TÉCNICA OPERACIONAL DE ANÁLISE FORENSE COMPUTACIONAL: CARACTERIZAÇÃO

Moysés Pereira da Silva Costa[1]
Adriano Aleixo **Bossonaro**[2]

Idealizada acerca do contexto bélico e avanço tecnológico vivenciado pelos Estados Unidos da América, a Internet origina-se na década de sessenta, com a idealização da Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos (DARPA). Seu precípuo objetivo era coibir todo e qualquer tipo de intervenção em suas comunicações durante a Guerra Fria.

Em decorrência da premente necessidade de segurança, foi criado um sistema informacional integrado, independente e distribuído, sem localização geográfica definida, que não permitisse sua completa destruição.

Neste sentido, paralelo aos fins militares, modernos sistemas computacionais foram desenvolvidos, visando um incremento tecnológico para melhorar o relacionamento intersocial favorável à política, cultura, medicina, entretenimento, educação e economia, dentre outras áreas, sendo este conjunto muitas vezes utilizado pelo Estado como forma de expansão de sua soberania.

Findada a Segunda Guerra Mundial, o homem associou as telecomunicações aos recursos computacionais, gerando uma nova área do conhecimento humano, denominada Tecnologia da Informação.

Originou-se então, por meio da expansão daquela, a concepção de Globalização Informacional, acarretando o entendimento de que a evolução tecnológica é capaz de transpor barreiras geográficas.

No contexto desta Revolução Informacional, surgiram novos métodos, técnicas e tecnologias para a comunicação e armazenamento de dados digitais. Estes se desenvolveram rapidamente desde a segunda metade da década de setenta e, com maior ênfase, nos anos noventa. A conversão das informações para o formato digital e a comunicação em rede foram utilizadas para maximizar as capacidades das pessoas, que aderiram gradativamente aos computadores pessoais e smartphones. O advento destes, ressaltando a forma como foram utilizados pelos governos, empresas, indivíduos e setores sociais, possibilitou o surgimento da Sociedade da Informação.

A partir de então, a tecnologia da informação se transformou na base de todos os ramos do conhecimento, impondo uma dependência cada vez maior à sociedade.

A consequente popularização das ferramentas e serviços disponibilizados por estas tecnologias ocasionaram grande alteração comportamental dos indivíduos, que passaram ao uso indiscriminado destas facilidades informatizadas, atingindo um

1 Oficial de Infantaria do Exército Brasileiro, Academia Militar das Agulhas Negras, Especialista em Ciências Militares - moyses.psc@gmail.com
2 Oficial de Infantaria do Exército Brasileiro, Academia Militar das Agulhas Negras, Mestre em Ciência da Computação - bossonaro@uol.com.br

nível extremo de onipresença da informática em seu cotidiano, caracterizando assim, a evolução da Computação Ubíqua[3].

Nesta perspectiva, os recursos computacionais pessoais, empresariais, financeiros, institucionais e governamentais se tornaram importante base de informações, caracterizando uma nova fonte voltada para Atividade de Inteligência, denominada Fonte Cibernética. O Manual MD 35-G-01 define Fonte Cibernética como:

> Recurso por intermédio do qual se pode obter dados no Espaço Cibernético utilizando-se ações de busca ou coleta, normalmente realizadas com auxílio de ferramentas computacionais. A Fonte Cibernética poderá ser integrada a outras fontes (Humanas, Imagens e Sinais) para produção de conhecimento de Inteligência. (BRASIL, 2015, p. 119).

Com o objetivo de melhor explorar as potencialidades desta nova fonte de informações pela Atividade de Inteligência, verificou-se a necessidade de implementar e adaptar procedimentos capazes de atender às demandas especificamente técnicas de tal ambiente. Desta demanda nasceu a Inteligência Cibernética.

Apesar das lacunas conceituais na área da disciplina de Inteligência Cibernética, procedimentos operacionais para a exploração de sua principal fonte já têm sido realizados. Dentre estes, destaca-se a Análise Forense Computacional, cuja precípua finalidade é a obtenção de dados a partir do fluxo de informações em redes de computadores e/ou de dispositivos de armazenamento computacionais.

Com características próprias, a exploração da Fonte Cibernética constitui um novo desafio para a Atividade de Inteligência, demandando a caracterização de Técnicas Operacionais para a busca de dados protegidos.

3 Computação Ubíqua: tem como objetivo tornar invisível a interação entre homem e computador, ou seja, integrar a informática com as ações e comportamentos naturais das pessoas. O termo "invisível" deve ser entendido como uma forma em que as pessoas não percebam que estão dando comandos a um computador, mas sim como se tivessem conversando com alguém.

Considerando que o ambiente operacional de Inteligência Cibernética é o Espaço Cibernético, um ambiente ainda bastante desconhecido, surge o seguinte questionamento: Poderíamos de fato considerar a Análise Forense Computacional como Técnica Operacional de Inteligência Cibernética?

1. A INTELIGÊNCIA E SUA DISCIPLINA CIBERNÉTICA

O termo Inteligência tem significados diversos, que estão associados a uma área ou tema específico. Legg e Hutter (2006) descrevem vários conceitos acerca do termo Inteligência, segundo diferentes áreas de pesquisa, como: definição coletiva, definição segundo a psicologia e definição na perspectiva dos pesquisadores de inteligência artificial.

Nesse trabalho foram consideradas as definições coletivas, que procuram dar uma ideia mais apropriada ao foco do estudo em pauta. Dessas definições, segundo Soares Júnior (2013), destaca-se a seguinte conceituação chancelada por 52 (cinquenta e dois) especialistas.

> Inteligência é a capacidade geral que, entre outras coisas, envolve a habilidade do raciocínio, do planejamento, da solução de problemas, do pensamento abstrato, da análise de ideias complexas, da apreensão rápida e da aprendizagem pela experiência. (GOTTFREDSON, 1997, p. 13).

Portanto, Inteligência constitui a habilidade humana de processar dados e produzir novos conhecimentos por meio do raciocínio. A capacidade cognitiva humana é limitada e isso acarreta a necessidade do uso de metodologias específicas, de forma dedicada a essa atividade, quando em situações complexas, como pode ser observado nos governos e instituições militares (JÚNIOR, 2013).

