprobatórios dos crimes de armazenamento e de divulgação de imagens de abuso sexual de crianças e de adolescentes. Para que os policiais pudessem transitar nesse ambiente virtual foi necessária uma prévia autorização judicial, em conformidade a Lei 11.829/2008 que, entre outros objetivos, intenta “criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet” (BRASIL, 2008). Essa prévia autorização foi imprescindível, haja vista que, no Brasil, as legislações anteriores, de modo particular o Estatuto da Criança e do Adolescente, Lei 8.069/1990, não validava este tipo de prova criminal.

No intuito de salientar a importância dessa Operação, da qual realizou detenções e até possibilitou o resgate de crianças em situação de vulnerabilidade sexual, descrevemos a informação a seguir:

> (...) Pelo menos seis crianças foram resgatadas de situações de abuso ou do iminente estupro, em diversos locais do Brasil. Em um dos casos, um pai relatava que iria abusar da filha assim que ela nascesse (POLÍCIA FEDERAL, 2014).

Sendo assim, graças a ação dos policiais federais possibilitou atingir dois objetivos: primeiramente, a ação policial impediu que as crianças permanecessem nessa situação de vulnerabilidade, em função da eventual exploração que sofreria; 2) impediu que as crianças se tornassem potenciais vítimas, inclusive de seus progenitores.

Na segunda fase da Operação administrada pela Polícia Federal, que ocorreu no ano de 2016, a ação impetrou sessenta e um mandados de busca e de apreensão, quatro mandados de prisão e quinze detenções em delito flagrante (POLÍCIA FEDERAL, 2016). Apenas para ilustrar, dos 61 (sessenta e um) mandados expedidos, 19 (dezenove) deles foram executados no Estado de São Paulo, inclusive com um flagrante, conforme ilustra a Figura 2.

Figura 2 - Balanço da Operação DarkNet II

SÃO PAULO			
CIDADE	MANDADO DE BUSCA	MANDADO DE PRISÃO	PRISÃO EM FLAGRANTE
CAMPINAS	3	0	0
POPULINA	2	0	0
SÃO JOSÉ DO RIO PRETO	2	0	0
SOROCABA	1	0	0
SANTOS	1	0	0
SÃO PAULO	7	0	0
GUARULHOS	1	0	1
MOGI DAS CRUZES	1	0	0
SANTO ANDRÉ	1	0	0

Fonte: Polícia Federal (2016)

Essa ação foi considerada um sucesso, em função do uso de métodos de rastreamento para identificação de endereço IP (Internet Protocol) dos usuários conectados à rede mundial de computadores que, em virtude da investigação, desenvolveu aplicativos para efetuar a análise dos dados coletados na rede *Tor*, rede que prevê navegação anônima e indetectável, os quais foram desenvolvidos exclusivamente pela Polícia Federal. Não obstante, em função da natureza sigilosa da criação e do desenvolvimento desses aplicativos, dados técnicos não podem ser ofertados:

> O tipo da ação realizada só foi possível uma vez que a Polícia Federal desenvolveu métodos próprios de rastrear e identificar o endereço de IP dos usuários que estão acessando a rede no momento. O delegado [Fernando Casarin] garante que a tecnologia empregada em quebrar o anonimato na rede Tor é totalmente nacional, embora não possa dar muitos detalhes sobre o método (MARCHETTI, 2016).

Os fóruns investigados no ambiente *Deep Web,* por meio da rede *Tor*, continham compartilhamento de imagens e discussões sobre meios de realizar abusos nas crianças sem deixar evidências corpóreas. Muitos criminosos sexuais creem que essa rede é plenamente anônima. No entanto, nos últimos anos

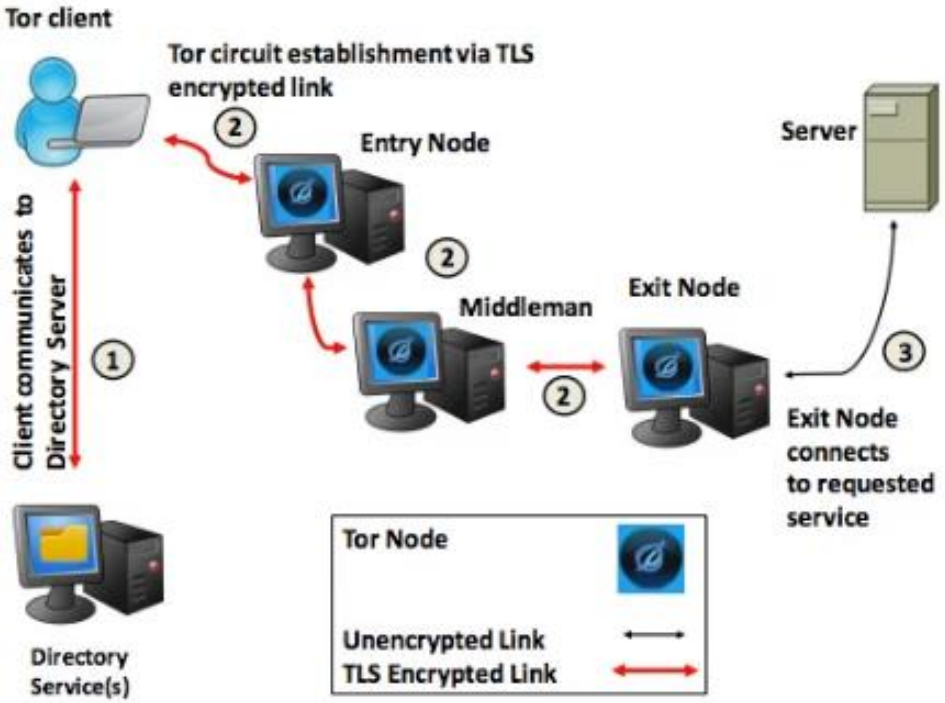
> com a prisão de muitos traficantes e redes de pedofilia, a rede Tor se provou não tão anônima assim. O FBI, a Scotland Yard, a Polícia Federal Australiana e outros órgãos internacionais aplicam diversas técnicas de investigação, de agentes infiltrados à aplicação de malwares rastreadores (MARCHETTI, 2016).

A fim de esclarecer o funcionamento da rede *Tor*, seu tráfego de dados é encriptado por *TLS* (*Transport Layer Security*), o que dificulta o rastreamento de navegação, possibilitado por meio de vários roteadores, os quais propagam dados entre si, até atingir um destinatário final. Em outras palavras, a informação circula na rede encriptada, como se fossem nodos que se interligam e se repetem constantemente, gerando uma comunicação aparentemente anônima.

De acordo com Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis, Angelos D. Keromytis, da Universidade de Columbia, Estados Unidos, no artigo “On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records”, apresentam meios para decodificar o anonimato da rede *Tor*. Eles, graças aos estudos e pesquisas avançadas, alicerçados em laboratório computacional e no ambiente real da rede *Tor*, descobriram uma vulnerabilidade que permitiu identificar usuários conectados em 100% do tempo verificado em laboratório computacional, e em 81,4% do tempo conectado desses usuários no ambiente real desta rede (CHAKRAVARTY; BARBERA; PORTOKALIDIS; POLYCHRONAKIS; KEROMYTIS, 2014, p. 247).

O *link* encriptado TLS é o motivo do anonimato, pois ao embaralhar os pacotes de dados, gera-se certo atraso que, consequentemente, camufla a origem dos dados. Desta forma, os pesquisadores investigaram como diferentes nodos, propagados por distintos servidores, os denominados “nodos de saída”, se identificados, tornam-se possíveis detectar o ponto de origem da conexão, e, consequentemente, anular o suposto anonimato, conforme revela a Figura 3.

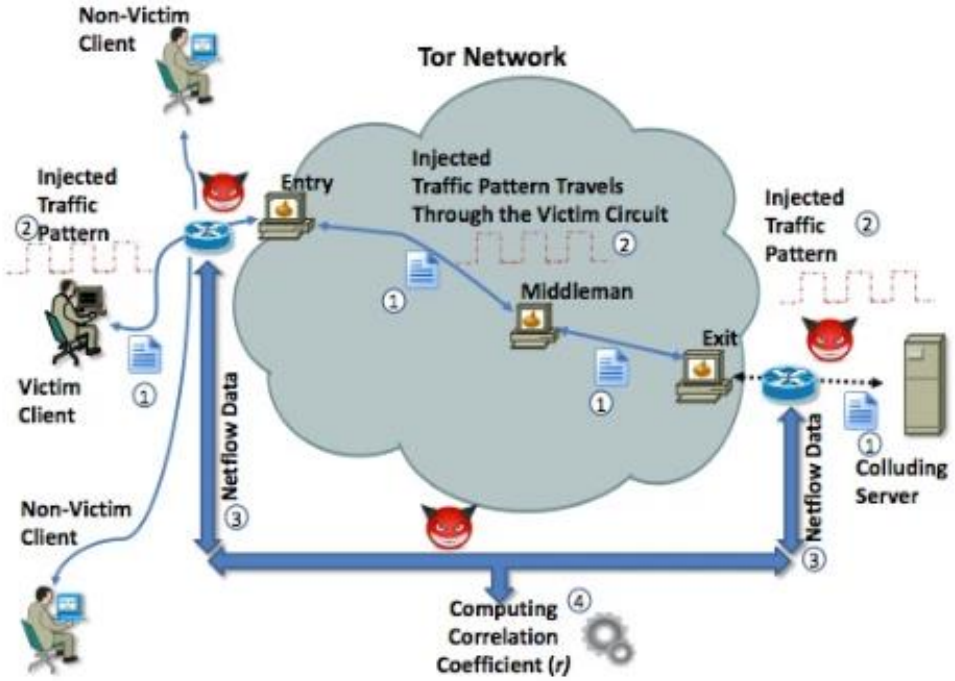
Figura 3 - O funcionamento Tor



Fonte: (CHAKRAVARTY; BARBERA; PORTOKALIDIS; POLYCHRONAKIS; KEROMYTIS, 2014, p. 248)

O método de Chakravarty e outros pesquisadores exploram uma vulnerabilidade codificada em todo o roteador, que faz uma análise estatística para descobrir os “nodos” de origem, por meio da configuração de um servidor de *sites* falsos; quando o usuário está baixando um arquivo grande isso permite que a vulnerabilidade explore as configurações da máquina do usuário e colete informações da *NetFlow*, funcionalidade desenvolvida pela Cisco que divide o tráfego por tipo de dados (CHAKRAVARTY; BARBERA; PORTOKALIDIS; POLYCHRONAKIS; KEROMYTIS, 2014). Enquanto ocorre a conexão com o servidor do *site* falso, os dados são enviados de volta para os nodos, e, se o usuário continuar roteado por esses nodos (conexão estabelecida) é conquistado o acesso ao *NetFlow*, o que possibilita "adivinhar" a origem real do nodo de entrada, conforme a ilustração da Figura 4.

Figura 4 - Processo geral para análise com base em NetFlow contra o Tor



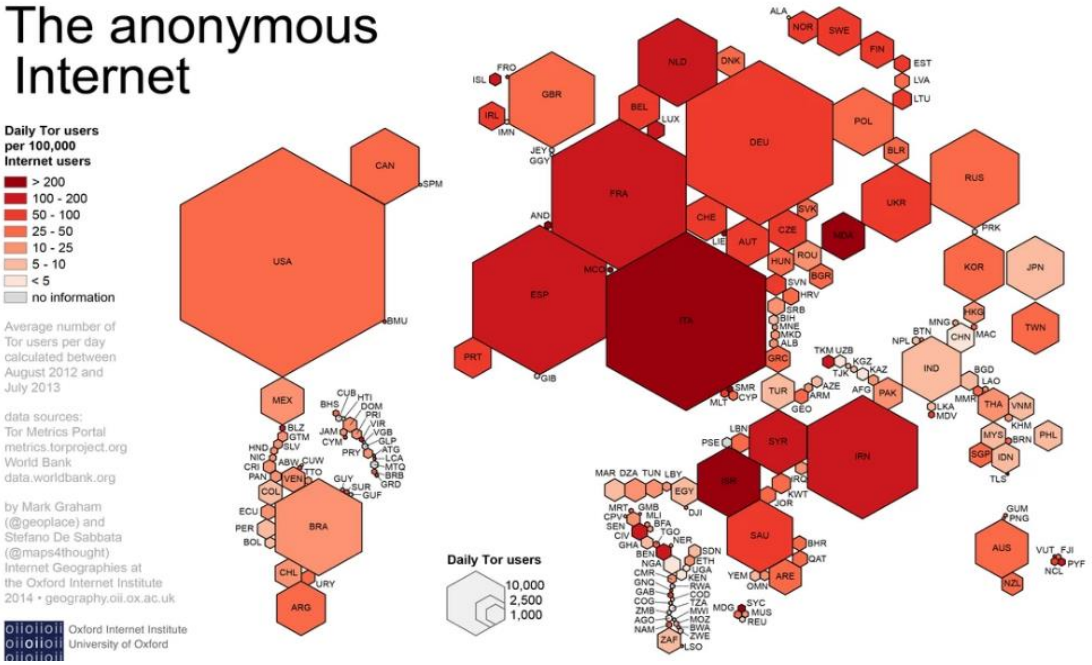
Fonte: (CHAKRAVARTY; BARBERA; PORTOKALIDIS; POLYCHRONAKIS; KEROMYTIS, 2014, p. 254)

De acordo com os autores mencionados, o processo geral para a análise com base em *NetFlow* contra a Rede *Tor* dá-se da seguinte maneira:

> O usuário baixa um arquivo do servidor 1, enquanto o mesmo injeta um padrão de tráfego na conexão TCP do nodo de saída 2. Após um tempo, a conexão é encerrada e o adversário recebe dados de fluxo correspondentes ao servidor de saída e do nodo de entrada para o tráfego de usuário 3, e computa o coeficiente de correlação entre o servidor de saída de tráfego e entrada com as estatísticas do usuário 4 (CHAKRAVARTY; BARBERA; PORTOKALIDIS; POLYCHRONAKIS; KEROMYTIS, 2014, p. 254).

Isso indica que qualquer instituição ou pessoa física é capaz de conhecer o suposto anonimato da rede *Tor*, os pesquisadores destacaram o uso de *software* livre para realizar o estudo. A Figura 5 ajuda-nos a entender a proporção de usuários da rede *Tor* no ano de 2014.

Figura 5 - Proporção de usuários da rede Tor no mundo em 2014



Fonte: Universidade de Oxford (2014)

Supondo a exploração da rede *Tor*, utilizando a metodologia dos pesquisadores Chakravarty e outros, identificar criminosos virtuais não é impossível, entretanto, não se trata de uma abordagem simples, extremamente dependente de múltiplas variáveis para o sucesso (CHAKRAVARTY; BARBERA; PORTOKALIDIS; POLYCHRONAKIS; KEROMYTIS, 2014).

Pelas razões exploradas, o cotidiano policial exige mais de uma abordagem de extração de dados, para que a proteção da infância e juventude seja eficiente no ambiente virtual. Atualmente a abordagem mais conhecida para a coleta de dados, ocorre através da Rede *peer-to-peer*, por meio dos aplicativos EspiaMule, IPED, LED e *NuDetective*, desenvolvidos por membros da Polícia Federal, que atuam no âmbito da Perícia Forense (BRASIL, 2017).

1.3 Análise da existência de aplicativos utilizados pelo aparato policial (Polícias Federal, Militar, Civil) para a identificação de criminosos que cometem ações civis e penais dessa natureza

Para auxiliar nos trabalhos de Perícia Forense, mais especificamente no que diz respeito a extração e análises de dados, as técnicas devem ser constantemente melhoradas e, em busca destas, novos métodos e aplicativos são implementados pela Polícia Federal brasileira à medida que as legislações sofrem alterações. Com

o objetivo de melhorar o processamento de dados e garantir a aplicação das devidas punições aos crimes cibernéticos, os peritos integrantes das organizações policiais ao longo do tempo passaram a desenvolver aplicativos próprios com algoritmos e metodologias que atendem as demandas de investigações. Através de pesquisas no Portal da Polícia Federal, foram reunidas as informações sobre os aplicativos utilizados atualmente para coleta, para exame e para análise de dados que possuem conteúdos de pornografia infantil em redes ponto a ponto e em dispositivos eletrônicos apreendidos via mandado de busca e apreensão.

Para monitoramento de clientes de redes ponto a ponto é utilizado um aplicativo que foi desenvolvido por peritos da área chamado EspiaMule, que atua como um "espião" na Rede *peer-to-peer,* coletando dados na rede (DALPIAN; BENITES; 2007). Para a análise Forense dos dados já coletados, que facilita a visualização das mídias ópticas, é utilizado o aplicativo IPED (Indexador e Processador de Evidências Digitais) (BRASIL, 2017, p. 45), responsável por indexar o conteúdo apreendido.

Por último, especificamente para dados relacionados à pornografia infantil, faz-se o uso das ferramentas LED (BRASIL, 2017, p. 40-41) e *NuDetective* (POLASTRO; ELEUTÉRIO, 2010, p.17). As ferramentas IPED e LED são softwares livres e estão disponíveis para *download* e utilização no Portal da Polícia Federal e serão objetos de análise a seguir, entre outros.

1.3.1 EspiaMule

O aplicativo EspiaMule, amplamente utilizado pela Polícia Federal, atua na comunidade *peer-to-peer,* rede na qual é permitida a troca de dados por meio de vários dispositivos conectados ponta a ponta, criando várias conexões servidor/cliente, que acelera a transmissão dos dados (*Vide* Figura 6).

O EspiaMule trata-se de um cliente modificado na rede, desenvolvido com base no código livre do aplicativo *eMule*, muito utilizado para o compartilhamento de dados pela comunidade *peer-to-peer*, o qual suporta as redes *eDonkey* e *Kad*. Entretanto, o EspiaMule possui característica de armazenamento de todos os IPs clientes disponíveis na rede, o que permite o rastreamento de informações físicas dos usuários, podendo ser descoberto inclusive o país do usuário que está compartilhando arquivos. Conforme explicam Dalpian e Benites (2007), o aplicativo apenas registra a numeração dos IPs clientes encontrados na fila de *download* da

rede, que são realizados por meio de links ED2K. O EspiaMule faz a busca de *links* para os arquivos disponíveis na rede através de palavras-chave; logo em seguida, em posse dos arquivos selecionados os links ED2K são calculados e distribuídos pela interface do *eMule* ou o aplicativo *LinkCreator*, os *links* calculados possuem informações como *hashes* MD4, e caso exista um alerta de *hash* conhecido como ilegal, os peritos prosseguem com mais análises, como, por exemplo, utilizar o comando "*Whois*" para identificar o provedor de comunicação responsável, que, por meio de termos de cooperação, fornecem informações dos usuários em questão (DALPIAN; BENITES, 2007, p.72) .

