Procedimento de análise forense digital a dispositivos móveis em Portugal

Digital forensic analysis procedure for mobile devices in Portugal

10.29073/j2.v8i1.1110

Recebido: 01 de março de 2026.
Aprovado: 30 de março de 2026.
Publicado: 04 de abril de 2026.

Autor/a 1 (Correspondente): Carla Pinto, ESTG-IPP, Portugal, pinto.carla@gmail.com.

Autor/a 2: Patrícia Azevedo, ESTG-IPP, Portugal. pamv@estg.ipp.pt.

Autor/a 3: Pedro Pinto, ISEP, Portugal, pfp@isep.ipp.pt.

Resumo

A análise forense digital de dispositivos móveis constitui uma área emergente e de crescente relevância no âmbito da investigação criminal, atendendo à quantidade e à relevância da informação armazenada nestes dispositivos. O presente trabalho tem como objetivo definir um procedimento estruturado e padronizado para a realização de análise forense digital a dispositivos móveis em Portugal, em conformidade com o enquadramento jurídico nacional e europeu, designadamente a Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro) e o Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679).

No desenvolvimento deste trabalho, são identificados diversos desafios técnicos e jurídicos, entre os quais a encriptação de dados, os mecanismos de autenticação biométrica e a inexistência de uma metodologia uniformizada aplicável ao contexto português. A ausência de procedimentos padronizados pode comprometer a integridade da prova digital e a sua admissibilidade em processo judicial, tornando necessária a definição de boas práticas alinhadas com normas internacionais de investigação forense digital.

Pretende-se, assim, contribuir para o apoio aos profissionais da área jurídica e forense, propondo um procedimento estruturado que assegure a preservação da cadeia de custódia, a integridade dos dados e o cumprimento das exigências legais e éticas aplicáveis à recolha e análise de prova digital.

Palavras-Chave: Cadeia de Custódia; Dispositivos Móveis; Forense Digital; Lei do Cibercrime; Prova Digital.

Abstract

Digital forensic analysis of mobile devices is an emerging and increasingly relevant area in criminal investigation, given the quantity and relevance of the information stored on these devices. This work aims to define a structured and standardized procedure for conducting digital forensic analysis of mobile devices in Portugal, in accordance with the national and European legal framework, namely the Cybercrime Law (Law No. 109/2009, of September 15) and the General Data Protection Regulation (Regulation (EU) 2016/679).

In the development of this work, several technical and legal challenges are identified, including data encryption, biometric authentication mechanisms, and the lack of a standardized methodology applicable to the Portuguese context. The absence of standardized procedures can compromise the integrity of digital evidence and its admissibility in judicial proceedings, making it necessary to define best practices aligned with international standards for digital forensic investigation.

The aim is to contribute to supporting professionals in the legal and forensic field by proposing a structured procedure that ensures the preservation of the chain of custody, the integrity of the data, and compliance with the legal and ethical requirements applicable to the collection and analysis of digital evidence.

Keywords: Chain Of Custody; Cybercrime Law; Digital Evidence; Digital Forensics; Mobile Devices.

1. Introdução

Com o crescimento das tecnologias de comunicação e informação, a análise forense digital tem assumido um papel cada vez mais relevante no contexto da investigação criminal, particularmente no que respeita à análise de dispositivos móveis. Estes equipamentos armazenam grandes volumes de informação pessoal e profissional, podendo conter dados essenciais para a reconstrução de acontecimentos e para a obtenção de prova digital com relevância processual. Ao contrário do que sucedia em décadas anteriores, em que a investigação se baseava sobretudo em registos de chamadas telefónicas, os dispositivos atuais armazenam mensagens, correio eletrónico, fotografias, vídeos, dados de localização e histórico de utilização, ampliando significativamente o potencial probatório da análise digital (Xu, 2019; Kiran et al., 2019; Santos, 2024; Cruz-Cunha & Mateus-Coelho, 2020).

Neste contexto, crescente digitalização da sociedade tem transformado profundamente os métodos de investigação criminal, conduzindo ao aumento da relevância da análise forense digital como instrumento de recolha e interpretação de prova eletrónica.

A elevada taxa de utilização de dispositivos móveis na sociedade contemporânea reforça a importância da informática forense neste domínio. Estudos recentes indicam que a maioria da população utiliza diariamente smartphones para comunicação, acesso à Internet e armazenamento de dados pessoais, aumentando a probabilidade de estes dispositivos conterem elementos relevantes para processos judiciais. Consequentemente, a perícia forense aplicada a dispositivos móveis tornou-se uma área crítica da investigação digital, exigindo métodos rigorosos e tecnicamente fundamentados que garantam a integridade, autenticidade e fiabilidade da prova obtida[1].

Apesar da sua relevância, a análise forense de dispositivos móveis apresenta diversas dificuldades técnicas. Cada equipamento possui características próprias, diferentes sistemas operativos e mecanismos específicos de segurança, o que implica a utilização de metodologias distintas para a recolha e análise de dados. A constante evolução tecnológica agrava esta complexidade, uma vez que novos dispositivos incorporam mecanismos avançados de proteção, como encriptação de dados, autenticação biométrica e códigos de acesso, dificultando o acesso à informação armazenada. Como consequência, as ferramentas forenses necessitam de atualização permanente para acompanhar estas alterações, garantindo que os dados podem ser extraídos de forma fiável e sem comprometer a sua integridade (Kiran et al., 2019).

Outro fator que contribui para a complexidade desta área é a inexistência de procedimentos uniformes e universalmente aceites na prática forense, em especial no contexto jurídico português. Embora existam orientações internacionais para a recolha, preservação e análise de prova digital, designadamente as publicadas pelo National Institute of Standards and Technology (NIST) e por organismos internacionais de cooperação policial, a sua aplicação prática pode variar entre instituições, tribunais e investigadores. Esta falta de uniformização pode originar inconsistências metodológicas e colocar em causa a credibilidade da prova digital, comprometendo a sua admissibilidade em tribunal e a eficácia das investigações (Ramalho, 2013).

Para além das dificuldades técnicas e metodológicas, a análise forense digital encontra-se fortemente condicionada por requisitos legais e éticos. A recolha e o tratamento de dados pessoais devem respeitar o enquadramento jurídico aplicável, nomeadamente as normas relativas à proteção de dados e aos direitos fundamentais dos cidadãos. O Regulamento (UE) 2016/679 estabelece regras rigorosas quanto ao tratamento de dados pessoais, impondo que a recolha seja realizada de forma proporcional, transparente e segura, garantindo o respeito pela privacidade e pelos direitos dos titulares dos dados (European Union, 2016). No ordenamento jurídico português, a investigação criminal deve ainda observar o Código de Processo Penal, a Lei do Cibercrime e a legislação relativa à proteção de dados, que definem os limites legais da obtenção de prova

[1] https://invoicexpress.com/relatorio-digital-portugal-2024/

digital e as condições da sua utilização em processo judicial (República Portuguesa, 1987; Assembleia da República, 2009; Portugal, 2019).

Face a este enquadramento, torna-se necessário desenvolver procedimentos técnicos e jurídicos que permitam realizar a análise forense de dispositivos móveis de forma consistente, garantindo simultaneamente a validade científica e a admissibilidade legal da prova.

O presente artigo tem como objetivo contribuir para a normalização da análise forense digital de dispositivos móveis no contexto jurídico português, propondo um procedimento estruturado para a recolha, preservação e análise de evidência digital, alinhado com a legislação nacional e europeia e com as boas práticas internacionais na área da informática forense.