No âmbito militar brasileiro, o Ministério da Defesa publicou a Portaria Normativa nº 9/GAP/MD, de 13 de janeiro de 2016, conhecida como Manual MD 35-G-01 (Glossário das Forças

Armadas). Nela consta que a Inteligência é o ramo da Atividade de Inteligência de Defesa, responsável pela produção de conhecimentos relativos a fatos e situações atuais ou potenciais que afetem o processo decisório. Neste sentido a referida norma também aduz que:

> INTELIGÊNCIA MILITAR - É a atividade técnica-militar especializada exercida em caráter permanente, que visa a produzir conhecimentos para apoiar o planejamento e o processo decisório dos comandantes (em qualquer nível hierárquico) e de seus Estados-Maiores, bem como proteger conhecimentos sensíveis sobre a tropas amigas, impedindo seu acesso pela Inteligência oponente/ adversa. (BRASIL, 2015, p. 149).

Nesta senda, a Atividade de Inteligência tem por finalidade produzir e salvaguardar conhecimento de interesse. Desdobra-se em dois grandes segmentos: Inteligência, objetivamente voltado para a produção de conhecimentos; e Contrainteligência, objetivamente voltado para a salvaguarda de conhecimentos (BRASIL, 2015a, p. 40).

Com a finalidade de apoiar a produção de conhecimento, são realizadas Operações de Inteligência, que podem ser representadas por um conjunto de ações de busca, com o emprego de técnicas operacionais e meios especializados, planejado e executado com vistas à obtenção de dados de interesse dos trabalhos desenvolvidos pela Atividade de Inteligência, visando ao atendimento de seus usuários (BRASIL, 2015a, p. 193). Insta ressaltar que o MD35-G-01(2015, p. 50) apresenta a ação de busca como a "atividade sigilosa voltada para a obtenção de dados não disponíveis e protegidos por medidas de segurança estabelecidas por quem os detém e exige, para sua execução, pessoal especializado e emprego de técnicas operacionais".

Segundo o Manual EB20-MF-10.107 (Inteligência Militar Terrestre), as operações de inteligência pressupõem disciplinas que compreendem os meios, sistemas e procedimentos utilizados para observar, explorar, armazenar e difundir informação referente à situação, ameaças e outros fatores do entorno operativo. No escopo deste trabalho, o ambiente operacional, caracterizado pelo Espaço Cibernético, está diretamente relacionado à disciplina de Inteligência Cibernética, cujos conhecimentos são elaborados a partir de dados, protegidos ou não, obtidos no referido ambiente. Ressalta-se que a utilização da Fonte Cibernética na Atividade de Inteligência já tem previsão normativa na Política Cibernética de Defesa:

> São objetivos da Política Cibernética de Defesa: [...] colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) [...].Diretrizes atinentes ao Objetivo Nr III - colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o SINDE e para os órgãos envolvidos com a SIC e Segurança Cibernética, em especial o GSI/PR: a) Adequar a doutrina de Inteligência de modo a inserir a fonte cibernética no contexto da integração de fontes de dados visando à produção de conhecimento; b) criar estruturas de Inteligência Cibernética, conforme a necessidade dos órgãos centrais de Inteligência das FA e do SMDC, para aplicar métodos científicos e sistemáticos, buscando extrair e analisar dados oriundos da fonte cibernética, produzindo conhecimento de interesse; [...] (BRASIL, 2012, p.13-20).

Com relação à disciplina de Inteligência Cibernética, Mota *et al* (2014, p. 19) cita Mandarino Júnior quando ressalta que esta "exerce papel fundamental nos ambientes de Segurança, Defesa e Guerra Cibernética. Ela é essencial na busca de informações, empregando todas as fontes disponíveis, para identificar e prevenir ameaças cibernéticas e proporcionar respostas mais adequadas, com oportunidade". Assim, considerando a multidisciplinaridade do tema em pauta, serão apresentados a seguir, alguns conceitos considerados relevantes acerca da Ciência Cibernética.

2. CIBERNÉTICA: A CIÊNCIA E O AMBIENTE OPERACIONAL

Preliminarmente, há de se enfatizar que a etimologia do termo "cibernética" tem origem na palavra grega *kybernetes,* que está relacionada com a arte do timoneiro, sendo a ciência geral dos sistemas de informação (SILVA, 2015).

Segundo Marcelo Xavier de Freitas Crespo (2011, p.45), a "[...] cibernética é a ciência que trata das matérias, do cérebro, do sistema nervoso do homem, buscando descobrir seu funcionamento, analisando, de forma crítica e profunda, o modo de realização das coisas."

É, portanto, a ontologia que busca entender as comunicações e os sistemas que controlam não só as pessoas como também as máquinas, mas que precisam da ação humana para funcionar. Possui como principal fundamento a interação entre sistemas de controle e processamento de informações entre máquina, seres vivos e sociedade (SILVA, 2015).

Assim, observa-se que em um sistema computacional, sob a ótica da cibernética, o homem alimenta a máquina com dados, que irá produzir um resultado ocasionado em função desde comando humano. Esse processo, alcançado pela vontade humana através do cérebro e da máquina, pode ser denominado cibernética (CRESPO, 2011).

No campo da Defesa Cibernética, cuja responsabilidade foi delegada pelo Presidente da República, por meio do Decreto nº 6.703/2008 (Estratégia Nacional de Defesa) ao Exército Brasileiro, observa-se que foco similar é dado ao conceito de Cibernética. A Doutrina Militar de Defesa Cibernética diz que o "[...] termo se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação." (BRASIL, 2014, p.18).

Neste sentido, pode-se inferir que a Ciência Cibernética busca entender os aspectos atinentes à comunicação, caracterizada pela transmissão e recebimento de informações, e seu funcionamento, englobando seres humanos e máquinas, que possuem sistemas capazes de fazer circular as informações. Este conjunto de humanos e dispositivos computacionais é conhecido como Espaço Cibernético, ou simplesmente Ciberespaço.

Um conceito interessante acerca do Ciberespaço é apresentado por Patrícia Santos da Silva, tendo como base a definição da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO):

> O ciberespaço é um novo ambiente humano e tecnológico de expressão, informação e transações econômicas. Consiste em pessoas de todos os países, de todas as culturas e linguagens, de todas as idades e profissões fornecendo e requisitando informações; uma rede mundial de computadores interconectada pela infraestrutura de telecomunicações que permite à informação em trânsito ser processada e transmitida digitalmente. (SILVA, 2015, p. 70).