Figura 6 - Interface inicial do aplicativo EspiaMule

Fonte: (OLIVEIRA; SILVA, 2009, p.109)

1.3.2 Indexador e Processador de Evidências Digitais (IPED)

O IPED, segundo a edição 3.13.5 do Manual projetado pela Coordenação Geral de Tecnologia da Informação da Polícia Federal, Departamento vinculado ao Ministério da Justiça do governo federal, atualizada em 22 de junho de 2018, é um programa que utiliza linhas de comando e apresenta diversas funcionalidades presentes em *softwares* forenses, dentre elas estão o processamento de imagens, de categorização de arquivos, de detecção de arquivos criptografados, de cálculo e de

consulta a base de *hashes* e principalmente de indexação de conteúdo, o que facilita e aumenta a velocidade das buscas (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018). O IPED utiliza outros programas de código aberto, entre eles *The Sleuthkit (TSK)*, *Apache Tika*, entre outras bibliotecas, processando os principais sistemas de arquivos existentes, inclusive o *Microsoft* NTFS (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018, p. 2). Esses programas e bibliotecas facilitam a visualização, melhoram a qualidade de laudos contendo palavras-chave, assim como a análise dos dados. Além de ser uma alternativa de *software* Forense para a recuperação de dados apagados. A sua velocidade de processamento superior a *300GB*/*h*, permite a análise de dados de forma simultânea em até cem dispositivos diferentes (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018, p. 3).

As funcionalidades desse programa refletem os principais passos das análises realizadas em mídias digitais, dentre elas podemos destacar: Cálculo de múltiplos *hashes*, que suportam os formatos md5, sha-1, sha-256, sha-512, *edonkey*, entre outros (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018, p. 2). Através da base de *hashes,* esse *software* pode alertar arquivos suspeitos ou descartar arquivos comuns, assim como, separar arquivos por categorias com base nos formatos mais utilizados, além de, indexar os textos que são extraídos de vários tipos de arquivos diferentes (BRASIL, 2017).

A ferramenta também pode realizar recuperação de arquivos que foram apagados utilizando referência das remoções, assim como, extração de arquivos em espaços não alocados no disco. Para acessar os espaços não alocados são utilizadas as bibliotecas *The Sleuthkit* (TSK) e *Libewf*, as quais fazem indexação do conteúdo e o submetem a *data carving* (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018, p. 3).

Para ativar o *data carving* é necessário habilitar o parâmetro *enableCarving* no arquivo IPEDConfig.txt. Nesse arquivo de configuração é possível incluir ou excluir arquivos do processamento, realizar *carving* apenas sobre o espaço não alocado e/ou sobre os alocados (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018, p. 3).

Uma das principais funcionalidades que o IPED pode exercer é a indexação do conteúdo, porém antes é realizada a extração de texto dos arquivos com a biblioteca *Apache Tika*, dentre os formatos suportados por esta biblioteca estão:

> MS Office (doc, docx, xls, xlsx, ppt, pptx e similares), OpenOffice (odt, ods, etc), Apple iWork (key, pages, numbers), PDF, HTML e XML, RTF e TXT, e-mails (RFC822 e Outlook MSG) e metadados de audio (midi, mp3), imagens (bmp, jpg, psd, png, tif, etc) e vídeos (flv, mp4 e derivados e ogg e derivados), dentre outros (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018, p. 3).

A partir da versão 3.9 do software IPED passaram a ser geradas miniaturas de imagens por padrão durante o processamento, cuja função pode ser desabilitada, dessa maneira, a visualização de figuras na galeria se torna instantânea. A partir da versão 3.13 foi alterado também o processador de imagens, que foi do *GraphicsMagick* (GM) para o *ImageMagick* (IM). Com o novo processador, tornou-se possível visualizar centenas de formatos de imagens que até então não eram suportados pelo Java, reduzindo o custo de processamento das miniaturas. Na versão 3.4 foi incluída a função que extrai cenas de vídeos utilizando o *software MPlayer*. As configurações de extração de cenas, como resolução e quantidade de quadros extraídos podem ser alteradas no arquivo *conf/VideoThumbsConfig.txt* (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018, p. 3-4). Uma grande vantagem é que as miniaturas de vídeos podem ser visualizadas na galeria de imagens, permitindo uma boa visualização. Na versão 3.13 também foi adicionada a funcionalidade de localização de expressões regulares durante o processamento. As expressões existentes de dados pessoais como: CPF (Cadastro de Pessoa Física), CNPJ (Cadastro Nacional de Pessoa Jurídica), PIS (Programa de Integração Social) / Pasep (Programa de Formação do Patrimônio do Servidor Público), CNH (Carteira Nacional de Habilitação), e-mail (endereço eletrônico), URL (Uniform Resource Identifier), IP (Internet Protocol), valores monetários, contas bancárias, boletos, cartão de crédito, Iban (International Bank Account Number, isto é, Número Internacional de Conta Bancária), *Swift* (Society for Worldwide Interbank Financial Telecommunication, isto é, Sociedade de Telecomunicações Financeiras Interbancárias Mundiais) e título de eleitor, foram adicionadas ao IPED. Caso existam algumas dessas informações, é checado o dígito verificador e elas são encontradas durante a pesquisa. As expressões regulares podem ser configuradas em *conf/RegexConfig.txt.* Outra função possível de ser utilizada a partir da versão 3.13 é a de reconhecimento de entidades mencionadas via *StanfordCoreNLP*. Essa função, por meio de processamento de linguagem natural, permite identificar nomes de pessoas, organizações e lugares nos textos. Ela pode aumentar o tempo de

processamento em até quatro vezes, e por isso essa função não vem habilitada por padrão; para utilizá-la é necessário configurar no parâmetro *enableNamedEntityRecogniton* no arquivo IPEDConfig.txt (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018, p. 4).

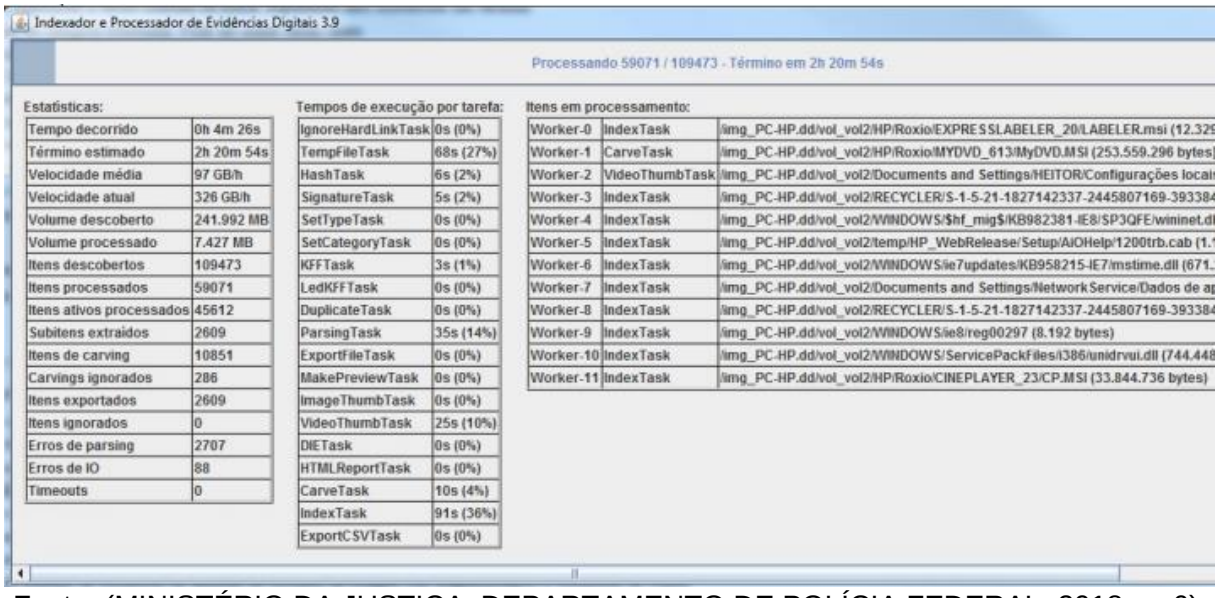
Na versão 3.11 foram criados marcadores automáticos para itens localizados na evidência e compartilhados pelo Emule, Ares e *Shareaza*, e, na versão 3.12, para arquivos enviados por *Skype* e *WhatsApp*. Para ativar esta função é necessário habilitar os *hashes* utilizados por cada um dos programas, no caso md5 para *Shareaza*, sha-1 para Ares, *edonkey* para emule e sha-256 para WhatsApp.

> Basicamente os *hashes* presentes nos arquivos de controle de transferências são pesquisados no caso e, caso encontrados, são criados marcadores automáticos para esses itens por aplicativo (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018, p. 8).

É importante salientar que, no caso específico do *Skype*, por não haver registro de *hashes* de arquivos transferidos, são utilizadas informações de tamanho original.

Além de todas essas funcionalidades citadas, o *software* Iped também realiza agrupamento por Metadados, no qual agrupa e filtra arquivos usando como base valores de qualquer Metadados; também realiza georreferenciamento de imagens, que permite visualizar a localização de origem da imagem utilizando *GPS*. É possível, ainda, verificar a localização de documentos por sua similaridade, utilizando uma fonte para identificar palavras que representam documentos e, quanto mais palavras em comum, mais similares eles são e, finalmente, realiza a análise simultânea ao processamento (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018). Os resultados apresentados pelo Iped são considerados satisfatórios por sua precisão, porém devido ao grande número de arquivos e formatos a serem tratados, ela nunca será 100%, podendo ser diferente do resultado de outras ferramentas utilizadas, conforme os resultados da Figura 7.

Figura 7 - Tela de processamento IPED – Versão 3.9



Fonte: (MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL, 2018, p. 6).

1.3.3 Localizador de Evidências Digitais (LED)

De acordo com a matéria jornalística efetuada pelo “Jornal da USP”, em 14 de agosto de 2017, o LED é uma tecnologia exclusiva da Polícia Federal que visa identificar o padrão de arquivos criminosos, a partir de banco de dados específicos, conforme detalha o Perito Judicial Federal, Evandro Lorens:

> O monitoramento é feito através das redes sociais e sites de compartilhamento de arquivo. A partir do acompanhamento de ações suspeitas, a PF emite um mandado de busca e apreensão (USP, 2017).

Quando há a necessidade de busca e apreensão de equipamentos que possuem dados relacionados à pornografia infantil, é utilizado o Localizador de Evidências Digitais (LED), que facilita a localização dos vestígios de uma maneira rápida e eficaz (BRASIL, 2017, p. 40). Por sua velocidade de processamento, O LED é muito utilizado *in loco*, ou seja, no momento da apreensão das mídias, porém apenas quando houver condições técnicas e táticas, a fim de validar a sua utilização (BRASIL, 2017, p. 38).

Originalmente, esse software surgiu como uma opção ao *script* que investigava expressões ilícitas em nomes de arquivos e fazia uma comparação de *hashes* de imagens e mídias com uma lista de *hashes* conhecidos. Durante seu desenvolvimento foram incrementadas várias outras funcionalidades, que serão

citadas a seguir. A ferramenta possui interface gráfica acessível; para fazer uma varredura, basta selecionar várias pastas utilizando as teclas *Ctrl* ou *Shift.* Esse método funciona para varredura das pastas raízes e suas subpastas. Abaixo, na Figura 8, temos a interface gráfica da ferramenta LED.

Figura 8 - Tela inicial do aplicativo LED

Fonte: (BRASIL, 2017, p.41)

Em entrevista com o Presidente da APECOF (Associação Nacional de Peritos em Computação Forense) e Perito Judicial, prof. Marcos Monteiro, explicou que, no processo de busca das pastas selecionadas na tela inicial do aplicativo LED, a ferramenta emite alerta em algumas situações, como, por exemplo, arquivos ou diretórios que possuem termos relacionados à pornografia infantil (definidos pelo próprio usuário); alerta de tamanho, pois em casos onde o arquivo é muito grande há suspeita de extensões *ISO*, NRG, etc.; alerta quando são encontrados nomes iguais aos que contêm na lista de arquivos conhecidos de pornografia infantil; inclusive alerta para arquivos relevantes, como, por exemplo, arquivos que vieram do *e-Mule*, *Shareaza*, *Limewire*, *Tor*, *Skype* e, por último, alerta para arquivos ou diretórios inacessíveis (MONTEIRO, 2019).

Como acontece com outras ferramentas, o LED possui a funcionalidade de busca de arquivos por *hash.* Para classificar se o arquivo é um vídeo ou imagem, é utilizada a sua extensão, conforme lista que é definida no arquivo de configurações. A diferença do LED para os outros aplicativos é que caso a varredura de *hashes* encontre uma grande quantidade de *gigabytes* em vídeos, ele implementa uma otimização que reduz o volume de dados e, consequentemente, o tempo de análise. Essa otimização consiste primeiramente em verificar o tamanho do arquivo, ou seja, caso o tamanho seja diferente dos que estão na base de dados, a consulta por *hash* deixa de ser necessária. Caso o tamanho seja conhecido, é feito o cálculo do *hash* MD5 dos primeiros 512 *bytes* do início do arquivo; se eventualmente esse *hash* inicial for diferente dos arquivos já estimados, o cálculo é interrompido, reduzindo drasticamente o tempo de análise (MONTEIRO, 2019).

Caso as buscas por nome ou por *hash* não funcionem, é feita a busca por conteúdo, na qual consiste em fazer uma configuração para realizar uma varredura por extensões, como TXT, HTML e EML ou dados que estejam armazenados em navegadores. Para agilizar o processo, o tamanho dessa busca é limitado a 10MB, sendo que, em arquivos maiores, são buscados apenas os primeiros *bytes*. Arquivos com extensão EXE, DLL e ZIP são excluídos, pois a busca resume-se na verificação de determinados termos, não sendo feita nenhuma codificação binária. Nesses casos é feita uma verificação de termos suspeitos nos nomes dos arquivos que estão contidos nos subitens destas extensões; se esta verificação não for feita corretamente, é gerado um alerta de conteúdo inacessível (MONTEIRO, 2019).

Apesar da ferramenta LED ter foco em buscas relacionadas à pornografia infantil, é possível alterar a configuração de *hashes* e palavras-chave para outros tipos de crimes virtuais, como, por exemplo, o racismo, crime de ódio, etc. (MONTEIRO, 2019).

Em 2017, a base de dados de pornografia infantil do LED contava com cerca de 2,35 milhões de arquivos, sendo que 66 mil desses arquivos eram vídeos, contabilizando um total de 4,6 *TeraBytes* de dados (MONTEIRO, 2019).

Quanto maior for essa base, maior será a probabilidade de identificação de arquivos de interesse do usuário. É dada preferência de inserção de arquivos não só nos *hashes*, mas na base de dados em si, permitindo consultas em situações onde os arquivos não estão mais acessíveis. Permite também que mais informações possam ser extraídas posteriormente dos arquivos originais (MONTEIRO, 2019).

1.3.4 NuDetective

Através da linguagem de programação *Java Standard Edition* (JSE), uma ferramenta Forense denominada *NuDetective*, de autoria dos peritos judiciais Pedro Monteiro da Silva Eleutério e Mateus de Castro Polastro, criada sem fins lucrativos e para uso exclusivo das instituições públicas. Elaborada para auxiliar no cumprimento da mudança ocorrida no Estatuto da Criança e do Adolescente (ECA), efetuada em 25 de novembro de 2008, a qual tipificou como crime a posse de arquivos de pornografia infanto-juvenil. A atualização legal desencadeou a necessidade de identificar com rapidez, arquivos ilegais presentes em dispositivos computacionais, dentre os milhões de arquivos que podem eventualmente estar armazenados em dispositivos. Na intenção de garantir a eficiência do processo de análise, a tecnologia criada estabelece quatro funcionalidades principais, tais como, a análise de imagem, a análise de nomes, a análise de *hash*, e, por último, inclui a análise de vídeo nas versões mais recentes (ELEUTERIO.COM, 2011).

Com a detecção de arquivos suspeitos armazenados, a ferramenta NuDetective analisa imagens por meio de detecção automática de nudez, através de uso de técnicas que identificam *pixels* de pele e de geometria computacional. Em seguida, faz-se a análise de nomes, por meio de expressões linguísticas para captar expressões mais comuns de pedofilia. Analisa o *hash* que compara os valores *hashes* dos arquivos com uma lista de valores de arquivos ilegais conhecidos, kff (Known File Filter). E, no caso de vídeos, analisa-se e calcula a amostra ideal extraídas de “frames” (fragmentos) dos vídeos, realizando a detecção de nudez nos *frames* por meio de algoritmos utilizados pela análise de imagem (ELEUTERIO.COM, 2011).

De acordo com estudo de Gustavo Aranha Araújo Costa dos Reis é possível fazer a comparação de assinaturas únicas de arquivos, a detecção de pele nos conteúdos digitais, como também a identificação de partes do corpo humano e gerar métodos de classificação por conjunto de características visuais (REIS, 2016, p. 82-83).

Por exemplo, o método de análise de assinaturas únicas consiste em atribuir a cada imagem já evidenciada como pornografia infantil um número específico, o que gera a criação de uma base global de dados de arquivos impróprios, a qual é,

normalmente, conhecida por autoridades aplicadoras da lei (ULGES; STAHL, 2011*Apud* REIS, 2016, p. 83), as quais, após o agrupamento de arquivos suspeitos, calcula e atribui aos arquivos uma assinatura digital única, que, em sequência, é confrontada com os registros ilegais armazenados em Bancos de Dados específicos. Segundo Reis, a metodologia pode ser empregada continuamente no monitoramento de redes de transferência de arquivos entre usuários (*peer-to-peer),* para verificar o tráfego das mídias de assinatura registrada. Entretanto, a metodologia não pode ser aproveitada para casos desconhecidos, ou para imagens editadas, sendo que essas, possuem *hashes* diferentes dos cadastrados no banco de dados (REIS, 2016, p. 83).

Reis reproduz uma afirmação de Polastro e Eleutério, desenvolvedores da ferramenta *NuDetective*:

> As técnicas baseadas na detecção de pele e identificação de partes do corpo possuem como pressuposto que o conteúdo visual das imagens de pornografia infantil a ser destacado é, em grande parcela, composto de pele e formato humano. Sendo assim, faz utilização de mecanismos de filtros para detecção de pele infantil em conjunto com o uso de algoritmos computacionais para percepção de nudez (...) (POLASTRO; ELEUTÉRIO, 2010, *Apud* REIS, 2016, p. 83).

No entanto, Reis explicita um limitador da abordagem deste tipo de detecção, pois:

> As abordagens baseadas no método de detecção de pele possuem um grande limitador já apresentado em trabalhos científicos e demonstrado empiricamente: a ocorrência de falsos positivos. Essa característica pode facilmente ser observada, uma vez que a exposição de pele (ou a exposição explícita de órgãos genitais) em arquivos digitais não está necessariamente relacionada à pornografia infantil (REIS, 2016, p. 83).