A prova digital pode ser definida como qualquer informação armazenada, processada ou transmitida por sistemas informáticos ou redes de comunicações que possua valor probatório, incluindo ficheiros, registos de atividade, mensagens, dados de tráfego ou metadados (National Institute of Standards and Technology, 2006). A natureza desta prova apresenta características específicas, como intangibilidade, volatilidade e facilidade de alteração, o que exige procedimentos especializados para garantir a autenticidade e integridade da informação recolhida (National Institute of Justice, 2008).

Para alcançar este objetivo, definem-se dois objetivos específicos. O primeiro consiste na análise do enquadramento legal nacional e europeu aplicável à prova digital, com especial destaque para a Lei do Cibercrime, o Código de Processo Penal, a legislação de proteção de dados e o Regulamento Geral sobre a Proteção de Dados. A revisão destas normas permite identificar limitações jurídicas, lacunas regulatórias e requisitos formais que devem ser respeitados para garantir a validade da prova digital em tribunal.

O segundo consiste na definição de um procedimento técnico para a análise forense de dispositivos móveis, destinado a ser utilizado por autoridades judiciais e órgãos de investigação criminal. Este procedimento deverá ser adaptável a diferentes tipos de dispositivos e sistemas operativos, respeitando simultaneamente as exigências legais e as boas práticas internacionais de informática forense. A padronização das etapas de recolha, preservação e análise pretende reduzir erros metodológicos e assegurar a cadeia de custódia da prova digital.

O restante artigo encontra-se organizado da seguinte forma: a Secção 2 apresenta o enquadramento da análise forense digital, incluindo os principais conceitos, o enquadramento jurídico e as principais normas e diretrizes internacionais aplicáveis; a Secção 3 discute o atual enquadramento e as lacunas identificadas; a Secção 4 apresenta o procedimento proposto para a análise forense digital de dispositivos móveis; por fim, são apresentadas as conclusões finais do estudo.

2. Análise Forense Digital - Enquadramento e Desafios Técnicos e Éticos

A análise forense digital corresponde ao conjunto de métodos técnicos e procedimentos jurídicos destinados à recolha, preservação, exame, análise e apresentação de dados digitais com relevância probatória. Esta prática é utilizada em investigações criminais, processos civis, auditorias e outras situações em que a informação eletrónica possa assumir valor de prova (Cohen, 2012).

A prova digital pode ser definida como qualquer informação armazenada, processada ou transmitida por sistemas informáticos ou redes de comunicações que possua valor probatório, incluindo ficheiros, registos de atividade, mensagens, dados de tráfego ou metadados (National Institute of Standards and Technology, 2006). A natureza desta prova apresenta características específicas, como intangibilidade, volatilidade e facilidade de alteração, o que exige procedimentos especializados para garantir a autenticidade e integridade da informação recolhida (National Institute of Justice, 2008).

Para que os resultados obtidos sejam admissíveis em tribunal, é necessário assegurar simultaneamente o cumprimento de requisitos técnicos e legais, garantindo a autenticidade, integridade e fiabilidade da informação analisada (Kist, 2019). No ordenamento jurídico português, a admissibilidade da prova digital encontra

fundamento nos princípios constitucionais do processo penal, designadamente nas garantias de defesa, no princípio da legalidade e na proibição da utilização de provas obtidas por meios ilícitos. O Código de Processo Penal não contém uma definição autónoma de prova digital, sendo aplicáveis, por analogia, os regimes previstos para outros meios de obtenção de prova, complementados por legislação específica relativa ao cibercrime e à obtenção de dados eletrónicos.

A Lei n.º 109/2009, conhecida como Lei do Cibercrime, introduziu no ordenamento jurídico português mecanismos próprios para a obtenção de prova digital, adaptando o sistema processual às exigências do ambiente tecnológico. Este diploma transpõe para o direito interno a Convenção sobre o Cibercrime e estabelece medidas como a pesquisa informática, a apreensão de dados, a interceção de comunicações e a preservação de informação eletrónica (Assembleia da República, 2009; Conselho da União Europeia, 2001). Complementarmente, a Lei n.º 32/2008 regula a conservação e transmissão de dados de tráfego e de localização por operadores de comunicações, permitindo o seu acesso em investigações criminais, sobretudo em crimes graves (Lei n.º 32/2008, 2008).

Do ponto de vista técnico, a análise forense digital segue frequentemente modelos metodológicos reconhecidos internacionalmente. Um dos mais utilizados é o modelo proposto pelo National Institute of Standards and Technology (NIST), que organiza o processo forense em quatro fases principais: apreensão, aquisição, análise e reporte (National Institute of Standards and Technology, 2006). A fase de apreensão visa assegurar a preservação dos dados desde o momento da recolha; a aquisição corresponde à extração e tratamento da informação; a análise envolve a interpretação dos resultados e a reconstrução de eventos; e o reporte consiste na elaboração de um relatório técnico detalhado destinado às autoridades judiciais (Cohen, 2012).

A validade da prova digital depende da conformidade com normas legais e com boas práticas técnicas reconhecidas pela comunidade científica. A utilização de mecanismos de verificação de integridade, como funções de hash, bem como a preservação da autenticidade e confidencialidade dos dados são essenciais para garantir que a prova não foi alterada desde a sua recolha até à sua apresentação em tribunal (Cohen, 2012; Ramos, 2014). Neste contexto, a cooperação entre peritos forenses, autoridades de investigação criminal e magistrados assume particular relevância para assegurar o respeito simultâneo pelos requisitos técnicos e jurídicos.

Um elemento fundamental na análise forense digital é o conceito de metadados, entendidos como dados que descrevem outros dados e que fornecem informação sobre a sua origem, estrutura e contexto (Gilliland, 2016). A norma ISO 23081-1 classifica os metadados em categorias descritivas, estruturais e administrativas, todas relevantes para a gestão e preservação da informação digital (International Organization for Standardization, 2017). No contexto forense, os metadados permitem estabelecer a proveniência de um ficheiro, reconstruir sequências temporais e detetar alterações.

Outro conceito essencial é o da cadeia de custódia, correspondente ao conjunto de procedimentos destinados a documentar todas as fases do tratamento da prova digital, desde a sua identificação até à sua apresentação em tribunal. Este registo deve assegurar a integridade da prova, identificando responsáveis, datas, locais e transferências de responsabilidade (National Institute of Justice, 2008). A doutrina portuguesa sublinha que a observância rigorosa destes procedimentos é determinante para a admissibilidade da prova digital em juízo (Ramos, 2014).

Deste modo, a análise forense digital constitui uma área interdisciplinar que exige a articulação entre conhecimento técnico e enquadramento jurídico, sendo necessária a atualização permanente de métodos e normas para assegurar que a prova digital possa ser utilizada de forma válida, fiável e juridicamente admissível.

Esta secção apresenta o enquadramento da análise forense digital, abordando o enquadramento jurídico da prova digital em Portugal, seguido das principais normas e diretrizes internacionais aplicáveis à investigação forense digital.

2.1. Enquadramento Jurídico da Prova Digital

A análise forense digital de dispositivos móveis desenvolve-se no âmbito de um enquadramento jurídico complexo, destinado a garantir simultaneamente a eficácia da investigação criminal e a proteção dos direitos fundamentais. Em Portugal, este enquadramento resulta da articulação entre legislação penal, processual penal, normas específicas relativas à criminalidade informática e legislação de proteção de dados pessoais.