Outra consideração importante refere-se à concepção de que o Espaço Cibernético não é, de fato, considerado como território fisicamente delimitado. Este ambiente é caracterizado especificamente pelo fluxo de informações por intermédio de redes informatizadas. Com isso, o que se caracteriza como extremamente importante é a localização da informação, tendo em vista ser esta a indicadora do território, sendo preciso considerar ainda que as ações hostis realizadas nesse ambiente cibernético têm caráter transnacional, fato esse que vem a exigir dos países maior compromisso para combater em conjunto esse novo tipo de delinquência (CRESPO, 2011).

No contexto militar, o MD35-G-01 - Glossário das Forças Armadas (2015a, p. 106) traz uma conceituação de Espaço Cibernético, que se caracteriza por ser um "[...] espaço virtual, composto

por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas".

O conceito acima nos permite inferir que o Espaço Cibernético considera tanto o fluxo de informações nas redes informatizadas, quanto seu armazenamento físico em dispositivos *standalone*[4]. É fato que as informações em fluxo no espaço cibernético têm caráter transnacional. Neste sentido, considerando o escopo de atuação da atividade operacional de Inteligência Cibernética, torna-se extremamente importante a possibilidade de produção de conhecimentos a partir de informações fisicamente armazenadas. Para isso, é premente a necessidade de procedimentos operacionais sistemáticos e bem definidos, com vistas à obtenção do dado protegido no espaço cibernético, em sua vertente não conectada em redes computacionais, que caracteriza a delimitação desta pesquisa.

3. A FORENSE COMPUTACIONAL

No que tange à exploração de informações fisicamente armazenadas em um dispositivo computacional, a Ciência Forense[5] foi pioneira.

A Forense Computacional é uma área do conhecimento que surgiu a partir da necessidade dos tribunais de justiça, com vistas ao uso de evidências obtidas por meio da análise de dispositivos computacionais. É, portanto, uma área originária da interseção de outras duas grandes áreas do conhecimento humano: a Ciência da Computação e a Ciência Jurídica (RUBACK, 2011).

O pesquisador Brian Carrier adota a definição utilizada pela *High Technology Investigative Unit* do Departamento de Justiça dos Estados Unidos, que apresenta a forense em computadores como o processo de identificar evidências potenciais em meios eletrônicos para serem utilizadas em tribunais de Justiça. Ele envolve a preservação, extração, documentação e interpretação de dados de computadores. Em complemento, evidência digital é um objeto digital que contém informação confiável que apoia ou refuta uma hipótese (CARRIER, 2005, p. 21).

Desta forma, verifica-se que a Forense Computacional é caracterizada pelo uso de técnicas cientificamente testadas e comprovadas para a preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais provenientes de Fontes Cibernéticas. Sua finalidade é facilitar ou promover a reconstrução de eventos ou antecipar atos ou ações não autorizadas que se mostrarem prejudiciais para as operações planejadas ou que reflitam em determinado cenário ou conjuntura (PALMER, 2001).

Ressalta-se ainda que tais técnicas demandam cuidados com vistas à preservação de um aspecto judicial relevante, denominado Cadeia de Custódia. Esta pode ser caracterizada como o registro do rastreamento da evidência desde sua fonte original até o que é oferecido como evidência em um tribunal, demonstrando que a evidência coletada é autêntica (SCHWEITZER, 2003).

Com vistas a premente necessidade de se estabelecer um conjunto ordenado de procedimentos para padronizar o processo de perícias computacionais, várias metodologias foram criadas (CARROLL; BRANNON; SONG, 2008). A seguir, serão sumariamente apresentadas as principais idéias de algumas das metodologias implementadas nesta área, ao longo dos anos. A apresentação destes

4 No contexto deste trabalho, dispositivos *standalone* são dispositivos computacionais autossuficientes, ou seja, seu funcionamento não necessita de conexão com a Internet ou qualquer outro tipo de conexão de rede. Pode ser entendido como um computador isolado, que mantém suas funcionalidades convencionais.

5 A Ciência Forense é compreendida como o conjunto de todos os conhecimentos científicos e técnicas que são utilizados para elucidar incidentes, crimes e diversos outros assuntos legais nas esferas cível, penal ou administrativa. É considerada uma ciência multidisciplinar que envolve diferentes áreas do conhecimento humano.

modelos é importante para que se possa identificar os procedimentos comuns a estas metodologias.

3.1 Modelo de Pollitt

Mark Pollitt[6] (1995), apresentou um modelo baseado no fato de que as evidências digitais devem ter credibilidade, bases sólidas estabelecidas, dúvidas completamente dirimidas e ainda devem ser afastadas quaisquer inseguranças existentes.

O pesquisador supracitado enfatiza que a cadeia digital que compõe o arquivo digital precisa passar por um processo de aquisição e conversão para então dar origem a um formato inteligível. Somente depois deste momento é que um avaliador, após identificar algo possivelmente relacionado ao quesito apurado, julgará se a informação contida no arquivo identificado é relevante (COSTA, 2012).

Neste sentido, Pollitt propõe uma metodologia baseada em 4 (quatro) fases: **Aquisição** tem o objetivo de alcançar as provas digitais, utilizando recursos que devem obedecer às regras definidas pela lei; A fase de **Identificação**: tem o objetivo de converter a cadeia binária que dá origem ao arquivo para um formato compreensível ao leigo; A fase de **Avaliação**: tem o objetivo de determinar se a informação contida no arquivo digital é relevante; A fase de **Admissão**: tem o objetivo de apresentar a prova propriamente dita (POLLIT, 1995).

3.2 Modelo de Palmer

De acordo com Gary Palmer[7] (2001), houve a necessidade de se conceber um modelo de processo genérico e aplicável a grande parte das investigações envolvendo sistemas digitais e ambientes computacionais.