No intuito de explicitar o funcionamento do aplicativo *NuDetective*, abordaremos alguns conceitos de aprendizagem de máquina, ou seja, "*Machine Learning*". Esses são amplamente empregados no treinamento de ferramentas computacionais, visto que as habilidades da tecnologia servem para identificar automaticamente padrões e objetos homogêneos, os quais são incentivados via configuração específica. E no caso da ferramenta *NuDetective*, ela é "treinada" para reconhecer as regiões de interesse nas imagens suspeitas, em prol do mapeamento e do reconhecimento imagético, dos temas convergentes de interesse, no caso, imagens de pornografia infantil. Eleutério e Polastro (2010), desenvolvedores da ferramenta *NuDetective*, publicaram alguns artigos a respeito deste aplicativo, dentre eles "*Identification of*

High-Resolution Images of Child and Adolescent Pornography at Crime Scenes", em 2010, que revela a evolução dos testes na ferramenta para usar imagens em escala de *pixels* para otimizar o tempo de processamento.

Os resultados do experimento comprovam a capacidade da ferramenta de reconhecer automaticamente arquivos que possam conter cenas de nudez, e, em seu segundo experimento, foi comprovado que o uso do *NuDetective* é viável, confiável e que reduziu significativamente o tempo gasto pelos peritos para detectar conteúdo ilegal, conforme Tabela 1.

Tabela 1 - Processamento de 200 fotos usando o *NuDetective*

Resolution (Megapixels)	Total Time	Average Time per Image
12.0	17m 21s	5.20s
8.0	12m 46s	3.83s
4.0	5m 48s	1.74s
2.0	3m 02s	1.1.1. 0.91s
0.7	1m 09s	0.34s
0.075	0m 09s	0.04s

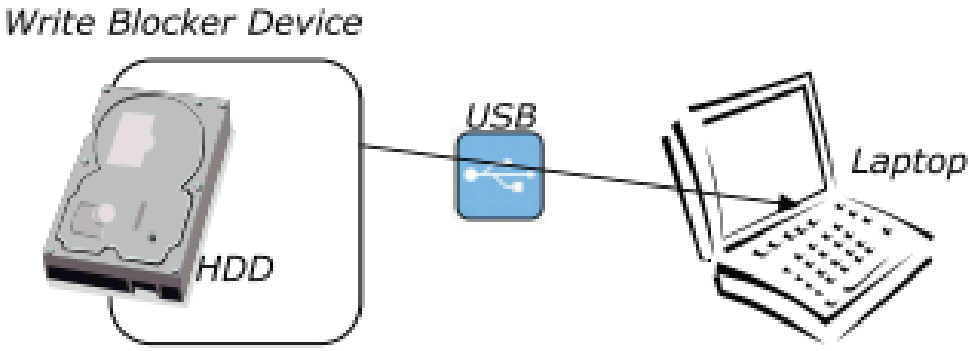
Fonte: (POLASTRO; ELEUTÉRIO, 2010, p. 55)

Em outro experimento realizado por Eleutério e Polastro, tendo em vista a análise de imagens com nudez, o *NuDetective* procurou e analisou mais de 300.000 arquivos no disco rígido em, aproximadamente 13 minutos[1].

A Perícia com o *NuDetective* foi realizada em um HDD apreendido, o qual foi colocado em uma garra Forense por uma porta de conexão USB de um computador, no exemplo divulgado no artigo de Eleutério e Polastro (2010), representado por um computador portátil. Os autores garantiram que o procedimento preservou os dados contidos no HDD, por meio de um *Talon*, que age como um bloqueador de gravação de dispositivo de armazenamento para o experimento, conforme a Figura 9.

[1] "The results of the second experiment proved that the use of NuDetective was feasible, highly reliable, and significantly reduced the time spent by forensic examiners to detect illegal content. NuDetective searched and analyzed all files (>300,000) on the HDD in less than 13 minutes". Pedro Monteiro da Silva ELEUTERIO; Mateus de Castro POLASTRO. Identification of High-Resolution Images of Child and Adolescent Pornography at Crime Scenes. *In*.: **The International Journal of Forensic Computer Science,** 2010: The Fifth International Conference on Forensic Computer Science: 15th to 17th, 2010, p. 49-59. Disponível em: http://ijofcs.org/V05N1-PP06-IDENTIFICATION-CHILDPORN.pdf. Acesso em: 25 jun. 2019, às 21h43min.

Figura 9 - Abordagem de detecção via Talon



Fonte: (POLASTRO; ELEUTÉRIO, 2010, p. 54)

Polastro e Eleutério descrevem que a ferramenta *NuDetective* faz uso de encadeamentos presentes da tecnologia empregada (Java), o que permite a execução paralela de tarefas, e um *Thread*, responsável por pesquisar endereços selecionados. Enquanto um segundo *Thread* conduz a análise de imagens, um terceiro exibe os resultados em tempo real, por meio de interface gráfica (GUI, isto é, graphical user interface), assim, o perito judicial pode realizar a análise gráfica e visual dos resultados (2010, p. 53).

A fim de esclarecer, Eleutério e Polastro asseveram que o aplicativo *NuDetective* é utilizado em computadores desconectados da rede, após as apreensões policiais (MONTEIRO, 2019).

1.4 (IN)Eficácia dos *softwares* Forenses utilizados pela polícia técnica para a identificação de crimes contra a Infância e Juventude

Na descrição dos aplicativos utilizados pela Polícia Federal brasileira, observamos que são extremamente específicos e, ainda que de boa qualidade e eficácia, ainda são ineficazes para algumas situações, como exemplificaremos neste item, primeiramente com o *Youtube* e, em seguida, com a utilização em massa de conteúdo *Sexting* e por fim, Aliciamento.

Antes de abordar a utilização do *Youtube*, precisamos compreender alguns pontos importantes relacionados à pesquisa, os quais no darão entendimento de como

acontecem as sugestões de vídeos dentro dessa Plataforma digital. Um algoritmo computacional, por exemplo, se trata de um conjunto de regras, operações e procedimentos matemáticos ordenados que dão origem a aplicações/softwares de computadores. Esses são usados em prol da solução de um problema em um número finito de etapas.

De acordo com o Portal Devmedia (2019), “em termos mais técnicos, um algoritmo é uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa”, e por meio desses os programadores criam um caminho lógico que a aplicação/software deve seguir. Os principais *sites* que conhecemos fazem o uso de algoritmos próprios, tais como *Twitter, Instagram*, *LinkedIn* e *Youtube*.

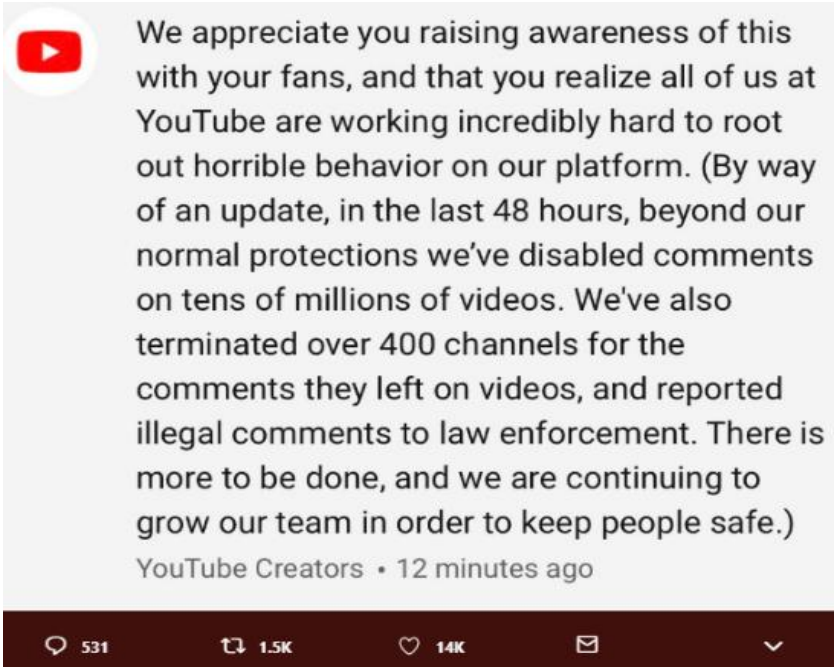
O *Twitter* quando acessado pelo usuário exibe um ranqueamento com as principais postagens do momento (HUTCHINSON, 2019), já o *Instagram* possui uma ordem de postagens baseadas no relacionamento dos usuários (SPROUT SOCIAL, 2019); o *LinkedIn*, por sua vez, tem os algoritmos empenhados a realizar uma análise detalhada do conteúdo exibido, eliminando possíveis *spams*, e, por fim, filtra os conteúdos de qualidade, conforme o grau de relevância das pesquisas, trazendo maior engajamento (THE MARKETING PEOPLE, 2019). O Portal *Youtube* realiza as mesmas funções que as demais mídias sociais citadas, no entanto, esta plataforma utiliza o compartilhamento de vídeos, faz o uso de filtros, sugere vídeos aos usuários, tendo como base pesquisa realizada previamente, o que garante diversas possibilidades de conteúdos similares. Porém, cada uma das mídias sociais possui algoritmos específicos, cada qual com suas peculiaridades técnicas e estratégicas.

A exploração da abordagem do algoritmo utilizada na Plataforma *Youtube* possibilitou que um grupo de pessoas pudesse usar do recurso de forma específica, o que permitiu o contato entre supostos criminosos virtuais, cujo assunto, abordado por vários *youtubers*, gerou algumas denúncias no decorrer do ano de 2019, conforme noticiou, inclusive, o Jornal “El País”, em 21 de fevereiro desse ano, na versão em Português (EL PAÍS, 2019). As denúncias mencionadas nessa matéria jornalística revelam imagens de crianças, as quais têm entre 7 a 13 anos, que estão fazendo atividades peculiares às idades, tais como ballet, ginástica, tomando sorvete, fazendo cambalhotas, brincando na piscina, sentadas no chão, ensinando a fazer maquiagens, imagens as quais, aparentemente, foram gravadas por elas mesmas.

A problemática central está relacionada com a divulgação desses vídeos em canais diferentes da fonte original, como, por exemplo, ambientes de circulação de conteúdo erótico infantil. Nos comentários dos vídeos há alguns “time stamps*”*, ou seja, marcações específicas de tempo, para indicar os momentos em que as crianças aparecem em posições supostamente eróticas. Por essa razão, o uso desse tipo de proliferação de imagens, alheias as verdadeiras intenções infantis, é tratado como uma espécie de *soft porn,* ou seja, pornografia leve. Uma das denúncias realizada por Matt Watson, inserida na Plataforma Youtube e comentada no Blog “Papo de homem”, além do jornal espanhol, questiona a gravidade do assunto, tendo em vista que as imagens infantis, provenientes dos vídeos, estão sendo utilizadas por eventuais criminosos sem nenhuma autorização. É possível identificar dentre os comentários desses vídeos, alguns contatos para traficar pornografia infantil explícita, inclusive com a inserção de links para encaminhar eventuais pedófilos para o conhecimento de outras imagens e vídeos correlatos (EL PAÍS, 2019).

Os responsáveis pelos comentários incentivam as crianças a participarem de supostos “desafios”, como tomar um picolé, fazer determinada posição de yoga na frente da câmera e sugestão de outras atitudes similares. A quantidade de denúncias, dentro e fora da Plataforma *Youtube*, levou a criação da *hashtag* #*YoutubeWakeUp,* que acabou chamando a atenção dos responsáveis do *Youtube*. Um porta-voz, inclusive após as denúncias efetuadas, informou publicamente que medidas estariam sendo tomadas em relação ao assunto tratado. O comunicado oficial da Plataforma dizia que, após as 48 horas da postagem da denúncia de Watson, a qual aconteceu no dia 20 de fevereiro de 2019, foram “desabilitados comentários em mais de 10 milhões de vídeos, 400 canais foram excluídos e os comentários inapropriados foram reportados para a polícia”, como mostra a Figura 10.

Figura 10 - Resposta do Youtube às denúncias de M. Watson



Fonte: Youtube (2019) apud Papo de homem (2006-2019)

A segunda questão da análise é referente a propagação de imagens com conteúdo sexual, comumente utilizada por usuários de mídias sociais.

Os conteúdos denominados *Sexting* são produzidos e compartilhados pelos usuários, com intuito erótico, convidativo e insinuativo, para parceiros, pretendentes e/ou amigos(as) (SAFERNET BRASIL, 2005-2019b). A expressão *Sexting* é constituída pela junção de duas palavras do idioma inglês: *sex* (sexo) + *texting* (torpedo) (SAFERNET BRASIL, 2005-2019b). Segundo o Portal SaferNet Brasil, por meio do "Perfil Helpline", o problema se instala quando as imagens são compartilhadas, sem autorização, para terceiros, ou em canais de comunicação ilícitos (SAFERNET BRASIL, 2005-2019b). Tal comportamento permitiu a criação de um ambiente virtual para denúncias e remoção de conteúdos publicados indevidamente. Dessa forma, quem tiver imagens vazadas poderá recorrer ao órgão de denúncias "Helpline" ou às delegacias de combate ao crime cibernético, e solicitar a remoção do conteúdo das redes sociais. No Portal SaferNet, por exemplo, o usuário é instruído para preservar as provas, por meio de impressões ou salvando em dispositivos de armazenamento; as evidências podem ser: comentários em rede sociais; e-*mails;* e/ou *links* com o conteúdo vazado indevidamente. Logo em seguida o usuário poderá procurar uma delegacia em posse dessas evidências e realizar a denúncia, acrescentando a solicitação para a remoção do conteúdo ilegal e/ou

ofensivo que o infringe. Outro agravante digital é o aliciamento de menores por meios digitais, o qual normalmente ocorre em mídias sociais, como salas de bate-papo, *Twitter*, *Facebook*, *Instagram,* etc*.*

O aliciamento inicia quando um usuário finge ser uma criança/adolescente e, em seguida, começa a coagir a vítima para realizar encontros secretos ou exigir ações que não condizem com a vontade da vítima.

> Aliciadores são pessoas que fingem ser amáveis e fazem muitos elogios, só para ganhar a confiança e pedir informações [...]. Quando ganham a confiança, pedem que [...] envie fotos e use a webcam. Manipulam e fazem montagem para [...] chantagear e obrigar a fazer algo que [...] não queira. Nos piores casos, podem terminar em sequestro e abuso sexual das vítimas. Adultos que pressionam crianças e adolescentes a fazer qualquer coisa que eles não se sentem confortáveis devem ser punidos (CUNHA; NEJM, 2015, p. 18).

Como nenhum dos exemplos citados acima podem ser identificados pela abordagem de Perícia Forense da Polícia Federal brasileira, esses casos só podem ser investigados após a realização de denúncias no canal indicado; SaferNet, portanto, visa proteger a dignidade das vítimas afetadas.

1.5 Delegacias especializadas de combate aos crimes sexuais de menores no ambiente virtual no Estado de São Paulo

Embora qualquer delegacia esteja apta a receber denúncias sobre quaisquer crimes, os Estados brasileiros possuem delegacias específicas para o combate de crimes cibernéticos. Para compreendermos melhor o relacionamento entre a denúncia e a instauração de processo jurídico, explicitaremos as delegacias de crimes virtuais presentes no Estado de São Paulo, as quais têm a colaboração direta do SaferNet, que, por meio do termo de cooperação mútua, auxilia nas investigações de crimes virtuais no Brasil.

Iniciamos brevemente a menção à 4ª Delegacia de Delitos Cometidos por Meios Eletrônicos (DIG/DEIC), atualmente localizada na Avenida Zack Narchi, 152, bairro Carandiru, na cidade de São Paulo/SP, cujo telefone é: (11) 2224-0300. Entretanto, conforme explicita o Portal SaferNet, essa delegacia: “atende apenas demandas relacionadas a fraudes financeiras por meios eletrônicos. Em casos de outros crimes por meios digitais, o cidadão deve se dirigir a uma delegacia comum” (SAFERNET BRASIL, 2005-2019a).

No que diz respeito aos homicídios, proteção à pessoa, na qual se enquadra a vida da criança e do adolescente, além da dignidade sexual de vulneráveis, sequestros, assistência policial e administração, a responsabilidade pela apuração desses delitos compete ao Departamento de Homicídios e de Proteção à Pessoa (DHPP), o principal responsável do Estado no combate a tais crimes, o qual se localiza na Rua Brigadeiro Tobias, 527 - 5º Andar, CEP – 01.032-001, centro, São Paulo/SP, cujo telefone é: (11) 3311-3950 (SAFERNET BRASIL, 2005-2019a).

Em função das inúmeras denúncias relacionadas à exploração de pornografia infantil no âmbito virtual, além da existência de diversas discussões no Senado Federal sobre essa temática, os estados brasileiros estabeleceram termos de compromisso entre órgãos técnicos especializados para auxiliar nos processos de investigações. No caso específico de São Paulo, estabeleceu-se em 29 de março de 2006 o “Termo de Mútua Cooperação Técnica, Científica e Operacional”, entre o Ministério Público de São Paulo (MPF-SP) e SaferNet Brasil, o qual prevê a união de esforços para prevenir e combater a pornografia infantil, a prática de racismo e outras formas de discriminação, instrumentalizadas via Internet (SAFERNET BRASIL, 2008).

O presente Termo determina que todas as denúncias sediadas no Estado de São Paulo sejam encaminhadas, exclusivamente, à Procuradoria da República para investigação, no intuito de gerar “a centralização do recebimento, processamento, encaminhamento e acompanhamento online de notícias de crimes contra os Direitos Humanos praticados com o uso da rede mundial de computadores, Internet, no Brasil” (SAFERNET BRASIL, 2008). O Termo ainda contempla o intercâmbio e difusão de tecnologias baseadas em plataformas livres e de código aberto, as quais são gratuitamente utilizadas pelas Procuradorias da República nos Estados e no Distrito Federal e autoridades brasileiras. Ademais, o Termo obriga as respectivas partes manter absoluto sigilo dos dados e das informações concernentes aos projetos e ações confidenciais, não permitindo, direta ou indiretamente, “dar conhecimento não autorizado a terceiros”, das informações compartilhadas (SAFERNET BRASIL, 2008).

O Portal SaferNet disponibiliza filtros específicos de pesquisas relacionadas as denúncias, com quatro centrais relacionadas aos crimes cibernéticos, sendo elas: 1) SaferNet Brasil; 2) Polícia Federal; 3) Secretaria de Direitos Humanos e 4) Central de Denúncias.

Em pesquisa referencial no *link* “Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos”, produzido pelo Portal SaferNet, entre os anos de 2005 e 2017, cujas informações podem ser filtradas por “Zoom do Mapa”, “Escala da bolha” e “Linha do tempo”, tomando como parâmetro as denúncias ocorridas entre os anos de 2006 e 2018, inserimos o termo “Pornografia infantil”, digitamos como parâmetro de análise o ano de 2018, e escolhemos três dos quatro canais de denúncias indicados, a fim de verificar o funcionamento destes filtros de denúncias.

