RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano V, v.1, n.1, jan/julho 2025. | submissão: 09/05/2025 | aceito: 11/05/2025 | publicação:13/05/2025

Investigação criminal sobre meios digitais

Criminal investigation on digital media

Investigación criminal en medios digitales

Raúl de Miguel Benjamim Jofrisse Nhamitambo[1]

RESUMO

A presente pesquisa tem por fim abordar sobre Investigação Criminal sobre Meios Digitais. A investigação criminal é a actividade que compreende o processo de deteção, recolha de indícios e provas que, nos termos da lei processual penal, visa averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade, no âmbito de um processo judicial. Deve referir-se que a investigação criminal só existe como tal no âmbito de um processo de natureza penal. num Estado de direito, a validade dos novos meios de obtenção de prova propiciados pela evolução tecnológica não se dá de forma automática. Pelo contrário, estes, pela sua lesividade, encontram-se cobertos por uma intransponível proibição de prova, requerendo uma intervenção legislativa no sentido de os prever em norma clara, expressa e determinada, com um regime jurídico denso e autónomo, para que a sua utilização de se torne admissível e a prova obtida por via desse surja como legítima.

Palavras-chave: Investigação criminal; agentes e a sua responsabilidade; processo judicial; Meios Digitais.

ABSTRACT

This research aims to address Criminal Investigation on Digital Media. Criminal investigation is the activity that comprises the process of detection, collection of evidence and proof that, according to the criminal procedural law, aims to ascertain the existence of a crime, determine its agents and their responsibility, within the scope of a judicial process. It should be mentioned that criminal investigation only exists as such within the scope of a criminal process. In a State of law, the validity of new means of obtaining evidence provided by technological evolution does not occur automatically. On the contrary, these, due to their harmfulness, are covered by an insurmountable prohibition of evidence, requiring legislative intervention in order to provide

[1] Doutor em Ciências Jurídicas, pela Universidade Para La Cooperación Internacional México (UCIMEXICO) – México (2020); Mestre em Assessoria Jurídica de Empresas, pela Universidad a Distancia de Madrid (UDIMA) - Madrid (2016); Licenciado Ciências Jurídicas e Investigação Criminal, pelo extinto Instituto Superior de Ciências e Tecnologia Alberto Chipande (ISCTAC) – Beira (2011); Advogado e Membro da Ordem dos Advogados de Moçambique (desde Abril de 2018); Professor Auxiliar de Direito das Tecnologias de Informação e Comunicações (Direito das TIC's) – na Universidade Joaquim Chissano (UJC) – Maputo (desde Fevereiro de 2020), no Curso de Licenciatura em Engenharia de Tecnologias e Sistemas de Informação; Professor Auxiliar de Direito Administrativo e Noções de Direito Administraticvo – na Universidade Pedagógica de Maputo (UP - Maputo), nos Cursos de Licenciaturas em Gestão de Recursos Humanos e Gestão Pública e Educacional; Técnico Superior de Assistência Jurídica – Gabinete Jurídico (UP - Maputo); Docente Universitário de Introdução ao Direito, Direito Administrativo I e II e, Direito de Trabalho, nos Cursos de Licenciatura em Direito, Contabilidade e Auditoria e, Administração Pública e Autárquica – no Instituto Superior Maria Mãe de África (ISMMA); Professor Auxiliar no Instituto Superior de Contabilidade e Auditoria de Moçambique (ISCAM), leccionando a disciplina Complementos de Fiscalidade no Curso de Mestrado em Auditoria; Autor, Revisor, Avaliador Externo e Parecista na Revista Científica Multidisciplinar O Saber (desde II Semestre de 2024); Autor, Avaliador e Parecista na Revista Multidisciplinar RECIMA21 (desde I Semestre de 2025) e na Revista Internacional Consinter de Direito (Conselho Internacional de Estudos Contemporâneos em Pós-Graduação – CONSINTER), desde II Semestre de 2025 e Organizador da Editora Científica Digital (Desde I Semestre de 2025). Matola – Maputo. ORCID: 0009-0006-4118-1970. rnhamitambo@gmail.com.(+258) 872058783/847417800.

for them in a clear, express and determined norm, with a dense and autonomous legal regime, so that their use becomes admissible and the evidence obtained through them appears legitimate.
Keywords: criminal investigation; agents and their responsibility; judicial process; Digital Media.

RESUMEN
Esta investigación tiene como objetivo abordar la Investigación Criminal en Medios Digitales. La investigación criminal es la actividad que comprende el proceso de detección, recolección de evidencia y prueba que, de acuerdo con el derecho procesal penal, tiene como objetivo determinar la existencia de un delito, sus agentes y su responsabilidad, en el ámbito de un proceso judicial. Cabe mencionar que la investigación criminal solo existe como tal en el ámbito de un proceso penal. En un Estado de derecho, la validez de los nuevos medios de obtención de prueba proporcionados por la evolución tecnológica no se produce automáticamente. Por el contrario, estos, debido a su lesividad, están cubiertos por una prohibición probatoria insalvable, requiriendo la intervención legislativa para preverlos en una norma clara, expresa y determinada, con un régimen jurídico denso y autónomo, para que su uso sea admisible y la prueba obtenida a través de ellos parezca legítima.
Palabras - clave: investigación criminal; agentes y su responsabilidad; proceso judicial; Medios Digitales.

INTRODUÇÃO

No presente trabalho abordaremos sobre Investigacao Criminal sobre Meio Digital. Constitui um truísmo afirmar o extenso âmbito da utilização de sistemas informáticos no quotidiano de cada cidadão na sociedade moderna, sendo igualmente evidente que, com a utilização destes dispositivos, cada um de nós deixa uma espécie de rasto ou pegada digital, composta pelos inúmeros dados informáticos criados a cada momento e a cada passo no uso de tecnologias de informação e comunicação[2].

Pelo seu potencial relevo probatório, a obtenção destes dados, processados, armazenados e comunicados por sistemas e redes informáticas, e da informação neles contida, poderá ser – e, tendo em conta a ubiquidade destas tecnologias e a constante digitalização da sociedade, as

[2] Este rasto ou pegada digital é constituído pelos vestígios criados como resultado da utilização das tecnologias de informação e comunicação, pode ser activo (ou evitável) – composto por dados providenciados pelo utilizador – ou passivo (ou inevitável) – composto por dados obtidos e registados pelo dispositivo sem qualquer acção do utilizador –, e, tendo em conta a multiplicidade das informações processadas, armazenadas e transmitidas pelos sistemas e redes informáticas, pode conter inúmera informação relevante sobre o seu utilizador e as suas características pessoais e sobre a sua utilização do sistema. Assim, UNODC, «Introduction to digital forensics», em Sharing Electronic Resources and Laws on Crime, disponível em https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-4/index.html, acessado em 01 de Maio de 2025.

mais das vezes efectivamente será[3] – do interesse da investigação criminal e da realização da justiça.

Segundo Nhamitambo (2025), o Governo de Moçambique está também plenamente consciente da ameaça e dos efeitos negativos do crime informatico ou cibernético sobre a sua Nação e por isso tem sido feito esforços para garantir que hajam instrumentos que possam proteger o cidadão e penalizar os que cometem estes crimes com recurso as TIC's. Estes esforços incluem:

- ✧ O Código Penal, aprovado pela Lei n.º 24/2019, publicada no dia 24 em Dezembro de 2019, que cobre os Crimes informáticos, a saber: Pornografia de menor (artigo 211), Utilização de menores em pornografia (artigo 212), Distribuição ou posse de pornografia de menores (artigo 213), Devassa da vida privada (artigo 252), Violação de correspondência ou de comunicações (artigo 253), Base de dados automatizada (artigo 254), Acesso ilegítimo (artigo 256), Gravações ilícitas (atigo 257), Furto de fluidos (artigo 276), Burla informática e nas comunicações (artigo 289), Fraudes relativas aos instrumentos e canais de pagamento electrónico (artigo 294), Abuso de meios de pagamento electrónicos (artigo 295), Falsidade informática (artigo 336), Interferência em dados (artigo 337), Interferência em sistemas (artigo 338), Uso abusivo de dispositivos (artigo 339), Instigação pública a um crime (artigo 345), Apologia pública ao crime (artigo 346), Publicidade da decisão condenatória (artigo 448);
- ✧ Lei das Transacções Electrónicas, aprovado pela Lei n° 3/2017, de 9 de Janeiro, que visa proteger os consumidores e regular o uso de sistemas electrónicos no Governo, sector privado e sociedade civil;
- ✧ Regulamento de controlo de Tráfego de Telecomunicações, aprovado pelo Decreto n.º 75/214, de 12 de Dezembro;
- ✧ Regulamento de Segurança de Redes de Telecomunicações, aprovado pelo Decreto 66/2019, de 1 de Agosto;
- ✧ Regulamento de Registo de Cartões SIM, aprovado pelo Decreto 18/2015, de 28 de Agosto;

[3] Segundo DAVID SILVA RAMALHO, Métodos Ocultos de Investigação em Ambiente Digital, Almedina, 2017, p. 102, a prova digital está, actualmente, presente na generalidade dos processos de natureza penal. Já PEDRO DIAS VENÂNCIO, «A prova digital e a digitalização da prova», em Boletim da Ordem dos Advogados, n.º 57, 2009, p. 33, afirma que «o futuro da Justiça está intimamente ligado à prova digital». Por sua vez, JOÃO CONDE CORREIA, «Prova digital: as leis que temos e a lei que devíamos ter», em Revista do Ministério Público, n.º 139, 2014, p. 55, constata que esta constitui hoje «o cerne da prova».