A Lei n.º 109/2009, conhecida como Lei do Cibercrime, estabelece os principais mecanismos de recolha e preservação de prova digital, em conformidade com a Convenção sobre o Cibercrime do Conselho da Europa (Convenção de Budapeste) (Assembleia da República, 2009; Council of Europe, 2001). O Regulamento (UE) 2016/679, relativo à proteção de dados pessoais, complementado pela Lei n.º 58/2019, impõe limites rigorosos ao tratamento de informação, atendendo à natureza sensível dos dados armazenados em dispositivos móveis.

O Código Penal tipifica crimes informáticos, enquanto o Código de Processo Penal regula as diligências de busca, apreensão e perícia, garantindo a integridade e a rastreabilidade da prova. Neste contexto, a investigação digital exige uma articulação permanente entre requisitos técnicos e princípios jurídicos, sob pena de comprometer a validade da prova em tribunal.

Como refere Rakha (2024), o combate ao cibercrime exige uma abordagem integrada entre os aspetos técnicos da investigação digital e os princípios jurídicos e éticos que a sustentam, sendo que a ausência dessa harmonização pode comprometer a admissibilidade e a legitimidade da prova digital.

Em conjunto, estas normas procuram assegurar um equilíbrio entre a eficácia da investigação criminal e o respeito pela legalidade processual e pela privacidade dos cidadãos, impondo que a recolha e análise de dados digitais sejam autorizadas, fundamentadas e realizadas segundo procedimentos controláveis.

2.1.1. Lei Cibercrime

A Lei n.º 109/2009, de 15 de setembro, conhecida como Lei do Cibercrime, estabelece o regime jurídico aplicável à criminalidade informática e define mecanismos específicos de obtenção de prova digital, transpondo para o ordenamento jurídico português a Convenção sobre o Cibercrime do Conselho da Europa e instrumentos europeus relativos à cooperação penal em matéria informática (Assembleia da República, 2009; Council of Europe, 2001; União Europeia, 2005).

O diploma introduz conceitos fundamentais como sistema informático, dados informáticos e fornecedor de serviços, que constituem a base para a aplicação das normas penais e processuais relativas à investigação digital. No plano substantivo, prevê crimes como acesso ilegítimo, interceção ilícita, sabotagem informática, falsidade informática e reprodução não autorizada de programas protegidos, bem como a responsabilidade penal das pessoas coletivas e a perda de instrumentos utilizados na prática do crime (Assembleia da República, 2009).

No plano processual, a lei estabelece meios específicos de obtenção de prova digital, incluindo a preservação expedita de dados, a revelação de dados de tráfego, a injunção para apresentação de informação, a pesquisa em sistemas informáticos, a apreensão de dados e a interceção de comunicações. Estes mecanismos assumem especial relevância na investigação forense digital, atendendo à natureza volátil da informação eletrónica, que pode ser rapidamente alterada ou eliminada.

A Lei do Cibercrime prevê ainda a aplicação subsidiária do Código de Processo Penal sempre que não exista regime próprio, assegurando que as diligências respeitam as garantias processuais fundamentais. A jurisprudência constitucional tem reforçado a necessidade de autorização judicial prévia quando estejam em causa direitos fundamentais, nomeadamente no acesso a comunicações eletrónicas, sublinhando a importância do controlo judicial na obtenção de prova digital (Tribunal Constitucional, 2021).

2.1.2. Proteção de Dados Pessoais e RGPD

A investigação forense digital envolve frequentemente o tratamento de dados pessoais, pelo que deve respeitar o regime jurídico da proteção de dados. O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho

estabelece o quadro jurídico aplicável ao tratamento de dados pessoais na União Europeia, reconhecendo a proteção de dados como direito fundamental e definindo princípios como a limitação da finalidade, a minimização dos dados, a proporcionalidade e a responsabilidade do responsável pelo tratamento (União Europeia, 2016).

Em Portugal, a Lei n.º 58/2019 assegura a execução do regulamento no ordenamento jurídico nacional, enquanto a Lei n.º 59/2019 regula o tratamento de dados pessoais por autoridades competentes para efeitos de prevenção, investigação e repressão de infrações penais, estabelecendo salvaguardas específicas para conciliar a segurança pública com a proteção dos direitos fundamentais (Portugal, 2019a; Portugal, 2019b).

A supervisão do cumprimento destas normas cabe à Comissão Nacional de Proteção de Dados, autoridade independente responsável pela fiscalização do tratamento de dados pessoais e pela aplicação de sanções em caso de violação das regras legais (Portugal, 2004).

A doutrina tem destacado o impacto do Regulamento Geral sobre a Proteção de Dados na investigação digital, exigindo que a recolha e tratamento de informação sejam autorizados, documentados e limitados ao estritamente necessário para a finalidade processual. Técnicas como a pseudonimização e a anonimização são frequentemente recomendadas para reduzir riscos para os titulares dos dados, mantendo simultaneamente a utilidade probatória da informação (Osório, 2023; Limberger et al., 2023).

No contexto da análise forense digital, o cumprimento destas normas é essencial para garantir que a prova obtida respeita os direitos fundamentais e pode ser utilizada validamente em processo judicial.

2.1.3. Código Penal

O Código Penal português define os tipos legais de crime e estabelece as respetivas sanções, tendo sido progressivamente adaptado para incluir normas relativas à criminalidade informática (Portugal, 1982). A ratificação da Convenção de Budapeste reforçou a necessidade de harmonização legislativa, conduzindo à introdução de disposições específicas relativas a sistemas informáticos e comunicações eletrónicas (Portugal, 2009).

A Lei do Cibercrime complementa o Código Penal ao tipificar condutas relacionadas com sistemas informáticos e redes de comunicação, devendo a interpretação destas normas respeitar os princípios gerais da tipicidade, ilicitude e culpa. Entre os crimes relevantes destacam-se o acesso ilegítimo, a sabotagem informática, a falsidade informática e a burla informática, frequentemente associados à obtenção de prova digital em dispositivos móveis.

A investigação de crimes informáticos exige a recolha de prova digital capaz de demonstrar a autoria, a materialidade do facto e a ligação entre o agente e o sistema informático. A volatilidade dos dados eletrónicos obriga à utilização de procedimentos técnicos adequados, como a criação de cópias forenses e a verificação de integridade através de funções de hash, de modo a assegurar a fiabilidade da prova (Casey, 2011).

A doutrina portuguesa tem sublinhado que a validade da prova digital depende da utilização de métodos reconhecidos e da intervenção de peritos qualificados, capazes de garantir que a análise respeita os padrões técnicos e jurídicos exigidos pelo processo penal (Marques Branco, 2021).

2.1.4. Código Processo Penal

O Código de Processo Penal estabelece o regime geral da prova e define as regras aplicáveis à recolha, preservação e apresentação de elementos probatórios (Portugal, 1987). No contexto da análise forense digital, assumem especial relevância as normas relativas à prova pericial, às buscas e apreensões e à interceção de comunicações.

A prova pericial é necessária sempre que a apreciação dos factos exige conhecimentos técnicos ou científicos, sendo essencial na informática forense, onde a interpretação dos dados requer competências especializadas. O relatório pericial deve documentar todas as operações realizadas, permitindo o controlo judicial e o exercício do contraditório (Veríssimo, 2023).