A respeito do ano “2018”, escolhemos a central “SaferNet” e, conforme explicado, inserimos para buscar o termo “Pornografia infantil”, informações que geraram a seguinte resposta:

> Em 2018, a SaferNet Brasil recebeu e processou 57.816 denúncias anônimas de Pornografia Infantil envolvendo 23.627 páginas (URLs) distintas (das quais 2.308 foram removidas) escritas em 9 idiomas e hospedadas em 5.531 domínios diferentes, de 143 diferentes TLDs e conectados à Internet através de 5.359 números IPs distintos, atribuídos para 59 países em 5 continentes (SAFERNET BRASIL, 2005-2017).

Digitamos os mesmos dados quanto ao ano “2018” e ao termo de pesquisa e escolhemos a central “Secretaria de Direitos Humanos”, as seguintes informações foram geradas:

> Em 2018, a Secretaria de Direitos Humanos recebeu e processou 1.981 denúncias anônimas de Pornografia Infantil envolvendo 930 páginas (URLs) distintas (das quais 168 foram removidas) escritas em 8 idiomas e hospedadas em 298 domínios diferentes, de 52 diferentes TLDs e conectados à Internet através de 358 números IPs distintos, atribuídos para 24 países em 4 continentes (SAFERNET BRASIL, 2005-2017).

E, por último, com os mesmos ano e termo, especificamos a “Central de denúncias”, os dados fornecidos foram os seguintes:

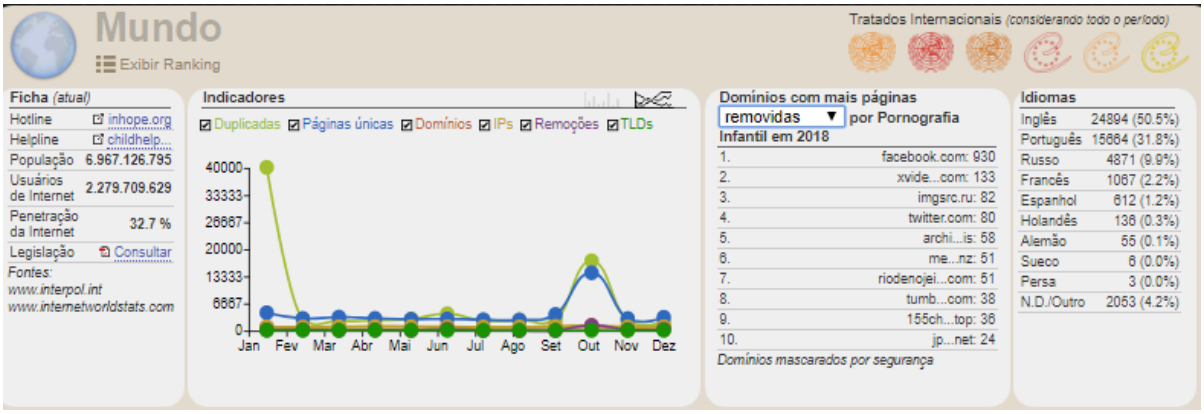
> Em 2018, a Central de Denúncias recebeu e processou 60.002 denúncias anônimas de Pornografia Infantil envolvendo 24.612 páginas (URLs) distintas (das quais 688 foram removidas) hospedadas em 5.684 domínios diferentes, de 146 diferentes TLDs e conectados à Internet através de 5.657 números IPs distintos, atribuídos para 60 países em 6 continentes. As denúncias foram registradas pela população através dos 3 hotlines brasileiros que integram a Central Nacional de Denúncias de Crimes Cibernéticos (SAFERNET BRASIL, 2005-2017).

Os resultados das pesquisas também podem ser representados graficamente. Configurados os filtros para o ano e o termo indicado, pudemos visualizar o *ranking* mundial das páginas dos domínios removidas. Para que essa informação pudesse

ser fornecida, em uma das abas (“Domínio com mais páginas”), em vez de acionar “denunciadas”, substituímos por “removidas”.

Como observaremos, na Figura 11, o Brasil está em segundo lugar no *ranking* mundial de páginas removidas, as quais foram identificadas e denunciadas via canais pesquisados.

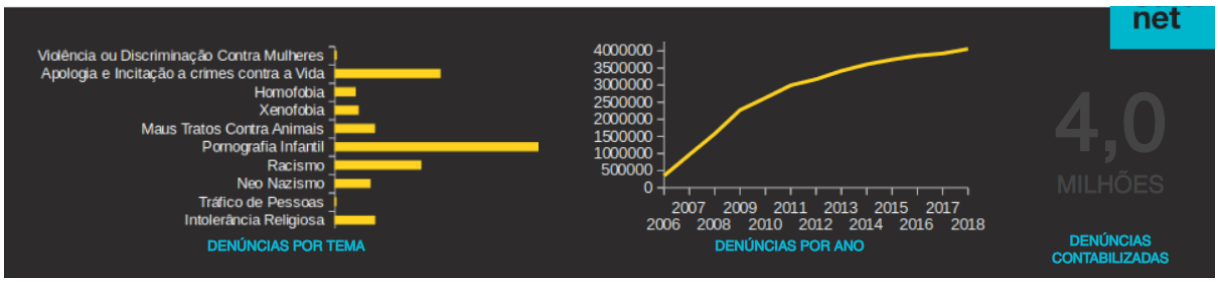
Figura 11 - Ranking de páginas removidas com pornografia infantil, em 2018



Fonte: (SAFERNET BRASIL, 2005 - 2017).

A título de curiosidade, de acordo com o Portal *SaferNet*, através do canal “*Hotline*”, no qual é possível elencar vários temas geradores de polêmicas no ambiente virtual (pornografia infantil; racismo; apologia e incitação a crimes contra a vida; xenofobia; neonazismo; maus tratos contra animais; intolerância religiosa; homofobia; tráfico de pessoas; violência ou discriminação contra mulheres), de um total de 4 milhões de denúncias realizadas entre 2006 e 2018, a grande maioria estava relacionada à pornografia infantil (SAFERNET BRASIL, 2019c), conforme ilustra a Figura 12.

Figura 12 - Índice de denúncia da pornografia infantil processada pelo Hotline/SaferNet entre os aos de 2006 e 2018



Fonte: (SAFERNET BRASIL, 2019c)

O *SaferNet* também disponibiliza o fluxo que a denúncia percorre, desde quando a) o usuário se depara com a evidências de um crime, b) o acesso ao portal eletrônico da *SaferNet* por parte da vítima, na aba “Denuncie”, o c) envio do *link* do site onde

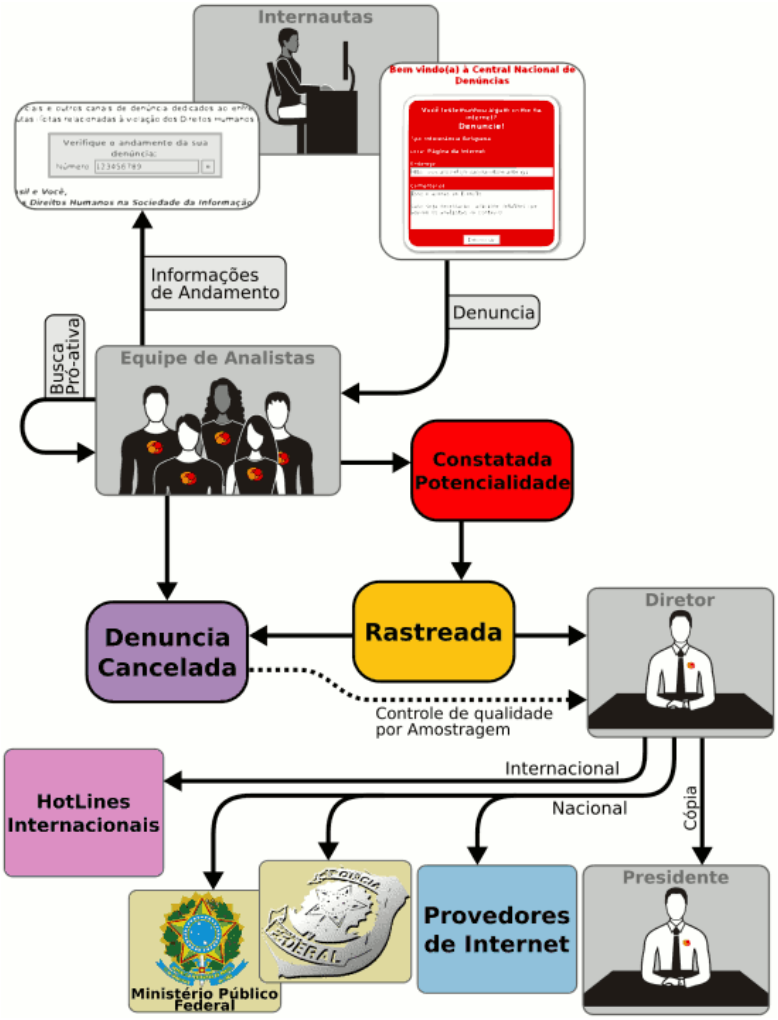
está o suposto crime virtual e d) a geração do sistema de um número automático de *ticket* por meio do qual poderá ser realizado o andamento da denúncia em tempo real. Para todos os fins, a identificação do usuário não é necessária (SAFERNET BRASIL, 2008).

A análise de conteúdo é realizada pela equipe *SaferNet*, formada em Direito e Ciência da Computação, com o auxílio de ferramentas próprias, desenvolvidas pelo departamento de tecnologia da informação da *SaferNet*; porém, são encaminhadas para a próxima etapa os *sites* que constataram indícios de crime. Uma vez comprovada a existência desses indícios, é realizado o rastreamento das informações relevantes disponíveis na Internet para obter a comprovação, a materialidade e a documentação dos indícios de autoria (SAFERNET BRASIL, 2008). Em seguida, de posse das informações e evidências, são criados relatórios de rastreamento, para configurar a notícia-crime, alicerçando-se na legislação brasileira em vigência, além do Código Processual Penal, para que se instaure o processo formal de investigação policial (SAFERNET BRASIL, 2008).

Os relatórios que contêm evidências relacionadas a *sites* hospedados no Brasil são enviados às autoridades brasileiras competentes. Em caso de s*ites* estrangeiros, as denúncias são encaminhadas para os canais de denúncias internacionais. No caso da eventual existência de uma filial no território brasileiro, o prestador de serviço online é notificado formalmente, por meio de recomendação expressa para a remoção do material ilegal da internet. Entretanto, a fim de validar a existência do crime formal, as provas da materialidade do(s) crime(s) e os respectivos indícios são preservados (SAFERNET BRASIL, 2008).

A Figura 13, abaixo citada, nos ajuda a compreender o fluxo de denúncia.

Figura 13 - Fluxo de Denúncia SaferNet



Fonte: (SAFERNET BRASIL, 2008)

Além de computar as denúncias, a comunicação via Portal SaferNet também realiza a orientação dos usuários através de campanhas preventivas, as quais são apoiadas pelo Ministério Público, no intuito de amenizar dúvidas existentes.

Tendo em vista que o Primeiro Capítulo intencionou apresentar a Perícia Forense efetuada pela Polícia Federal brasileira para identificar, rastrear e documentar crimes virtuais relacionados à pornografia infantil, foram estudados dois tipos de abordagens utilizadas pelos peritos. A primeira abordagem tratou-se de uma análise complexa, na qual envolveu inúmeras variáveis, que possibilitam a identificação do usuário mesmo na rede supostamente anônima Deep Web, e a segunda, tratou-se da análise realizada no cotidiano pericial, esta atua na Rede *peer-to-peer* com auxílio de ferramentas forenses desenvolvidas pelos próprios peritos brasileiros, as quais permitem o rastreamento de forma mais clara e mais objetiva. Entretanto,

foram realizadas as exposições de casos que não podem ser abordados por essas ferramentas, e, assim é possível visualizar a dimensão da problemática, na qual se divide em diversos ambientes para dar continuidade as atividades de compartilhamento de imagens de pornografia infantil, cujo exemplo oferecido por meio da Plataforma de vídeos do *Youtube*. Seguindo as análises, verificou-se que para iniciar um processo jurídico é necessária a criação de documentos bem elaborados, os quais devem ser capazes de manter a integridade da evidência e detalhados o suficiente para embasar à instauração do processo jurídico. Verificou-se também de qual maneira podem ser denunciados os crimes que ocorrem nos ambientes virtuais, com mais objetividade em denúncias relacionadas à pornografia infantil, e, desta forma, conhecer o fluxo dessas denúncias no Estado de São Paulo, e, consequentemente, para representar intencionalmente as estatísticas atuais, foram apresentados alguns gráficos específicos. Ainda se observou, o denominado "Termo de Mútua Cooperação entre MPF e SaferNet", no qual se assegura o cumprimento da Lei no Estado de São Paulo. No que diz respeito à Legislação brasileira, pode-se encontrar descrições específicas no Segundo capítulo. Sendo assim, concluímos parcialmente neste capítulo que as informações apresentadas são de caráter informativo e que serviram de base para explicar a Perícia forense.

CAPÍTULO II – DIMENSÃO TÉCNICO-JURÍDICA DA CLASSIFICAÇÃO E DA PENALIZAÇÃO DOS CRIMES SEXUAIS CONTRA A INFÂNCIA E A JUVENTUDE

Neste Capítulo, o objetivo principal é esclarecer as dúvidas técnico-jurídicas relacionadas aos crimes sexuais cometidos contra crianças e adolescentes, sejam os de natureza eletrônica ou não, para isso serão analisados os conceitos proeminentes desta temática nos Códigos Civil e Penal, no Estatuto da Criança e do Adolescente, e na abordagem dos dados presentes na Legislação referente à área de Informática e de Computação no combate ao crime contra a infância e juventude, na dimensão virtual.

2.1 Pressupostos de crimes contra a Infância e Juventude no Código Civil e no Estatuto da Criança e do Adolescente

O Código Civil (CC) brasileiro vigente está descrito na Lei nº 10.406, de 10 de janeiro de 2002, e trata-se do conjunto sistemático de normas que consideram às relações jurídicas de ordem privada (BRASIL, 2002).

São baseadas no Código Civil, as medidas para o convívio em sociedade, garantindo à população direitos e obrigações. Graças as medidas protetivas previstas no Código Civil no tocante às crianças e adolescentes, dispuseram-se na criação e na legitimação do Estatuto da Criança e do Adolescente, Lei nº 8.069, de 13 de julho de 1990.

Primeiramente, ressaltamos o Parágrafo único da Lei nº 8.069, que estabelece que:

> Os direitos enunciados nesta Lei aplicam-se a todas as crianças e adolescentes, sem discriminação de nascimento, situação familiar, idade, sexo, raça, etnia ou cor, religião ou crença, deficiência, condição pessoal de desenvolvimento e aprendizagem, condição econômica, ambiente social, região e local de moradia ou outra condição que diferencie as pessoas, as famílias ou a comunidade em que vivem (incluído pela Lei nº 13.257, de 2016) (BRASIL,1990).

Nesta citação, temos duas informações importantes: 1) A Lei n.º 13.257/2016 fez alterações significativas no tocante à dimensão social, econômico-financeira das crianças e dos seus respectivos familiares; 2) As predisposições desse Parágrafo único da Lei 8069/1990 estão em harmonia com o Código Civil, que trata crianças e adolescentes com fundamento na igualdade.

Por meio do artigo art. 5º do Estatuto da Criança e do Adolescente, doravante chamada ECA, “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,1990a).

Por meio deste fundamental artigo do ECA, faremos uma reflexão do conceito de exploração sexual, por meios físicos e eletrônicos. Entretanto, antes disto, analisaremos o conceito “pedofilia” e, em seguida, efetuaremos as abordagens tecnológicas utilizadas com o mesmo intuito de combate à exploração sexual de menores no Brasil.

Segundo Fani Hisgail, no estudo psicanalítico “Pedofilia de 2007”, publicado por *Latin American Journal of Fundamental Psychopathology On Line*, a pedofilia existe há muitos anos, ao redor do mundo, desde ritos na Nova Guiné até costumes abusivos na China, passando por práticas realizadas na Antiga Grécia, onde era considerada um rito de passagem de infância para adolescência (HISGAIL, 2007, p. 126). No final dos anos 90, o abuso sexual infantil foi considerado pela OMS (Organização Mundial da Saúde) como um problema de saúde pública em proporções mundiais. Para tanto, a fim de esclarecer, exporemos as diferenças existentes entre a parafilia e o puro abuso infantil.

Diferentemente do que muitos pensam, a pedofilia não é crime. De acordo com o *Dicio*, o dicionário *online* de Língua Portuguesa, a pedofilia é: “Psicopatologia. Distúrbio ou perversão que faz com que uma pessoa em idade adulta se sinta atraída por crianças” (DICIO, 2009-2019).

Ademais, segundo os pesquisadores Delton Croce e Delton Croce Júnior,

> Trata-se de desvio sexual caracterizado pela atração por crianças ou adolescentes sexualmente imaturos, com os quais os portadores dão vazão ao erotismo pela prática de obscenidades ou de atos libidinosos (CROCE; CROCE JÚNIOR, 2012. Item 16.2.1.19)

Entretanto, os abusos infantis não são exclusivamente cometidos por pessoas que sofrem de parafilia, visto que o pedófilo não necessariamente incorrerá a crimes sexuais praticados contra menores, segundo estatísticas reveladas por Sandro D´Amato Nogueira:

> 80 a 90% dos contraventores sexuais não apresentam nenhum sinal de alienação mental, portanto, são juridicamente imputáveis. Entretanto, desse grupo de transgressores, aproximadamente 30% não apresenta nenhum transtorno psicopatológico da personalidade evidente e sua conduta sexual social cotidiana e aparente parece ser

> perfeitamente adequada. Nos outros 70% estão as pessoas com evidentes transtornos da personalidade, com ou sem perturbações sexuais manifestas (disfunções e/ou parafilias). Aqui, se incluem os psicopatas, sociopatas, borderlines, antissociais etc. Destes 70%, um grupo minoritário de 10 a 20%, é composto por indivíduos com graves problemas psicopatológicos e de características psicóticas alienantes, os quais, em sua grande maioria, seriam juridicamente inimputáveis. Assim sendo, a inclinação cultural tradicional de se correlacionar, obrigatoriamente, o delito sexual com doença mental deve ser desacreditada. A crença de que o agressor sexual atua impelido por fortes e incontroláveis impulsos e desejos sexuais é infundada, ao menos como explicação genérica para esse crime (NOGUEIRA, 2001).

Sendo assim, o senso comum que generaliza pedófilos, está equivocado, e mesmo não havendo legislação própria para a pedofilia, o pesquisador Roger Spode Brutti adverte:

> [...] A legislação penal brasileira, acertadamente, não utiliza explicitamente referida terminologia, expondo, isto sim, em vários tipos penais, tipificações que abarcam como sujeitos passivos de crimes sexuais pessoa de tenra idade [...] (BRUTTI, 2008).