- ✧ Regulamento de Registo e Licenciamento de Provedores Intermediários de Serviços Electrónicos e de Operadores de Plataformas Digitais, aprovado pelo Decreto n° 59/2023 de 27 de Outubro;
- ✧ Regulamento de Protecção do Consumidor do Serviço de Telecomunicações, aprovado por Decreto 44/2019, de 22 de Maio;
- ✧ Lei de Telecomunicações, Lei n.º 4/2016, de 3 de Junho.

Segundo Nhamitambo (2025), Crime ou delito é o facto voluntário declarado punível pela lei penal, nos termos do art. 1 do CP.

Segundo Marques e Martins (2000, p.493) citado por Nhamitambo (2025), "crime informático é todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é o alvo desse acto."

A pesquisa é qualitativa e com método bibliográfico.

EMBASSAMENTO TEÓRICO

O cibercrime: a relevância moderna da prova digital

A prova digital é, e cada vez mais será, um meio de prova fulcral que poderá existir e ser necessário obter em processos relativos a todo e qualquer tipo de crime. No entanto, é inegável que existe uma relação umbilical e inextricável entre a prova digital e o fenómeno da cibercriminalidade, uma vez que esse tipo de prova é fundamental na investigação deste, ocorrendo ambos no mesmo ambiente digital, e que os meios de obtenção de prova digital.

Assim, é mister procedermos a uma breve análise do fenómeno do cibercrime, da sua importância actual e da evolução legislativa a nível nacional e internacional no combate a esse.

A ciência forense digital: princípios e procedimentos para uma válida e eficaz recolha de prova digital

Estabelecida a natureza sui generis da prova digital, a sua complexidade técnica e a sua importância hodierna, facilmente se compreende a necessidade do surgimento de uma área especializada para lidar com este meio de prova: a ciência forense digital, o ramo das ciências forenses dedicada à utilização de métodos cientificamente comprovados para a identificação,

aquisição, preservação, análise e apresentação de dados com relevo probatório processados, armazenados ou transmitidos por sistemas informáticos – em geral, para o procedimento de obtenção de prova digital –, em função dos propósitos da investigação criminal e da realização da justiça e com respeito pela legislação vigente[4].

Actualmente, é praticamente unânime que a obtenção deste meio de prova, para se mostrar válida aos olhos da ciência forense digital e, consequentemente, admissível em tribunal com plena força probatória, deve orientar-se em virtude de quatro máximas: a legalidade da actuação de todos os intervenientes; a existência de treino apropriado e de apoio especializado de forma a mitigar a complexidade técnica; a preservação da integridade dos dados informáticos na sua forma original e inalterada; e a documentação de todo o procedimento e manutenção da cadeia de custódia que consigam garantir a autenticidade da prova em Tribunal.

Quanto à legalidade do procedimento de obtenção de prova digital, a entidade à qual incumbe a direcção da investigação criminal é responsável por assegurar o pleno cumprimento da lei aplicável ao longo de todo o procedimento, bem como o cumprimento dos requisitos do princípio da proporcionalidade e o respeito pelos direitos, liberdades e garantias dos visados.

Quanto à especialização, sempre que o responsável pela investigação criminal se depare, ou seja expectável que vá deparar-se, com prova digital no curso dessa, deverá notificar um especialista (ou uma equipa especializada) em ciência forense digital de forma atempada e, se possível, assegurar a sua presença no procedimento, de forma a garantir o seguimento das melhores práticas internacionais nesta área ao longo de todo o procedimento; este apoio especializado deverá, naturalmente, estar constantemente actualizado e ciente dos novos desenvolvimentos na área e ser dotado de recursos e equipamentos adequados à complexidade técnica do procedimento. Adicionalmente, qualquer participante no manuseamento da prova digital deverá ter a formação necessária para tal, nomeadamente nos casos em que não é possível a presença no local de um perito em tempo útil, devendo ainda tal formação ser extensível a qualquer interveniente processual, de modo que estes detenham conhecimento

[4] Definição adaptada de DIGITAL FORENSIC RESEARCH WORKSHOP, «A road map for digital forensics», em Proceedings of the Digital Forensic Research Conference, 2001, p. 16. COE, EEG, pp. 135-137 subdivide este ramo em computer forensics – focada especificamente em computadores –, mobile forensics – focada em sistemas informáticos móveis, como smartphones e wearables –, network forensics – focada em redes informáticas –, e embedded forensics – focada em sistemas integrados, como os pertencentes à Internet-of Things, dispositivos de smart home, e sistemas electrónicos de automóveis –, cada uma com os seus conhecimentos especializados devido ao quão diferente é o procedimento de obtenção de prova em cada um deles. Em sentido similar, MÁRIO ANTUNES / BALTAZAR RODRIGUES, Introdução à Cibersegurança, 2.ª ed., FCA Editora, 2022, p. 149.

técnico suficiente para poder detectar qualquer irregularidade procedimental que possa comprometer o valor probatório da prova digital apresentada em tribunal e, assim, aferir da validade desta.

Quanto à preservação da integridade da prova, deve-se evitar que qualquer acção tomada ao longo do procedimento seja passível de alterar quaisquer dados informáticos no sistema objecto da diligência, priorizando-se realização de uma cópia integral (bit stream imaging)[5] de todo o suporte de armazenamento do mesmo, cumulada com a utilização de um bloqueador de escrita (write-blocker)[6], cópia essa que deverá depois ser alvo de um método de verificação de integridade (checksum, hashing ou digital fingerprinting)[7] e de assinatura digital[8], e sobre a qual incidirão as restantes providências a ser tomadas na apreensão e análise de concretos dados informáticos, de forma a garantir a autenticidade destes e a diminuir a ocorrência de evidence dynamics (a ocorrência de qualquer influência que altere, obscureça ou oblitere a prova, independentemente da intenção, no período que intermedeia a sua aquisição e a sua apresentação em tribunal).

Quanto à documentação e manutenção da cadeia de custódia, é crucial que todas as fases do procedimento sejam meticulosamente documentadas pelo investigador responsável, efectuando nomeadamente a identificação dos sistemas relevantes, o registo dos dados informáticos obtidos, a descrição dos métodos, técnicas e ferramentas utilizados na aquisição e análise desses, e a forma como foram preservados durante todo este trâmite. A documentação elaborada será a principal fonte de comprovação da conformidade com os princípios que norteiam a obtenção de prova digital, da validade das diligências efectuadas e da admissibilidade e valor da prova obtida, devendo permitir que o procedimento seja externamente auditável98, sendo também com base nesta que será elaborado o relatório final.

---

[5] Isto é, a criação de uma cópia exacta (ou duplicação), bit-por-bit do conteúdo do suporte de armazenamento original e de todos os dados neste contidos (inclusive os de natureza temporária e volátil).

[6] Um dispositivo ou um programa informático que impede a alteração de qualquer dado informático durante o processo de duplicação ou cópia, um passo necessário devido ao conteúdo volátil da memória do sistema, que se pode modificar com qualquer operação efectuada.

[7] Que corresponde à atribuição de um valor único ao clone obtido no processo de duplicação, calculado pelo computador através de uma função criptográfica, e que permite garantir que não ocorre qualquer modificação do mesmo, uma vez que o valor resultante do cálculo aos dados alterados seria completamente diferente, mesmo que essa modificação se resumisse a um bit, permitindo assim verificar posteriormente que não ocorreu qualquer alteração e que a imagem forense é uma cópia exacta do suporte original.

[8] O investigador deve, por esta forma, autenticar que todos os dados informáticos foram, à sua responsabilidade, obtidos em conformidade com as exigências técnicas e científicas vigentes na área a cada momento.

Quanto à prova digital em si, os critérios gerais de admissibilidade técnica desta contendem principalmente com[9] a sua integridade, autenticidade, fiabilidade e credibilidade: esta deve ser obtida do modo menos intrusivo possível e preservada durante todo o procedimento, não devendo a forma como foi recolhida, manuseada, preservada e analisada lançar qualquer dúvida sobre a veracidade da mesma; os dados gerados pelo utilizador devem poder ser atribuídos a este e os dados gerados pelo sistema devem poder ter-se como resultantes do funcionamento adequado desse no momento em que foram produzidos, devendo comprovar-se que ambos estes foram recolhidos mediante a utilização de métodos de preservação que impeçam uma qualquer modificação dos mesmos; a informação obtida deve estabelecer os factos de uma forma que seja representativa do seu estado original e, como tal, indisputável, e deve ser persuasiva quanto aos factos que representa de modo a poder ser reputada como verdadeira pelos intervenientes processuais ao ponto de fundamentar uma decisão judicial.