As buscas e apreensões dependem, em regra, de autorização judicial e devem ser realizadas de forma proporcional e devidamente documentada. A Lei do Cibercrime adapta estas regras ao ambiente informático, prevendo procedimentos específicos para a pesquisa e apreensão de dados, mantendo, contudo, a exigência de controlo judicial sempre que estejam em causa direitos fundamentais.

A jurisprudência tem afirmado que a apreensão de comunicações eletrónicas requer despacho do juiz de instrução, distinguindo-se entre interceção de comunicações em trânsito e acesso a mensagens armazenadas, regimes que obedecem a requisitos legais distintos. O regime de interceção de comunicações é restrito a determinados crimes e depende de autorização judicial prévia, incluindo regras rigorosas quanto à execução e conservação dos registos.

Embora o Código de Processo Penal não utilize expressamente o termo cadeia de custódia, as regras relativas à apreensão, guarda e documentação de objetos impõem a preservação da integridade da prova. Na análise forense digital, essa integridade é garantida através de técnicas como o cálculo de valores de hash e o registo de metadados, que permitem verificar que os dados não foram alterados desde a sua recolha (Casey, 2011).

Assim, o Código de Processo Penal fornece o enquadramento legal geral da prova, enquanto a Lei do Cibercrime estabelece mecanismos específicos adaptados ao ambiente digital. A conjugação entre normas jurídicas, procedimentos técnicos e controlo judicial é essencial para assegurar que a prova digital obtida em dispositivos móveis seja válida, fiável e admissível em tribunal.

2.2. Normas e Diretrizes Internacionais

A análise forense digital é orientada não apenas por legislação nacional, mas também por normas e diretrizes internacionais que estabelecem boas práticas para a recolha, preservação e análise de evidência digital. Estas orientações contribuem para a uniformização de procedimentos, promovendo maior rigor metodológico e reforçando a credibilidade da prova digital em contexto judicial. Entre os referenciais mais relevantes destacam-se as publicações do National Institute of Standards and Technology (NIST), as diretrizes da INTERPOL para primeiros intervenientes em evidência digital e as normas da International Organization for Standardization (ISO), que estabelecem princípios e procedimentos amplamente reconhecidos na comunidade científica e forense.

Nos pontos seguintes serão analisadas estas normas e orientações, evidenciado o seu contributo para a investigação forense digital em dispositivos móveis.

2.2.1. Publicações NIST

O NIST, organismo norte-americano de referência na definição de normas e boas práticas nos domínios da segurança da informação e da ciência forense digital, tem publicado um conjunto relevante de documentos orientadores para profissionais, académicos e instituições. Estas publicações assumem particular importância por fornecerem metodologias estruturadas, tecnicamente sólidas e internacionalmente reconhecidas, promovendo procedimentos rigorosos na recolha, preservação, análise e apresentação de prova digital.

Entre os documentos mais relevantes para a forense digital destacam-se a NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response, dedicada à integração de técnicas forenses nos processos de resposta a incidentes; a NIST SP 800-72: Guidelines on PDA Forensics, centrada nos dispositivos PDA, precursores dos smartphones; a NIST SP 800-115: Technical Guide to Information Security Testing and Assessment, voltada para testes e auditorias de segurança; e, sobretudo, a NIST SP 800-101 Revision 1: Guidelines on Mobile Device Forensics, que constitui atualmente uma das principais referências internacionais para a análise forense de dispositivos móveis (National Institute of Standards and Technology, 2006; Ayers et al., 2014).

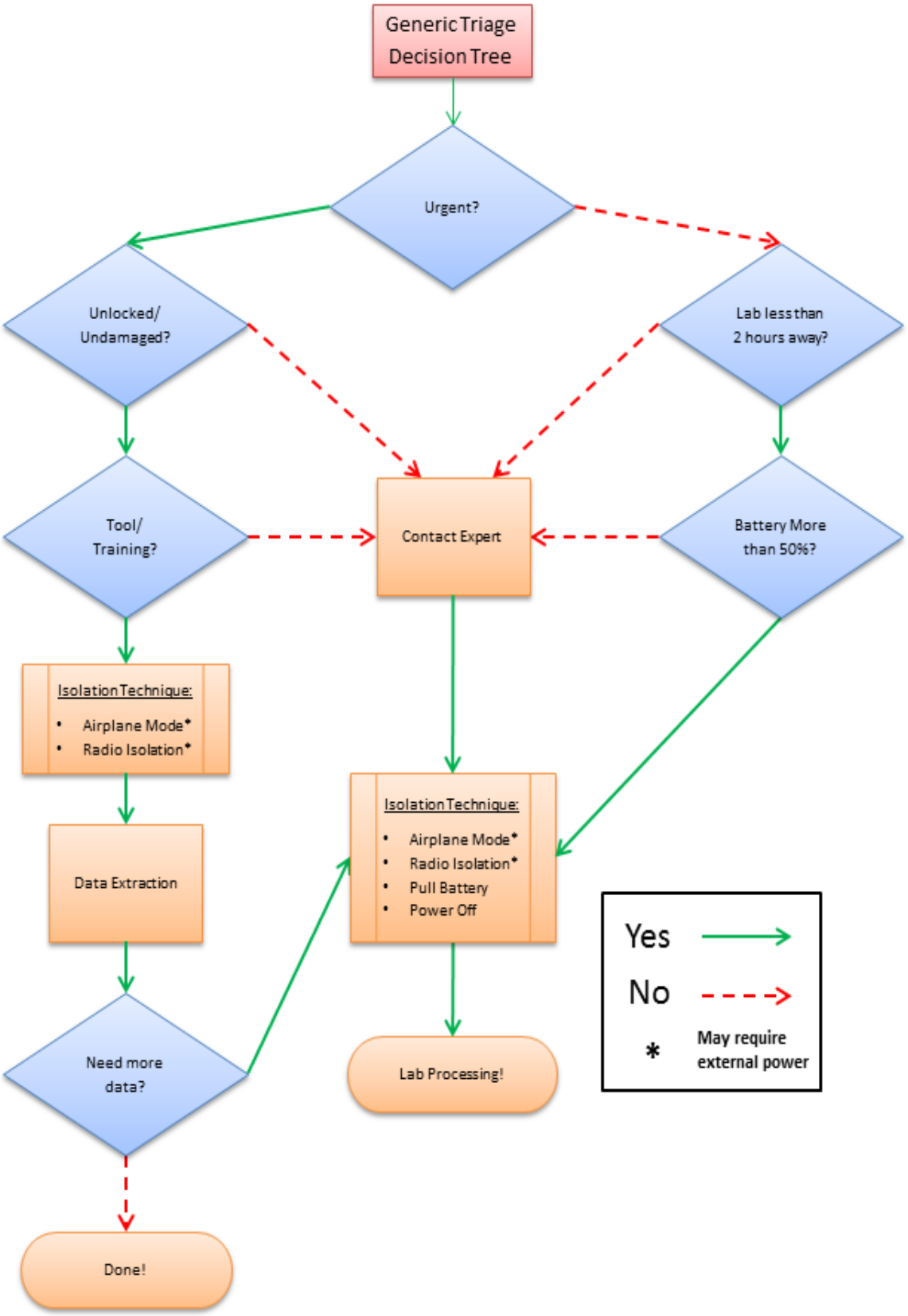
No que respeita à análise forense aplicada a dispositivos móveis, a NIST SP 800-101 Revision 1 ocupa lugar central. O documento surgiu como resposta à transformação tecnológica que converteu smartphones e tablets em repositórios de informação pessoal e profissional. Estes equipamentos concentram hoje comunicações, registos de localização, contas de correio eletrónico, conteúdos multimédia, aplicações bancárias, redes sociais e acesso a serviços em nuvem, tornando-se fontes privilegiadas de prova digital. Em simultâneo, essa evolução tecnológica aumentou a complexidade da sua análise forense, devido à diversidade de plataformas, ao ritmo acelerado de atualização dos sistemas e à crescente sofisticação dos mecanismos de segurança.