O modelo descrito por Gary Palmer é composto por 7 (sete) fases: a fase de **Identificação** consiste da detecção do evento, monitoramentos de eventos e auditoria de fatos; a fase de **Preservação** consiste da gestão do caso, cadeia de custódia, geração de imagens forenses; a fase de **Coleta** consiste da obtenção da autorização legal, do uso de técnicas de recuperação, preservação, adoção de software e hardwares apropriados, utilização de métodos confiáveis e técnicas de recuperação; a fase de **Exame** consiste da preservação do material a ser examinado, na aplicação de técnicas de filtragem e pesquisas e na descoberta de dados ocultos; a fase de **Análise** consiste da busca pela descoberta da prova do evento; a fase de **Apresentação** consiste da documentação dos trabalhos e formalização da prova; a fase de **Decisão** consiste da avaliação final dos trabalhos investigatórios (PALMER, 2001).

3.3 Modelo de Carrier

Adotando como premissa que cada dispositivo computacional traduz a própria cena do objeto da investigação em si, o modelo forense proposto por Brian Carrier (2005) oferece uma alternativa de abordagem em análises periciais. O pesquisador traz para a Forense Computacional a Teoria de *Locard*[8], afirmando que condutas que se utilizam de computadores deixam rastros perceptíveis aos investigadores (CARRIER, 2005).

O modelo proposto por Brian Carrier é estruturado da seguinte forma: a fase de **Prontidão** tem por objetivo alcançar uma infra estrutura capaz de suportar a investigação; a fase de **Implantação** tem por objetivo fornecer os meios para que o incidente seja identificado, representando o início da investigação, propriamente dita; a fase de **Investigação da Cena do Crime** visa coletar e analisar os vestígios e reconstituir as ações

6 Doutor em Tecnologia pela Universidade da Florida Central - EUA (2013). Foi Agente Especial do *Federal Bureau of Investigation* (FBI) e Diretor do Programa de Forense Computacional do FBI.

7 Analista e pesquisador da MITRE Corporation - Cyberforensics Science & Technology Center. A MITRE é uma organização sem fins lucrativos que opera centros de pesquisa patrocinados pelo governo dos EUA.

8 Em síntese, esta teoria preconiza que qualquer pessoa, ao entrar em um local de crime, deixa algo novo na cena e, ao retirar-se, leva consigo algo que lá estava, mesmo que não tenha esta intenção.

que aconteceram durante o incidente; a fase de **Investigação da Cena de Crime Digital** se inicia quando dispositivos computacionais são coletados na cena do crime ou quando comunicações telemáticas relacionadas ao delito são interceptadas. Esta fase aborda um computador como uma cena do crime onde vestígios digitais devem ser procurados. Os pesquisadores enfatizam que a condução dessa fase deveria ser realizada por alguém tecnicamente capacitado, especialista em ferramentas e técnicas forenses (COSTA, 2012).

3.4 Modelo de Kent

Os pesquisadores Kent, Chevalier, Grance e Dang (2006) propuseram um modelo forense composto de 4 (quatro) fases: na fase de **Coleta**, os equipamentos referentes a um evento específico são identificados, rotulados, registrados e recolhidos, preservando-os em relação a sua integridade; na fase de **Exame**, as ferramentas forenses e técnicas adequadas são empregadas para identificar e extrair dados dos materiais coletados; a fase de **Análise** envolve a avaliação dos resultados obtidos na fase de exame para alcançar informações relacionadas aos fatos e alvos; a fase de **Relatório** tem por objetivo explicitar os resultados dos exames (COSTA, 2012).

Diante do exposto pelos modelos apresentados acima e, diante do que foi verificado na literatura disponível, de maneira geral, essas metodologias são basicamente compostas por 04 (quatro) etapas e o processo tende a ser interativo, podendo ser repetido quantas vezes for necessário. A seguir, serão sumariamente apresentadas cada uma dessas etapas, nas palavras de Evandro Pereira[9] (2007, p. 18):

> • **Coleta dos dados**: Os dados relativos ao evento digital são coletados com foco na sua integridade. O material é identificado, embalado, etiquetado e registrado;
> • **Exame dos dados**: Ferramentas são selecionadas e técnicas de operação são elencadas, a fim de identificar e extrair os dados relevantes. Existe a preocupação constante em manter a integridade dos dados;
> • **Análise das informações**: É realizada a análise dos dados, com o objetivo de obter informações relevantes ao caso. A identificação de vínculos entre as informações de interesse deve ser observada;
> • **Interpretação dos resultados**: ocorre a geração de relatórios que contém, além dos resultados obtidos, as técnicas e procedimentos realizados.

A concepção de um modelo pericial está relacionada ao seu emprego. Cada proposta possui características que atendem a certas particularidades. No segmento policial, por exemplo, as exigências legais são significativas, enquanto que as atividades correlatas à Inteligência necessitam de informações que permitam produzir conhecimentos consistentes.

Nesta perspectiva, verificou-se a necessidade de se analisar os aspectos relativos às duas principais abordagens relativas à Forense Computacional, quais sejam: a Análise Forense Computacional e a Perícia Forense Computacional, com vistas a identificar suas diferenças sob o prisma da caracterização destes procedimentos como Técnica Operacional de Inteligência Cibernética. A fim de subsidiar a caracterização em questão, serão apresentados a seguir conceitos relativos às Técnicas Operacionais de Inteligência.

4. TÉCNICAS OPERACIONAIS DE INTELIGÊNCIA

O termo "técnica" advém do grego *téchne*, que significa arte ou ciência. De fato, uma técnica pode ser entendida como procedimentos que visam a obtenção de um determinado resultado científico ou tecnológico, em qualquer outra área do conhecimento humano.

Uma técnica pode ser caracterizada como um conjunto de regras, normas ou protocolos por meio do qual pode se chegar a uma determinada meta e pressupõe que, em situações semelhantes, uma mesma conduta produzirá o mesmo efeito desejado ou semelhante. Assim, esta refere-se ao ordenamento de uma forma de atuação ou de um conjunto de ações.

9 PEREIRA, Evandro; et al. **Forense Computacional**: Fundamentos, tecnologias e desafios atuais. VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Rio de Janeiro, 2007.

Na disciplina de Inteligência Cibernética, as técnicas operacionais requerem o uso de ferramentas, habilidades e conhecimentos bastante variados. Estas surgem da necessidade de não modificar, sempre que possível, o Espaço Cibernético[10], adaptando-se às suas peculiaridades.