RESULTADOS E DISCUSSÃO

Classificação dos Crimes Informaticos

Segundo Nhamitambo (2025), **Crimes informáticos puros**, segundo Amabélia Chuquela, são aqueles em que a utilização do sistema informático é o meio necessariamente utilizado para a prática delitiva.

Crimes Informáticos impuros, segundo Amabélia Chuquela, são aqueles em que a utilização do sistema informático trata-se apenas de um novo modus operandi.

No nosso entender, **Crimes informáticos puros ou próprios** são aqueles em que foram legislados pela primeira na lei penal, no momento em que nasce os delitos cometidos pelo computador e sem o uso deste, não existiria. E, **Crimes informáticos impuros ou impróprios** são aqueles em que os delitos já existiam antes da tipificação dos crimes informáticos. Para a existência dela, o agente activo ou o criminoso apenas usa uma nova forma de executar o crime, uma nova táctica.

[9] Consoante o modelo seguido, a divisão poderá ser diferente, situando-se um ou outro acto em localizações diferentes. Em sentido similar ao que aqui seguimos, ANTUNES / RODRIGUES, Cibersegurança, cit., pp. 154 155 e RAMALHO, Métodos Ocultos, cit., pp. 111 e ss. RODRIGUES, Prova Penal IV, cit., pp. 497 e ss. apresenta um «modelo dinâmico-reversivo» próprio, mas cujas fases, em termos gerais, também aqui se enquadrariam.

Várias são as classificações doutrinárias sobre os crimes informáticos ou virtuais. Duas categorias são utilizadas: a dos crimes informaticos próprios ou puros e a dos crimes informáticos impróprios ou impuros.

Barreto e Brasil (2016, p.17) citado por Nhamitambo (2025), conceituam crime virtual próprio como aqueles em que o dispositivo informatizado e/ou seu conteúdo é o alvo dos criminosos - os sistemas informatizados, bancos de dados, arquivos ou terminais (computadores, smartphones, tablets) são atacados por criminosos, normalmente após a identificação de vulnerabilidades, seja por meio de programas maliciosos ou por engenharia social (golpista engana a vítima, fazendo com que forneça informações pessoais e/ou estratégicas).

Para Albuquerque (2006, p.168) citado por Nhamitambo (2025), os crimes virtuais impuros "diriam respeito aos crimes em que os recursos informáticos constituem o meio de execução, tendo como objecto bens jurídicos que já são protegidos por tipos penais existentes". Na sociedade da informação, a incidência de ilícitos penais "têm por objecto material ou meio de execução o objecto tecnológico informático: hardware, software, redes, etc.

Investigação criminal sobre meios digitais

Segundo Delbono (2018), "**informática forense, cómputo forense, computação forense, análise ou exame forense digital** é a aplicação de técnicas científicas e analíticas especializadas a infraestruturas tecnológicas que permitem identiifcar, preservar, analisar e apresentar dados que sejam válidos dentro de um processo jurídico. Tais técnicas incluem reconstruir o bem informático, examinar dados residuais, autenticar dados e explicar as características técnicas do uso aplicado de dados e bens informáticos".p . 160

Os meios de obtenção de prova digital face às medidas anti-forenses

Exposta a prevalência da criptografia[10] no funcionamento das tecnologias de informação e comunicação, bem como a acessibilidade de medidas anti-forenses, facilmente se depreendem as dificuldades que esta conjuntura representa face aos normais meios de obtenção de prova

[10] A criptografia é usada para proteger os dados contra furto, alteração ou comprometimento e funciona transformando os dados em um código secreto que só pode ser desbloqueado com uma chave digital exclusiva.

digital[11]. Com efeito, «dia para dia, apuram-se novas técnicas de dissimulação ou ocultação que dificultam a identificação do agente das actividades por parte das autoridades», o que tem «potenciado uma generalizada desadequação do direito e processo penais ao combate eficaz da criminalidade informática»[12]. Exploremos em maior detalhe a forma como a criptografia e outras medidas anti-forenses dificulta (ou impossibilita) a aquisição de prova digital, confrontando os meios de obtenção desta com a protecção concedida por essa.

Desde logo, a utilização de medidas anti-forenses pode dificultar ou impossibilitar a identificação dos sistemas informáticos relevantes e do utilizador responsável pelos actos em investigação, nomeadamente quando estas medidas ocultem o rasto digital deste ou anonimizem o seu tráfego em rede, cortando as pernas à investigação antes desta sequer ter hipótese de correr. No entanto, mesmo quando esses sistemas estejam já identificados – ou sejam, no mínimo, identificáveis –, as medidas anti-forenses poderão, na fase de obtenção de prova stricto sensu.

À progressiva protecção do tráfego em rede por protocolos criptográficos vem associada uma perda de acesso legível[13] a cada vez mais dados relativos às comunicações informáticos por parte dos tradicionais operadores de comunicações, que constituem as entidades cooperativas

[11] Na resolução do Conselho da União Europeia sobre a encriptação (13084/1/20), que visa conciliar «segurança através da encriptação e segurança apesar da encriptação», este reconheceu que a criptografia constitui um meio necessário para proteger os direitos fundamentais e a segurança digital, mas que simultaneamente é preciso assegurar a capacidade de as autoridades competentes no domínio da segurança e da justiça penal exercerem os seus poderes legais. Reconheceu também a tendência para as aplicações e dispositivos informáticos encriptarem por defeito os dados armazenados, e os canais de comunicação estarem cada vez mais protegidos por encriptação ponta-a-ponta, mas que a inclusão destas soluções de encriptação (concebidas para fins legítimos) no modus operandi dos criminosos, contraposta à cada vez mais evidente dependência das autoridades em acederem a provas electrónicas para combaterem eficazmente a criminalidade grave e organizada, dificulta ou praticamente impossibilita a prevenção, investigação e repressão criminais. Por fim, reconheceu que é necessário «encontrar o equilíbrio certo» que, independentemente do ambiente tecnológico, permita preservar os poderes das autoridades competentes no desempenho das suas funções, através de um acesso legal aos dados informáticos que salvaguarde as garantias processuais e os direitos fundamentais dos visados e que respeite os princípios da necessidade, da proporcionalidade e da subsidiariedade. Para este efeito, a União Europeia visa, em estreita consulta com os prestadores de serviços e outros intervenientes pertinentes, combinar os esforços e coordenar as capacidades de investigação das suas instituições e organismos e dos seus Estados-membros, definindo e estabelecendo abordagens inovadoras tendo em conta as novas tecnologias e analisando soluções técnicas e operacionais adequadas.

[12] RAMALHO, Métodos Ocultos, cit., p. 98. Também a Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre a estratégia da União Europeia para lutar contra a criminalidade organizada (2021-2025), COM(2021)/170, reconhece a continuada perda de eficácia dos meios de obtenção de prova e a necessidade de capacitar de forma adequada as autoridades na era digital.

[13] Isto é, os dados continuam a existir, mas na sua versão encriptada e, como tal, inútil enquanto prova, por não se conseguir aceder à informação neles contida.

na investigação criminal em ambiente digital por excelência, e que, por esta via, vêm sendo substituídos por outras entidades de dificultada cooperação (como fornecedores de serviços web ou de serviços anonimizadores), passando a obtenção desses dados a estar dependente destas em caso de encriptação em transporte, ou, nos casos de onion routing e encriptação ponta-a-ponta, em que inexiste por completo uma entidade terceira de carácter centralizado com acesso aos mesmos, da obtenção directa dos seus registos (ou, como veremos, uma sua intercepção na fonte) nos dispositivos dos intervenientes na comunicação, i.e., nas pontas[14].

Adicionalmente, também as restantes medidas anti-forenses poderão tornar a pesquisa e apreensão de dados infrutífera, nomeadamente quando os dados potencialmente relevantes se encontrem dissimulados por técnicas de esteganografia[15], quando sejam previamente eliminados de forma a não deixar qualquer vestígio dos mesmos ou alterados para despistar a investigação, ou quando sejam utilizadas ferramentas de ofuscação do rasto digital que impeçam a própria criação desses dados.

Em síntese apertada, se as autoridades podem – cumpridos, naturalmente, os respectivos pressupostos – ordenar a quem tem disponibilidade ou controlo dos dados em causa que os comunique ao processo ou que permita o acesso aos mesmos, realizar directamente uma pesquisa e apreensão de dados informáticos presentes num determinado sistema informático, ou interceptar comunicações informáticas, estes meios de obtenção de prova têm vindo a revelar-se cada vez mais infrutíferos face ao crescente uso de medidas anti-forenses destinadas à sua frustração.