A publicação estrutura o processo forense em quatro grandes fases – apreensão, aquisição, análise e reporte – concebidas para assegurar não apenas a extração de dados relevantes, mas também a sua validade, integridade e admissibilidade em tribunal (Ayers et al., 2014). Estas fases não devem, contudo, ser entendidas como etapas rígidas e absolutamente lineares. Em contexto prático, podem ocorrer sobreposições, repetições e ajustamentos metodológicos em função das características concretas de cada caso, nomeadamente quando há necessidade de validar dados intermédios, repetir aquisições ou agir rapidamente perante informação volátil em risco de perda. Essa flexibilidade não fragiliza o processo; pelo contrário, reforça-o, porque permite adaptar a metodologia às circunstâncias da investigação sem comprometer o rigor técnico e jurídico.

A Figura 1 apresenta a triagem recomendada pela NIST SP 800-101 (Ayers et al., 2014). Esse fluxograma orienta o processo decisório nas fases iniciais da recolha de dispositivos, considerando fatores como a urgência do caso, o estado do equipamento, o nível de bateria e os recursos técnicos disponíveis. Em situações urgentes, a prioridade incide sobre a avaliação imediata do estado do dispositivo, a aplicação de técnicas de isolamento e, quando possível, a extração de dados. Em contextos menos urgentes, o modelo orienta o envio seguro do dispositivo para o laboratório, reduzindo o risco de perda, alteração ou contaminação dos dados e reforçando a fiabilidade da prova recolhida.

Deste modo, a Lei do Cibercrime constitui o principal instrumento jurídico na investigação forense digital, definindo simultaneamente o quadro penal e os procedimentos de recolha de prova em ambiente informático.

Figura 1: Procedimento geral proposto na NIST SP 800-101.



Fonte: NIST.

Cada uma das fases referidas é detalhada de seguida.

Fase 1: Apreensão

A apreensão constitui o ponto de partida do processo forense e assume importância decisiva para a validade da evidência digital. O seu objetivo é garantir que os dados existentes no dispositivo permanecem inalterados desde o momento da apreensão até à análise laboratorial, preservando a integridade, a autenticidade e a admissibilidade da prova.

No local da ocorrência, a primeira exigência consiste na documentação rigorosa do dispositivo e do contexto em que foi encontrado. Devem ser registadas as condições em que o equipamento se apresenta, nomeadamente se está ligado ou desligado, bloqueado ou desbloqueado, ligado à rede ou em modo offline, bem como o ambiente físico da apreensão. Esta documentação deve incluir fotografias, anotações detalhadas e identificação dos intervenientes presentes, de modo a fixar o estado inicial da evidência.

Um dos aspetos mais sensíveis desta fase é o isolamento do dispositivo, destinado a impedir alterações remotas aos dados, resultantes de sincronizações automáticas, atualizações, comunicações de rede ou ações deliberadas de terceiros. Para esse efeito, podem ser utilizadas bolsas de Faraday ou, quando operacionalmente viável, ativado o modo de voo. Em paralelo, deve ser assegurada a conservação física do equipamento, com recurso a invólucros adequados e embalagens seladas, protegendo-o contra danos mecânicos e ambientais.

O transporte até ao laboratório deve ocorrer em condições controladas e devidamente documentadas, de modo a manter a cadeia de custódia. Cada intervenção sobre o dispositivo deve ser registada, incluindo a identificação de quem apreendeu o equipamento, em que circunstâncias, que procedimentos foram adotados e quem teve acesso posterior à evidência. Em síntese, a apreensão constitui a base de todo o procedimento forense: sem uma recolha inicial rigorosa, a análise subsequente pode perder valor técnico e jurídico.

Fase 2: Aquisição

A aquisição representa uma das fases mais críticas da análise forense em dispositivos móveis, pois dela dependem a preservação do conteúdo digital e a possibilidade de replicação futura da análise. A NIST SP 800-101 organiza esta fase segundo uma classificação em cinco níveis, diferenciados pelo grau de complexidade técnica, intrusividade e profundidade de acesso à memória do equipamento (Ayers et al., 2014).

O primeiro nível corresponde à aquisição manual, em que o perito interage diretamente com o dispositivo e regista a informação visível no ecrã. Trata-se de um método simples e pouco intrusivo, útil em cenários urgentes ou na ausência de ferramentas especializadas, mas limitado à informação acessível visualmente e sujeito a erro humano (Ayers et al., 2014).

O segundo nível é a aquisição lógica, que permite extrair objetos de dados através do sistema operativo do dispositivo e das interfaces de comunicação disponíveis. Este método possibilita o acesso a mensagens, contactos, registos de chamadas, emails, ficheiros multimédia e dados de aplicações, sendo amplamente suportado por ferramentas forenses e apresentando a vantagem de ser relativamente rápido e não intrusivo. Contudo, raramente permite recuperar dados apagados ou aceder a áreas protegidas da memória.

O terceiro nível corresponde à aquisição física, que produz uma cópia bit a bit da memória do dispositivo, permitindo aceder a dados ativos, apagados ou fragmentados. Entre as técnicas possíveis incluem-se o recurso a interfaces de depuração JTAG e a utilização de bootloaders modificados (Joint Test Action Group, 2013). Embora este método seja mais completo, exige equipamento especializado, maior conhecimento técnico e comporta riscos acrescidos para o equipamento (Ayers et al., 2014).

O quarto nível, designado chip-off, consiste na remoção física do chip de memória para leitura externa, sendo reservado para situações em que o dispositivo está danificado ou em que os métodos anteriores falharam. É uma técnica altamente invasiva e potencialmente destrutiva, que requer condições laboratoriais adequadas e elevada especialização (Ayers et al., 2014).

O quinto e último nível é o micro-read, técnica extremamente especializada que consiste na leitura direta das células de memória através de microscopia eletrónica. Dada a sua complexidade, custo e morosidade, constitui uma solução de último recurso, aplicável apenas em casos excecionais.

Para além da memória interna do dispositivo, a aquisição deve abranger outras fontes relevantes de prova, como cartões SIM/UICC, cartões de memória removíveis e dados armazenados em cloud. Os cartões SIM/UICC podem conter identificadores como o IMSI e o ICCID, bem como mensagens, contactos e outros registos relevantes, sendo analisados com leitores especializados (MSAB, 2025).

Os cartões SD ou microSD devem ser tratados como suportes removíveis e sujeitos a clonagem forense, com verificação de integridade por meio de hashes. Já os dados em cloud assumem importância crescente, dado que muitos sistemas e aplicações realizam cópias automáticas para serviços remotos. A sua recolha amplia o alcance da investigação, mas exige cuidados acrescidos de ordem técnica e jurídica, nomeadamente no que respeita à obtenção de credenciais ou autorizações judiciais (Ayers et al., 2014).