Técnica Operacional é um termo tradicionalmente utilizado pelo Sistema Brasileiro de Inteligência (SISBIN) para designar determinada prática ou procedimento empregado pelo segmento operacional nas atividades de busca do dado protegido, enquadradas em uma Operação de Inteligência (BRASIL, 2015a).

Neste sentido, faz-se necessário definir que fontes protegidas são aquelas cujos dados não estão disponíveis a qualquer pessoa e, normalmente, necessita de técnicas apropriadas para que se tenha acesso a eles. Paralelamente, é importante conceituar também o termo "busca", que compreende a atividade sigilosa voltada para a obtenção de dados não disponíveis e protegidos por medidas de segurança estabelecidas por quem os detém. Exige, para sua execução, pessoal especializado e emprego de técnicas operacionais (BRASIL, 2015a, p. 50).

Aos moldes do que ocorre nas demais disciplinas, as operações no âmbito da Inteligência Cibernética podem ser classificadas como exploratórias, quando de caráter eventual, proporcionando dados de inteligência sobre um assunto específico em um determinado momento, ou sistemáticas, quando de caráter contínuo, com fim de produzir um fluxo constante de dados e informações sobre um fato ou situação, cuja evolução deve ser acompanhada (BRASIL, 2015a, p. 51).

Assim, com amparo nos conceitos e definições apresentados acima, serão apresentadas idéias relativas ao emprego dos procedimentos de Forense Computacional, buscando caracterizá-los como Técnica Operacional de Inteligência Cibernética.

10 Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas. (MD35-G-01, 2015, p. 106).

5. FORENSE COMPUTACIONAL COMO TÉCNICA OPERACIONAL DE INTELIGÊNCIA CIBERNÉTICA

Preliminarmente, das pesquisas realizadas na literatura, foram observadas 2 (duas) grandes vertentes da Forense Computacional como ciência, quais sejam: Perícia Forense Computacional e Análise Forense Computacional.

Para que se possa caracterizar os procedimentos de Análise Forense Computacional como Técnica Operacional de Inteligência Cibernética, são necessárias algumas reflexões acerca dos principais aspectos de sua diferenciação. Esses aspectos são apresentados a seguir.

5.1 Aspecto Jurídico

Considerando o Espaço Cibernético, o primeiro aspecto a ser observado na diferenciação entre Análise Forense e Perícia Forense está relacionado ao aspecto jurídico que as envolve, principalmente com relação à necessidade de sua validade como prova judicial.

Para Marinoni e Mitidiero (2011), a prova judicial pode ser entendida como um meio retórico, regulado pela legislação, destinado a convencer o Estado da validade de proposições controversas no processo, dentro de parâmetros fixados pelo direito e de critérios racionais.

Neste sentido, observa-se que a prova judicial é tudo o que pode influenciar na formação da convicção do magistrado para decidir acerca de uma demanda judicial, desde que respeitados os parâmetros legais (MACHADO, 2009).

A técnica de Forense Computacional, em sua vertente pericial, tem a finalidade de levar ao juiz os elementos de convicção, formais e constituídos na forma da lei, sobre fatos que dependem de conhecimentos especificamente técnicos, isto é, juízos de valor especializados sobre os fatos relevantes da causa (MARINHO, 2011).

Assim, a Perícia Forense Computacional deve subministrar ao processo a experiência técnica, para que seja empregada na dedução judicial e só é necessária no meio jurídico quando a prova do fato depender de conhecimento técnico ou científico específico (MORO, 2005).

Esta deve então se valer de dispositivos que permitam garantir que a prova judicial apresentada não foi adulterada. Um destes dispositivos é a Cadeia de Custódia, que contribui para a validação da prova pericial e o seu respectivo laudo, que será gerado posteriormente.

Da mesma forma, na Atividade de Inteligência Cibernética, a finalidade da Análise Forense Computacional é produzir conhecimentos baseados em elementos de convicção importantes a partir de dados técnico-computacionais. Ressalta-se, porém, que as questões relativas à manutenção destas salvaguardas legais são minimizadas em prol da velocidade na obtenção do dado protegido, caracterizando maior observância do Princípio da Oportunidade em detrimento dos aspectos jurídicos formais.

5.2 Aspecto de Pessoal

Outro importante aspecto a ser considerado refere-se ao recurso humano destinado à realização da Forense Computacional em ambas as vertentes consideradas. De maneira geral, os profissionais responsáveis pelos procedimentos de investigação computacional devem ser absolutamente imparciais e possuir sólidos conhecimentos e habilidades técnicas especializadas nesta área do conhecimento.

Com relação à Perícia Forense Computacional, os trabalhos devem ser realizados por perito legalmente constituído. Assim, nos termos do Código de Processo Civil[11] brasileiro, nas demandas judiciais em que a matéria envolvida exija conhecimentos técnicos ou científicos próprios de determinada área do conhecimento, o magistrado deve ser assistido por perito ou órgão para isso competente. Ambos, perito ou órgão, devem ser nomeados entre os profissionais legalmente habilitados e os órgãos técnicos ou científicos devidamente inscritos em cadastro mantido pelo Judiciário (BRASIL, 2015c).

No mesmo dispositivo da legislação supracitada, retrata-se também o caso de não existência de perito ou órgão inscrito no cadastro de peritos judiciais. Nesta hipótese, a referida legislação permite que o magistrado escolha livremente um profissional ou órgão que, comprovadamente, detenha conhecimento especializado para a realização da Forense Computacional (BRASIL, 2015c).

Outra questão que merece destaque é a aplicação dos motivos de impedimento e suspeição dos magistrados aos peritos, conforme consta nos termos dos Artigos 148 e 467 do Código de Processo Civil, preservando assim o Princípio da Imparcialidade. Nesta senda, existem situações em que os peritos judiciais podem se encontrar e que comprometa a imparcialidade do processo. Assim, é necessária a operacionalização de seu afastamento da atividade pericial em que esteja envolvido. Como exemplo, pode ser citada a atuação do perito como mandatário de qualquer uma das partes envolvidas na disputa, vínculo de amizade com qualquer das partes, a situação de herdeiro, donatário ou empregador de uma das partes do processo, dentre outras.

Em contrapartida, no campo da Inteligência Cibernética, a Análise Forense Computacional pode ser realizada por qualquer agente de inteligência, com a finalidade de obtenção do dado e produção de conhecimento. É necessário que o agente de inteligência seja habilitado para realizar operações de inteligência e desejável que possua habilidades técnicas computacionais.

