RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano IV, v.1, n.2, ago./ dez 2024. | submissão: 01/12/2024 | aceito: 03/12/2024 | publicação:05/12/2024

ANÁLISE LITERÁRIA DE FERRAMENTAS DA COMPUTAÇÃO FORENSE NO COMBATE ÀS IMAGENS DE ABUSO E EXPLORAÇÃO INFANTIL

LITERARY ANALYSIS OF COMPUTER FORENSIC TOOLS IN COMBATING IMAGES OF CHILD ABUSE AND EXPLOITATION

Ana Maria Cardoso de Souza[1] – Universidade do Estado de Mato Grosso
Prof.ª Ma. Déborah Barbosa Camacho[2] – Universidade do Estado de Mato Grosso
Prof.ª Ma. Raquel da Silva Vieira Coelho[3] – Universidade do Estado de Mato Grosso

RESUMO
Este artigo aborda o papel de ferramentas gratuitas de computação forense, como Autopsy, IPED e NuDetective, no enfrentamento ao abuso e exploração infantil em ambientes digitais. A análise, embasada em revisão bibliográfica e investigação exploratória, destaca a importância dessas ferramentas ao avaliar sua eficácia e identificar limitações. O trabalho também busca alinhá-las às diretrizes do Estatuto da Criança e do Adolescente (ECA) e da Lei Geral de Proteção de Dados (LGPD), assegurando que a aplicação de tais tecnologias respeite direitos legais e éticos. Os resultados indicam que, apesar das limitações em relação às ferramentas pagas, as soluções gratuitas são úteis quando combinadas com capacitação técnica e políticas públicas, contribuindo para a investigação e prevenção desses crimes no ciberespaço.
Palavras-chave: Computação Forense; Cibercrime; Ferramenta Forense; Pedofilia e Exploração Infantil.

ABSTRACT
This article addresses the role of free computer forensic tools, such as Autopsy, IPED and NuDetective, in combating child abuse and exploitation in digital environments. The analysis, based on a literature review and exploratory research, highlights the importance of these tools when evaluating their effectiveness and identifying limitations. The work also seeks to align them with the guidelines of the Child and Adolescent Statute (ECA) and the General Data Protection Law (LGPD), ensuring that the application of such technologies respects legal and ethical rights. The results indicate that, despite the limitations in relation to paid tools, free solutions are useful when combined with technical training and public policies, contributing to the investigation and prevention of these crimes in cyberspace.
Keywords: Computer Forensics; Cybercrime; Forensic Tool; Pedophilia and Child Exploitation.

1. INTRODUÇÃO

O abuso e a exploração infantil são problemas profundamente preocupantes, que afetam crianças em todo o mundo, independentemente de sua origem socioeconômica, cultural ou étnica. Com o avanço da tecnologia e a expansão do uso da internet, esses crimes têm se adaptado ao ambiente digital, assumindo novas formas, como a produção, distribuição e consumo de material de abuso infantil online. Esse cenário cria desafios significativos para as autoridades e a sociedade em geral, pois as imagens e vídeos de abuso infantil podem circular indefinidamente, perpetuando o sofrimento das vítimas e dificultando a erradicação desse tipo de crime.

No combate a essas atividades criminosas, a Computação Forense surge como uma ferramenta essencial. A Computação Forense pode ser definida como o processo de identificação, coleta, preservação, análise e apresentação de evidências digitais para uso em processos judiciais. Segundo Maras (2015), a computação forense abrange todo o ciclo de vida das evidências digitais, desde sua coleta até sua apresentação em tribunal. Essa área da ciência forense é crucial para a investigação de cibercrimes, incluindo aqueles que envolvem o abuso e exploração infantil. Como apontado por Chawki, Darwish e Khan (2015), os cibercrimes abrangem uma ampla gama de delitos, sendo o abuso infantil um dos mais graves.

O presente artigo tem como objetivo realizar uma análise literária de algumas das principais ferramentas gratuitas de Computação Forense utilizadas no combate às imagens de abuso e exploração infantil. A finalidade é não apenas identificar e discutir essas ferramentas, mas também contextualizá-las dentro do marco legal brasileiro, incluindo o Estatuto da Criança e do Adolescente (ECA) e a Lei Geral de Proteção de Dados Pessoais (LGPD). Além disso, o estudo pretende enumerar e discutir trabalhos relacionados que abordam o

uso dessas ferramentas na proteção dos direitos das crianças.

No cenário atual, existem diversas ferramentas forenses gratuitas disponíveis que podem ser utilizadas de forma eficaz para combater o abuso infantil online. A escolha desse tema se justifica pela gravidade do problema e pelo crescimento alarmante no número de denúncias relacionadas a imagens de abuso infantil, como evidenciado pelos dados da ONG Safernet, que registrou um aumento de 77,13% nas denúncias de 2022 para 2023.

Portanto, a análise literária proposta neste artigo busca contribuir para o entendimento das capacidades e limitações das ferramentas de Computação Forense no combate ao abuso infantil online, fornecendo *insights* que possam ser úteis para profissionais e pesquisadores na luta contra essa violação dos direitos das crianças.

2. FUNDAMENTAÇÃO TEÓRICA

Esta seção tem como objetivo apresentar de maneira clara e concisa as subseções deste artigo. Na subseção 2.1, é abordada a definição da Computação Forense, crucial para a investigação de crimes cibernéticos. A subseção 2.2 explora diversas ferramentas fundamentais para análise forense digital, como o Autopsy (2.2.1), IPED (2.2.2) e NuDetective (2.2.3), cada uma contribuindo com recursos específicos para a investigação de crimes digitais.

A subseção 2.3 enfatiza os crimes cibernéticos, com destaque para a investigação de imagens de abuso e exploração infantil (2.3.1), discutindo as técnicas necessárias para lidar com esse tipo de crime. Já na subseção 2.4, são abordadas as legislações relevantes que protegem dados e imagens, incluindo o Estatuto da Criança e do Adolescente (2.4.1) e a Lei Geral de Proteção de Dados (2.4.2), garantindo direitos e regulando o tratamento de informações pessoais.

Por fim, a seção 3 apresenta a metodologia utilizada para o desenvolvimento do artigo, enquanto a seção 4 revisa estudos e trabalhos que exploram o uso de ferramentas de Computação Forense no combate ao uso indevido de imagens de abuso infantil.

2.1 Computação Forense

A Computação Forense pode ser definida como uma área da Ciência da Computação que se desenvolve gradualmente para atender à demanda oriunda da Criminalística e como uma parte da Criminalística que se apropria de fundamentos da Ciência da Computação (Melo, 2009). Essa área tem como base investigar e reconstituir fatos ilícitos através da identificação, coleta e análise de evidências ou informações magneticamente armazenadas ou codificadas (Mercuri, 2005).

Em termos práticos, a computação forense se resume a um conjunto de práticas adotadas para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais que tenham validade em processos judiciais (Silva Filho, 2016).