Entretanto, aqueles diagnosticados como pedófilos ou não, que praticam condutas para satisfazer seus desejos sexuais por meio de vulneráveis, cometem crimes previstos no Código Penal (CP) e no Estatuto da Criança e do Adolescente (ECA). Pois embora o acusado seja diagnosticado como portador da parafilia pedofilia, possui capacidade plena de conhecer que essas condutas são de ordem ilícitas, ou não sendo capaz de assim determinar, pode se enquadrar como “semi-imputável”, definição explorada na declaração do Código Penal. Porém, em hipótese alguma, essa caracterização pode ser reconhecida como regra geral. Sendo assim, as leis brasileiras enquadram as consequências dos atos que a pedofilia ou o simples abuso sexual possam vir a causar nas vítimas, podendo estas práticas serem descritas como 1) pornografia Infantil, 2) estupro de crianças ou adolescentes, 3) exploração sexual e 4) criminalização sexual de variada natureza.

No caso da pornografia infantil, podemos afirmar que fere diretamente a Declaração Universal dos Direitos Humanos, como, por exemplo, o artigo III, que diz que “todo ser humano tem direito à vida, à liberdade e à segurança pessoal” (DUDH, 1948). Pois, em função da explícita exposição da criança ou do adolescente na Rede Mundial de Computadores, como vítima de exploração sexual, pode impactar diretamente na liberdade e na segurança pessoal destes menores molestados.

As considerações em prol de garantir direitos à crianças e adolescentes no âmbito digital, trouxe mudanças significativas por meio da Lei n° 11.829/08, que passou a tipificar condutas que antes eram silenciadas e acabou preenchendo algumas lacunas importantes na legislação brasileira, além do incentivo à instauração da Comissão Parlamentar de Inquérito sobre a Pedofilia (CPI da Pedofilia), instituída no Senado Federal, em 2010, por meio do Requerimento nº 200, de 4 de março de 2008, “com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de “pedofilia”, bem como a relação desses crimes com o crime organizado” (BRASIL, 2010, p. 5).

Por meio da CPI da Pedofilia, as decisões relacionadas à proteção de crianças e adolescentes foram discutidas no Senado Federal e proporcionaram diagnósticos de crimes sexuais desta natureza, elaboração legislativa, ações perante empresas provedoras de internet, telefonia e cartões de crédito, termos estatais de cooperação mútua, ajustamento de conduta relacionada à empresa Google, entre outros, quais podem ser acessos via portal de notícias do Senado, e por meio da redação do Relatório Final CPI Pedofilia, disponível em *pdf*, por meio do sítio eletrônico do Senado Federal, documento com 1.696 páginas (BRASIL, 2010).

2.2 Código Penal

O Código Penal brasileiro foi criado por meio do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, porém a sua vigência se deu a partir de 1º de janeiro de 1942, conforme artigo 361 deste mesmo Código, instituído pelo presidente Getúlio Vargas (BRASIL, 1940).

O Código Penal brasileiro trata-se do conjunto de legislatura punitiva para crimes. Nesta seção, abordaremos alguns pontos pertinentes ao Código Penal: 1) nas questões punitivas, primeiramente, a culpabilidade, a qual está diretamente ligada ao indivíduo sob acusação; 2) as diferenças punitivas como reclusão, detenção e prisão simples, seguidos da mobilização recorrente no país em prol da conscientização sobre o problema; e 3) principais mudanças na matéria penal relacionadas ao ambiente virtual.

Em prol do entendimento de culpabilidade, observaremos a imputabilidade plena, inimputável e semi-imputável. Primeiramente a imputabilidade plena, se trata da capacidade do indivíduo compreender sua responsabilidade penal. Segundo Cezar

Roberto Bitencourt, diz respeito “à capacidade de culpabilidade, é a aptidão para ser culpável” (2006, p. 447-448). Em contrapartida, a inimputabilidade diz respeito ao indivíduo que por razões psíquicas e de maturidade não é capaz de entender sua culpabilidade, previsto no Código Penal, no artigo 26, que assim preconiza:

> É isento de pena o agente que, por doença mental ou desenvolvimento mental incompleto ou retardado, era, ao tempo da ação ou da omissão, inteiramente incapaz de entender o caráter ilícito do fato ou de determinar-se de acordo com esse entendimento (BRASIL, 1940).

Além dos doentes mentais e aqueles portadores de desenvolvimento mental incompleto, os menores de 18 (dezoito) anos de idade também recebem este mesmo tratamento penal (BRASIL, 1940).

Há, ainda, uma área intermediária entre a imputabilidade e a inimputabilidade, denominada de “semi-imputabilidade”; nesta classificação incorre a diminuição da capacidade de censura e, por consequência, a culpabilidade. Determinado no Código Penal, no Parágrafo único do art. 26, a redução da pena quando

> [...] o agente, em virtude de perturbação de saúde mental ou por desenvolvimento mental incompleto ou retardado não era inteiramente capaz de entender o caráter ilícito do fato ou de determinar-se de acordo com esse entendimento (BRASIL, 1940).

As diferenças entre as medidas punitivas como reclusão, detenção e prisão simples, podem ser analisadas, quando fazemos a observação das determinações previstas no Código Penal (Decreto-Lei no 2.848, de 7 de dezembro de 1940) e no Decreto-Lei nº 3.688/1941, representados, respectivamente, pelos artigos 33, 5º e 6º:

No tocante ao artigo 33 do Código Penal diz que:

> A pena de **reclusão** deve ser cumprida em regime fechado, semiaberto ou aberto. A de **detenção**, em regime semiaberto, ou aberto, salvo necessidade de transferência a regime fechado. (Redação dada pela Lei nº 7.209, de 11.7.1984) complementado pelos **§ 1º** - Considera-se: (Redação dada pela Lei nº 7.209, de 11.7.1984) a) **regime fechado** a execução da pena em estabelecimento de segurança máxima ou média;
> b) **regime semiaberto** a execução da pena em colônia agrícola, industrial ou estabelecimento similar;
> c) **regime aberto** a execução da pena em casa de albergado ou estabelecimento adequado.
> **§ 2º** - As penas privativas de liberdade deverão ser executadas em forma progressiva, segundo o mérito do condenado, observados os seguintes critérios e ressalvadas as hipóteses de transferência a regime mais rigoroso: (Redação dada pela Lei nº 7.209, de

> 11.7.1984) a) o condenado a **pena superior a 8 (oito) anos** deverá começar a cumpri-la em regime fechado;
> b) o condenado não reincidente, cuja **pena seja superior a 4 (quatro) anos e não exceda a 8 (oito),** poderá, desde o princípio, cumpri-la em regime semi-aberto;
> c) o condenado não reincidente, **cuja pena seja igual ou inferior a 4 (quatro) anos**, poderá, desde o início, cumpri-la em regime aberto.
> **§ 3º** - A determinação do regime inicial de cumprimento da pena far-se-á com observância dos critérios previstos no art. 59 deste Código (Redação dada pela Lei nº 7.209, de 11.7.1984).
> **§ 4º** - O condenado por **crime contra a administração pública** terá a progressão de regime do cumprimento da pena condicionada à reparação do dano que causou, ou à devolução do produto do ilícito praticado, com os acréscimos legais (BRASIL, 1940. *Grifo nosso!*).

Portanto, no Brasil, dependendo da natureza do delito cometido, tanto na legislação pensada na década de 40 e aprimorada na década de 80, o indivíduo terá maior tempo de privação de liberdade, o que implicará na perda de tempo do convívio social. O critério penal sempre será a natureza do crime praticado.

No que se refere a Lei das Contravenções Penais, o Decreto-Lei nº 3.688, de 3 de outubro de 1941, assim estabelece nos artigos abaixo mencionados:

> Art. 5º - As penas principais são: I – prisão simples. II – Multa. Essa modalidade de pena privativa de liberdade deve ser cumprida, sem rigor penitenciário, em estabelecimento especial ou seção especial de prisão comum, em regime semi-aberto ou aberto. Isto é, não há previsão do regime fechado em nenhuma hipótese para a prisão simples. Outrossim, o condenado à pena de prisão simples fica sempre separado dos condenados à pena de reclusão ou de detenção e nos casos em que a pena aplicada não excede a 15 dias o trabalho é facultativo (BRASIL, 1941a).
>
> Art. 6º - A pena de prisão simples deve ser cumprida, sem rigor penitenciário, em estabelecimento especial ou seção especial de prisão comum, em regime semi-aberto ou aberto. [...]
> § 1º - O condenado à pena de prisão simples fica sempre separado dos condenados à pena de reclusão ou de detenção.
> § 2º - O trabalho é facultativo, se a pena aplicada não excede a 15 (quinze) dias (BRASIL, 1941a).

Portanto, a legislação de contravenções penais, de 1941, coaduna com o Código Penal de 1940, imputando ao criminoso a privação de liberdade condizente à natureza do crime praticado, apenas acrescentando que os detentos cujas ações sejam de menor gravidade que cumpram suas sentenças em estabelecimentos especiais e em ambiente diferente dos criminosos de maior periculosidade.

Por outro lado, ainda que se saiba que o crime no Brasil não compensa, visto que pode implicar em perda de liberdade e de direitos individuais, há uma forte

movimentação no país para conscientizar os cidadãos a respeito da problemática que fere crianças e adolescentes, no tocante aos delitos de natureza sexual; tais ações ocorrem principalmente protagonizadas pelo Ministério Público do Distrito Federal e Territórios (MPDFT), que desenvolveu uma cartilha informativa em relação ao tema, com a primeira versão em 2005, denominada “Violência Sexual contra Crianças e Adolescentes: identificação e enfrentamento”. A cartilha ainda apresenta informação sobre o Dia Nacional de Combate ao Abuso Sexual e à Exploração Sexual de Crianças e Adolescentes, determinando a data de 18 de maio, a qual foi instituída pela Lei Federal nº 9.970, de 17 de maio de 2000, no intuito de sensibilizar a sociedade para o enfrentamento do tema, em razão dos diversos casos ocorridos no Brasil, mas de modo particular, ao da menina Araceli Cabrera Sanches:

> A escolha da data foi relativa a 1973, quando um crime bárbaro chocou o Brasil em 18 de maio. Com apenas oito anos de idade, Araceli Cabrera Sanches foi sequestrada, drogada, espancada, estuprada e morta por membros de uma tradicional família capixaba. O caso teve grande repercussão na mídia (SÃO PAULO, 2019).

As principais mudanças que ocorreram nas penalidades deram- se após 2008, quando entrou em vigor um Decreto que aprimora o Estatuto da Criança e do Adolescente, a Lei 11.829/2008, que passou a tipificar o crime de pedofilia pela internet. Depois da aprovação desta lei, a pena de reclusão passou de no máximo 4 anos de reclusão para um período de 4 a 8 anos, aumentando em alguns casos, quando, por exemplo, há grau de parentesco até terceiro grau com a vítima (BRASIL, 2008).

Uma mudança considerável também ocorreu no artigo 241, alínea D, do ECA: “Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso”, ou seja, incentivar a criança a se exibir de forma pornográfica, via webcam, por exemplo, terá pena de reclusão de 1 a 3 anos, e multa (BRASIL, 2008).

Como se sabe, assim como toda a legislação brasileira que apenas retrata os crimes existentes não podendo hipotetizar sobre crimes ainda desconhecidos, o Código Penal, fundamento legal e precípuo na análise dos crimes, pode ser adaptado conforme os surgimentos de novas inconformidades, assim como acontece desde sua instauração, como complemento, o Código Processual Penal, denominado de “Direito Penal em movimento”, por meio do qual são julgados os crimes e emitidas as sentenças, punitivas ou absolutórias.

2.3 Estatuto da Criança e do Adolescente

O ECA, Lei n.º 8.069, foi sancionado durante o governo do presidente Fernando Collor, em 1990. O ECA é o estatuto que estabelece aparato legal sobre a proteção integral às crianças e adolescentes brasileiros. Igualmente estabelece os direitos e deveres do Estado e dos cidadãos responsáveis, com absoluta prioridade dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária. Garantindo que a criança e adolescente tenham preferência para receber proteção e socorro, nos atendimentos públicos. Não permitindo a nenhum deles ser objeto de qualquer negligência, discriminação, exploração, violência, crueldade e opressão. Sendo, ainda, de responsabilidade dos pais, o dever de sustento, isto é, alimentação, a guarda e educação; sendo assim, estabelece-se a obrigatoriedade dos pais em manter os filhos matriculados em rede de ensino.

O Estatuto valida e privilegia o conselho tutelar, formado por um grupo de especialistas, que tem a função de zelar e proteger as crianças e adolescentes; estes membros são eleitos pela comunidade local e são responsáveis por assegurar o bem-estar dos menores, tendo como parâmetro de ação o atendimento e aconselhamento de crianças e adolescentes, além de prestar a mesma atividade aos pais e responsáveis pela tutela ou pela guarda dos filhos e afins; também atuam na propagação de informação dos direitos e deveres (limites) da criança e adolescente. Como especialistas, ouvem queixas e reclamações dos direitos e deveres ameaçados e/ou violados, requisitam serviços públicos nas áreas de saúde, educação, serviço social, providência, trabalho e segurança, estabelecem a criação de garantia e de fiscalização dos direitos e dos deveres dos menores; participam, ainda, de ações de combate à violência, à discriminação no ambiente escolar, familiar e comunitário, entre outras atividades, conforme a necessidade ou a ocorrência de atendimento requerida.

Para Patrícia Bezerra,

> O Estatuto da Criança e do Adolescente tinha como objetivo pôr fim ao Código de Menores que havia sido criado durante a Ditadura Militar no Brasil. (...) Surge da necessidade de acabar com todo resquício de autoritarismo que ainda restava do regime militar, (...)

> (pois) o Estado repressor justificava a punição desses menores sem se comprometer em melhorar suas condições de vida e do seu em torno social. Desta maneira, a criação do ECA era um desdobramento das garantias à infância e à adolescência previstas na Constituição de 1988 (BEZERRA, 2019).

Segundo informações do Ministério Público do Distrito Federal e Territórios, os artigos presentes na Convenção Internacional dos Direitos da Criança, na Constituição Federal de 1988 e no Estatuto da Criança e do Adolescente, relevantes ao tema são os abordados, respectivamente, nos artigos 34 ao 36; no Art. 227; e nos artigos 4º e 5º, além dos instituídos nos artigos 22, 70 e 130.

No que se refere à Convenção Internacional dos Direitos da Criança, destacaremos três artigos:

> Artigo 34 - Os Estados Membros se comprometem a proteger a criança contra todas as formas de exploração e abuso sexual. Nesse sentido, os Estados Membros tomarão, em especial, todas as medidas de caráter nacional, bilateral e multilateral que sejam necessárias para impedir: a) O incentivo ou coação para que uma criança se dedique a qualquer atividade sexual ilegal; b) A exploração da criança na prostituição ou outras práticas sexuais ilegais; c) Exploração da criança em espetáculos ou materiais pornográficos (BRASIL, 1990b).

No tocante ao Artigo 35, diz que os Estados Membros tomarão todas as medidas de "caráter nacional, bilateral ou multilateral que sejam necessárias para impedir o sequestro, a venda ou o tráfico de crianças para qualquer fim ou sob qualquer forma" (BRASIL, 1990b). Já no Artigo 36 endossa que os Estados Membros deverão proteger "a criança contra todas as demais formas de exploração que sejam prejudiciais a qualquer aspecto de seu bem-estar" (BRASIL, 1990b).

Enfim, nos três artigos da Convenção Internacional dos Direitos da Criança, os Estados membros da Organização das Nações Unidas se comprometem em zelar pela integridade da criança e livrá-la de quaisquer atividades sexuais ou ilícitas, no intuito de garantir o seu bem-estar, uma infância livre das mazelas corruptíveis peculiares aos adultos infratores.

Quanto à Constituição Federal de 1988, destacamos o Artigo 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.

> § 1º O Estado promoverá programas de assistência integral à saúde da criança, do adolescente e do jovem, admitida a participação de entidades não governamentais, mediante políticas específicas (...).
> § 4º A lei punirá severamente o abuso, a violência e a exploração sexual da criança e adolescente (BRASIL, 1988).

Portanto, o parágrafo 4º do Artigo 227 é notadamente expressivo no combate à exploração sexual de crianças e de adolescentes no Brasil.

No que se refere ao ECA, Lei nº 8.069/1990, a fim de subsidiar nossa reflexão, separamos os artigos 4º e 5º, além dos artigos 22, 70 e 130.

> Art. 4º - É dever da família, da comunidade, da sociedade em geral e do poder público assegurar, com absoluta prioridade, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária (BRASIL, 1990a).
> 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 fundamentos (BRASIL, 1990a).

Nesta ótica, o legislador federal imputa não só a família, responsável direta pela vida, pelo sustento e pela proteção dos descendentes, mas também a sociedade, de modo particular, a comunidade local onde os menores estão e deverão ser assistidos.

> Art. 22 - Aos pais incumbe o dever de sustento, guarda e educação dos filhos menores, cabendo-lhes ainda, no interesse destes, a obrigação de cumprir e fazer cumprir as determinações judiciais (BRASIL, 1990a).
>
> Art. 70 - É dever de todos prevenir a ocorrência de ameaça ou violação dos direitos da criança e do adolescente (BRASIL, 1990a).
>
> Art. 130 - Verificada a hipótese de maus-tratos, opressão ou abuso sexual impostos pelos pais ou responsável, a autoridade judiciária poderá determinar, como medida cautelar, o afastamento do agressor da moradia comum (BRASIL, 1990a).

As informações apresentadas na presente seção visam a compreensão acerca das competências instituídas pelo Estatuto da Criança e do Adolescente, para que seja possível combater crimes de natureza sexual contra a infância e juventude, além de prevalecer, hierarquicamente, a família e a sociedade como células mantenedoras dos menores, que deverão ser assistidos e protegidos e, em caso de ameaça, violência ou exploração, cabem-lhes a denúncia aos órgãos responsáveis, para que haja a aplicação das medidas cautelares, previstas em lei.