É importante ressaltar que, pela natureza da atividade, o Sistema de Inteligência possui órgãos com níveis técnico-operacionais ciberneticamente distintos. Assim, as fases do processo de Análise Forense Computacional podem ser realizadas por diferentes profissionais. Um agente de inteligência,

11 Código de Processo Civil, instituído pela Lei nº 13.105, de 16 de março de 2015.

por exemplo, pode realizar as atividades de coleta de dados e evidências por meio da produção de imagens dos dispositivos de armazenamento computacional e repassar este material para uma equipe de analistas mais capacitada, para que seja realizada a busca do dado protegido nas melhores condições. Essa transmissão de encargos certamente não é permitida ao perito judicial, vez que o mesmo é formalmente nomeado para tratar da perícia em voga e deve pessoalmente prestar contas ao juízo competente.

Neste sentido, outra característica que diferencia um agente de inteligência de um perito forense é o fato de não haver a necessidade do primeiro ser devidamente inscrito como perito nos quadros da Instituição. Na Atividade de Inteligência, como foi dito, todos os agentes operacionais têm condições de participar de pelo menos uma fase do processo de Análise Forense Computacional, contribuindo para a realização do processo nas melhores condições.

5.3. Aspecto Temporal

Segundo Rossi[12] (2016), o principal objetivo que orienta a atividade pericial é encontrar, tempestivamente, respostas conclusivas para os quesitos formulados pelo juiz ou pelas partes de uma demanda judicial.

Naturalmente, ao iniciar seu trabalho, o perito judicial se debruça sobre o objeto da perícia buscando responder tudo que lhe foi indagado, devendo concluir seus trabalhos dentro do prazo fixado pelo magistrado, incluída sua eventual prorrogação. Porém, uma vez concluídas as diligências periciais, caso não haja a apresentação por completo, ou a mera apresentação intempestiva das respostas, ocasionará prejuízo às partes litigantes, comprometendo a segurança e o resultado útil do processo judicial (ROSSI, 2016).

Com efeito, ressalta-se que a ausência da manifestação do perito quanto aos quesitos, mesmo que haja um complemento tardio das respostas, pode ocasionar nova perícia, interferindo nos prazos e provocando uma dilação no tempo do processo. Em outras palavras, quando o resultado da Forense Computacional é imprescindível, o tempo processual pode ser delongado até que as conclusões técnicas possam ser recebidas e analisadas no processo judicial em curso (ROSSI, 2016).

Concorrentemente, quando se trata da Análise Forense Computacional na disciplina de Inteligência Cibernética, ocorre o mesmo fenômeno apresentado por Rossi (2016), caracterizado pela busca do dado protegido de forma tempestiva. No entanto, a necessidade de inteligência demanda que o agente de inteligência sempre atenda ao Princípio da Oportunidade, resguardada sua segurança pessoal e a segurança do próprio Sistema de Inteligência, visto que, de forma contrária ao preconizado pela legislação relativa à Perícia Forense Computacional, não há forma de se suspender ou adiar a prossecução dos eventos ou incidentes alvo de uma Operação de Inteligência.

5.4 Aspecto Procedimental

No que tange aos aspectos procedimentais, é basilar que a Forense Computacional seja realizada a partir de uma prova devidamente armazenada sob custódia de um agente autorizado.

Segundo Machado (2009, p. 18), a Cadeia de Custódia é procedimento preponderante para a garantia e transparência da prova material, sendo relato fiel de todas as ocorrências da evidência, vinculando os fatos e criando um lastro de autenticidade jurídica entre o evento, o autor e a vítima.

Nos termos da Perícia Forense Computacional, a Cadeia de Custódia é constituída por uma série

12 Carlos Alberto Del Papa Rossi é advogado, especialista em Direito Processual Civil (PUC/SP).

de atos interligados, que visa dar segurança e confiabilidade ao processo em que os vestígios estão submetidos, bem como a manutenção de sua integridade. Neste sentido, todos os atos devem ser registrados, inclusive os profissionais que preservaram o local e os que manusearam as provas desde a coleta, passando pelo transporte e recebimento pelos órgãos de perícia oficial e seu armazenamento (MARINHO, 2011).

Na seara da Atividade de Inteligência, a preservação da Cadeia de Custódia não é exigida nestes termos. Existe a preocupação no sentido de manter o ambiente operacional inalterado, mas as questões jurídicas desta salvaguarda não são normalmente levadas em consideração. Apesar disso, seria desejável tal conduta, vez que os achados da Análise Forense Computacional podem direcionar o decisor no sentido de uma demanda investigatória formal, como é o caso do Inquérito Policial Militar (IPM), ou até mesmo de uma ação judicial, onde tais provas necessitariam das garantias fornecidas pela Cadeia de Custódia.

Outro aspecto importante refere-se ao fato de que o perito judicial tem liberdade para escolher as técnicas e ferramentas que serão utilizadas na atividade de perícia, devendo respeitar os limites de seu encargo, sendo vedada a apresentação de opiniões pessoais que excedam ao que é balizado pelo exame técnico ou científico do objeto da perícia (BRASIL, 2015c).

Na esfera da Perícia Forense Computacional, o perito deve relatar detalhadamente, por meio de linguagem simples, a forma como desenvolveu seu trabalho técnico ou científico, de modo a permitir que o juiz e as partes do processo compreendam todos os fundamentos que o levaram a uma determinada conclusão. O método utilizado para o trabalho técnico-pericial, com os devidos esclarecimentos e demonstrações, deve ser predominantemente aceito pela comunidade de especialistas da área computacional (ROSSI, 2016).

Em contrapartida, sob o prisma da Atividade de Inteligência, o agente executa o processo de Análise Forense Computacional, visando identificar e correlacionar as evidências em busca da verdade real, relatando o conhecimento produzido já classificado segundo as Técnicas de Avaliação de Dados[13] (TAD). Assim, o emprego da clareza e objetividade na redação dos conhecimentos de inteligência são requisitos necessários tanto na área da perícia legal, como na área da análise forense como técnica de inteligência cibernética em dispositivos computacionais.