Ela tem como principal objeto de investigação os crimes cibernéticos. De acordo com Maras (2015), são definidos como "O uso da Internet, de computadores e de tecnologias relacionadas na prática de um crime". Os crimes cibernéticos são identificados e investigados com o auxílio de diversas ferramentas, conforme descrito na subseção 2.3.

2.2 Ferramentas da computação forense

As ferramentas forenses desempenham um papel crucial na busca, detecção e recuperação de possíveis evidências digitais em dispositivos de armazenamento e processamento. Seu uso é fundamental para investigar crimes cibernéticos, incluindo abuso e exploração infantil. As ferramentas: Autopsy, Sistema IPED e NuDetective que auxiliam os investigadores a identificar arquivos de imagem, vídeos, mensagens e registros de atividades relevantes, contribuindo assim para a responsabilização dos culpados por esses crimes.

2.2.1 Autopsy

O Autopsy Linux é uma ferramenta forense digital de código aberto que permite a análise de um sistema de arquivo de uma determinada imagem forense, podendo ser utilizado para fins militares e corporativos de forma a realizar a reconstrução dos eventos que aconteceram em determinado host e que geraram o comprometimento do mesmo (Autopsy, 2003).

De acordo com Richardson, Marjie, (2018) *apud* Evaristo (2023) o autopsy é conhecido pela sua capacidade de realizar análises temporais, permitindo aos investigadores visualizar eventos numa linha do tempo, ou seja, ele detalha desde a criação até a exclusão dos arquivos. Isso é fundamental para entender a sequência de atividades num dispositivo e identificar padrões ou ações suspeitas. Outra característica significativa é a funcionalidade de pesquisa por palavras-chave, que facilita a identificação rápida de informações relevantes.

A ferramenta também possui uma variedade de módulos internos que permitem aos usuários identificar dados específicos, como históricos de navegação na web, conexões ou registos de geolocalização. Além disso, a comunidade forense pode desenvolver e compartilhar os seus próprios módulos, ampliando ainda mais as capacidades da ferramenta (Richardson; Marjie, 2018 *apud* Evaristo, 2023).

2.2.2 Sistema Indexador e Processador de Evidências Digitais (IPED)

De acordo com a Polícia Federal do Brasil (Polícia Federal, 2019) o IPED é um sistema de código aberto e desenvolvido em Java, utilizado para indexação e processamento de evidências digitais, que busca e organiza dados de interesse em arquivos visíveis. Além disso, o IPED recupera arquivos ocultos, apagados e fragmentados que estejam em dispositivos como discos rígidos, pendrives, cartões de memória, SSDs, CDs, DVDs e outros tipos de mídias de armazenamento.

O IPED é uma ferramenta gratuita que possui ótimo desempenho e alta velocidade de processamento, que é necessária para grandes volumes de dados em mídias de alta capacidade que são utilizadas pelos peritos brasileiros. Este software possui uma interface simples, intuitiva e integrada para análises e exames periciais detalhados dos dados armazenados (Polícia Federal, 2019).

A ferramenta oferece uma ampla gama de funcionalidades comuns em softwares forenses. Estas incluem o processamento de imagens, categorização de arquivos, detecção de arquivos criptografados, cálculo e consulta à base de hashes, e, sobretudo, indexação de conteúdo. Esta última característica é a mais vantajosa, pois agiliza e aumenta a eficiência das buscas (Polícia Federal, 2019).

2.2.3 NuDetective

O NuDetective é uma ferramenta forense gratuita que está disponível somente para autoridades e instituições públicas, foi desenvolvida por especialistas criminais da Polícia Federal Brasileira, Mateus de Castro Polastro e Pedro Monteiro da Silva Eleutério. É utilizada para examinar dados armazenados em dispositivos eletrônicos, com o objetivo de localizar possíveis materiais de exploração e abuso infantil.

Ela possui quatro funcionalidades principais, a análise de imagem, a análise de nomes, a análise de hash, e, por último, inclui a análise de vídeo nas versões mais recentes (Eleutério, Machado, 2011).

A ferramenta filtra imagens e vídeos por meio de informações textuais, assinaturas únicas e detectores de pele. Ela é capaz de buscar pelo nome do arquivo, comparando-o com uma lista de nomes e frases predefinidos comumente usados para compartilhar dados de pornografia infantil na Internet (Polastro, Eleutério, 2010).

Através da detecção de arquivos suspeitos armazenados, a ferramenta NuDetective utiliza métodos abrangentes para identificá-los. Inicialmente, emprega detecção automática de nudez para analisar imagens, identificando pixels de pele e aplicando técnicas de geometria computacional. Em seguida, realiza uma análise linguística dos nomes de arquivos para identificar expressões comuns associadas à pedofilia. Além disso, compara os hashes dos arquivos com uma lista conhecida de hashes ilegais, denominada KFF (Known File Filter) (Polastro, Eleutério, 2010).

No caso de vídeos, extrai amostras ideais de frames e aplica algoritmos de detecção de nudez para analisar o conteúdo visual. Esses procedimentos são fundamentais para identificar potenciais casos de pornografia infantil (Eleutério, Machado, 2011).

2.3 Crimes cibernéticos

Ao longo das últimas décadas a tecnologia passou por um rápido desenvolvimento e consequentemente os computadores também, se tornando cada vez mais rápidos, eficientes e menores. Nos dias de hoje os computadores e celulares estão presentes não somente em empresas, mas também nas casas, nas mãos e no dia a dia de pessoas do mundo todo. A popularização da Internet permitiu que usuários de computadores espalhados

pelo mundo pudessem trocar dados e informações em um curto espaço de tempo, tornando a comunicação entre máquinas e pessoas mais veloz (Eleutério, Machado, 2011).

Este avanço tecnológico trouxe inúmeros benefícios para a humanidade, em contrapartida também serve de palco para diversos crimes cibernéticos, que se aproveitam das vulnerabilidades dos sistemas e da conectividade global para praticar atividades ilícitas (Almeida *et al.,* 2015).

Os crimes cibernéticos englobam diversas atividades ilícitas, que vão desde ações mais simples, como phishing e roubo de identidade, até esquemas altamente sofisticados, como fraudes financeiras e invasões de redes corporativas. Entre os principais exemplos de crimes cibernéticos, destacam-se:

- Phishing – É um dos golpes mais antigos presente na internet. Para Olivo (2010), phishing é uma técnica que utiliza da engenharia social para fazer suas vítimas, persuadindo-os com objetivos de capturar as informações pessoais e depois usá-las de forma a causar-lhes prejuízos.
- Roubo de identidade - O "roubo de identidade" se caracteriza ela exploração simultânea de elementos identificadores da vítima por ela e pelo delinquente (Koops *et al.,* 2009).
- Ataques de Malware - Este tipo de ataque consiste na instalação de software malicioso em computadores ou redes sem o consentimento do usuário. O malware pode ser projetado para roubar informações seguras, como senhas ou dados bancários, danificar sistemas ou controlar computadores remotamente para enviar spam ou realizar outros ataques. Exemplos de malware incluem vírus, worms, cavalos de tróia e ransomware (Melo *et al*., 2011).
- Ransomware - O ransomware é um tipo de código malicioso (malware) que impede o acesso a arquivos ou sistemas de computador, exigindo um resgate para sua liberação (Pinto, 2018).