As Evidências Digitais ou de Tecnologias de Informações (TI)

Evidência digital é um elemento protegido em um meio digital. No entanto, uma avaliação correta de qual seria a sua razão de ser em qualquer informação que, sujeita a intervenção humana, não tenha sido extraída de um computador. A evidência de TI deve estar de uma forma

[14] Não admira, assim, que tenha já havido uma declaração conjunta da Europol e dos chefes de polícia europeus contra a progressiva utilização de encriptação ponta-a-ponta em serviços de comunicação de instante messaging e Voice-over-IP. EUROPOL, «European Police Chiefs call for industry and governements to take action against end-to-end encryption roll-out», disponível em https://www.europol.europa.eu/medi press/newsroom/news/european-police-chiefs-call-for-industry-and-governments-to-take-action-against-end to-end-encryption-roll-out., acessado em 03 de Maio de 2025.

[15] É a técnica de ocultar dados dentro de um arquivo ou mensagem comum e não secreto para evitar a detecção; os dados ocultos são então extraídos no seu destino. O uso da esteganografia pode ser combinado com a criptografia como uma etapa extra para ocultar ou proteger dados.

humana legível ou capaz de ser interpretada por pessoas especialistas em representar essas informações com a ajuda de um programa de computador.

As principais características de todas as evidências digitais são: que elas podem ser voláteis, anónimas, duplicáveis, alteráveis, modificáveis e descartáveis. Esses elementos são de extrema importância no momento de uma análise forense.

Fontes de evidência digital

As fontes de evidência digital são recipientes de elementos susceptíveis de investigação, porque, em seu conteúdo, as informações geralmente associadas ao proprietário do meio são protegidas.

A tabela a seguir mostra a mídia digital e quais são as fontes de evidência que elas contêm:

MEIO DIGITAL	RECURSO	EVIDÊNCIA
Computadores de excritórios e pessoais	Discos rígidos internos	Arquivos de logs Cookies Arquivos ocultos Históricos de navegação Spool de imprensão Arquivos temporários, comprimidos, protegidos com passwords e de SWAP
Dispositivo com control de acesso	Pen drice Cartão de proximidad biométrica	Dados identificativos de usuários Níveis de acesso Permissão Configurações
Câmaras digitais	Cartão de memória	Imagens Vídeos Sons Data e hora de gravação
Cartão de memória		Imagens Documento ou planilhas Fotografias
Impressoras - Scanners	Cartão de memória em scanners	Documentos
Pontos de acesso em routers wireles		Arquivos de configuração
Diskettes - CD e DVD		
GPS - Celulares	Cartão de memória Memória interna do dispositivo celular	SMS Whatssap Telegrama Fotografias Emails Vídeos Notas de voz

Fonte: Autor.

A identificação de um disco rígido, por exemplo, é importante para a validade de qualquer meio de prova, pois uma vez removido do computador, ele entra na cadeia de custódia e é essencial para cumprir os requisitos de identificação ao executar uma habilidade.

Perícia Informática

A aplicação da informática na perícia criminal, pode estar directamente relacionada à computação forense, uma área específica da ciência forense, e actuante no ramo militar, governamental e de inteligência, que segundo (ALTIMUS & KATEEB: 2014) a computação forense pode ser definida como formas de análises com o intuito de envolver a preservação, extracção e documentação de evidências obtidas em mídias digitais, advinda de evidências digitais. O papel da computação forense tem funções como de um processo investigativo, que conforme (SONNTAG: 2008), pode ser considerado a mistura entre elementos da Ciência da Computação e do Direito, tendo em foco a análise e colecta de informações de computadores, redes, dados de GPS, sistemas wireless, dispositivos de armazenamento (pendrives, HDs, celulares e afins) como solucionar e entender também as práticas relacionadas aos crimes cibernéticos e de informática, a fim de avançar os processos jurídicos, sendo passível de encaixe em penas legais conforme o delito praticado em questão obtido através de prova durante a perícia.

Na maioria dos casos a computação forense estará directamente ligada à polícia científica, sua prática será realizada por um perito, o qual utilizará de ferramentas e recursos específicos para a extracção das informações que sejam necessárias para a confecção de um laudo pericial. Nesta fase, a prudência e o conhecimento do perito, farão papéis de extrema importância para o desenvolvimento do processo criminal, visto que, o laudo deverá ser preciso e imparcial, assim sendo, no presente laudo, o perito deverá descrever de maneira formal, sucinta e objetiva todos os procedimentos e exames técnicos utilizados em sua perícia.

(FRANÇA: 2005), atesta que um perito deverá ser entendido como uma pessoa qualificada ou experiente no assunto ao qual esteja sendo tratado, visando, quando for solicitado esclarecer factos que sejam de interesse da justiça.

Examinando a Evidência

Na computação forense segundo (POLLIT et al., 2000), uma evidência poderá ser representada por impressoras, chips e placas em geral, unidades centrais de processamento, meios de armazenamento e monitores, podendo ser facilmente descritos como uma unidade física. No entanto, as evidências, enquanto armazenadas nestes meios físicos, será latente e só existirá em um formulário eletrónico metafísico. O processo de examinação fará com que a prova se torne visível e ao mesmo tempo explicará a sua origem e significância.

Assim sendo, segundo (NIJ, 2001), implica que na fase de examinação, várias coisas deverão ser realizadas. Primeiro, deverá ser realizada a documentação do conteúdo e o estado da evidência em sua totalidade. Essa documentação permitirá que todas as partes descubram o que estará contido na prova. Neste processo, a busca de informações que podem estar escondidas também é incluída. Uma vez que toda a informação se torne visível, o processo de redução de dados pode começar, como uma prática de refinamento ou filtragem. Dada a enorme quantidade de informações que poderão estar armazenadas em uma mídia de armazenamento, esta parte é considerada fundamental. Todavia, (POLLIT et al., 2000), salienta que uma evidência nem sempre existirá de maneira isolada, esta evidência é um produto de dados armazenados criados através da utilização de um aplicativo.

Extraindo Evidências

Segundo (NIJ, 2004), a extracção de uma evidência digital deverá ser cautelosa devido a sua fragilidade, ou seja, um manuseio ou examinação indevida, poderá acarretar no dano, alteracção ou até mesmo destruição da evidência. Uma examinação decorrente de falhas cometidas pelo encarregado da perícia, poderão ser passíveis de conclusões imprecisas, sendo então altamente recomendado levar em consideração a preservação deste tipo de evidência. Todavia (POLLIT et al.,2000), argumenta que o maior desafio para a computação forense está em desenvolver métodos e técnicas que permitam a obtenção de resultados válidos e confiáveis ao mesmo tempo que protejam a evidência de um possível dano. A extracção de uma evidência digital será realizada a partir de uma utilização ampla de recursos, por meio de software, hardware ou ferramentas para este propósito. Deste modo, a extracção de uma evidência poderá ser realizada através dos mais variados métodos.

Extração Lógica

A extração lógica, é constituída pela aquisição de dados em arquivos e directórios a partir do sistema operacional do dispositivo. (MOOIJ, 2010), explica que a extração lógica pode ser realizada através de duas formas: Unidades Software-Hardware ou Softwares próprios para a realização da extracção lógica. Entretanto (BEN-MOSHE, 2012), ractifica que, por mais que a extracção lógica passe a ser um processo consideravelmente rápido, de baixa complexibilidade, todavia leva a desvantagem na limitação de aquisição de dados, visto que, nesta prática não será possível a obtenção de dados apagados do sistema. "A extração lógica implica extracção de dados usando o sistema operacional do dispositivo através de um conjunto de comandos conhecido (por exemplo, comandos AT). Isto significa que as ferramentas de extracção de dados se comunicam com o sistema operacional do dispositivo e solicitam as informações do sistema. Isto faz com que haja aquisição da maior parte dos dados do dispositivo em tempo real." (CELLEBRITE MOBILE SYNCHRONIZATION LTD, 2014).

Extração Física

A extracção física consiste em uma varredura seguida da aquisição de dados contidos na memória flash do dispositivo, sendo então realizada uma cópia minuciosa (bit a bit). Segundo (MURPHY, 2014), sintetiza, afirmando que a extração física também poderá ser chamada de aquisição física, ou senão despejo de memória física, tal qual o dado obtido venha como um despejo hexadecimal de forma bruta, no qual poderá ser analisado posteriormente a fim de obter informações legíveis que se julguem necessárias. Neste método de extração por ser de alta complexibilidade, tem-se a vantagem na possibilidade da aquisição de arquivos apagados do sistema, sendo que pela extração lógica, isto poderia passar por despercebido. Entretanto, existe sua desvantagem, esta prática demanda de tempo e requer decodificação (MOSHE, 2012).

Vale ressaltar, que a memória flash foi desenvolvida a partir de uma EEPROM (Electrically Erasable Programmable Read-Only Memory), ou Memória Somente para Leitura Programável e Apagável Eletronicamente é uma memória não volátil, ou seja, suas informações ainda serão armazenadas mesmo sem a presença de uma fonte de energia. No caso de uma varredura para extracção de dados em um dispositivo móvel, a ferramenta fará uma aquisição directamente na Memória Flash do mesmo.