2.4 Legislação referente à área de Informática e de Computação no combate ao crime de natureza sexual, na dimensão virtual

O Ministério Público Federal, por meio de Cartilhas e subsídios pedagógicos orientadores, relaciona informações legislativas e penais relevantes para o combate de crimes de natureza agressiva contrárias as crianças e adolescentes, inclusive informando em seu Portal eletrônico, quais são estes crimes e as respectivas medidas punitivas. Alguns destes crimes podem assim ser classificados: estupro; atentado violento ao pudor; sedução; corrupção de menores; pornografia; abuso; violência e exploração Sexual de crianças e adolescentes. Algumas destas orientações podem ser encontradas em alguns *links*, por exemplo, “Turminha do Ministério Público Federal: assunto de gente grande para gente pequena”, de 2019, em função do dia 18 de maio, data nacional de combate à exploração sexual de menores (http://www.turminha.mpf.mp.br/direitos-das-criancas/18-de-maio/copy_of_a-lei-garante-a-protecao-contra-o-abuso-e-a-exploracao-sexual),
“Guia escolar: métodos para identificação de sinais de abuso e exploração sexual de crianças e adolescentes”, material desenvolvido pelo Ministério Público do Distrito Federal e Territórios (MPDFT), em conjunto com Secretaria Especial de Direitos Humanos da Presidência da República, em formato *pdf*, disponibilizado em 2004, 164p.
(http://www.mpdft.mp.br/portal/pdf/unidades/promotorias/pdij/Publicacoes/Guia_Escolar.pdf) e a Cartilha denominada “Violência contra crianças e adolescentes: identificação e enfrentamento”, material desenvolvido exclusivamente pelo Ministério Público do Distrito Federal e Territórios (MPDFT), em formato *pdf*, disponibilizado em 2015, documentado orientador contendo 40 páginas (http://www.mpdft.mp.br/portal/pdf/imprensa/cartilhas/cartilha_violencia_contra_criancas_adolescentes_web.pdf).
O ECA também possui crimes previstos relacionados ao tema, conforme já ilustramos no Capítulo anterior, inseridos na Lei nº 8.069/1990, dos quais são considerados relevantes pelo Ministério Público Federal os seguintes artigos: 239; 240; 241; 241–A; 241–B; 241-C; 241-D; 241-E; e 244-A.
Dos diversos crimes arrolados e mencionados pelo Ministério Público Federal, o estupro é tipificado no Art. 213 do Código Penal: "Constranger à conjunção carnal, mediante violência ou grave ameaça".

Por conjunção carnal entende-se a penetração sexual, completa ou não, com ou sem ejaculação, com penalidade prevista de reclusão de seis (6) até dez (10) anos. Entretanto, o Parágrafo primeiro afirma que se a conduta resultar em lesão corporal “de natureza grave ou se a vítima é menor de 18 ou maior”, esta reclusão poderá chegar a 12 (doze) anos, e se esta conduta resultar em morte da vítima, o Parágrafo segundo determina que a penalidade poderá atingir até 30 (trinta) anos (BRASIL, 1940).

Acerca da violência sexual mediante fraude, prevista no artigo 215 do Código Penal brasileiro (CP), assim descreve:

> Art. 215. Ter conjunção carnal ou praticar outro ato libidinoso com alguém, mediante fraude ou outro meio que impeça ou dificulte a livre manifestação de vontade da vítima:
> Pena – reclusão, de 2 (dois) a 6 (seis) anos.
> Parágrafo único. Se o crime é cometido com o fim de obter vantagem econômica, aplica-se também multa (BRASIL, 1940).

Segundo o jurista José Nabuco Filho, Mestre em Direito Penal, a violação sexual mediante fraude sofreu alterações importantes com o advento da Lei 12.015, publicada em 7 de agosto de 2009, “que deu nova redação ao art. 215, assim como fez com o estupro, unindo sob um só tipo os antigos crimes de posse sexual mediante fraude (art. 215, CP) e atentado ao pudor mediante fraude (art. 216, CP)” (NABUCO FILHO, 2016).

A respeito do crime de atentado violento ao pudor, previsto originalmente no artigo 214 do CP de 1940, passou a ser denominado de “crime de assédio sexual”, com nova redação, a partir da instauração da Lei 10.224, de 15 de maio de 2001, pelo Presidente Fernando Henrique Cardoso, como artigo 216-A do CP atualizado, sob a seguinte definição: “Constranger alguém com o intuito de obter vantagem ou favorecimento sexual, prevalecendo-se o agente da sua condição de superior hierárquico ou ascendência inerentes ao exercício de emprego, cargo ou função" (BRASIL, 2001).

No que se refere ao crime estabelecido no *caput* do artigo 234 do CP, sob o título original de “Do crime de escrito ou objeto obsceno”, assim descreve:

> Art. 234 - Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno:
> Pena - detenção, de seis meses a dois anos, ou multa.
> § 1º. Incorre na mesma pena quem:
> I - vende, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo;

> II - realiza, em lugar público ou acessível ao público, representação teatral, ou exibição cinematográfica de caráter obsceno, ou qualquer outro espetáculo, que tenha o mesmo caráter;
> III - realiza, em lugar público ou acessível ao público, ou pelo rádio, audição ou recitação de caráter obsceno (BRASIL, 1940).

No intuito de categorizar a pornografia infantil como crime, além do Decreto n.º 5.007, de 8 de março de 2004, expedido pelo Presidente Luiz Inácio Lula da Silva, que acatou o texto do Protocolo Facultativo à Convenção sobre os Direitos da Criança referente à venda de crianças, à prostituição infantil e à pornografia infantil, adotado em Nova York em 25 de maio de 2000, novas alterações foram efetuadas no intuito de adequar as legislações existentes aos novos crimes derivados da realidade, como, por exemplo, a Lei 11.829, de 25 de novembro de 2008, alterando os artigos 240 e 241 do Estatuto da Criança e do Adolescente, no intuito de "aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet" (BRASIL, 2008), e, por último, a Lei 13.718, de 24 de setembro de 2018, publicada pelo presidente do Supremo Tribunal Federal, Ministro José Antonio Dias Toffoli, sob o intuito de

> (...) tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais) (BRASIL, 2018).

Neste sentido, atentos as mudanças, a velocidade dos crimes de ordem sexual na Rede Mundial de Computadores contrários às crianças e adolescentes, os legisladores brasileiros buscam acompanhar as novas práticas delituosas, propagadas pela mídia e denunciadas pelos órgãos de controle, visando sincronizar os novos fatos criminais à redação de novas leis, a fim de evitar a sensação de impunidade, de naturalização de crimes abomináveis e, sobretudo, a supressão da ideia de que o crime compensa, em decorrência da morosidade das ações penais, que podem gerar na consciência do cidadão a ideia de que o Estado brasileiro é omisso, em face da crueldade e bestialidade impetrada contra menores.

CAPÍTULO III – ESTUDO DE CASO: ANÁLISE LABORATORIAL BASEADA NA FUNCIONALIDADE DO PROGRAMA IPED

No desenvolvimento do estudo de caso foi utilizado o programa IPED (Indexador e Processador de Evidências Digitais), citado no item 1.3.2 do presente trabalho. O seu objetivo, em resumo, é a análise de imagens e a indexação de conteúdo. O *download* do programa foi obtido por meio do Portal eletrônico da Polícia Federal, bem como a aquisição do manual e dos termos de licença. A versão utilizada foi a 3.13.5, lançada em 2018.

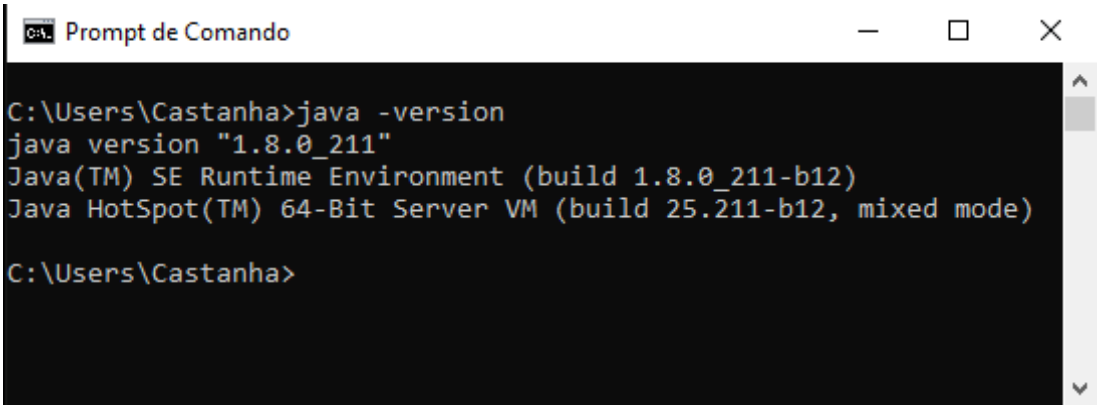
Para a realização desta simulação laboratorial foi utilizado um dispositivo com as seguintes especificações:

a) Sistema Operacional – Windows 10 Professional 64 bits;
b) Processador – Intel Core i5 CPU 2.50GHz;
c) Memória (RAM) – 4,00 GB;
d) Disco rígido - SATA 128gb SSD (Solid State Drive).

Verificamos que o IPED não necessita de uma máquina com especificações notáveis para o seu funcionamento, visto que a sua performance demanda de configurações do próprio usuário e de suas pretensões, ou seja, se o conteúdo a ser varrido não for muito amplo, não é necessário realizar ajustes para utilizar grande quantidade de memória.

Por ser um programa desenvolvido em Java, não necessita ser instalado, porém este tem uma única exigência para seu correto funcionamento: possuir Java versão de 64 bits no dispositivo que ele será executado, conforme imagem abaixo:

Figura 14 – Verificando a versão do Java no dispositivo utilizado



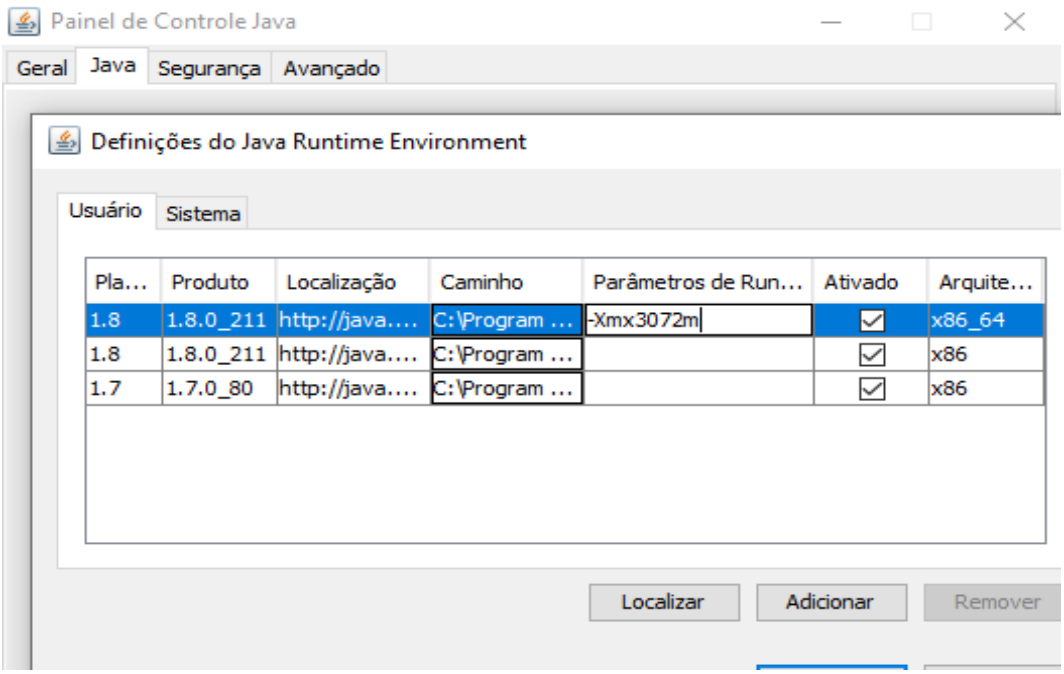
Fonte: Autoria própria (2019) com base no Prompt de Comando

3.1 – Análise e verificação da funcionalidade do Programa IPED

Antes da execução, são necessárias algumas configurações de parâmetros para podermos definir o que será processado e indexado. Primeiramente, é definida a quantidade de memória *RAM* que o Java irá utilizar para a indexação de evidências, para isso, devemos acessar o painel de controle do Java pesquisando por “Configurar Java” na aba de pesquisa do próprio Windows 10.

Após adentrarmos no Painel de controle, acessamos a aba “Java”, disponível no canto superior esquerdo e, dentro dela, entramos em “Exibir”, onde aparecerá a opção de alterar os parâmetros de memória RAM. No caso foram utilizados 3072 Megabytes, ou seja, 3,072 Gigabytes, resultando em ¾ (três quartos) da capacidade total do dispositivo, conforme figura 15:

Figura 15 – Definindo a quantidade de memória RAM em MB (megabytes)



Fonte: Autoria própria (2019) com base no painel de controle do Java

Definida a quantidade de memória utilizada, acessamos o arquivo “LocalConfig.txt”, que vem junto dos arquivos baixados do IPED.

Dentro do “LocalConfig.txt” temos várias opções de alteração para um melhor desempenho e varredura de evidências.

Para a realização desta simulação laboratorial, foi efetuada a mudança do caminho de indexação das evidências, de “*Default*” para um dispositivo móvel (pendrive), pois quando se armazena os arquivos temporários em um caminho diferente do disco a ser varrido, ele terá um melhor desempenho, conforme explicita a Figura 16:

Figura 16 – Definido um caminho para indexação

```
# Diretório temporário de indexação: "default" utiliza o diretório temporário
padrão do sistema.
# Configurar indexTemp num disco livre de antivirus, principalmente num SSD, pode
aumentar consideravelmente o desempenho.
indexTemp = F:\TCCC\IPED\tempIPED
```

Fonte: Autoria própria (2019) com base nos arquivos de configuração do IPED

A segunda alteração foi concernente a mudança do parâmetro “indexTempOnSSD” de “false” para “true”, pois este parâmetro, quando indicado como verdadeiro, realiza otimizações que podem diminuir o tempo de processamento para menos da metade, nos casos em que são utilizados um SSD (*solid-state drive,* ou seja, unidade de estado sólido), conforme aponta a Figura 17:

Figura 17 – Alterando parâmetro para reduzir tempo de processamento

```
# Habilite caso indexTemp esteja em disco SSD. Nesse caso, são feitas otimizações
que podem reduzir
# o tempo de processamento em até 60%: o número de merge threads do índice é
aumentado e
# são utilizados arquivos temporários para evitar múltiplas
leituras/descompactações dos itens.
indexTempOnSSD = true
```

Fonte: Autoria própria (2019) com base nos arquivos de configuração do IPED

E, por último, a terceira alteração efetuada relaciona-se ao parâmetro "outputOnSSD" de "false" para "true", sob o objetivo de criar o arquivo indexado diretamente na pasta de saída definida e não na pasta temporária do IPED, podendo diminuir o requisito de espaço livre no "temp", conforme indica a Figura 18.

Figura 18 – Alterando parâmetro para diminuir requisito de espaço livre no "temp"

```
# Habilite caso a pasta de saída -o esteja em disco SSD. Nesse caso o índice é
criado diretamente
# na pasta de saída e não na pasta temporária, diminuindo o requisito de espaço
livre no temp.
outputOnSSD = true
```

Fonte: Autoria própria (2019) com base nos arquivos de configuração do IPED

Para a varredura, foram utilizados arquivos que já estavam no computador anônimo, dentro de uma pasta localizada na área de trabalho. Dentre estes arquivos existem vários tipos de extensões, como imagens .png, planilhas ".xlsx", documentos de texto ".docx", arquivos com extensão ".rar", etc.

Além destes, foi criado um arquivo de texto ".txt" com uma única palavra digitada, "Pedofilia", no intuito de se desenvolver o teste em análise.

Com estes parâmetros ajustados e os arquivos definidos, a simulação foi iniciada.

Para isso, foi aberto uma caixa de comando no próprio Prompt do Windows e nela foi iniciada a execução do IPED através do comando "java -jar iped.jar".

Com o comando digitado, foram mostradas as opções disponíveis, conforme explicita a Figura 19:

Figura 19 – Iniciando a execução do IPED

```
C:\Users\Castanha\Desktop\IPED>cd iped-3.13.5

C:\Users\Castanha\Desktop\IPED\iped-3.13.5>java -jar iped.jar
Indexador e Processador de Evidências Digitais 3.13.5
Uso: java -jar iped.jar -opcao  argumento [--opcao_sem_argumento]
-d:     dados diversos (pode ser usado varias vezes):
        pasta, imagem DD, 001, E01, AFF (apenas linux), ISO, disco físico,
        ou arquivo *.iped (contendo seleção de itens a exportar e reindexar)
-dname: nome (opcional) para dados adicionados via -d
-o:     pasta de saida da indexacao
-r:     pasta do relatorio do AsAP3 ou FTK3
-l:     arquivo com lista de expressoes a serem exibidas na busca.
        Expressoes sem ocorrencias sao filtradas
-ocr:   aplica OCR apenas na categoria informada. Pode ser usado varias vezes.
-log:   Especifica um arquivo de log diferente do padrao
-asap:  arquivo .asap (Criminalistica) com informacoes para relatorio HTML
-Xxxx:  parâmetros extras de módulos iniciados com -X
-nocontent:     não exporta conteúdo de itens do marcador/categoria informado
-importkff:     importa diretorio com base de hashes no formato NSRL
-tz:    timezone de origem de dispositivos FAT: GMT-3, GMT-4, etc
        Caso não especificado, utiliza o timezone local do sistema.
-b:     tamanho em bytes do setor do dispositivo, necessario informar para discos com setores de 4k
-profile:       usa um profile de processamento: forensic, pedo,
                 fastmode, blind. Para detalhes consulte o manual.
--addowner:     indexa o proprietario dos arquivos ao processar pastas (mto lento via rede)
--append:       adiciona indexação a um indice ja existente
--nogui:        nao exibe a janela de progresso da indexacao
--nologfile:    imprime as mensagem de log na saida padrao
--nopstattachs: não inclui automaticamente no relatorio anexos de emails de PST/OST
--portable:     utiliza caminhos relativos para as imagens no lugar de caminhos absolutos
```

Fonte: Autoria própria (2019) com base nos arquivos de configuração do IPED

Para a realização desta simulação laboratorial, utilizamos dois parâmetros: 1) “-d”, para a definir a pasta de pesquisa, e 2) “-o”, para definir o local onde serão armazenados os *logs* e os arquivos indexados, conforme revela a Figura 20:

Figura 20 – Parâmetros definidos e execução do IPED

```
C:\Users\Castanha\Desktop\IPED\iped-3.13.5>java -jar iped.jar -d C:\Users\Castanha\Desktop\Felipe -o F:\Saida
```