2.3.1 Imagens de abuso e exploração infantil

De acordo com o Ministério da Saúde (Brasil, 2015), violência é definida como ações praticadas por indivíduos, grupos, classes ou nações, que tenham como consequência danos físicos, emocionais, morais e/ou espirituais a si próprio ou a outro. Especificamente a violência contra a criança e o adolescente é classificada das seguintes formas: a física, a psicológica, a sexual e a negligência.

A legislação brasileira para proteção de crianças e adolescentes é uma das mais avançadas do mundo. Entretanto, indicadores de uma pesquisa do G1 apontam para alarmante estatística segundo a qual cerca de 41,2% desses indivíduos são vítimas de alguma forma de violência (Garcia, Mazui e Parreira, 2023). Como previsto na Constituição Federal (Brasil, 1988) é atribuído à sociedade e ao Estado o dever de assegurar à criança e ao adolescente o respeito aos seus direitos fundamentais.

No ano de 2008 a Safernet registrou 56.115 novas denúncias (Gráfico 1) de imagens de abuso e exploração infantil, "Ano em que explodem as denúncias recebidas pela Safernet de imagens de abuso e exploração sexual infantil no Orkut. Dono da plataforma Google, assina acordo com o MPF em 2 de julho, e passa a entregar informações dos criminosos às autoridades" (Safernet, 2024).

Em 2020 registrou um total de 46.019 novas denúncias (Gráfico 1) "Primeiro ano de pandemia de covid-19. Com o isolamento social aumenta o número de dispositivos conectados e o tempo de uso das telas, aumentando também a interação não presencial entre as pessoas e as denúncias de todos os tipos de crimes à Safernet" (Safernet, 2024).

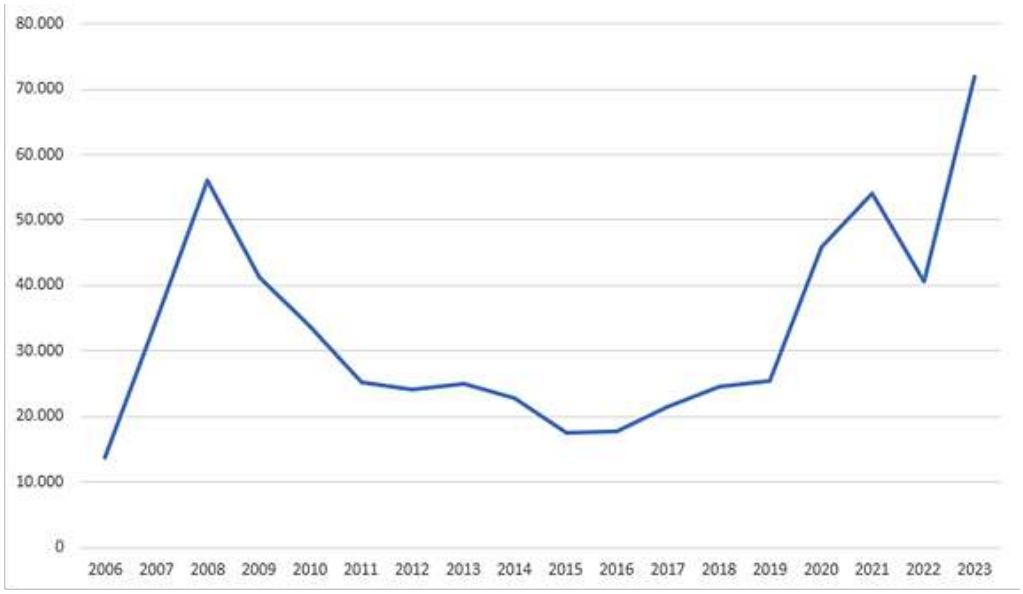
E em 2021 realizou o registro de 53.960 novas denúncias (Gráfico 1), "Segundo ano da pandemia de covid-19. O isolamento social prossegue e o número de dispositivos conectados e o tempo de uso das telas segue alto. Novo recorde consecutivo de denúncias recebidas pela Safernet desde 2009" (Safernet, 2024).

E no ano de 2023 registrou 71.867 novas denúncias (Gráfico 1), Safernet (2024) afirma que nesse ano foi registrado um recorde histórico de denúncias de imagens de abuso e exploração sexual infantil. Uma combinação de fatores explica o aumento:

1) a iniciação da Inteligência Artificial para a criação desse tipo de conteúdo;
2) o comércio ilegal de imagens de nudez e sexo autogeradas por adolescentes;
3) grandes empresas de tecnologia realizaram demissões em massa, de equipes como: segurança, integridade e moderação de conteúdo das plataformas.

O Gráfico 1 apresenta a linha do tempo de denúncias de imagens de abuso e exploração sexual infantil.

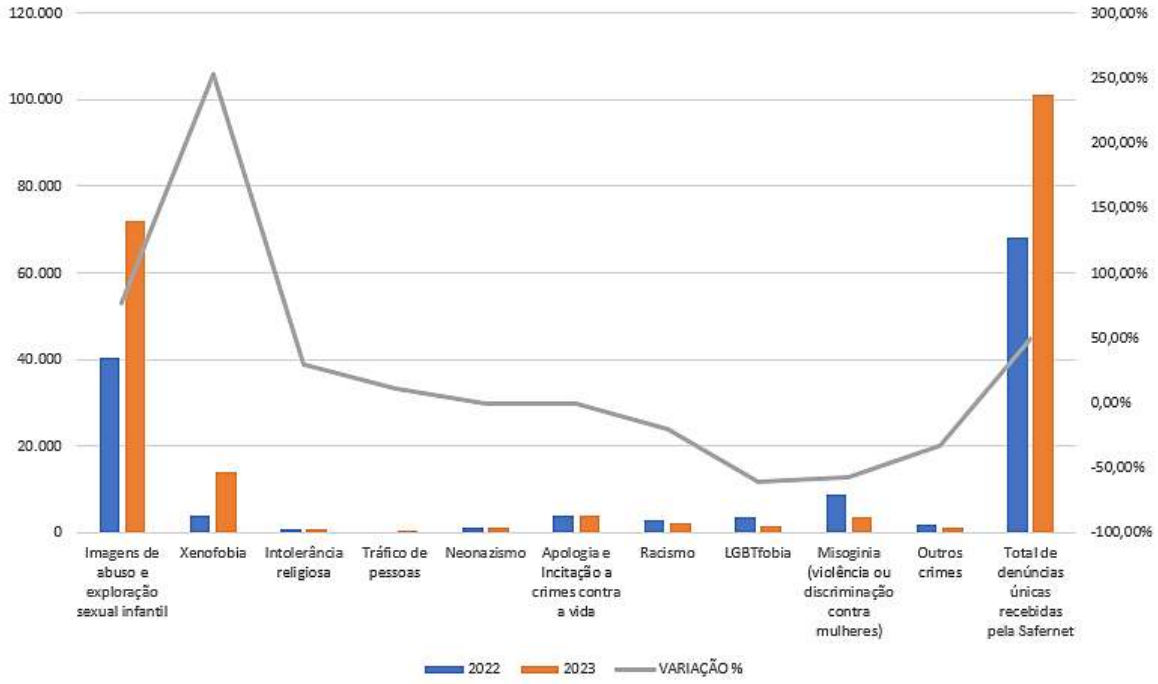
Gráfico 1 - Linha do Tempo.