Extração Manual

Este método é considerado como um meio de último recurso e não muito recomendado, visto que, depende do trabalho manual propriamente dito do perito encarregado, e como citado anteriormente, poderá ocasionar perdas ou possíveis danos à evidência, o que de facto acarretará em conclusões imprecisas e de caráter pobre em obtenção de provas. Nesta fase de extracção, o usuário em questão, extrairá as informações através do acesso no sistema operacional e então de maneira selectiva, far-se-á a aquisição de evidências que sejam consideradas relevantes ao facto a ser julgado. É um processo bastante moroso que exige paciência e tempo, portanto, é utilizado somente como último recurso disponível.

Ferramentas Utilizadas

Na computação forense, inúmeros são os dispositivos, técnicas, recursos e ferramentas utilizadas para a extração de evidências, seja em soluções de Software ou Hardware. Exemplos como XRY, Cellebrite UFED, Solo4 e a linha de writeblocker Tableau estão entre os mais famosos dispositivos utilizados no ramo forense computacional.

Micro Systemation XRY

Desenvolvido a partir de 2003 pela empresa sueca Micro Systemation, o XRY é um software designado à extracção forense de dados de dispositivos móveis como Celulares, Smartphones, Tablets e também sistemas de navegação por GPS.

"O sistema XRY é a primeira escolha entre as agências de aplicação da lei em todo o mundo, e representa um sistema forense móvel completo fornecido com todo o equipamento necessário que se precisa para realizar um exame forense de um dispositivo móvel" (MICRO SYSTEMATION, 2014)

Dispõe de algumas versões, tais como as seguintes:

Logical

Como a versão mais simples, o XRY logical é a solução baseada em software para qualquer PC com plataforma Windows. Nesta versão, ele dispõe do hardware necessário para a realização de perícias em dispositivos móveis, sendo então própria para a realização de uma extracção lógica de dados.

Physical

O XRY Physical, é a solução baseada na obtenção forense de dados apagados ou protegidos, sendo assim, obtidos pela extracção física dos dados do dispositivo.

Complete

Consiste no kit contendo as funções logical e physical inclusas. Amplamente utilizado e recomendado na obtenção de evidências de dispositivos móveis, nesta versão, o usuário contará também com os dispositivos para clonagem de cartões do tipo SIM, uma unidade de comunicação e suas devidas ferramentas necessárias para uma extracção física ou lógica, de maneira que o usuário obtenha uma extracção de dados com o máximo de eficiência possível.

Field Version

Nesta versão do dispositivo, ela está adequada ao meio portátil de utilização imediata, sendo então de utilização em campo (do inglês Field, Campo). Segundo (MICRO SYSTEMATION, 2014), esta versão satisfaz algumas organizações, que frequentemente requisitavam kits forenses que fossem portáteis, ergonómicos e flexíveis, de tal forma que pudessem ser realizadas as perícias in loco e então pudessem facilmente conectar-se à rede ou em computadores remotos. Nesta versão acompanha o Panasonic CF-18, ou então intitulado Toughbook, um computador bastante robusto, portátil e de alta autonomia de carga, que foi desenvolvido a partir do padrão militar MIL-STD-810F para suportar condições extremas, tendo em vista que seu caso seja composto por uma resistente liga de magnésio.

Cellebrite UFED

Desenvolvido a partir de 1999 pela empresa israelense Cellebrite Mobile Synchronization LTD, a série UFED ou Dispositivo Universal de Extracção Forense, é actuante como um concorrente direto do Micro Systemation XRY. Amplamente utilizado pelas forças militares e também pelas agências de inteligência, é uma ferramenta importante para extracção, decodificação e análise de dados de dispositivos móveis. A série UFED possui também uma ampla variedade de versões, sendo as opções de campo (TK - Turn Key), Touch Logical, Touch Ultimate, 4PC Logical, 4PC Ultimate.

Versões Touch

Segundo (CELLEBRITE, 2014), a versão Touch foi desenvolvida como um standalone, um dispositivo independente criado exclusivamente para a realização da extracção forense de dispositivos móveis. O UFED Touch possui uma interface intuitiva e sensível ao toque (touchscreen), possibilitando também a realização de extracção física (na versão Ultimate), lógica (na versão Logical), sistemas de arquivos e todos os tipos de dados e senhas, incluindo também arquivos apagados de uma ampla variedade de dispositivos móveis. Além de ser uma versão portátil, o UFED Touch conta também com o kit operacional (cabos, conectores e etc).

Versões 4PC

A versão 4PC foi desenvolvida como uma solução forense que funcione em um hardware existente, ou seja, num computador ou um notebook. Esta versão é versátil e conta com uma variedade de aplicativos, acessórios e periféricos. Na versão Ultimate, conta com a possibilidade da realização de extracção física.

Versão TK – Turn Key

Podendo ser considerada como a versão mais completa da série UFED, a versão TK ou Turn Key, foi desenvolvida para o uso recomendado em campo, fornecendo ao usuário todas as aplicações juntamente com todo o aparato necessário para a realização de análises forenses em condições adversas. Assim como, o XRY Field Version da empresa Micro Systemation, a versão TK além de contar também com a linha de laptops resistentes e robustos da Panasonic, a versão TK conta com o Toughbook CF-18 e CF-53, ou o Toughpad G1.

Solo4

Desenvolvido pela empresa americana Intelligent Computer Solutions – ICS, o Image MASSter Solo4 é constituído de um hardware especialista em aquisição e duplicação em alta velocidade de dados de Discos Rígidos, amplamente utilizado no meio forense. A taxa de transferência e cópia de dados através deste dispositivo, correspondente a 13GB/min podendo alcançar incríveis 18GB/min, com suporte às interfaces SATA-2, IDE, SAS e USB. A utilização deste equipamento, está relacionada a duplicação de dispositivos de grande quantidade de armazenamento, ou seja, HDs, ao qual poderá realizar a duplicação do Disco Rígido sem o

auxílio de um computador, logo o SOLO-4 funciona como um dispositivo caracterizado como standalone, ou seja, poderá ser utilizado em campo. Todavia, o SOLO-4, também é capaz de realizar a sanitização de um disco rígido, o que segundo (ARANHA, 2013), resume-se em eliminar de maneira efectiva todos os dados de um disco.

Tableau

No ambiente da computação forense, a empresa americana Guidance Software desenvolveu o dispositivo denominado "Tableau" funcionando como Duplicador e Write Blocker, mas segue a pergunta: O que é um Write Blocker? "As forensics bridges (bloqueadores de escrita) são fundamentais em qualquer kit de computação forense. Os examinadores têm em mãos uma tecnologia de alta velocidade capaz de gerar imagem dos actuais discos rígidos, grandes e velozes, tanto em ambiente de laboratório quanto em campo." (FORENSE DIGITAL, 2014) Os bridges forenses, conhecidas como Write Blockers, consistem em ferramentas que realizem a imagem forense da evidência tendo somente o acesso à função Read-Only, ou seja, que tenha acesso apenas à leitura de um dispositivo de armazenamento sem comprometer a integridade da evidência, protegendo seus dados. Esta ferramenta está ligada directamente ao fundamento principal da computação forense, baseada na máxima preservação dos dados em cadeia de custódia.

Investigando a Nube

Em toda investigação forense, não apenas procuramos informações relevantes em dispositivos digitais, mas também ascendemos ao espaço virtual, actualmente chamado **nuvem** ou **cloude**, onde estão localizadas as redes sociais e a deep web.

Deve-se esclarecer que, como a nuvem é um espaço virtual, existe uma abordagem oportuna de pesquisa tecnológica, mas também há um aspecto legal no qual os investigadores forenses têm uma limitação. Muitas das informações contidas em redes ou sites sociais são privadas e, para obtê-las, deve - se pedir autorização ao juiz da área de jurisdição e, se os sites suspeitos forem estrangeiros, o pedido far-se-a ao nível internacional.

Sem dúvida, no trabalho técnico apenas reafirma evidências ou as propicias ao procedimento para que o operador judicial, em face de uma reclamação, inicie seu trabalho de investigação.

Um elemento importante para qualquer evento na nuvem é a preservação da evidência, que é observada usando ferramentas ou software específicos para dar-lhes uma existência verdadeira. Pode ser útil a participação de um notário, que contribuirá com o relatório do especialista em informática para seu acto notarial.

Teoria de seis graus de separação

O surgimento de redes sociais gerou no homem um tipo de fenómeno social raramente correspondido. Facebook, Twitter, LinkedIn e outros que permitem estabelecer relações pessoais entre usuários, podendo compartilhar material (arquivos ou imagens), pensamentos ou reflexões de sua vida íntima. Não é estranho descobrir nessas redes que seus usuários sentem dor ou alegria, bem como a história de uma viagem ou a aquisição de algo de bom.

A teoria dos seis graus de separação tenta provar que qualquer pessoa na Terra pode ser conectada a outra através de uma cadeia de conhecidos que não tem mais que cinco ou seis intermediários.