A aquisição de dados em *Cloud* tornou-se parte das investigações forenses, pois dispositivos móveis podem criar cópias de segurança em serviços como iCloud, Google Drive ou OneDrive. A informação pode estar armazenada fora do equipamento. A recolha desses dados requer credenciais do utilizador ou ordens judiciais para acesso aos conteúdos. Ferramentas forenses incluem módulos de extração em *Cloud*, permitindo sincronizar e descarregar dados de contas online. A aquisição aumenta o alcance da investigação e exige controlo da cadeia de custódia e cumprimento do enquadramento jurídico (Ayers et al., 2014).

Fase 3: Análise

A fase de análise é aquela em que os dados adquiridos são processados, interpretados e correlacionados, com vista à produção de informação dotada de valor probatório. Se nas fases anteriores se privilegia a preservação da evidência, aqui a ênfase recai sobre a sua interpretação contextual e técnica, permitindo responder a questões concretas da investigação (Ayers et al., 2014).

O tratamento inicial da evidência inclui a organização e filtragem dos dados, a identificação de estruturas de ficheiros, a extração de bases de dados internas, a indexação de documentos e a recuperação de informação oculta, fragmentada ou eliminada. Técnicas de parsing permitem reconstruir conteúdos de aplicações móveis, tais como mensagens, históricos de navegação e registos de localização, mesmo quando dispersos por múltiplos ficheiros ou diretórios.

A análise pressupõe também a correlação dos dados com hipóteses investigatórias. Entre as operações mais relevantes incluem-se a associação entre chamadas, mensagens e contactos, a reconstrução de percursos com base em dados de GPS ou torres de telecomunicações, a identificação de comunicações em redes sociais e a deteção de programas maliciosos ou técnicas de ocultação de atividade. Em casos complexos, é frequente recorrer à validação cruzada com diferentes ferramentas, para confirmar a consistência e fiabilidade dos resultados.

Entre os principais desafios desta fase destaca-se a encriptação, cada vez mais presente nos dispositivos modernos. PIN, passwords, padrões de desbloqueio e mecanismos biométricos podem limitar o acesso à informação, obrigando ao recurso a técnicas específicas, sempre em conformidade com o enquadramento legal. Também os formatos proprietários e os mecanismos de compressão exigem ferramentas forenses atualizadas e adequadas.

Os dispositivos móveis oferecem uma grande diversidade de fontes de evidência, incluindo registos de chamadas, mensagens SMS e MMS, correio eletrónico, histórico de navegação, dados de geolocalização, fotografias e vídeos com metadados embutidos, aplicações de mensagens instantâneas e redes sociais. A dimensão temporal da evidência é igualmente decisiva: a correlação entre timestamps, registos de chamadas e eventos de GPS permite reconstruir cronologias de atividade essenciais para a prova dos factos.

As ferramentas utilizadas nesta fase incluem soluções comerciais e plataformas de código aberto, cuja escolha deve atender à fiabilidade, capacidade de validação e documentação do processo. O essencial é que a análise seja repetível, tecnicamente sustentada e adequadamente registada, de forma a garantir a admissibilidade legal da prova (Sutikno, 2024; Ferreira, 2020). Em síntese, esta fase transforma a evidência digital em conhecimento útil, articulando sofisticação técnica com capacidade interpretativa do perito.

Fase 4: Reporte

A fase final consiste na elaboração do relatório pericial, documento técnico em que os resultados da análise devem ser apresentados de forma estruturada, clara, objetiva e auditável. O relatório não se limita à enumeração dos dados extraídos; deve descrever pormenorizadamente os métodos aplicados, as ferramentas utilizadas, as versões de software, os valores de integridade e as operações realizadas, permitindo que terceiros compreendam, avaliem e, se necessário, reproduzam o procedimento (Ayers et al., 2014).

Um relatório forense robusto deve incluir, em primeiro lugar, a identificação da evidência analisada, com descrição do dispositivo, suportes associados, características técnicas e estado em que foi apreendido. Deve igualmente explicitar as metodologias adotadas, justificando a escolha de determinadas técnicas de preservação, aquisição, exame e análise, bem como indicar as ferramentas utilizadas em cada etapa e as respetivas limitações conhecidas.

Os resultados devem ser apresentados de forma sistematizada, acompanhados de elementos de suporte como capturas de ecrã, logs e registos de hashes. Devem também ser identificadas as limitações encontradas, incluindo dados inacessíveis devido a encriptação, incompatibilidades técnicas ou ausência de credenciais de acesso a serviços remotos. A documentação da cadeia de custódia é igualmente indispensável, assegurando a rastreabilidade completa do processo e a identificação de todos os intervenientes que tiveram contacto com a evidência.

Por fim, o relatório deve culminar em conclusões objetivas, diretamente relacionadas com as questões formuladas pela autoridade judiciária ou com os objetivos da investigação. A inclusão de anexos técnicos, como relatórios automáticos, cronologias ou listas detalhadas de hashes, reforça a transparência e a auditabilidade do processo, permitindo uma apreciação crítica por especialistas e pelo tribunal.

Outros Aspetos

Para além da estrutura metodológica, o NIST chama a atenção para vários aspetos técnicos que podem condicionar a eficácia da análise forense em dispositivos móveis. Um deles é a distinção entre memória volátil e não volátil. A memória volátil pode conter dados temporários particularmente relevantes, como credenciais ou chaves de sessão, mas perde o seu conteúdo quando o dispositivo é desligado. Já a memória não volátil armazena dados persistentes e pode, devido a mecanismos internos de gestão, conservar fragmentos ou múltiplas versões de ficheiros suscetíveis de recuperação (Ayers et al., 2014).

Outro aspeto relevante respeita aos cartões SIM/UICC, cuja análise autónoma pode revelar dados não acessíveis através do terminal, como identificadores de rede e certos registos de comunicações. O NIST sublinha também a importância dos CDR mantidos pelas operadoras, que complementam a análise realizada ao dispositivo ao fornecerem informação sobre localização aproximada, duração das chamadas, volume de tráfego e interações entre utilizadores.

Finalmente, a publicação aborda o problema dos dispositivos protegidos por bloqueios ou encriptação. Embora descreva abordagens técnicas para ultrapassar tais barreiras, o documento alerta para os riscos significativos de perda ou alteração da evidência, recomendando que essas técnicas sejam empregues apenas por peritos altamente especializados e em estrita conformidade com as exigências legais.

Em conclusão, a NIST SP 800-101 estabelece um quadro metodológico de referência que conjuga rigor técnico com conformidade legal, promovendo práticas orientadas para a eficácia da extração de dados e para a sua

aceitabilidade em tribunal. Mais do que um manual prescritivo, constitui um guia de boas práticas fundamental para a normalização internacional da análise forense digital em dispositivos móveis e para o desenvolvimento de capacidades institucionais nesta área.

2.2.2. Diretrizes INTERPOL

A INTERPOL, enquanto organização policial internacional, tem como missão promover a cooperação entre diferentes jurisdições no combate ao crime transnacional. No domínio da cibercriminalidade, essa missão traduziu-se na definição de orientações técnicas e operacionais destinadas a apoiar os primeiros intervenientes no local — agentes policiais, investigadores ou peritos que contactam inicialmente com incidentes envolvendo dispositivos digitais. Estas orientações procuram harmonizar procedimentos, reduzir o risco de adulteração da evidência e assegurar que os métodos de recolha permanecem compatíveis com a realidade tecnológica contemporânea (INTERPOL Innovation Centre, 2021).