Fonte: (a autora, 2024)

É possível verificar no Gráfico 2 que durante os anos de 2022 e 2023 as imagens de abuso e exploração sexual infantil é o tipo de crime que mais recebe denúncias.

Gráfico 2 – Denúncias Novas Recebidas pela Safernet, por Crime.



Fonte: (a autora, 2024).

Prevista pela Legislação Brasileira no Estatuto da Criança e do Adolescente, conforme o decreto n° 11.829, de novembro de 2008, a Pornografia Infantil é crime punido por lei para quem possui, produz, reproduz, vende, divulga ou publica, por qualquer meio de comunicação – virtual ou não virtual -, fotografias, vídeos, ilustrações ou outro tipo de imagens com pornografia, cenas de sexo explícito envolvendo crianças ou adolescentes, ou qualquer representação dos órgãos sexuais de uma criança para fins sexuais ou de exibição pornográfica (Brasil, 2008).

2.4 Legislações vigentes na proteção de imagens e dados

No Brasil, proteger as imagens e os dados de crianças e adolescentes no Brasil é uma questão fundamental, e muitas legislações tratam exclusivamente da privacidade e da segurança dos dados. As principais legislações são o Estatuto da Criança e do Adolescente descritas na subseção 2.4.1, a LGPD apresentadas na subseção 2.4.2 e algumas normas e provisões específicas do Código Civil.

O artigo do Código Civil Brasileiro (Lei nº 10.406/2002) também aborda a questão da proteção da imagem, ele prevê que a utilização da imagem de uma pessoa, sem a sua autorização ou de seu representante legal, pode resultar em responsabilidade civil. No caso de menores de idade, é necessária a autorização dos pais ou responsáveis para a utilização de sua imagem (Brasil, 2002).

2.4.1 Das disposições do Estatuto da Criança e do Adolescente, Lei Federal nº 8.069, de 13 de julho de 1990 aplicáveis

O Estatuto da Criança e do Adolescente (ECA), Lei Federal nº 8.069, de 13 de julho de 1990, é uma legislação brasileira que estabelece os direitos fundamentais das crianças e dos adolescentes, regulando sua proteção integral.

Segundo descreve o ECA em seu Art. 4°, é dever da família, da comunidade, da sociedade 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, ao respeito, à liberdade e à convivência familiar e comunitária (Brasil, 1990).

A legislação brasileira em vigor caracteriza como crime condutas de "apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive pela Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente" (Brasil, 2008).

Além disso, o ECA também prevê no Art. 17º (Brasil, 1990) "O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, idéias e crenças, dos espaços e objetos pessoais."

Enquanto o Art. 247° proíbe:

> Divulgar, total ou parcialmente, sem autorização devida, por qualquer meio de comunicação, nome, ato ou documento de procedimento policial, administrativo ou judicial relativo a criança ou adolescente a que se atribua ato infracional: Pena - multa de três a vinte salários de referência, aplicando-se o dobro em caso de reincidência (Brasil, 1990, p. 1).

Portanto, tais disposições visam garantir a proteção integral e o respeito aos direitos das crianças e adolescentes, assegurando que sejam tratados com a dignidade em todas as circunstâncias.

2.4.2 Das disposições da Lei Geral de Proteção de Dados (LGPD): Lei nº 13.709/2018 aplicáveis

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, entrou em vigor em setembro de 2020. Ela regula o tratamento de dados pessoais, seja por pessoas físicas ou jurídicas, públicas ou privadas, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Sobre a divisão da Lei n° 13.709/2018 Pinheiro (2020), diz que:

> [...] está dividida em 10 Capítulos, com 65 artigos [...]
> • Capítulo I - Disposições Preliminares (arts. 1 ao 6º).
> • Capítulo II - Do Tratamento de Dados Pessoais (arts. 7º ao 16): possui Seção I (Dos Requisitos para o Tratamento dos Dados), Seção II (Do Tratamento de Dados Pessoais Sensíveis), Seção III (Do Tratamento de Dados Pessoais de Crianças e Adolescentes) e Seção IV (Do Término do Tratamento de Dados).
> • Capítulo III - Dos Direitos do Titular (arts. 17 ao 22).
> • Capítulo IV Do Tratamento de Dados Pessoais pelo Poder Público (arts. 23 ao 32): possui Seção I (Das Regras) e Seção II (Da Responsabilidade).
> • Capítulo V - Da Transferência Internacional de Dados (arts. 33 ao 36).
> • Capítulo VI - Dos Agentes de Tratamento de Dados Pessoais (arts. 37 ao 45): possui Seção I (Do Controlador e do Operador), Seção II (Do Encarregado pelo Tratamento de Dados Pessoais) e Seção III (Da Responsabilidade e do Ressarcimento de Danos).
> • Capítulo VII - Da Segurança e das Boas Práticas (arts. 46 ao 51): possui Seção I (Da Segurança e do Sigilo de Dados) e Seção II (Das Boas Práticas e da Governança).
> • Capítulo VIII - Da Fiscalização (arts. 52 ao 54): possui Seção I (Das Sanções Administrativas).
> • Capítulo IX Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (arts. 55 ao 59): possui Seção I (Da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Seção II (Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade) - veto presidencial.
> • Capítulo X - Disposições Finais e Transitórias (arts. 60 ao 65). (Brasil, 2020, p. 9-10)

A LGPD estabelece princípios fundamentais para o tratamento de dados pessoais. Segundo o Art. 6º, inciso VI, é garantida a transparência aos titulares de informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados, respeitando segredos comerciais e industriais. Além disso, conforme o Art. 6º, inciso VII, são exigidas medidas técnicas e administrativas para assegurar a segurança dos dados pessoais, protegendo contra acessos não autorizados e incidentes de destruição, perda ou alteração ilícita. O Art. 6º, VIII, da LGPD determina a adoção de medidas preventivas para evitar danos decorrentes do tratamento de dados pessoais (Brasil, 2018).