Isso é aplicável às redes sociais actuais, nas quais um usuário possui um número significativo de contactos que realmente provêm de um contacto de gerador e geralmente não conhece ou compartilha gostos ou afinidades.

Mas nem tudo o que reluz é ouro e nem tudo o que é mostrado nas redes é uma informação agradável. Muitas vezes, essas redes foram usadas para fins complexos, como pornografia ou pedofilia. Para esses casos e no caso de uma denúncia ilícita, aspectos essenciais como: a validação dos usuários agressores (eles têm um ID de identificação), a captura de evidências do conteúdo observado na tela devem ser levados em consideração, identificando, validando e registrando evidências eletrónicas por meio de protocolos ou boas práticas estabelecidas.

Além disso, a possibilidade de preservar evidências digitais deve ser gerenciada com o desempenho de um notário que forneça uma estrutura legal de primeiro nível para o trabalho do especialista em computadores.

Se alguma das premissas discutidas não for cumprida correctamente, as evidências apresentadas poderão ser contestadas e as evidências que sustentam o caso serão perdidas.

Alerta profundo

Na Web profunda ou a Web invisível você não pode apenas navegar na Internet através de navegadores convencionais, como Firefox, Chrome ou Internet Explorer e com os quais pode obter uma variedade de informações, geralmente indexadas e frequentemente repetitivas, que é chamada de superfície web ou web superficial.

A chamada deep web, dark web ou invisible web faz parte do conteúdo da Internet que não pode ser acessado por mecanismos de pesquisa convencionais, como Google, Yahoo! Bing ou Duck Duck Go, ou por navegadores clássicos, mencionados anteriormente.

Ao navegar em navegadores convencionais, nossas visitas são rastreadas através do nosso endereço IP, fornecido pelo nosso provedor de serviços de Internet. Por outro lado, navegar na deep web é practicamente anónimo e nossas visitas não são rastreadas.

A navegação na deep web nos permite entrar em um mundo que geralmente é perigoso e sem segurança, principalmente para usuários inexperientes da Internet. O material é geralmente variado, de pornografia infantil a narcotráfico, hackers e pessoas que limpam registros criminais.

As páginas da Web na navegação de superfície são www.unapagina.com; em vez disso, na deep web, o formato se parece com cebola asd67asdt124byasdfyieerbhi34y8 (ponto) e eles são criptografados.

O aplicativo de primeiro nível para navegar na deep web é chamado tor ou tor network.

Este navegador utiliza a privacidade optimizada do Mozilla Firefox e é um software de código aberto[16], que permite ao usuário navegar anonimamente, pois oculta seu endereço IP. Você pode acessar sites potencialmente bloqueados e, o mais importante, ele não rastreia o usuário.

Investigando elementos criminosos nesta etapa, existem inúmeros conteúdos com material potencialmente susceptível de cometer um crime, sua verificação não é fácil, principalmente quando o ser humano deve ser encontrado atrás do teclado. A realização de uma tarefa de inteligência nessa rede implica a aparência do agente secrecto, uma figura nem sempre aceita no campo judicial.

[16] O direito autoral fornece o direito de estudar, modificar e distribuir o software de graça para qualquer um e para qualquer finalidade.

Em princípio, haveria outra alternativa para detectar criminosos. Além disso, deve - se saber profundamente como navegar e avaliar, se criminosos em potencial cometem um erro, para que eles revelem sua identidade.

Pesquisa em nuvem usando fontes abertas. "Informação é poder"

O termo fontes abertas ou osint refere-se a todas informações publicadas na Internet e abertas ao público. Essas informações são caracterizadas por serem caóticas, desordenadas e desclassificadas, além de permitir que decisões sejam tomadas para a pessoa que encomendou a investigação.

A palavra "int" não está associada apenas ao osint, mas a outras maneiras de executar a inteligência, que são:

- Humint: São fontes de informação geradas por seres humanos.
- Sigint: Fontes de informação obtidas de elementos digitais.
- Geoint: Essas são informações que vêm dos satélites.

Para realizar pesquisas com fontes abertas, é útil saber o que são usadas nas fontes, bem como poder encontrá-las. Quase como uma derivação do ponto anterior em que a navegação profunda e seus perigos foram explicados, fontes de pesquisa potencialmente úteis são encontradas na deep web e também na superfície.

Outro elemento que o pesquisador deve ter em conta, é que muitas ferramentas são gratuitas, mas outras pagas, nem todas as ferramentas obtêm informações localmente e só podem ser usadas fora.

As informações obtidas são caóticas e desclassificadas, sendo o pesquisador quem deve dar a ele, com sua experiência, uma abordagem práctica e precisa para futuras decisões.

Problemas probatórios nos crimes informáticos

Enquanto instrumento fundamental para determinar e condicionar um modelo de investigação forense digital, a prova digital será identificada, de forma a reconhecer as várias fases processuais, e qual o conteúdo correspondente a cada uma. No entanto, apesar do impacto que teve na determinação dos standards necessários que devem caracterizar a prova digital, a realidade é que, por se tratar de uma prova tecnicamente complexa e de carente de interpretação especializada, esse cenário será difícil de se afirmar. No vasto mundo cibernético, a prova

digital deverá ser recolhida de forma célere, cumprindo todos os cuidados necessários, sob pena de perder integridade. Assim, o investigador deverá considerar a prova pela sua natureza efémera, o que dificulta a sua conservação num dispositivo eletrónico-digital que permita aumentar o seu período de utilidade investigativa, para além do naturalmente considerado. Para além de temporária, a prova digital também é frágil e alterável, caindo sobre o investigador forense a necessidade de redobrar os cuidados a tomar. Antes de recolher a prova, deverá identificar, de forma ainda mais rigorosa, qual o tipo de prova digital em causa. Apenas com essa identificação, poderá o investigador garantir a força probatória da prova digital, sem perigo de esta, ser alterada ou desaparecer. Havendo esta possibilidade de alteração ou desaparecimento, o investigador deverá ainda considerar a prova digital pela sua natureza volátil e instável. A instabilidade demonstrada por esta prova, provindo da constante mutabilidade que lhe caracteriza, torna mais difícil a sua apreensão. Tal dificuldade verifica-se em situações em que o investigador se depara inicialmente com uma prova com certas características, e mais tarde, esta se modifica, total ou parcialmente. A prova digital consiste ainda numa prova imaterial. Desta forma, a imaterialidade da prova digital imporá ao investigador forense ser conhecedor de técnicas específicas, sob pena de se perder a força de prova, na eventualidade de o investigador a alterar significativamente, por desconhecer a sua presença. Esta necessidade de o investigador possuir conhecimentos técnicos e científicos deve-se, particularmente, à complexidade e codificação caracterizadoras da prova digital. De modo a aceder a sistemas ou redes informáticos, o investigador deverá munir-se de todas as técnicas e conhecimentos científicos, para dar uso de palavras-chave ou servir-se de técnicas de desencriptação. Em certas situações, a investigação forense deverá ter em conta a dispersão da prova digital, ou seja, esta poderá encontrar-se distribuída por vários "terminais, computadores e redes que se estendem por uma vasta área espacial ou geográfica".

Surgindo em ambiente digital, a abordagem da investigação forense deverá fundamentar-se com o caráter difuso e disperso da criminalidade informática, não havendo concentração dos seus elementos integrantes do complexo informático. Como referido, a prova digital abrange impulsos eletromagnéticos momentâneos relevantes para a rede ou sistema informático de comunicações eletrónicas. Por tal, a prova digital caracteriza-se como dinâmica e mutável. As competências do investigador exigem que este realize uma investigação estruturada

temporalmente, comparando vários períodos temporais, permitindo aceder à prova digital de maior utilidade para a investigação.

Uma abordagem gera, no campo de trabalho aparece em cena com suas próprias vicissitudes probatórias. Antes de tudo, deve-se lembrar que na lei particularmente no direito processual penal, o princípio da liberdade é regido em virtude do qual, como é sabido, os factos investigados podem ser comprovados pelo recurso a todos os tipos de elementos de condenação, desde que as garantias constitucionais dos envolvidos não sejam violadas.

Como **Sueiro** explica em seu livro sobre casos de crime de computador: "embora até o momento não tenha havido uma reforma na área de crime de computador …, a verdade é que cada vez mais é imperativo, indispensável e necessário, devido à mudança gradual nos procedimentos criminais, de evidências físicas, corporais ou tangíveis para evidências digitais, eletrônicas ou intangíveis. "

O uso de serviços como Google Maps, e-mails, fotografias de telas, são antigos - gravações de áudio e / ou vídeo em CD, DVD ou USB ou seus respectivos quadros - servem para muitos as vezes, como evidência crucial para a descoberta de crimes cibernéticos.

É claro que os desafios que o crime cibernético coloca como operadores judiciais não são menores, obrigando-nos todos os dias a fazer grandes esforços para acompanhar os tempos, se nossa função é criar uma imputação ou, por pelo contrário, contrariar uma acusação por meio de contra-testes e automáticos por sites da Internet ou de estenografias - desenhos ocultos nos quais, quando clicados, são activados e permitem descobrir o oculto abaixo do original.