As orientações da INTERPOL sintetizam aquilo que a organização entende como melhores práticas forenses internacionais e assumem especial relevância no contexto da apreensão inicial de dispositivos digitais, incluindo smartphones e tablets. Tal como sucede com outros referenciais internacionais, nomeadamente os documentos do NIST, estas diretrizes procuram assegurar que a atuação dos primeiros intervenientes seja rápida, eficaz e juridicamente sustentada. Contudo, ao contrário do modelo do NIST, mais abrangente e estruturado em quatro fases, as orientações da INTERPOL concentram-se sobretudo na fase inicial da intervenção, privilegiando a preparação da apreensão e a própria apreensão, com especial atenção às exigências operacionais do trabalho de campo.

O documento mais relevante neste contexto é o Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence, por se destinar especificamente às equipas responsáveis pela apreensão e tratamento inicial de dispositivos digitais. O ponto de partida destas orientações é claro: a evidência digital, pela sua volatilidade e suscetibilidade de alteração ou destruição, deve ser tratada com elevado rigor metodológico, de forma a preservar a sua integridade, autenticidade e admissibilidade legal. Por isso, a INTERPOL recomenda que toda a intervenção seja cuidadosamente planeada, documentada e executada segundo procedimentos padronizados (INTERPOL Innovation Centre, 2021).

Fase 1: Preparação da Apreensão

A preparação da apreensão constitui o alicerce de qualquer operação forense em ambiente digital. Segundo a INTERPOL, uma intervenção mal preparada pode comprometer de forma irreversível a recolha da prova, conduzindo à perda de dados voláteis, à contaminação da evidência ou mesmo à sua rejeição em tribunal por incumprimento de requisitos legais. A preparação deve, por isso, ser entendida como um processo sistemático que integra dimensões jurídicas, técnicas, logísticas e humanas.

O primeiro passo consiste na definição clara dos objetivos e do âmbito da operação. A equipa deve compreender a natureza do crime em investigação, antecipar os tipos de dispositivos que poderá encontrar e identificar os dados cuja preservação deverá ser prioritária. Esta delimitação orienta a seleção das ferramentas, a composição da equipa e as prioridades operacionais no terreno.

A constituição da equipa de intervenção deve igualmente ser planeada com rigor. Para além dos primeiros intervenientes, podem ser necessários peritos em forense digital, técnicos especializados em redes ou servidores, agentes de segurança para o isolamento da cena e representantes legais que garantam a conformidade da operação com as normas aplicáveis. A definição prévia de funções e responsabilidades reduz o risco de falhas de comunicação, sobreposição de tarefas ou perda de informação crítica.

A preparação jurídica assume também um papel central. Antes da intervenção, devem ser obtidos e verificados os mandados de busca e apreensão ou outras autorizações legais relevantes, incluindo a sua validade temporal e territorial. Em determinadas situações, pode ainda ser necessário preparar pedidos destinados ao acesso a dados armazenados em servidores remotos ou serviços de nuvem, o que pode implicar mecanismos de

cooperação internacional. Sem esta base legal, a prova recolhida pode tornar-se inadmissível, independentemente da sua relevância material.

No plano técnico, a preparação exige a verificação rigorosa dos kits de apreensão digital. Estes devem incluir, entre outros materiais, sacos de Faraday para impedir comunicações sem fios, bloqueadores de escrita que permitam o acesso a suportes digitais sem alteração dos dados originais, duplicadores forenses, software de aquisição para criação de imagens bit a bit, câmaras fotográficas para registo da cena, etiquetas invioláveis, blocos de notas, fontes de energia portáteis e cabos compatíveis com diferentes equipamentos. Devem ainda estar disponíveis materiais de acondicionamento, como sacos antiestáticos e recipientes resistentes a impactos ou variações de temperatura.

Acresce a necessidade de uma avaliação prévia dos riscos associados à operação. Devem ser considerados não apenas riscos físicos, como condições perigosas do local, mas também riscos digitais, incluindo a possibilidade de eliminação remota de dados, sincronização automática com serviços em nuvem ou ativação de mecanismos de encriptação após desligamento do equipamento. Antecipar estes cenários permite à equipa preparar decisões críticas, nomeadamente sobre a conveniência de uma aquisição em vivo ou da apreensão imediata do dispositivo.

Por fim, a preparação envolve a coordenação entre todos os elementos da equipa. Antes da execução, todos devem conhecer o plano da operação, a sequência de entrada no local, os procedimentos de isolamento da cena, os responsáveis por cada tarefa e as medidas de contingência a adotar em caso de resistência, falha técnica ou descoberta imprevista. Esta coordenação reduz a margem de erro e aumenta a eficácia e robustez da recolha de prova digital.

Fase 2: Apreensão

A fase de apreensão corresponde ao momento em que a operação entra em execução e os primeiros intervenientes passam a interagir diretamente com a cena e com os dispositivos digitais. Trata-se de uma etapa particularmente sensível, porque as decisões tomadas no local podem determinar o sucesso ou fracasso da recolha e preservação da evidência. A INTERPOL sublinha que esta fase deve ser conduzida com disciplina, atenção ao detalhe e estrito respeito pelos princípios da integridade, autenticidade e legalidade da prova (INTERPOL Innovation Centre, 2021).

Ao chegar ao local, a prioridade consiste no controlo e isolamento da cena. É essencial impedir o acesso de pessoas não autorizadas aos dispositivos, evitando manipulações, apagamentos ou transmissões remotas de dados. Em seguida, deve ser efetuada uma avaliação rápida do espaço, com identificação de todos os equipamentos digitais relevantes, incluindo computadores, smartphones, tablets, servidores, sistemas de videovigilância, consolas ou dispositivos IoT. Antes de qualquer manipulação, deve ser realizada documentação fotográfica e descritiva do estado em que os equipamentos foram encontrados, preservando o contexto original da cena.

A manipulação dos dispositivos é um dos momentos mais delicados da operação. Os equipamentos podem estar desligados, ligados ou em modo de suspensão, e cada uma destas situações exige decisões técnicas próprias. Se o dispositivo estiver desligado, a recomendação é, em regra, não o ligar, pois isso pode desencadear alterações automáticas, rotinas de encriptação ou perda de vestígios em memória volátil. Quando o dispositivo se encontra ligado, deve ponderar-se cuidadosamente a conveniência de o manter ativo, de forma a preservar dados transitórios, como memória RAM, sessões abertas ou ligações de rede. Essa decisão, porém, comporta riscos, incluindo a possibilidade de acessos remotos não autorizados ou ativação de mecanismos de destruição de dados. Por isso, qualquer opção tomada deve ser rigorosamente documentada, incluindo a fundamentação técnica e jurídica subjacente.

Nos equipamentos em suspensão, a complexidade é ainda maior, uma vez que o retomar da atividade pode desencadear sincronizações, atualizações ou encriptação automática. Nestes casos, a decisão sobre o

procedimento adequado deve ser reservada a profissionais qualificados e orientada por protocolos previamente definidos.

Outro elemento central desta fase é o registo em tempo real de todas as ações realizadas. Cada intervenção sobre um dispositivo deve ser documentada, indicando o agente responsável, a hora da atuação e os meios utilizados. Este registo contínuo é essencial para a cadeia de custódia, permitindo demonstrar, em momento posterior, que a evidência permaneceu íntegra e juridicamente válida.