A lei também dedica atenção especial ao tratamento de dados de crianças e adolescentes. Conforme o Art. 14, § 1º, o consentimento específico e destacado de ao menos um dos pais ou responsável legal é exigido para o tratamento de dados de crianças. Já o Art. 14, § 3º, estabelece que, em circunstâncias específicas e controladas, dados pessoais de crianças podem ser coletados sem consentimento para contatar os pais ou para proteção da criança, desde que não sejam armazenados nem compartilhados com terceiros sem o consentimento mencionado anteriormente (Brasil, 2018).

Essas disposições da LGPD têm como objetivo assegurar que o tratamento de dados pessoais seja realizado de forma responsável, transparente e segura, protegendo os direitos fundamentais à privacidade e à proteção dos dados, especialmente aos indivíduos vulneráveis como crianças e adolescentes.

3. MATERIAL E MÉTODO

O artigo em questão utilizará a pesquisa exploratória para analisar literariamente as ferramentas de computação forense utilizadas no combate às imagens de abuso e exploração infantil. Através desta pesquisa, pretende-se obter uma compreensão abrangente das ferramentas disponíveis e sua eficácia no enfrentamento desse tipo de crime.

De acordo com Leão, pesquisa exploratória:

> [...] visa proporcionar maiores informações sobre um assunto investigado, familiarizar-se com o fenômeno ou conseguir nova compreensão desse, a fim de poder formular um problema mais preciso de pesquisa ou criar novas hipóteses. Pode ser também o passo inicial em um processo de pesquisa. Os estudos exploratórios conduzem apenas a hipóteses, não verificam, nem demonstram. (Leão, 2016, p. 14).

Também será adotada a metodologia da pesquisa bibliográfica para colaborar na investigação das fer-

ramentas. Por meio dessa abordagem, busca-se explorar a literatura existente para obter uma compreensão aprofundada das ferramentas disponíveis, sua aplicabilidade e os resultados obtidos em estudos anteriores sobre o tema. Casarin diz que pesquisa bibliográfica:

> [...] faz uso de artigos, teses, dissertações, livros etc, escritos por outros autores sobre o tema em questão. Nesse tipo de pesquisa, é possível verificar o que já foi produzido em estudos anteriores a respeito do assunto. (Casarin, H. e Casarin, S., 2012, p. 47).

Para descrever sobre os trabalhos relacionados, a pesquisa fará uso da revisão sistemática de literatura. Para Galvão e Ricarte a revisão sistemática de literatura pode ser definida como:

> [...] modalidade de pesquisa, que segue protocolos específicos, e que busca entender e dar alguma logicidade a um grande corpus documental, especialmente, verificando o que funciona e o que não funciona num dado contexto. Está focada no seu caráter de reprodutibilidade por outros pesquisadores, apresentando de forma explícita as bases de dados bibliográficos que foram consultadas, as estratégias de busca empregadas em cada base, o processo de seleção dos artigos científicos, os critérios de inclusão e exclusão dos artigos e o processo de análise de cada artigo. Explicita ainda as limitações de cada artigo analisado, bem como as limitações da própria revisão. (Galvão e Ricarte, 2019, p. 58-59).

A mesma utilizará as plataformas Google Scholar, Portal de Periódicos CAPES e Science Direct como bases de pesquisa, buscando nas plataformas pelas seguintes palavras-chaves: *forensic tools* e *exploitation of child images*, nos períodos de 2018 a 2024.

Inicialmente, no Portal de Periódicos CAPES, foram encontrados 45 artigos, dos quais 29 foram selecionados para uma análise mais aprofundada. Desses, 27 foram excluídos, resultando em 2 artigos adequados para a pesquisa final. No Google Scholar, de um total de 6.100 resultados, 100 foram selecionados, mas apenas 3 atenderam aos critérios de relevância. Já no Science Direct, de 502 resultados iniciais, 100 foram analisados, resultando em 3 artigos escolhidos após a exclusão de 97.

Então, foram identificados 229 artigos relevantes nas plataformas consultadas. No entanto, parte desses artigos foi excluída por estarem repetidos ou não serem pertinentes ao tema da pesquisa, garantindo assim a qualidade e a precisão dos dados selecionados. A partir dessa triagem inicial, procedeu-se à análise dos títulos e resumos dos artigos, com o objetivo de identificar aqueles que melhor se alinhavam ao foco do estudo. Os artigos considerados menos relevantes foram descartados, o que resultou na seleção de 8 artigos que atendiam aos critérios previamente estabelecidos. Esses artigos finais constituem a base da análise e discussão apresentada no estudo, que se apoia na contribuição científica das fontes selecionadas para enriquecer o entendimento sobre o tema pesquisado.

4. TRABALHOS RELACIONADOS

Conforme descrito na seção 2.3.1, a exploração e o abuso infantil constituem graves violações aos direitos fundamentais de crianças e adolescentes, abrangendo práticas como violência física, psicológica, sexual e negligência (Brasil, 2015). Embora o Brasil possua uma legislação avançada de proteção, incluindo o Estatuto da Criança e do Adolescente (ECA), o país ainda enfrenta altas taxas de violência infantil, com 41,2% das crianças e adolescentes sendo vítimas de algum tipo de abuso (Garcia, Mazui e Parreira, 2023). A ONG (Organização não governamental) Safernet registrou um aumento alarmante de denúncias de exploração sexual infantil nos últimos anos, especialmente durante a pandemia de COVID-19, quando o uso de dispositivos conectados aumentou significativamente (Safernet, 2024). Em 2023, as denúncias atingiram um recorde histórico, evidenciando a urgência de reforço na aplicação da legislação e de ações coordenadas entre o Estado e a sociedade para proteção integral de menores.

Sendo assim, esta seção apresenta alguns dos principais trabalhos relacionados. Para esta pesquisa, foi utilizada a string de busca (*forensic tools* AND *exploitation of child images*), com a seleção de trabalhos publicados no período de 2018 a 2024, conforme descrito na Seção 3. Na Tabela 1 “Artigos Relacionados”, são apresentados os trabalhos selecionados para a pesquisa.

Tabela 1 - Artigos Relacionados

Autor/Autores	Ferramentas	Crimes Investigados
Parizotto, Neves e Pinheiro (2022)	FTK, Encase e Autopsy.	Pornografia infantil
Salih e Ibrahim (2023)	Stellar, FTK, Nmap, OSFMount e Autopsy.	Phishing, Lavagem de dinheiro, Fraude bancária e Exploração infantil.
Andrade (2024)	FTK, CAINE, Autopsy, ImageJ, FotoForensics e The Sleuth Kit.	Phishing, Ransomware, Fraude financeira, Cyberbullying, Ataques DDoS e Pornografia infantil.
Gangwar *et al.,* (2021)	AttM-CNN e NuDetective.	Pornografia infantil
Westlake e Guerra (2023)	PhotoDNA	Abuso sexual infantil
Okutan e Çebi (2019)	EnCase, Enterprise, Forensic, Fastbloc e Guidance Software.	Pornografia infantil, Malware, Trojans, Cyberterrorism, Cyberstalking e KeyLogger.
Sanchez *et al.,* (2019)	Autopsy, Forensic Toolkit, Magnet Forensics e Cellebrite.	Pornografia infantil
Sarkara e Shukla (2023)	Autopsy, EnCase, Sleuth Kit e Nmap.	Exploração infantil, Pornografia de celebridades, Propagação de desinformação, Cyberbullying e Fraude financeira.