Fonte: Autoria própria (2019) com base nos arquivos de configuração do IPED

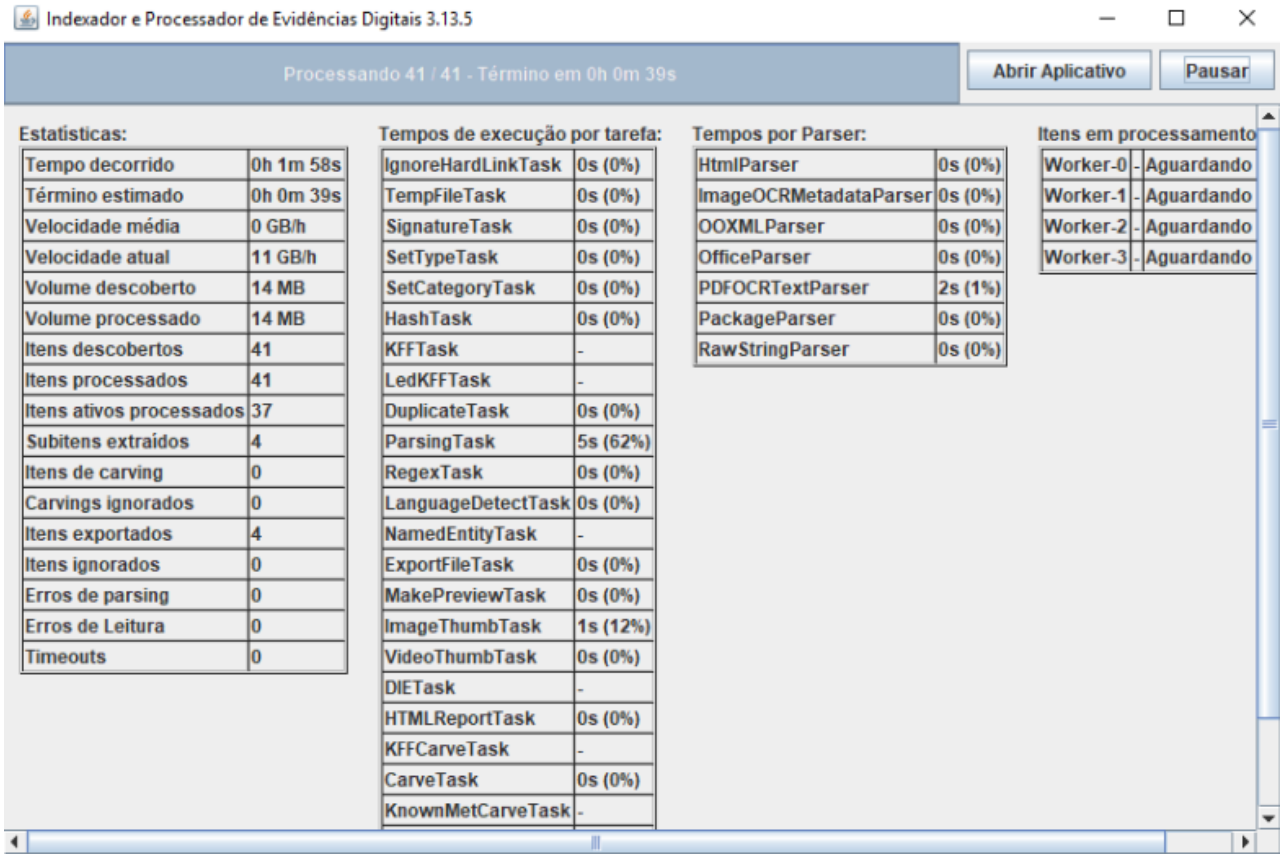
Após a especificação deste comando, o IPED inicia o seu processamento de acordo com os parâmetros previamente estabelecidos, conforme ilustra a Figura 21:

Figura 21 – Tela de inicialização do IPED

Fonte: Autoria própria (2019) com base no software IPED

Na tela de processamento, são mostradas estatísticas que exibem o desenvolvimento da aplicação, como o tempo decorrido, o tempo restante, velocidade de processamento, volume processado, entre outras amostras. Além destes, são mostrados detalhes de cada tarefa individual do IPED, conforme mostrado na Figura 22, por questões de espaço, inserida na página seguinte:

Figura 22 – Tela de processamento do IPED



Fonte: Autoria própria (2019) com base no software IPED

Após a conclusão do processamento, gerou-se uma mensagem no *prompt* de comando informando que o IPED foi finalizado, conforme Figura 23:

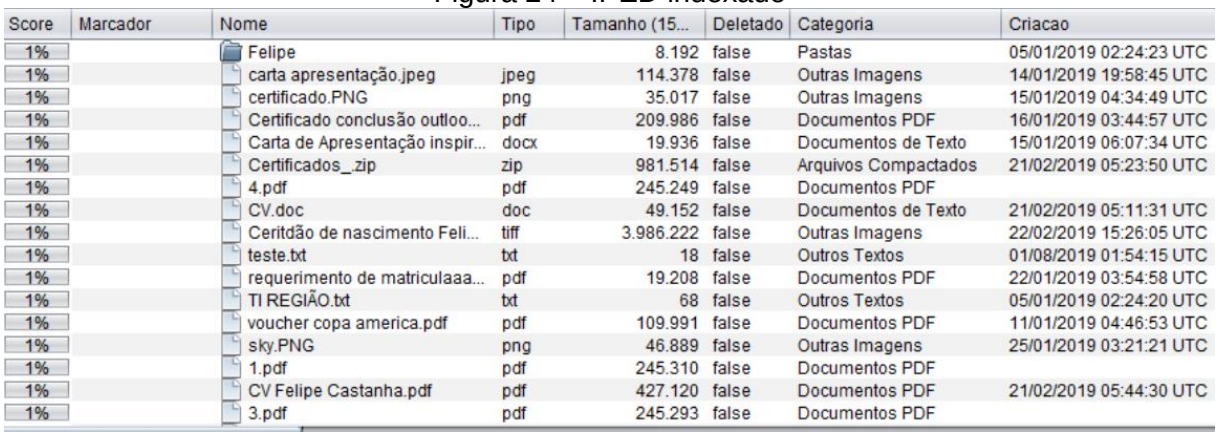
Figura 23 – Mensagem de conclusão do processamento do IPED

```
IPED finalizado.
Consulte o LOG em C:\Users\Castanha\Desktop\IPED\iped-3.13.5\log\IPED-2019-07-31-23-00-41.log
```

Fonte: Autoria própria (2019) com base nos arquivos de configuração do IPED

Além dessa mensagem, foram gerados *logs* do processamento em si, um arquivo ".xls" com as informações das evidências e também um arquivo executável chamado "IPED-SearchApp.exe", o qual, ao ser aberto, revela as evidências indexadas, prontas para serem pesquisadas e filtradas da maneira que o usuário julgar necessário, conforme ilustra a Figura 24:

Figura 24 – IPED indexado

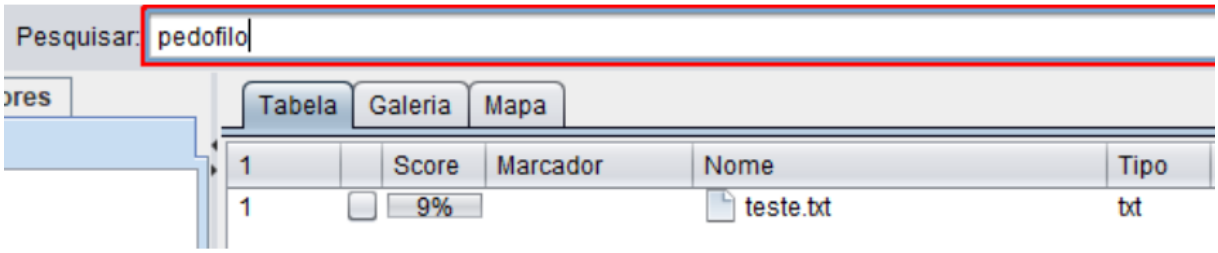


Score	Marcador	Nome	Tipo	Tamanho (15...	Deletado	Categoria	Criacao
1%		Felipe		8.192	false	Pastas	05/01/2019 02:24:23 UTC
1%		carta apresentação.jpeg	jpeg	114.378	false	Outras Imagens	14/01/2019 19:58:45 UTC
1%		certificado.PNG	png	35.017	false	Outras Imagens	15/01/2019 04:34:49 UTC
1%		Certificado conclusão outloo...	pdf	209.986	false	Documentos PDF	16/01/2019 03:44:57 UTC
1%		Carta de Apresentação inspir...	docx	19.936	false	Documentos de Texto	15/01/2019 06:07:34 UTC
1%		Certificados_.zip	zip	981.514	false	Arquivos Compactados	21/02/2019 05:23:50 UTC
1%		4.pdf	pdf	245.249	false	Documentos PDF	
1%		CV.doc	doc	49.152	false	Documentos de Texto	21/02/2019 05:11:31 UTC
1%		Ceritdão de nascimento Feli...	tiff	3.986.222	false	Outras Imagens	22/02/2019 15:26:05 UTC
1%		teste.txt	txt	18	false	Outros Textos	01/08/2019 01:54:15 UTC
1%		requerimento de matriculaaa...	pdf	19.208	false	Documentos PDF	22/01/2019 03:54:58 UTC
1%		TI REGIÃO.txt	txt	68	false	Outros Textos	05/01/2019 02:24:20 UTC
1%		voucher copa america.pdf	pdf	109.991	false	Documentos PDF	11/01/2019 04:46:53 UTC
1%		sky.PNG	png	46.889	false	Outras Imagens	25/01/2019 03:21:21 UTC
1%		1.pdf	pdf	245.310	false	Documentos PDF	
1%		CV Felipe Castanha.pdf	pdf	427.120	false	Documentos PDF	21/02/2019 05:44:30 UTC
1%		3.pdf	pdf	245.293	false	Documentos PDF	

Fonte: Autoria própria (2019) com base nos arquivos de configuração do IPED

Com os arquivos indexados, foi possível realizar uma pesquisa por filtro, na qual foi digitada a palavra “Pedofilia”, pois ela estava no conteúdo do .txt salvo anteriormente no diretório. O resultado da pesquisa consta na Figura 25:

Figura 25 – Resultado de pesquisa no IPED (Inserção de palavra-chave)

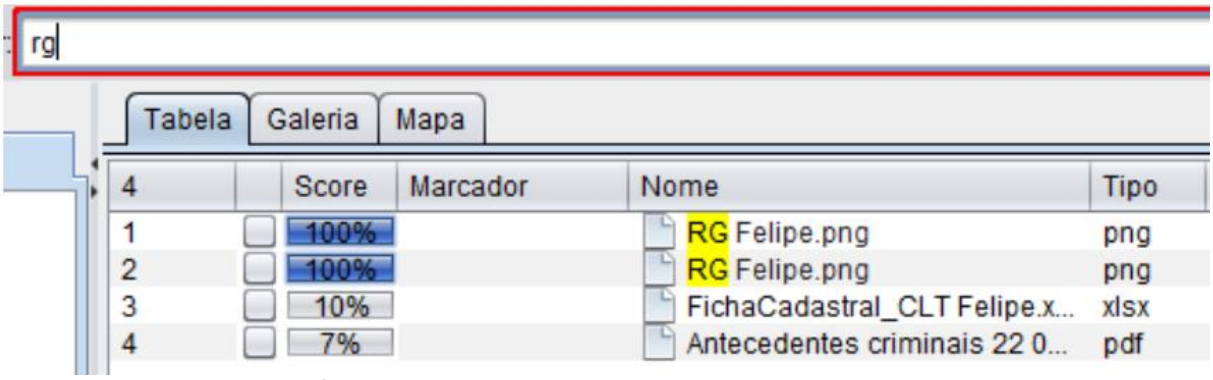


Fonte: Autoria própria (2019) com base nos arquivos de configuração do IPED

Com resultado apontado na Figura 25, percebemos o quanto é funcional o programa, pois o IPED filtra e retorna rapidamente os resultados com grande precisão. Além desta pesquisa, foi feita outra, utilizando a palavra-chave “rg”.

O resultado obtido demonstra a versatilidade do programa, pois filtra todo tipo de resultados na indexação, de acordo com a Figura 26:

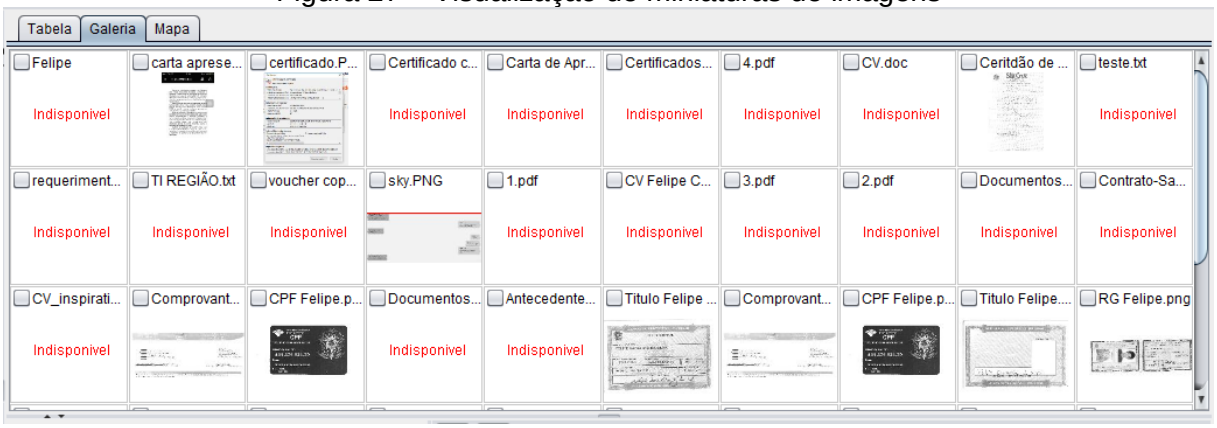
Figura 26 – Resultado de pesquisa no IPED



Fonte: Autoria própria (2019) com base nos arquivos de configuração do IPED

Outra utilidade considerável é quanto à exposição de miniatura de imagens, que está disponível por padrão a partir da versão 3.9 do IPED. Com esta funcionalidade, por exemplo, podemos realizar pesquisa rápida através do filtro e visualização de possíveis imagens suspeitas, conforme Figura 27:

Figura 27 – Visualização de miniaturas de imagens



Fonte: Autoria própria (2019) com base nos arquivos de configuração do IPED

3.2 – Análise dos resultados da funcionalidade do Programa IPED

Realizada a simulação laboratorial, foi evidenciada a facilidade e a velocidade que o software IPED oferece aos profissionais que instrumentalizam essa ferramenta em busca de evidências relacionadas a qualquer tipo de crime virtual, pois através de palavras-chave, pode-se filtrar e encontrar qualquer indício delitual.

Conforme ilustra a Figura 24, o software oferece uma interface simples, com várias categorias de pesquisa e uma alta capacidade de encontrar qualquer tipo de informação, visto que ele utiliza *hashes* para encontrar imagens ou até mesmo pode

fazer uma varredura dentro de arquivos compactados, como os que possuem extensão “.zip” ou “.rar”. Nesta linha de raciocínio, poderia, por exemplo, determinar a verdadeira idade de um(a) menor em ato libidinoso em portais eletrônicos desta natureza, o que daria subsídio para uma investigação mais aprofundada de elementos coletados na imagem disponível, desde que se faça uso de outros softwares, como, por exemplo, ilustramos nos Capítulo Primeiro, o *Led* e o *NuDetective*. Não obstante, é importante frisar que estes dois softwares, juntamente com o EspiaMule, desenvolvidos pela Polícia Federal brasileira não estão disponíveis para *download* no próprio site da Polícia Federal, em virtude da natureza confidencial, cuja aplicação é exclusivamente reservada em operações policiais, sob a intenção de detectar e captar evidências que configurem crimes de natureza sexual contra crianças e adolescentes, por esta razão não foram objetos desta simulação laboratorial, diferente do IPED, que está homologado e disponível para *download*.

Outro aspecto positivo é a facilidade na configuração de seus parâmetros, pois o programa IPED oferece, por padrão, um arquivo de configuração com as suas funcionalidades, por meio da qual o usuário deve apenas escolher ajustes, de acordo com as necessidades peculiares da busca realizada, visto que este programa não é útil apenas para crimes relacionados à infância e juventude, mas sim para qualquer tipo de crime no ambiente virtual, como fraudes eletrônicas, racismo, *cyberbullying*, crimes de ódio, entre outros.

CONSIDERAÇÕES FINAIS

O Trabalho de Conclusão de Curso realizado teve como objetivo demonstrar o fluxo de atividades da polícia brasileira relacionadas ao combate à pornografia infanto-juvenil no meio digital, mostrando os desafios encontrados, atualmente, por peritos e legisladores, para lidar com este tipo de crime que ocorre com muita frequência e em um volume significativo.

Para explanar os atos, foi realizada uma contextualização, na parte técnico-metodológica, por meio da qual foram apresentados conceitos que ajudaram a entender o funcionamento do processo de investigação, como banco e análise de dados, utilização de *hashes* para facilitar análises periciais, conceitos de internet, rede ponto-a-ponto e, por fim, os procedimentos técnicos empregados pela Perícia forense, que, segundo Sousa, possuem quatro etapas, sendo elas a coleta de evidências, exame, análise de dados e a demonstração dos resultados obtidos (2016, p. 101).

No intuito de demonstrar aos usuários os softwares utilizados pelos profissionais da área, foi realizada uma entrevista com o Perito Judicial, prof. Marcos Monteiro, na qual explicou o procedimento policial e pericial, além de mencionar os programas utilizados por profissionais da área forense, dos quais destacamos: EspiaMule, que é um software baseado no aplicativo *eMule* e utiliza conexão ponto a ponto para identificar práticas criminosas, o LED (Localizador de evidências digitais) e o IPED (Indexador e Processador de Evidências Digitais), aplicativos desenvolvidos pela Polícia Federal que, com muita rapidez, realizam a varredura de dados suspeitos, e, por fim o NuDetective, uma poderosa ferramenta com foco na busca de arquivos que são diretamente relacionados à pornografia infantil.

Após destacarmos os métodos e ferramentas instrumentalizados em uma operação policial até à instauração processual de inquérito, refletimos, a seguir, sobre a dimensão técnico-jurídica dos crimes sexuais contra menores no Brasil, no Capítulo Segundo, no qual detalhamos alguns artigos do Códigos Civil e Penal brasileiros, em consonância com o Estatuto da Criança e Adolescente, a fim de relacionar como essas práticas criminosas são definidas como delitos, explorando, em seguida, as respectivas punições preconizadas, nas esferas cível e penal.

A princípio, no entanto, o intuito deste presente trabalho era realizar um estudo de caso, por meio do qual iríamos analisar um evento real relacionado a crime sexual contra crianças e adolescentes, de modo particular ocorrido na Região Metropolitana de Campinas, explicando gradativamente a série de etapas necessárias para a criminalização do infrator. Com esta ideia em mente, visitamos algumas Delegacias convencionais de Polícia Civil e Delegacias especialistas em crimes cibernéticos, e entrevistamos alguns profissionais da área, como delegados das Polícias Civil e Federal, os quais não nos autorizaram o uso destas informações, pois a maioria dos casos relacionados à pornografia infanto-juvenil estavam inscritos como processos em “segredo de justiça”, ou seja, são casos em que são mantidos sigilo, pois como estão passando por processos judiciais ou investigações policiais, há risco de informações privativas, confidenciais, do réu ou de eventuais vítimas serem expostas.