Exemplo no Direito Comparado:

Um caso, que envolve um estudante universitário de engenharia de sistemas que, por meio de um IP localizado no exterior, fez uma transferência imprópria de dinheiro entre contas bancárias no País, Cassation confirmou sua condenação pelo crime de fraude por técnicas da manipulação do computador como autor-phishing. Além da incapacidade técnica invocada pela defesa, uma vez que isso não corresponde às tarefas que ele desempenhou em favor de seu empregador ou de seu carácter como estudante universitário de engenharia de sistemas, está presente a necessária relação lógica entre as diferentes evidências, através do qual foi possível descobrir quem fora, através de manipulações de computador, extraíra indevidamente fundos da conta bancária.

Protocolo da Internet

Protocolo da Internet - é um conjunto de números (quatro números decimais, separados por um ponto entre eles) que identificam a interface de um dispositivo (um computador, smartphone etc.) em uma rede que usa o Protocolo IP (Protocolo da Internet). A existência de IP deve-se ao facto de que as informações que circulam na rede precisam saber para onde fazê-lo e para onde devem ir. Pode haver dois tipos de IP: um estático (é único e sempre o mesmo) ou dinâmico (é alterado ao reconectar). Um provedor de acesso à Internet que tenha um contrato com um assinante da Internet normalmente mantém um arquivo histórico com o endereço IP atribuído (fixo ou dinâmico), o número de identificação do assinante, a data, a hora e a duração da atribuição de endereço da mesma forma, se o usuário da Internet estiver usando uma rede pública de telecomunicações, como um telefone móvel ou fixo, a companhia telefônica também registrará o número discado, juntamente com a data, a hora e a duração do facturamento subsequente.

Para fornecer aos testes as diretrizes de segurança necessárias (sem poluição, sem perda de cadeias de segurança, inalterabilidade), especialistas oficiais são usados, em comparação com outras evidências. Na fase de julgamento, eles devem ser apresentados a pedido da parte e com o controle deles, como qualquer outra evidência.

Practicamente não há actividade diária que não incorpore em seu desenvolvimento nenhum recurso digital ou computacional. Diz-se que todo meio digital associado ao ser humano é uma extensão de sua vida, onde eventos pessoais e profissionais se refugiam e, por que não, criminosos, dependendo da idiossincrasia do indivíduo.

Os testes de computador podem ser plantados em praticamente qualquer recurso digital, onde a capacidade do investigador e o conhecimento de suas ferramentas de computador fornecerão um resultado bem-sucedido ao que é investigado, fornecendo ao juiz ou que solicita uma investigação elementos suficientes para decidir sobre uma causa ou processo judicial.

O maior problema do regime propatorio nos crimes cibernéuticos, é a necessidade de pedir - se uma autorização judicial para a recolha de provas. Uma vez que, pode - se dar o caso de o perito tiver a devida autorização enquanto os vestígios não existam.

Outro problema que prevalece sobre a colheita de provas, é de não de existir a prática de um crime que manisfeste em flagrante delito.

Quebra de sigilo telemático para obter Prova em acções cíveis

A inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefónicas, tratando-se de verdadeiro princípio corolário das inviolabilidades previstas na CRM, coadunando-se com as garantias de privacidade, honra e dignidade da pessoa humana. A seara em questão, é a do direito à privacidade, considerado por grande parte da doutrina como parte integrante dos direitos da personalidade e, destinado a resguardar a dignidade da pessoa humana, pois "os direitos à privacidade e à própria imagem formam a protecção constitucional à vida privada, salvaguardando um espaço íntimo intransponível por intromissões ilícitas externas" (MORAES, Ibidem, p. 47).

O Constituinte originário entendeu por bem proteger especificamente a imagem, a vida privada e a privacidade dos cidadãos, assim dispondo sobre o assunto:

A qual, prevê o direito à privacidade, facultando a cada indivíduo a possibilidade de opôr resistência a intromissão não consentida em sua vida privada e familiar, impedindo a divulgação de informações de conteúdo privado.

Todavia, em que prese tratar-se de direito fundamental, destinado à protecção da própria integridade moral do indivíduo, a fruição do direito à privacidade não é absoluta. Como toda liberdade individual, o exercício deste direito está condicionada à realização da convivência social ideal, não podendo servir como carapaça protectora de práticas ilícitas.

Como todo direito individual previsto e garantido na CRM, o direito à intimidade está virado em prol de um interesse maior, que é o interesse social.

Dada a impossibilidade de previsão legal, caso a caso, do limite a ser estabelecido entre o interesse público e o privado, aos Tribunais cabe a dosimetria quanto à flexibilização dos direitos individuais, em nome da colectividade.

É neste diapso que surge a interceptação telefónica, como medida excepcional, considerada legítima, apenas e tão-somente, quando observadas as formalidades, exigências e requisitos impostos legalmente, uma vez que a intromissão na vida privada das pessoas é, em princípio, ofensiva ao direito fundamental.

A interceptação telefónica é fruto da necessidade, percebida pelo legislador, de se equipar a sociedade com instrumentos que possibilitem a contenção do crescente crime organizado diante da grande evolução nos sistemas de comunicação, principalmente da telefonia, ora utilizados pelo crime organizado em larga escala até mesmo pela facilidade em sua aquisição.

As interceptações telefónicas, uma vez legalmente disciplinadas e efectuadas com obediência aos requisitos impostos no nosso ordenamento jurídico, são aceitas como provas lícitas, sendo admissível seu resultado como fonte de prova no processo.

É indispensável que a ordem judicial seja acompanhada de uma verdadeira e própria motivação, especificamente vinculada à situação concreta. A ausência de fundamentação é motivo de nulidade da diligência, causando a imprestabilidade da prova e ensejando a inutilização do material.

O juiz deve verificar, ao ordenar a diligência, se, em relação à modalidade particular do facto imputado ao sujeito, resulta evidente a utilidade do recurso para fins probatórios ou convenientes à investigação criminal. A autoridade judiciária deverá fazer, na motivação da autorização para interceptação telefónica, as seguintes observações: conformidade da investigação com as finalidades da instrução criminal; ocorrência de um fundado motivo pelo qual se repute que a interceptação possa propiciar elementos úteis para o desenvolvimento das actividades instrutórias; avaliação da oportunidade que permitia tão grave ingerência na intromissão da vida alheia, com relação à provável obtenção de tais elementos probatórios.

Acesso a dados armazenados em dispositivos eletrónicos mediante mandados de busca e apreensão

A interpretação constitucional restritiva dada ao sigilo das comunicações, qual seja a de que ele só protegeria (conteúdo de) comunicações enquanto estão em fluxo, gera uma situação de descompasso normativo: os modernos celulares, tablets e computadores armazenam uma enorme quantidade de informações, fotos e comunicações que oferecem retratos fieis e detalhados de seus donos, mas que não gozariam da mesma protecção de comunicações em fluxo pelo mero facto de agora estarem arquivadas.

É nos termos do art. 68 da Lei de Telecomunicações, garantido o sigílo de comunicações transmitidas através das redes de telecomunicações de uso público. Salvo, tratar - se de matéria criminal.

A quebra do sigílo telemático para obtenção de provas em processo civil só é permitida mediante autorização judicial. Bem como, a responsabilidade por dano também pode ocorrer pela prática de um crime informático, nos termos do artigo 483 do Código Civil, a qual, "Aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição

legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação".

A Informática, a Internet e a Filosofia da Prova

O advento da internet fez surgir no âmbito dos tribunais novas problemáticas em diversas áreas que a jurisprudência paulatinamente tem tentado solucionar.

São inúmeras as questões de ordem jurídica que se podem suscitar e relacionar com a internet: prova digital e valoração desta prova, processo digital, responsabilidade civil, criminal, disciplinar, direitos autorais, privacidade e direitos fundamentais dos cidadãos, a responsabilidade por conteúdos inseridos na internet, a protecção de dados informáticos, entre outras.

É válida e necessária a prova digital, em momento que se torne imperativo consubstanciar ou apurar a veracidade de uma alegação de parte em audiência, não existindo outro meio, serve então esta, para comprovar declarações, acções e porventura decifrar intenções que se denotam fundamentais para a convicção do julgador no que diz respeito ao dolo.

Na justa medida, não será a prova digital, um meio de prova que dê resposta a todas as dúvidas colocadas em audiência, no entanto, demonstrar-se-á inúmeras vezes, que para certo tipo de criminalidade, ser o único meio de prova susceptível de criar convicção de veracidade no julgador.

Do mesmo modo, em sede de investigação, como meio de obtenção de prova, não vem substituir de forma alguma, nenhum meio de obtenção de prova já existentes no Código Processo Penal. Porém, em certo tipo de investigação (não somente as relacionadas directamente com o cibercrime), pode vir a ser uma ferramenta fundamental, tendo por característica a sua especial celeridade, imediata, contrapondo-se à investigação de um crime dito de 'tradicional'. A entidade competente, na sua investigação, conseguirá inspecionar os vestígios electrónicos deixados pelo crime em fase de preparação, no momento da execução, e mesmo que já consumados.