Fonte: a autora (2024)

Parizotto, Neves e Pinheiro (2022) exploram a relevância da perícia forense computacional na investigação de crimes, especialmente na luta contra a pornografia infantil. A perícia digital permite que especialistas coletem, preservem e analisem evidências eletrônicas, fundamentais tanto para crimes convencionais como para delitos virtuais, e atua como um apoio essencial na investigação de casos de exploração infantil online, que é amplamente priorizada devido à sua gravidade. Para a condução dessas investigações, é destacado no artigo o uso de ferramentas especializadas, como o FTK (Forensic Toolkit), que oferece agilidade na análise de dados, possibilita a recuperação de senhas e realiza a recuperação de blocos de dados. Já o Encase é amplamente utilizado para duplicação de conteúdos de dispositivos, análise de e-mails e recuperação de arquivos criptografados. Outra ferramenta essencial é o Autopsy, uma opção gratuita e intuitiva que opera em sistemas Linux e suporta análise de múltiplos sistemas de arquivos. Essas ferramentas permitem aos pe-

ritos acessar e examinar minuciosamente arquivos suspeitos, rastrear atividades e coletar provas digitais de maneira confiável e preservada, facilitando o processo judicial em crimes de pornografia infantil e outros delitos digitais.

Salih e Ibrahim (2023) analisam ferramentas de perícia digital usadas na coleta e análise de evidências eletrônicas para fins legais, abordando categorias como perícia computacional, de rede, ativa, de sistema operacional, de banco de dados e de e-mail. Entre as principais ferramentas, destaca o Stellar e o Forensic Tool Kit (FTK) para recuperação de dados e criação de imagens de disco, o Nmap para análise de redes, o OSF-Mount para análise ativa de RAM e registros, e o Autopsy, uma ferramenta de código aberto útil para recuperação de dados. A aplicação da Inteligência Artificial (IA) também é explorada, especialmente para analisar dados de dispositivos IoT, com algoritmos como Decision Stump e Bayes Net, este último eficaz na detecção de padrões suspeitos em redes. Desafios como o aumento do volume de dados, ambientes IoT e nuvem, e a necessidade de ferramentas avançadas para big data também são destacados. O artigo sugere a necessidade de aprimorar técnicas de IA para ambientes complexos e desenvolver métricas para validar a eficácia das ferramentas de perícia digital, contribuindo para o entendimento do papel crucial da IA na investigação criminal moderna.

Andrade (2024) revisa a aplicação da computação forense no combate aos crimes cibernéticos, destacando o papel das ferramentas gratuitas, como o Autopsy, no enfrentamento de atividades ilícitas online, incluindo a pornografia infantil. O estudo contextualiza a computação forense como essencial na coleta e análise de evidências eletrônicas, com ênfase na adaptação às tecnologias emergentes e na integração legal para garantir a segurança digital. Além disso, o artigo explora a complexidade dos crimes cibernéticos, abordando a pornografia infantil como uma das mais graves modalidades. Este crime envolve a produção, compartilhamento e armazenamento de imagens de exploração sexual infantil, demandando investigações meticulosas para identificação dos autores e contenção da distribuição dessas imagens. Andrade (2024) ainda enfatiza a necessidade de constante atualização das ferramentas e métodos forenses para garantir a integridade e eficácia na coleta de provas digitais, além de abordar os desafios legais e éticos que surgem na condução de investigações cibernéticas.

Gangwar *et al.,* (2021) discutem o uso da computação forense no combate a crimes cibernéticos, com foco em ferramentas para identificar material de abuso sexual infantil (*Child Sexual Abuse Material - CSAM*). Ele destaca o modelo AttM-CNN, baseado em aprendizado profundo, que identifica conteúdo pornográfico e classifica a idade de indivíduos, ajudando a detectar CSAM. Esse modelo é treinado com grandes bases de dados, como Pornography-2M e Juvenile-80k, para aprimorar a acurácia na identificação de conteúdos novos ou modificados. É ressaltado também o desafio do grande volume de dados digitais nas investigações e limitações das abordagens tradicionais, como a detecção por hash. A aplicação de redes neurais profundas é destacada como uma solução eficaz para agilizar a detecção de CSAM em bases de dados extensas, combinando detecção de pornografia e classificação etária para resultados mais precisos.

Westlake e Guerra (2023) abordam a aplicação de práticas de organização e nomeação de arquivos e pastas para melhorar a detecção automatizada de materiais de abuso sexual infantil (CSAM) na Dark Web. O estudo analisa 162 imagens conhecidas de CSAM e suas 7.289 exibições em 988 sites na Dark Web, destacando que a organização prevalece sobre tentativas de ocultação, com arquivos frequentemente organizados para facilitar o acesso dos usuários. Essa análise revela que, em vez de usar segurança avançada, os operadores priorizam termos explícitos e estruturações que facilitam a busca por esse material, com padrões comuns em URLs e nomes de arquivos que explicitamente indicam conteúdo de abuso infantil. Sugerem ainda que essas práticas de estruturação poderiam complementar ferramentas de detecção automatizadas já usadas, como o PhotoDNA, que se baseia em hashing. Ao incorporar padrões de nomeação e organização de arquivos e pastas, a detecção de CSAM previamente desconhecido pode ser melhorada, auxiliando as investigações. A análise também observa que muitos sites espelham seu conteúdo em domínios alternativos para manter a disponibilidade dos materiais em caso de remoção, uma prática que dificulta o combate efetivo à disseminação do CSAM na Dark Web.

Okutan e Çebi (2019) propõem um framework para investigar crimes cibernéticos, especialmente os que envolvem pornografia infantil. Ele aborda a coleta e preservação de evidências digitais, análise de dados e geração de relatórios, detalhando ferramentas como o EnCase para coleta forense de dados e o Guidance Software para monitoramento e resposta a ameaças. Também discute a importância de métodos de segurança, como firewalls e sistemas de prevenção de intrusão, para reduzir crimes cibernéticos. O estudo também destaca a necessidade de leis claras e cooperação internacional no combate à pornografia infantil online, bem como a atualização das tecnologias de detecção. Defende ainda a criação de centros especializados

e treinamentos para fortalecer investigações e proteger contra crimes digitais.