Com relação ao resultado do trabalho, na Perícia Forense o perito judicial expressa suas conclusões em um laudo pericial, que deve ser entregue no cartório judicial, e tem o potencial de influenciar decisivamente o magistrado na formação de sua convicção. A prova pericial, materializada no laudo pericial, não tem caráter vinculante, cogente, obrigatório ao juiz. Este poderá formar a sua convicção com outros elementos ou fatos provados nos autos. Conforme o Princípio da Persuasão Racional, o juiz apreciará livremente a prova, atendendo aos fatos e circunstâncias constantes dos autos, devendo indicar na sentença, os motivos que lhe formaram o convencimento. Entretanto, a prática tem demonstrado que os juízes se têm vinculado à prova pericial (ROSSI, 2016).

Em contrapartida, na Análise Forense realizada em proveito da Atividade de Inteligência, o resultado do trabalho é apresentado por meio da confecção de um Conhecimento de Inteligência, que representa o fato ou a situação de interesse para a Atividade de Inteligência, produzido mediante a aplicação de metodologia própria.

13 Técnica de Inteligência que possibilita a avaliação de dado por meio do julgamento da fonte e do julgamento de seu conteúdo. O julgamento da fonte tem a finalidade de estabelecer o grau de sua idoneidade e o julgamento do conteúdo representa o grau de veracidade do dado (MD35-G-01, p. 266).

5.5 Aspecto da Publicidade

Na Perícia Forense Computacional, a publicidade é de vital importância para atender aos Princípios do Contraditório e da Ampla Defesa. As partes sempre serão intimadas do local e da data de início da perícia, que serão fixados pelo juiz ou indicados pelo perito, incumbindo a este o dever de comunicar, com antecedência mínima de 05 (cinco) dias, todas as diligências e exames que tiver que realizar, garantindo aos assistentes técnicos de cada parte, total acesso e integral acompanhamento dos trabalhos periciais (BRASIL, 2015c).

Aos assistentes técnicos das partes é facultada a utilização de todos os meios necessários para a defesa dos interesses dos litigantes, obtendo informações, solicitando vistas de documentos, bem como instruir o laudo com planilhas, mapas, plantas, desenhos, fotografias ou outros elementos necessários ao esclarecimento do objeto da perícia (BRASIL, 2015c).

Diversamente, no trabalho de Análise Forense Computacional, realizado por um agente de inteligência, o sigilo é fundamental. As atividades são norteadas pela prudência, sensatez e discrição durante toda a operação, caracterizando uma postura contrária ao que deve seguir o perito judicial.

Em suma, observa-se que, apesar das diferenças substanciais acerca dos aspectos jurídico, de pessoal, temporal, procedimental e de publicidade que orbitam as áreas da Perícia Forense Computacional, no cenário judicial, e Analise Forense Computacional, no cenário da inteligência, é fato que ambas as atividades são realizadas por intermédio de um conjunto de procedimentos técnicos com objetivos bem definidos.

Quando se tratou da Análise Forense Computacional, restou claro que o conjunto de procedimentos realizados para sua execução em busca do dado protegido, aliado aos protocolos típicos da Atividade Operacional de Inteligência, com a finalidade de produzir conhecimentos de inteligência adequadamente classificados quanto à idoneidade de sua fonte, bem como à veracidade dos fatos descritos, pode caracterizá-la como uma Técnica Operacional de Inteligência Cibernética.

6. CONCLUSÃO

A popularização das tecnologias computacionais tem acarretado extrema mudança no comportamento do ser humano, vez que este passou a recorrer forma repousada e com habitualidade aos recursos informatizados disponíveis no seu cotidiano, para a realização de tarefas que variam de uma simples produção de um texto à mais complexa operação financeira.

Neste sentido, os recursos computacionais pessoais, institucionais e governamentais se tornaram importante base de conhecimento, da qual se pode obter informações utilizando-se de Operações de Inteligência Cibernética, realizadas por intermédio de técnicas especializadas e ferramentas informatizadas. A esta nova fonte de dados, deu-se o nome de Fonte Cibernética.

Da imprescindibilidade da exploração das novas potencialidades da fonte supracitada, adveio a necessidade de se implementar e adaptar procedimentos adequados para atender as demandas eminentemente técnicas a partir do Espaço Cibernético.

Nestes termos, a técnica de Análise Forense Computacional foi adotada pelo segmento operacional da Inteligência Cibernética, visando, em regra, a obtenção de dados protegidos a partir de dispositivos de armazenamento computacionais. Isso demandou a fusão de protocolos típicos da Atividade Operacional de Inteligência, com a finalidade de permitir o uso desta técnica, de forma segura pelos agentes, na busca do dado protegido em prol da potencialização da qualidade na produção de Conhecimentos de Inteligência.

Neste trabalho de pesquisa, foram apresentadas diferenças e semelhanças entre a Perícia Forense Computacional e a Análise Forense Computacional aplicada na Inteligência Cibernética, considerando aspectos judiciais, de pessoal, temporal e procedimental. Em síntese, verificou-se que as modalidades de investigação computacional supracitadas empregam diferentes paradigmas conforme a área de atuação.

Na esfera judicial, o perito deve ser legalmente constituído e segue uma rigorosa linha de procedimentos normatizados, direcionados à restrita produção de respostas aos quesitos apresentados. Apesar da existência de prazos formalmente definidos, pode haver dilações, influenciando na duração do processo judicial. Adicionalmente, os peritos são submetidos às formalidades da Cadeia de Custódia e, após a produção do laudo pericial, é protocolarmente necessária a apresentação das técnicas utilizadas para a consecução das conclusões elencadas, devendo estas serem avalizadas pela comunidade técnica-computacional e aceitas pelo magistrado e pelas partes do processo, nos termos da lei. Além disso, é extremamente necessário que todas as atividades do perito judicial sejam públicas, permitindo às partes o contraditório e a ampla defesa.

Concorrentemente, na seara da Inteligência Cibernética, o agente não é cerceado, de forma direta, pelos preceitos e restrições legais de suas ações, o que lhe permite maior versatilidade na busca do dado protegido, sem, contudo, menosprezar os protocolos de segurança da Atividade Operacional de Inteligência. O agente aplica, com sigilo e discrição, a técnica de Análise Forense Computacional visando busca do dado protegido com a flexibilidade de produzir conhecimentos adjacentes e correlatos ao assunto principal, atendendo ao Princípio da Amplitude. Apesar de não haver as formalidades legais da Cadeia de Custódia, é desejável que o agente envide esforços no sentido de não modificar o ambiente operacional, com vistas na possibilidade de existir posterior demanda judicial.