Para trabalhos futuros relacionados a este tema, sugerimos a criação de uma metodologia para facilitar, simplificar e otimizar o trabalho da polícia forense na busca e na criminalização de quem comete o crime digital de pornografia, inclusive, automatizando as buscas, a fim de desenvolver meios que ampliem a captação de mais resultados, os quais podem conduzir à detenção de violadores da infância e da juventude.

Outra recomendação para futuros trabalhos relacionados a este tema, é a de realizar um comparativo entre ferramentas forenses que podem ser utilizadas para a análise de imagens, as quais podem conter nudez, explicando, por exemplo, as vantagens e desvantagens de cada uma delas, de acordo com a situação nas quais estas ferramentas poderão ou potencialmente serão utilizadas.

REFERÊNCIAS

BEZERRA, Juliana. Estatuto da Criança e do Adolescente (ECA), 2018. *In*.: **Portal Toda Matéria**, 2011-2019. Disponível em: https://www.todamateria.com.br/estatuto-da-crianca-e-do-adolescente-eca/ hiperlink completo. Acesso em: 27 abr. 2019, às 23h28min.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**: vol. 1: parte geral. 10ª. ed. São Paulo: Saraiva, 2006.

BRASIL. Presidência da República. **Código Penal,** 1940 Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 3 jul. 2019, às 8h48min.

BRASIL [1941a]. Presidência da República. **Lei das Contravenções Penais,** 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3688.htm. Acesso em: 19 jun. 2019, às 19h14min.

BRASIL [1941b]. Presidência da República: Casa Civil, 1941. **Decreto-Lei 3.689, de 3 de outubro de 1941**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 19 jun. 2019, às 20h41min.

BRASIL. Presidência da República. **Constituição da República Federativa do Brasil,** 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 jun. 2019, às 19h14min.

BRASIL [1990a]. Presidência da República. **Lei n.º 8.069, de 13 de julho de 1990**: Estatuto da Criança e do Adolescente, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8069Compilado.htm. Acesso em: 2 jul. 2019, às 19h34min.

BRASIL [1990b]. Congresso. Câmara. **Convenção sobre os Direitos da Criança,** 1990: Decreto n.º 99.710, de 21 de novembro de 1990. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm/comite-brasileiro-de-direitos-humanos-e-politica-externa/ConvDirCrian.html. Acesso em: 25 jul. 2019, às 18h56min.

BRASIL. Presidência da República. **Lei 10.224, de 15 de maio de 2001:** crime de assédio sexual, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/LEIS_2001/L10224.htm#art216a. Acesso em: 26 jul. 2019, às 17h17min.

BRASIL. Presidência da República. **Lei n.º 10.406, de 10 de janeiro de 2002**: Código Civil, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 2 jul. 2019, às 19h34min.

BRASIL. Presidência da República. **Lei 11.829, de 25 de novembro de 2008:** alteração de Lei 8.069, de 13 de julho de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso em 25 jul. 2019, às 18h11min.

BRASIL. Congresso. Senado Federal. **Relatório Final da Comissão Parlamentar de Inquérito**: Pedofilia, 2010. Disponível em: http://www.senado.gov.br/noticias/agencia/pdfs/RELATORIOFinalCPIPEDOFILIA.pdf. Acesso em: 19 jun. 2019, às 16h46min.

BRASIL. Ministério da Justiça: Secretaria Nacional de Segurança Pública, 2014. **Portaria nº 82, de 16 de julho de 2014**: cadeia de custódia de vestígios, 2014. Disponível em: https://www.diariodasleis.com.br/legislacao/federal/227818-cadeia-de-custudia-de-vestugios-estabelece-as-diretrizes-sobre-os-procedimentos-a-serem-observados-no-tocante-u-cadeia-de-custudia-de-vestugios.html. Acesso em: 19 jun. 2019, às 20h34min.

BRASIL. Tribunal Regional Federal da 3ª. Região: Escola de Magistrados, 2017. **Investigação e prova nos crimes cibernéticos**. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 19 jun. 2019, às 21h15min.

BRASIL. Supremo Tribunal Federal. **Lei 13.718, de 24 de setembro de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm. Acesso em: 3 jul. 2019, às 23h14min.

BRUTTI, Roger Spode. Tópicos Cruciais sobre Pedofilia. **Revista IOB de Direito Penal e Processo Penal**, Porto Alegre, v. 8, n. 47, p. 18-25, dez/jan. 2008.

CHAKRAVARTY, Sambuddho; BARBERA, Marco V.; PORTOKALIDIS, Georgios; POLYCHRONAKIS, Michalis; KEROMYTIS, Angelos D. On the effectiveness of traffic analysis against anonymity networks using flow records. *In.:* **Passive and Active Measurement** (PAM), 2014: 15th International Conference, Los Angeles, CA, USA, March 10-11, 2014. P. 247-257. Disponível em: https://link.springer.com/book/10.1007/978-3-319-04918-2. Acesso em: 25 maio 2019, às 15h23min.

CONCEITO.DE. **Conceito de conhecimento**, 2010-2019. Disponível em: https://conceito.de/conhecimento. Acesso em: 19 jun. 2019, às 19h40min.

CONCEITO.DE. **Conceito de dispositivos de armazenamento**, 2010-2019. Disponível em: https://conceito.de/dispositivos-de-armazenamento. Acesso em: 19 jun. 2019, às 19h55min.

CONCEITO.DE. **Conceito de informação**, 2010-2019. Disponível em: https://conceito.de/informacao. Acesso em: 19 jun. 2019, às 19h35min.

CROCE, Delton; CROCE JÚNIOR, Delton. **Manual de Medicina Legal**. 8ª. ed. São Paulo: Saraiva, 2012. Disponível em: https://www.academia.edu/9393889/Manual_de_Medicina_Legal. Acesso em: 16 jun. 2019, às 16h40min.

CUNHA, Juliana Andrade; NEJM, Rodrigo. **Diálogo virtual 2.0**: Preocupado com o que acontece na internet? Quer conversar? 2015. Disponível em: https://new.safernet.org.br/sites/default/files/content_files/Di%C3%A1logo_Virtual_Low_Web_SN_Unicef_PFDC_CGI.pdf. Acesso em: 3 jul. 2019, às 20h36min

DALPIAN, Guilherme M.; BENITES, Carlos A. A., Ferramenta para monitoramento de redes P2P: EspiaMule. **The Second International Conference of Forensic Computer Science**, vol 2, n. 1, 2007, p 70-72.

DEVMEDIA. **Conceitos Fundamentais de Banco de Dados,** 2006. Disponível em: https://www.devmedia.com.br/conceitos-fundamentais-de-banco-de-dados/1649. Acesso em: 19 de jun. 2019, às 19h45min.

EL PAÍS. **YouTube enfrenta um escândalo com milhares de comentários pedófilos em vídeos de menores**, 2019. Disponível em: https://brasil.elpais.com/brasil/2019/02/21/tecnologia/1550748035_065824.html. Acesso em: 1 jul. 2019, às 19h40min.

ELEUTÉRIO, P. M. S.; MACHADO, M. P. **Desvendando a computação forense**. São Paulo: Novatec, 2011.

ELEUTERIO.COM. **Ferramenta Forense NuDetective,** 2011. Disponível em: http://www.eleuterio.com/nudetective.html. Acesso em: 25 jun. 2019, às 20h46min.

GALVÃO, R. K. M. **Introdução à análise forense em redes de computadores**: São Paulo: Novatec, 2013.

HISGAIL, Fani. **Pedofilia:** um estudo psicanalítico. São Paulo: Iluminuras, 2007

LILLARD, T. *et al*. **Digital forensics for network, internet and cloud computing**: Burlington: Syngress, 2010.

HUTCHINSON, Andrew. How Twitter's feed algorithm Works: as explained by Twitter. *In*.: **Social Media Today**, 11 maio 2017. Disponível em: https://www.socialmediatoday.com/social-networks/how-twitters-feed-algorithm-works-explained-twitter. Acesso em: 3 jul. 2019, às 19h18min.

MARCHETTI, Bruno. Como a Polícia Federal prendeu uma rede de pornografia infantil na deep web. *In.:* **Vice Media LLC**. 30 nov. 2016, às 12h43min. Disponível em: https://www.vice.com/pt_br/article/gvdx37/como-uma-operacao-da-policia-federal-prendeu-uma-rede-de-pedofilia-na-deep-web. Acesso em: 25 maio 2019, às 14h44min.

MINISTÉRIO DA JUSTIÇA; DEPARTAMENTO DE POLÍCIA FEDERAL. **Iped**: versão 3.13.5, 22 jun. 2018. Disponível em: https://servicos.dpf.gov.br/ferramentas/IPED/3.13.5/Manual%20IPED.pdf. Acesso em: 19 jun. 2019, às 21h50min.

MITNICK, K. D. **A arte de enganar**. Trad. de K. A. Roque. Pearson Education do Brasil, 2003. Disponível em: https://www.passeidireto.com/arquivo/31727628/a-arte-de-enganar-kevin-mitnick. Acesso em: 9 jun. 2019, às 15h45min.

MOECKE, Thiago Cristian. Forense computacional: processo de Investigação. *In.:* **CristianTM**, 2009-2012. Disponível em: https://sites.google.com/a/cristiantm.com.br/forense/forense-computacional/processo-de-investigacao. Acesso em: 4 jun. 2019, às 20h43min.

MONTEIRO, Marcos. **Entrevista da estudante Pâmela Cristina da Silva com o Perito Judicial e Presidente da Apecof, prof. Marcos Monteiro, em 26 de maio de 2019**. Campus Consolação da Puc São Paulo. São Paulo, 2019.

NABUCO FILHO, José. **Direito Penal:** Violação sexual mediante fraude (art. 215), 2016. Disponível em: http://josenabucofilho.com.br/home/direito-penal/parte-especial/937-2/. Acesso em: 26 jul. 2019, às 17h04min.

NOGUEIRA, Sandro D'Amato. Pedofilia e tráfico de menores pela Internet: O lado negro da web. *In*: **Âmbito Jurídico**, 31 ago. 2001. Disponível em: http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=5556. Acesso em: 1 jun. 2019, às 19h15min.

OLIVEIRA, Jorge Ricardo Souza de; SILVA, Edmar Edilton da., 2009. EspiaMule e Wyoming ToolKit: Ferramentas de Repressão à Exploração Sexual Infanto-Juvenil em Redes Peer-to-Peer. **The Fourth International Conference of Forensic Computer Science**, Volume 4, nº. 1, 2009, p 108-110. ICOFCS 2009. Disponível em: http://icofcs.org/2009/ICoFCS2009-PP14.pdf. Acesso em: 20 jul. 2019, às 15h50min.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Nações Unidas Brasil. **Declaração Universal dos Direitos Humanos** (DUDH): Artigo 3: Direito à vida, publicado em 16 nov. 2018. Disponível em: https://nacoesunidas.org/artigo-3-direito-a-vida/. Acesso em: 16 jun. 2019, às 16h40min.

PAPO DE HOMEM. **Denúncias acusam o YouTube de facilitar o acesso à pornografia infantil,** 2019**.** Disponível em: https://papodehomem.com.br/denuncias-acusam-o-youtube-de-facilitar-o-acesso-a-pornografia-infantil/.Acesso em: 21 mai. 2019, às 16h27min.

PEDOFILIA. *In.:* **Dicio**: Dicionário Online de Português, 2009-2019. Disponível em: https://www.dicio.com.br/pedofilia/. Acesso em: 19 jun. 2019, às 19h34min.

POLASTRO, Mateus de Castro; ELEUTÉRIO, Pedro Monteiro da Silva. **NuDetective**: A Forensic Tool to Help Combat Child Pornography through Automatic

Nudity Detection, 2010. Disponível em: https://ieeexplore.ieee.org/document/5591120. Acesso em: 19 jun. 2019, às 21h27min.

POLÍCIA FEDERAL. **PF combate a disseminação de pornografia infantil pela Deep Web**. 15 out. 2014. Disponível em: http://www.pf.gov.br/agencia/noticias/2014/10/pf-combate-a-disseminacao-de-pornografia-infantil-pela-deep-web-no-rs. Acesso em: 25 maio 2019, às 13h56min.

POLÍCIA FEDERAL. **PF divulga balanço da Operação DarkNet II**. 22 nov. 2016. Disponível em http://www.pf.gov.br/agencia/noticias/2014/10/pf-combate-a-disseminacao-de-pornografia-infantil-pela-deep-web-no-rs. Acesso em: 25 maio 2019, às 14h23min.

PORTAL DEVMEDIA. Lógica: uma ferramenta indispensável na programação de computadores. *In.:* **Devmedia,** 2019. Disponível em: https://www.devmedia.com.br/logica-uma-ferramenta-indispensavel-na-programacao-de-computadores/28386. Acesso em: 25 jun. 2019, às 22h17min.

REIS, Gustavo Aranha C. dos. Abordagens para detecção automática de pornografia infantil em imagens digitais. *In*.: **Acta de Ciências & Saúde**, Volume 2, n.º 5, 2016, p. 81-85. Disponível em: http://www2.ls.edu.br/actacs/index.php/ACTA/article/view/136/126. Acesso em: 25 jun. 2019, às 20h57min.

SAFERNET [2005-2019a]. **Passo a passo para quem teve imagens íntimas vazadas**, 2005-2019. Disponível em: https://new.safernet.org.br/sites/all/themes/helpline/infografico-sexting.pdf. Acesso em: 3 jul. 2019, às 20h23min.

SAFERNET [2005-2019b]. **Sexting é uma expressão da sexualidade na adolescência**: Sexting é uma expressão da sexualidade na adolescência, 2005-2019. Disponível em: https://new.safernet.org.br/content/sexting-é-uma-expressão-da-sexualidade-na-adolescência. Acesso em: 3 jul. 2019, às 19h20min.

SAFERNET. **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos,** 2005-2017. Disponível em: http://indicadores.safernet.org.br. Acesso em: 21 maio 2019, às 12h09min.

SAFERNET [2007-2018a]. **Perfil Helpline,** 2007-2018. Disponível em: https://helpline.org.br/helpline. Acesso em: 21 maio 2019, às 20h50min.

SAFERNET [2007-2018b]. **Pornografia infantil**, 2007-2018. Disponível em: https://new.safernet.org.br/denuncie. Acesso em: 3 jul. 2019, às 19h45min.

SAFERNET. **Como funciona,** 2008. Disponível em: http://www.safernet.org.br/site/institucional/projetos/cnd/como-funciona. Acesso em: 21 maio 2019, às 20h35min.

SAFERNET [2019a]. **Delegacias Cibercrimes,** 2019. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 3 de jul. 2019, às 19h10min.

SAFERNET [2019b]. **Parceria com o MPF-SP.** 2019. Disponível em: http://www.safernet.org.br/site/institucional/parcerias/mpf-sp. Acesso em: 21 maio 2019, às 20h42min.

SAFERNET [2019c]. **Denuncie,** 2019. Disponível em: https://new.safernet.org.br/denuncie. Acesso em: 21 maio 2019, às 20h42min.

SÃO PAULO (Município). **18 de maio:** Dia Nacional de Combate ao Abuso e à Exploração Sexual de Crianças e Adolescentes, 2017. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/direitos_humanos/noticias/?p=276666. Acesso em: 25 jul. 2019, às 18h11min.

SEARCH ENGINE LAND. YouTube Ranking Factors: Getting Ranked *In*: **The Second Largest Search Engine**, 2015. Disponível em: https://searchengineland.com/youtube-ranking-factors-getting-ranked-second-largest-search-engine-225533. Acesso em: 1 jul. 2019, às 19h43min.

SOUSA, Adriano Gomes. Etapas do processo de computação forense: uma revisão. **Acta de ciências e saúde**, Volume 2, n.º 1, 2016. Disponível em: http://www2.ls.edu.br/actacs/index.php/ACTA/article/view/138. Acesso em: 3 jun. 2019, às 20h15min.

SPROUT SOCIAL. **How to survive (and outsmart) the Instagram algorithm**, 2019. Disponível em: https://sproutsocial.com/insights/instagram-algorithm/. Acesso em: 1 jul. 2019, às 19h50min.

THE MARKETING PEOPLE. **8 ways to increase your ranking on LinkedIn**. EUA, 2015 Disponível em: https://themarketingpeople.com/8-ways-to-increase-your-ranking-on-linkedin/. Acesso em: 1 jul. 2019, às 20h03min.

UNIVERSIDADE DE SÃO PAULO. Localização de Evidências Digitais combate pornografia infantil. *In.:* **Jornal da USP**, 14/08/2017. Disponível em: https://jornal.usp.br/atualidades/localizacao-de-evidencias-digitais-combate-pornografia-infantil/. Acesso em: 25 jun. 2019, às 20h18min.

ANEXOS

ANEXO 1 - CARTA DE APRESENTAÇÃO DE ESTUDANTES DA FATEC AMERICANA

De: Fatec Americana
Para: Delegacias de Polícia Civil do Estado de São Paulo
Sobre: Carta de apresentação de estudantes da Fatec Americana

Nós, prof. Edson Roberto Gaseta, Coordenador do Curso Superior de Tecnologia de Segurança da Informação, e prof. Benedito Luciano Antunes de França, orientador de Trabalho de Graduação, ambos pertencentes à Fatec de Americana, apresentamos os estudantes **Felipe Castanha da Silva e Pâmela Cristina da Silva**, matriculados no 6º semestre letivo do curso de graduação tecnológica supracitado.

Os acadêmicos estão desenvolvendo uma pesquisa fundamentada nos aspectos técnicos-computacionais presentes nos Bancos de Dados e algoritmos de sítios eletrônicos de busca, que possibilitam uma investigação *online* de informações concernentes aos crimes infantis e juvenis de natureza sexual. Além do estudo da natureza técnica dos sistemas computacionais, a pesquisa também se alicerça em aspectos jurídicos, os quais validam a detenção e a posterior criminalização de ações sexuais contra crianças e adolescentes.

Não obstante, a terceira parte da pesquisa, *razão desta Carta de apresentação*, requer a exposição de um estudo de caso, que permita, por meio da triagem de fontes jornalísticas impressas e virtuais, identificar Delegacias empenhadas no combate dos crimes desta natureza, a fim de compreender o ofício policial que, com o uso de elementos tecnológicos (Banco de dados, aplicativos, sistemas eletrônicos afins, etc.), conduzam à compreensão da identificação do meliante, por meio de denúncias e coleta de dados em fontes computacionais, até a execução do mandado de prisão contra meliantes sexuais.

Agradecemos a atenção dispensada e renovamos nossos votos de elevada estima e consideração, dispondo-nos para eventuais esclarecimentos que a presente atividade acadêmica requerer.

Atenciosamente.

Americana/SP, 13 de abril de 2019.

Prof. Me. Edson Roberto Gaseta - Coordenador do Curso Superior de Tecnologia em Segurança da Informação

Prof. Me. Benedito Luciano Antunes de França - Orientador de Trabalho de Graduação