Sanchez *et al.,* (2019) exploram o uso de ferramentas forenses e tecnologias, como inteligência artificial (IA), para investigar material de abuso infantil (CSAM). Uma pesquisa com profissionais avaliou a eficácia dessas ferramentas, que incluem tecnologias para filtrar imagens e estimar idade, facilitando a triagem de grandes volumes de dados. O estudo também aborda desafios, como sobrecarga de trabalho e exposição a conteúdos traumáticos, e a necessidade de ferramentas mais precisas. O Autopsy é mencionado como uma ferramenta forense de código aberto, mas opções comerciais como Magnet Forensics e Cellebrite são mais comuns. Tecnologias que limitam a exposição ao CSAM são vistas como essenciais, embora ainda precisem melhorar em precisão e velocidade. O uso de IA para automatizar a detecção, como no kit iCOP, é destacado para aumentar a eficiência e reduzir a exposição dos profissionais. A pesquisa conclui que o desenvolvimento contínuo e a colaboração entre instituições são vitais para enfrentar os desafios das investigações de CSAM.

Sarkar e Shukla (2023) analisam o comportamento dos crimes cibernéticos e estratégias eficazes de policiamento, destacando desde a definição de tipologias até a criação de um framework para investigações. É abordado a utilização de artefatos digitais como evidências cruciais para rastrear e desmantelar crimes online, incluindo a pornografia infantil. O estudo enfatiza que investigações digitais eficazes dependem de métodos e ferramentas adequadas para coletar, analisar e preservar evidências, considerando as complexidades de crimes que atravessam fronteiras legais. Em relação à pornografia infantil, o artigo destaca os desafios na identificação e processamento de conteúdos ilícitos, ressaltando a necessidade de ferramentas de filtragem precisas e proteção para investigadores. A pesquisa reforça a importância de tecnologias avançadas para detectar crimes digitais de forma eficiente, além de promover a colaboração entre setores públicos e privados no combate a esses crimes.

CONSIDERAÇÕES FINAIS

A computação forense é uma área crucial no combate aos crimes digitais, especialmente em um cenário onde o ciberespaço se tornou palco para práticas ilícitas, como a disseminação de conteúdos de abuso e exploração infantil. Com o objetivo de coletar, preservar e analisar evidências digitais, os profissionais forenses dependem de ferramentas tecnológicas que viabilizam investigações precisas e eficientes. No entanto, o alto custo de muitas soluções avançadas limita seu acesso, especialmente para organizações com restrições orçamentárias. Nesse cenário, ferramentas forenses gratuitas surgem como alternativas importantes, permitindo que as investigações sejam conduzidas mesmo diante de limitações financeiras.

Essas ferramentas, como Autopsy, FTK, NuDetective e outras, demonstraram potencial para auxiliar na detecção, análise e combate às práticas criminosas que envolvem a produção e disseminação de imagens de abuso infantil. Além disso, estudos revisados destacam a eficácia de algumas dessas ferramentas na extração e preservação de evidências digitais, fundamentais para a condução de investigações.

Apesar das contribuições significativas das ferramentas gratuitas, é importante considerar que, em muitos casos, elas apresentam limitações em comparação com ferramentas pagas, especialmente em termos de recursos avançados, suporte técnico e atualizações. No entanto, quando bem utilizadas e combinadas com boas práticas de investigação, essas ferramentas podem desempenhar um papel crucial no enfrentamento desse tipo de crime.

Portanto, conclui-se, que a adoção de ferramentas forenses gratuitas, aliada à capacitação técnica dos profissionais e ao desenvolvimento de políticas públicas de combate à exploração infantil, representa uma estratégia viável e necessária no cenário atual. Em pesquisas futuras, sugere-se que seja realizada uma análise prática e comparativa dessas ferramentas, bem como estudos que avaliem sua aplicabilidade em diferentes contextos legais e investigativos.

REFERÊNCIAS

ALMEIDA, Jessica de Jesus *et al*. **Crimes cibernéticos.** Caderno de Graduação - Ciências Humanas e Sociais - UNIT – SERGIPE, Aracaju, v. 2, n. 3, mar., 2015. Disponível em: https://periodicos.grupotiradentes.com/cadernohumanas/article/view/2013/1217. Acesso em: 8 jun. 2024.

ANDRADE, Ingrid Lima de. **Forense digital aplicada ao combate de crimes cibernéticos:** uma revisão. *Revista Foco, Belo Horizonte*, v. 17, n. 7, p. 1-27, jul. 2024. DOI: 10.54751/revistafoco.v17n7-152. Disponível em: http://dx.doi.org/10.54751/revistafoco.v17n7-152. Acesso em: 15 nov. 2024.

AUTOPSY - THE SLEUTH KIT. **Autopsy.** 2003. Disponível em: https://www.sleuthkit.org/autopsy/. Acesso em 08 de maio de 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Promulgada em 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: < https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 01 jun. 2024.

BRASIL. Lei 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, DF, 11 jan. 2002. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm?ref=blog.suitebras.com>. Acesso em: 28 maio 2024.

BRASIL. Lei 11.829, de 25 de novembro de 2008. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, Brasília, DF, 26 nov. 2008. Disponivel em: <https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acesso em: 25 maio 2024.

BRASIL. Lei 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Alterada pela Lei 11.829, de 25 de novembro de 2008. **Diário Oficial da União**, Brasília, DF, 16 jul. 1990. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l8069compilado.htm>. Acesso em: 01 jun. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 06 de jul. 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm>. Acesso em: 03 jun. 2024.

BRASIL. Ministério da Saúde. Secretaria de Políticas para as Mulheres. Norma Técnica: Atenção Humanizada às Pessoas em Situação de Violência Sexual com Registro de Informações e Coleta de Vestígios. **Diário Oficial da União**, Brasília, DF, 2015. Disponível em:<https://bvsms.saude.gov.br/bvs/publicacoes/atencao_humanizada_pessoas_violencia_sexual_norma_tecnica.pdf>. Acesso em: 08 jun. 2024.
CASARIN, Helen de Castro Silva; CASARIN, Samuel José. **Pesquisa científica:** da teoria à prática. Curitiba: Intersaberes, 2012. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 19 abr. 2024.

CHAWKI, Mohamed; DARWISH, Ashraf; KHAN, Mohammad. **Cybercrime, Digital Forensics and Jurisdiction**. Londres: Springer, 2015. v. 593.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense**. São Paulo: Novatec, 2011.

EVARISTO, Tomás. **A cibersegurança aplicada no âmbito das PME's.** Santarém, 2022/2023 Dissertação (Mestrado em Engenharia de Tecnologias e Sistemas Web) - Instituto Superior de Gestão e Administração de Santarém. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/49385/1/Dissertacao_tomas_evaristo.pdf. Acesso em: 16 mai. 2024.

GALVÃO, Maria Cristiane; RICARTE, Ivan Luiz. **REVISÃO SISTEMÁTICA DA LITERATURA:** CONCEITUAÇÃO, PRODUÇÃO E PUBLICAÇÃO. Logeion: Filosofia da Informação, Rio de Janeiro, RJ, v. 6, n. 1, p. 57–73, 2019. DOI 10.21728/logeion.2019v6n1.p57-73. Disponível em: https://revista.ibict.br/fiinf/article/view/4835. Acesso em: 24 abr. 2024.