Assim, de acordo com as perspectivas apresentadas sobre a operacionalização da Análise Forense Computacional em prol da busca do dado protegido, agregado à constante preocupação em manter inalterado, sempre que possível, o ambiente operacional, incrementada ainda pelos protocolos típicos da Atividade Operacional de Inteligência, visando a produção de Conhecimentos de Inteligência, segundo metodologia específica, deve caracterizá-la como uma Técnica Operacional de Inteligência Cibernética.

REFERÊNCIAS

BRASIL. Congresso Nacional. Câmara dos Deputados. Comissão Parlamentar de Inquérito dos Crimes Cibernéticos: Relatório Final. Câmara dos Deputados, Brasília, 2016.

_____. Estado-Maior Conjunto das Forças Armadas. MD 35-G-01: Glossário das Forças Armadas. Exército Brasileiro: Brasília, 2015.

_____. Estado-Maior do Exército. EB20-MF-10.107: Inteligência Militar Terrestre. Exército Brasileiro: Brasília, 2015.

_____. IP 30-1 (reservada): Atividade de Inteligência Militar-1ª Parte (Conceitos Básicos). Brasília, 1995.

BRASIL. Ministério da Defesa. Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014. Doutrina Militar de Defesa Cibernética (MD31-M-07). Brasília, 2014.

_____. Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012.Política Cibernética de Defesa. Brasília, 2012.

BRASIL. Presidência da República. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Brasília, 2015.

_____. Presidência da República. Decreto nº 6.703, 18 dez. 2008. Estratégia Nacional de Defesa. Brasília, 2008.

CARRIER, Brian. File System Forensic Analysis. 1 ed. Addison-Wesley, 2005. ISBN 978-0321268174.

CARROLL, O. L; BRANNON, S. K; SONG, T. Computer Forensics: Digital Forensic Analysis Methodology. The United States Attorneys Bulletin, 2003. Disponível em: <http://www.justice.gov/usao/eousa/foia_reading_room/usab5601.pdf>. Acesso em: 22 abr. 2017.

COSTA, Levi Roberto. Metodologia e Arquitetura para Sistematização do Processo Investigatório de Análise da Informação Digital. Dissertação Mestrado. UNB: Brasília, 2012.

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

GOTTFREDSON, Linda Susanne. Mainstream science on intelligence: An editorial with 52 signatories, history and bibliography. University of Delaware, 1997. Disponível em: <http://www.udel.edu/educ/gottfredson/reprints/1997mainstream.pdf>. Acesso em: 15 abr. 2017.

JÚNIOR, Raphael Mandarino; CANONGIA, Claudia. Segurança Cibernética: O desafio da Nova Sociedade da Informação. Brasília/DF, v. 14, n. 29, p. 21-46, jul./dez., 2009.

JÚNIOR, Vandir Pereira Soares. O Sistema de Inteligência no Nível Operacional: o apoio à decisão na Era do Conhecimento. 2013. Tese (Doutorado em Ciências Militares)-Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2013.

KENT, K., CHEVALIER, S., GRANCE, T., e DANG, H. Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86. Gaithersburg: National Institute of Standards and Technology, 2006.

LEGG, Shane; HUTTER, Marcus. A Collection of Definitions of Intelligence. 2006. Disponível http://www.vetta.org/documents/A-Collection-of-Definitions-of-Intelligence.pdf. Acesso em: 1º abr. 2017.

MACHADO, Margarida Helena Serejo. A Regulamentação da Cadeia de Custódia na Ação Penal: Uma necessidade Premente. Corpo Delito, nº1, p. 18-23. Brasília, 2009.

MARINHO, Girlei Veloso. Cadeia de Custódia da Prova Pericial. 2011. Dissertação (Mestrado)-Escola de Administração Pública/Fundação Getúlio Vargas (FGV), Rio de Janeiro, 2011.

MARINONI, Luiz Guilherme; MITIDIERO, Daniel.Código de Processo Civil comentado. 3 ed. São Paulo: Editora RT, 2011.
MORO, Rolando Raul. Prova Pericial. Revista Páginas de Direito, nº 276, Porto Alegre.Publicado em 27 de junho de 2005. Disponível em: <http://www.tex.pro.br/home/artigos/101-artigos-jun-2005/5245-prova-pericial-cpc-arts-420-a-439>. Acesso em: 29 abr. 2017.

MOTA, Marcel Francisco de Souza; REZENDE, Claubert Santos de; GONÇALVES, Marco Aurélio. O Perfil do Militar de Inteligência Cibernética. Revista Lucerna, Brasília, ano 3, n. 5, 2014.

PALMER, Gary. A Road Map for Digital Forensic Research. Report from the First Digital Forensic Research Workshop (DFRWS).New York, 2001. Disponível em: http://www.dfrws.org/2001/dfrws-rm-final.pdf. Acesso em 22 abr. 2017.

POLLITT, Mark. Computer Forensics: anApproach to Evidence in Cyberspace. Proceeding of the National Information Systems Security Conference,p. 487-491. Baltimore, MD. 1995.

REITH, M., et al. An Examination of Digital Forensic Models International. 2002. Disponível em: <www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6F2 C1-98F94F16AF57232D.pdf>. Acesso em: 1º abr. 2017.

ROSSI, Carlos Alberto Del Papa. Prova pericial no novo CPC. Publicado em 19 maio 2016. Disponível em: <http://gilbertomelo.com.br/prova-pericial-no-novo-cpc>. Acesso em: 29 abr. 2017.

RUBACK, Marcelo Caldeira. Mineração de Dados Aplicada à Construção de Bases de Hash em Computação Forense. 2011. Dissertação (Mestrado)-Universidade de Brasília, Brasília, 2011.

SCHWEITZER, D. Incident Response: Computer Forensic Toolkit. Wiley, 2003. ISBN 978-0764526367.

SILVA, Patrícia Santos. Direito e Crime Cibernético: Análise da Competência em Razão do Lugar no Julgamento de Ações Penais. Brasília: Vestnik, 2015.