É por sua vez, também mais fácil e cómodo, conseguir as provas através de conteúdo de dados, do que recorrendo aos meios habituais de obtenção de prova.

Esta realidade é também susceptível de gerar um crescimento na amplitude da valoração da Prova indiciária[17] e especialmente uma simplificação da prova dos factos alegados em sede de julgamento.

As operadoras de telecomunicações, mostram-se reservadas quanto à preservação e apresentação desta prova, no sentido de que a simplificação da cooperação internacional neste registo, têm demonstrado um elevado índice de eficácia, levando a condenações sem realmente a necessidade de demonstração dos factos imputados aos arguidos, recorrendo-se à apreensão de conteúdo de dados. Entende-se aqui, o fundamento de que, a investigação elaborada segundo os trâmites de cooperação internacional, são bastantes para a descoberta dos factos relevantes. Apela-se desta forma, a utilização de provas consideradas mais seguras, e que por sua vez se reflecte numa investigação criminal com riscos diminutos para os respectivos agentes competentes da investigação.

CONCLUSÃO

De concluir que com a tipificação dos crimes informáticos em 2014, Moçambique hoje esta a caminhar a passos de camaleão. Havendo, atualmente necessidade de o legislador aprimorar aprovar a lei cibernética e que a mesma venha espelhar a realidade do dia-a-dia. O crime informático ou cibernético é cometido por meio das TIC's, atendendo a evolução no cenário da informação e tecnologia.

A identificação dos sujeitos ativos nos crimes informáticos é difícil, situação que se deve ao ao fato de que, em regra, os criminosos utilizam da rede de internet disponibilizada em espaços públicos. A transferência de dados não estaria protegida, situação que facilita a interceptação da prática delitiva, porém, dificulta a identificação dos agentes.

[17] É clássica a distinção entre prova directa e prova indiciária. A prova directa, refere-se aos factos probandos, ao tema da prova, enquanto a prova indirecta, ou indiciária, se refere a factos diversos do tema da prova, mas que permitem, com o auxílio de regras da experiência, uma ilação quanto ao tema da prova. Na prova indiciária, mais do que em qualquer outra, intervêm a inteligência e a lógica do juiz. A prova indiciária pressupõe um facto, demonstrado através de uma prova directa, ao qual se associa uma regra da ciência, uma máxima da experiência ou uma regra de sentido comum. Este facto indiciante permite a elaboração de um facto que revela uma consequência em virtude de uma ligação racional e lógica. Aliás, é importante que se refira que a prova indiciária, ou o funcionamento da lógica e das presunções, bem como das máximas da experiência, é transversal a toda a teoria da prova, começando pela averiguação do elemento subjectivo de crime, que só deste modo pode ser alcançado, até à própria creditação da prova directa constante do testemunho. (Intervenção no Centro de Formação Jurídica e Judiciária de Macau em 30 de Novembro de 2011)

O combate à criminalidade digital em Moçambique perpassa não apenas a necessidade de tipificação das condutas danosas praticadas no ambiente virtual, como, também, necessita de uma política pública dirigida à educação dos usuários das redes. Além disso, é imperiosa a constante evolução das técnicas investigativas concernentes a essas práticas, assim como a remoção de barreiras legislativas concernentes à obtenção de dados dos agentes.

A tipificação dos crimes informáticos em Moçambique evoluio bastante, tendo em 2014, sido aprovada a Lei n° 35/2014, de 31 de Dezembro. A qual, continham apenas 9 (nove) crimes informáticos. E, em 2019, com a aprovação da Lei n° 24/2019, de 24 de Dezembro, passou de 9 (nove) para 19 (dezanove) crimes informáticos tipificados e punidos pela lei penal.

Relativamente as provas nos crimes informáticos, requer a efectivação de um trabalho conjunto entre os Órgãos da Administração da Justiça para o efeito.

REFERÊNCIAS

Andrade, Manuel da Costa. 1994, "Sobre a valoração como meio de prova em processo penal das gra vações produzidas por particulares", Estudos em Homenagem ao Prof. Doutor Eduardo Correia, I Volume, Coimbra.

ANTUNES, Mário / RODRIGUES, Baltazar, Introdução à Cibersegurança, 2.ª ed., FCA Editora, 2022. ÅRNES, André, Digital Forensics, Wiley, 2018 AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS, «Quantum computing and cryptography», em TechDispatch, n.º 2, 2020.

AYCOCK, John, Computer Viruses and Malware, Springer, 2006.

BELEZA, Teresa Pizarro / PINTO, Frederico de Lacerda da Costa, «A prova criminal e as garantias de defesa: linhas de leitura e pontos de tensão», em Prova Criminal e Direito de Defesa, Almedina, 2010 BERCOVITZ, Rachel, «Law Enforcement Hacking», em Columbia Law Review, vol. 121, n.º 4, 2021.

ABEL, Wiebke / SCHAFER, Burkhard, «The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822», em SCRIPTed, vol. 6, n.º 1, 2009 ALBERGARIA, Pedro Soares de, «Artigo 125.º – Legalidade da prova», em Comentário Judiciário do Código de Processo Penal – Tomo II, 3.ª ed., Almedina, 2021.

NHAMITAMBO, Raul de Miguel Benjamim Jofrisse. ANÁLISE DA JURISPRUDÊNCIA NACIONAL E DAS LACUNAS EXISTENTES NA LEI MOÇAMBICANA EM RELAÇÃO AS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÕES: Analysis of national jurisprudence and gaps in mozambican law in relation to information and communications technologies. **RCMOS - Revista Científica Multidisciplinar O Saber**, Brasil, v. 1, n. 1, 2025. DOI: 10.51473/rcmos.v1i1.2025.972. Disponível em: https://submissoesrevistacientificaosaber.com/index.php/rcmos/article/view/972.. Acesso em: 3 maio. 2025.

NHAMITAMBO, Raul de Miguel Benjamim Jofrisse. CRIMES INFORMÁTICOS NO ORDENAMENTO JURÍDICO MOÇAMBICANO: Computer crimes in the mozambican legal system. **RCMOS - Revista Científica Multidisciplinar O Saber**, Brasil, v. 1, n. 1, 2025. DOI: 10.51473/rcmos.v1i1.2025.976. Disponível em: https://submissoesrevistacientificaosaber.com/index.php/rcmos/article/view/976.. Acesso em: 9 maio. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, «Guide to integrating forensic techniques into incident response», SP 800-86.

NEVES, António Castanheira, «A unidade do sistema jurídico: o seu problema e o seu sentido», em Digesta, vol. 2, Coimbra Editora, 1995 — Sumários de Processo Criminal, 1968.

NEVES, Rita Castanheira, As Ingerências nas Comunicações Electrónicas em Processo Penal, Coimbra Editora, 2011.

NIELSEN, Jakob, «Nielsen's law of internet bandwidth», em Nielsen Norman Group, 1998.

NUNES, Duarte Rodrigues, «A admissibilidade da obtenção, diretamente pelas autoridades, de dados de localização por meio de sistema de GPS à luz do direito processual penal português», em Julgar, n.º 32, 2017.

LEGISLAÇÃO

MOÇAMBIQUE, Lei nº 24/2019, de 24 de Dezembro. Aprova a Lei de Revisão do Código Penal. Imprensa Nacional, Moçambique, MPT, 24 de Dezembro.

MOÇAMBIQUE, Lei n.º 11/**2023**: Altera o número 3, do artigo 311 da Constituição da República de **2004**, alterada pela Lei n.º 1/**2018**, de 12 de Junho. Imprensa Nacional, Moçambique, MPT, 12 de Junho.

MOÇAMBIQUE, Lei nº 3/2017, de 9 de Janeiro. Estabelece os princípios, normas gerais e o regime jurídico das Transacções Electrónicas e do governo electrónico. Imprensa Nacional, Moçambique, MPT, 9 de Janeiro.

MOÇAMBIQUE, Lei nº 8/2004 de 21 de Julho. Aprova a Lei das Telecomunicações. Imprensa Nacional, Moçambique, MPT, 21 de Julho.

MOÇAMBIQUE, Decreto nº 75/2014 de, 12 de Dezembro. Aprova o Regulamento de Controlo de Trafego de Telecomunicações. Imprensa Nacional, Moçambique, MPT, 12 de Dezembro.

MOÇAMBIQUE, Lei nº 25/2019, de 26 de Dezembro. Aprova a Lei de revisão do Código de Processo Penal. Imprensa Nacional, Moçambique, MPT, 26 de Dezembro.

MOÇAMBIQUE, Decreto-Lei n2 1/2005, de 27 de Dezembro. Introduz alterações ao Código de Processo Civil. Imprensa Nacional, Moçambique, MPT, 27 de Dezembro.