GANGWAR, Abhishek, *et al.* **AttM-CNN:** Attention and metric learning based CNN for pornography, age and Child Sexual Abuse (CSA) Detection in images. *Neurocomputing*, v. 445, p. 81–104, 2021. DOI: 10.1016/j.neucom.2021.02.056. Disponível em: https://doi.org/10.1016/j.neucom.2021.02.056. Acesso em: 5 nov. 2024.
GARCIA, Gustavo; MAZUI, Guilherme; PARREIRA, Marcelo. **Brasil registrou 202,9 mil casos de violência sexual contra crianças e adolescentes de 2015 a 2021, diz boletim**. Portal G1**,** Brasília, 18 de maio 2023. Disponível em:< https://g1.globo.com/politica/noticia/2023/05/18/brasil-registrou-2029-mil-

casos-de-violencia-sexual-contra-criancas-e-adolescentes-de-2015-a-2021-diz-boletim.ghtml>. Acesso em: 13 maio 2024.

KOOPS, Bert-Jaap, *et al*. **A typology of identity-related crime:** Information, Communication and Society. 2009. v. 12, p.1-24. Taylor & Francis Online, 2009. Disponível em: https://www.academia.edu/3327927/A_typology_of_identity_related_crime_conceptual_technical_and_legal_issues. Acesso em: 05 jun. 2024.

LEÃO, Lourdes Meireles. **Metodologia do estudo e pesquisa:** facilitando a vida dos estudantes, professores e pesquisadores. 1. ed. São Paulo: Vozes, 2016. *E-book.* Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 19 abr. 2024.

MARAS, Marie. **Computer forensics:** cybercriminals, laws, and evidence. 2. ed. Burlington: Jones Bartlett Learning, 2015.

MELO, Laerte Peotta de *et al*. **Minicursos do XI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais.** Brasília: Sociedade Brasileira de Computação – SBC, 2011. *E-book.* Disponível em: https://books-sol.sbc.org.br/index.php/sbc/catalog/view/95/424/695. Acesso em: 10 maio 2024.

MELO, Sandro. **Computação Forense Com Software Livre - Conceitos, Técnicas, Ferramentas e Estudos de Casos.** Rio de Janeiro: Alta Books, 2009.

MERCURI, Rebeca. **Challenges in Forensic Computing.** Communications of the ACM, ACM, v. 48, p. 17-21, 01 dez. 2005. Disponível em: https://dl.acm.org/doi/10.1145/1101779.1101796. Acesso em: 20 abr. 2024.
OLIVO, Cleber Kiel. **Avaliação de características para detecção de phishing de e-mail**. Curitiba, 2010 Dissertação (mestrado em Informática) - Pontifícia Universidade Católica do Paraná. Disponível em: https://www.inf.ufpr.br/lesoliveira/download/CleberOlivoMSC.pdf. Acesso em: 10 maio 2024.

OKUTAN, Ayşe; ÇEBİ, Yalçın. **A Framework for Cyber Crime Investigation**. *Procedia Computer Science*, Izmir, v. 158, p. 287-294, 2019. DOI: 10.1016/j.procs.2019.09.054. Disponível em: https://doi.org/10.1016/j.procs.2019.09.054. Acesso em: 1 nov. 2024.

PARIZOTTO, Lucas Serafim; NEVES, Antonio Lucas; PINHEIRO, Nicolli Rinaldi. **A importância da perícia forense computacional na investigação de crimes.** *In: II Congresso FatecSeg - Congresso de Segurança da Informação das Fatec*, 17 e 18 nov. 2022. DOI: 123456789/12551. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/12551. Acesso em: 10 nov. 2024.
PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** comentários à Lei n. 13.709/2018. 2. ed. São Paulo: Saraiva, 2020.
PINTO, A. **Ransomware:** uma ameaça cibernética em ascensão. *In:* CONGRESSO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E SISTEMAS COMPUTACIONAIS, 1., 2018, Santa Maria. **Anais Congresso Brasileiro de Segurança da Informação e Sistemas Computacionais.** Santa Maria: UFSM, 2018.

POLASTRO, Mateus Castro; ELEUTÉRIO, Pedro Monteiro. **NuDetective:** A forensic tool to help combat child pornography through automatic nudity detection. *In*: Workshops on Database and Expert Systems Applications, 2010, p. 349–353. Disponível em: https://doi.org/10.1109/DEXA.2010.74. Acesso em: 10 de maio de 2024.

POLÍCIA FEDERAL. **Projeto IPED**. Brasília, 2019. Disponível em: https://github.com/sepinf-inc/IPED. Acesso em: 16 maio 2024.

SAFERNET. **Safernet recebe recorde histórico de novas denúncias de imagens de abuso e exploração sexual infantil na internet.** SAFERNET, 2024. Disponível em: https://new.safernet.org.br/content/safernet-recebe-recorde-historico-de-novas-denuncias-de-imagens-de-abuso-e-exploracao-sexual. Acesso em: 8 maio 2024.

SALIH, Karam Muhammed Mahdi; IBRAHIM, Najla Badi. **Digital forensic tools:** a literature review. *Journal of Education and Science, Mosul*, v. 32, n. 1, p. 109-124, mar. 2023. DOI: 10.33899/edusj.2023.137420.1304. Disponível em: http://dx.doi.org/10.13140/RG.2.2.10098.48321. Acesso em: 15 nov. 2024.

SANCHEZ, Laura, *et al.* **A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM)**. *Digital Investigation*, v. 29, p. S124-S142, 2019. DOI: 10.1016/j.diin.2019.04.005. Disponível em: https://doi.org/10.1016/j.diin.2019.04.005. Acesso em: 1 nov. 2024.

SARKAR, Gargi; SHUKLA, Sandeep K. **Behavioral analysis of cybercrime:** Paving the way for effective policing strategies. *Journal of Economic Criminology*, v. 2, 2023. DOI: 10.1016/j.jeconc.2023.100034. Disponível em: https://doi.org/10.1016/j.jeconc.2023.100034. Acesso em: 3 nov. 2024.

SILVA FILHO, Wilson. **Crimes Cibernéticos e Computação Forense**. *In:* XVI SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, n. 1. 2016. Anais [...] Niterói: Sociedade Brasileira de Computação, 2016, p. 44-81. Disponível em: https://sbseg2016.ic.uff.br/pt/files/MC2-SBSeg2016.pdf. Acesso em: 2 maio 2024.

WESTLAKE, Bryce; GUERRA, Enrique. **Using file and folder naming and structuring to improve automated detection of child sexual abuse images on the Dark Web**. *Forensic Science International: Digital Investigation*, v. 47, p. 301620, 2023. DOI: 10.1016/j.fsidi.2023.301620. Disponível em: https://doi.org/10.1016/j.fsidi.2023.301620. Acesso em: 8 nov. 2024.