A apreensão em contexto digital deve ainda incluir a recolha de informação complementar sobre o ambiente tecnológico envolvente. Elementos como redes Wi-Fi disponíveis, ligações Bluetooth ativas, cabos conectados e periféricos em uso podem fornecer dados relevantes sobre a utilização dos dispositivos e sobre as interações entre equipamentos ou utilizadores.

Fase 3: Preservação

A preservação consiste na adoção de medidas destinadas a garantir que a evidência recolhida se mantém íntegra e apta a ser analisada posteriormente. Uma das práticas centrais nesta fase é a criação de cópias forenses completas, através de imagens bit a bit da memória, acompanhadas de mecanismos de verificação de integridade, como resumos criptográficos.

Este procedimento permite demonstrar que a cópia corresponde fielmente ao original, assegurando a sua preservação para futuras análises e reforçando a sua aceitação em tribunal. No caso específico dos dispositivos móveis, recomenda-se a sua colocação imediata em modo de voo e o respetivo acondicionamento em sacos de Faraday. Simultaneamente, devem ser extraídos e preservados de forma autónoma os cartões SIM e os cartões de memória, por poderem conter dados relevantes que não estejam disponíveis no dispositivo principal.

Os cartões SIM podem armazenar elementos importantes, como o IMSI, o ICCID e determinados códigos de acesso, enquanto os cartões de memória podem conter fotografias, vídeos, bases de dados de aplicações ou outros ficheiros relevantes para a investigação. A sua análise deve ser realizada separadamente e sempre acompanhada de documentação adequada.

A INTERPOL chama também a atenção para a relevância das ligações de rede associadas aos dispositivos móveis. O registo de redes Wi-Fi conhecidas e de conexões Bluetooth pode fornecer informação útil sobre os locais frequentados pelo utilizador e as interações estabelecidas com outros dispositivos. Além disso, muitos smartphones estão sincronizados com serviços de nuvem, como Google Drive ou iCloud, o que significa que a preservação da prova não se pode limitar ao equipamento físico. Em muitos casos, será necessário recorrer a pedidos legais complementares dirigidos a fornecedores de serviços para obter acesso aos dados armazenados remotamente.

Outros Aspetos

As diretrizes da INTERPOL assumem especial importância por promoverem uma linguagem comum e uma metodologia partilhada entre diferentes países, facilitando a cooperação internacional entre autoridades policiais e aumentando a probabilidade de aceitação da prova digital em processos transnacionais. A sua utilidade é particularmente evidente em investigações que envolvem múltiplas jurisdições e exigem compatibilização de procedimentos operacionais.

Contudo, estas orientações não têm caráter vinculativo e devem ser sempre enquadradas nas exigências legais de cada ordenamento jurídico. Não substituem, por isso, normas técnicas nacionais ou regionais, como as do NIST nos Estados Unidos ou outras recomendações europeias, mas funcionam como referencial complementar particularmente útil em operações com dimensão internacional.

Em síntese, as diretrizes da INTERPOL representam um contributo relevante para a harmonização internacional da prática forense digital, sobretudo no que respeita à atuação dos primeiros intervenientes em operações de

busca e apreensão de dispositivos digitais. No caso dos dispositivos móveis, a sua importância é ainda maior, dada a centralidade destes equipamentos na vida quotidiana e o seu crescente valor enquanto fontes de evidência digital.

2.2.3. Normas ISO

A norma ISO/IEC 27037:2012, elaborada conjuntamente pela International Organization for Standardization (ISO) e pela International Electrotechnical Commission (IEC), centra-se na gestão da evidência digital e constitui um dos principais referenciais internacionais neste domínio. Publicada num contexto de crescente dependência das tecnologias da informação e de proliferação de incidentes com relevância probatória, esta norma estabelece orientações para a identificação, recolha, aquisição e preservação de evidência digital, com o objetivo de garantir a sua integridade, autenticidade e fiabilidade para utilização em processos judiciais ou disciplinares (International Organization for Standardization, 2012).

O seu âmbito de aplicação é amplo, abrangendo uma grande diversidade de dispositivos e suportes digitais, incluindo computadores pessoais, discos rígidos, dispositivos móveis, cartões de memória, sistemas de navegação, câmaras digitais, sistemas de videovigilância e infraestruturas de rede. A norma dirige-se quer aos primeiros intervenientes, quer aos peritos responsáveis pelo tratamento da evidência, impondo que o manuseamento dos vestígios digitais seja efetuado de forma sistemática, imparcial e conforme à legislação aplicável em cada jurisdição.

A ISO/IEC 27037:2012 assenta em três princípios gerais fundamentais: relevância, integridade e suficiência. A relevância reporta-se à capacidade da evidência para contribuir de forma significativa para provar ou refutar factos em investigação. A integridade exige que os dados correspondam efetivamente ao estado em que foram encontrados, o que implica a utilização de mecanismos de validação, como funções de verificação criptográfica. Por fim, a suficiência refere-se à necessidade de recolher dados em quantidade e qualidade bastantes para permitir uma análise completa e robusta. Estes princípios são ainda reforçados por exigências de auditabilidade, repetibilidade e reprodutibilidade, assegurando que os procedimentos adotados podem ser avaliados e, quando necessário, replicados por outros peritos de forma independente. A norma enfatiza igualmente a importância da justificação das decisões tomadas, exigindo que, cada ação ou método aplicado seja, tecnicamente fundamentado e defensável em sede judicial ou disciplinar.

A estrutura metodológica proposta pela norma organiza-se em quatro fases: identificação, recolha, aquisição e preservação. Estas fases estabelecem um encadeamento lógico destinado a assegurar o tratamento adequado da evidência desde o primeiro contacto com os suportes digitais até ao seu armazenamento seguro.

Fase 1: Identificação

A fase de identificação consiste na procura, reconhecimento e documentação dos dispositivos ou suportes suscetíveis de conter evidência digital. Esta etapa abrange tanto dados voláteis, como a informação presente em memória RAM ou em processos ativos, como dados não voláteis, armazenados em discos rígidos, cartões de memória ou outros suportes persistentes. O objetivo principal é reconhecer, de forma tão exaustiva quanto possível, todas as potenciais fontes de evidência e documentar o seu estado inicial, evitando omissões que possam comprometer a investigação posterior (International Organization for Standardization, 2012).

Fase 2: Recolha

A recolha corresponde à remoção física dos dispositivos e ao seu transporte para ambientes controlados, devendo ser efetuada de modo a preservar o estado original dos sistemas. Esta fase não se limita aos equipamentos principais, exigindo também atenção a elementos complementares que possam ser relevantes, como periféricos, suportes auxiliares, anotações manuscritas com credenciais de acesso ou outros objetos associados. A norma sublinha que a recolha deve ser planeada e executada com rigor, de forma a evitar alterações acidentais, perdas de informação ou contaminação da evidência.

Fase 3: Aquisição

A aquisição consiste na criação de cópias forenses da informação, preferencialmente por meio de imagens bit a bit dos suportes digitais. Estas cópias devem ser validadas por funções de verificação, assegurando que correspondem fielmente ao conteúdo original. A norma destaca a necessidade de documentar detalhadamente esta fase, incluindo as ferramentas utilizadas, as versões de software, as condições técnicas do procedimento e quaisquer limitações ou alterações inevitáveis, como a existência de setores defeituosos ou a impossibilidade de desligar determinados sistemas críticos. Esta exigência de documentação reforça a transparência do procedimento e a credibilidade dos resultados obtidos (International Organization for Standardization, 2012).

Fase 4: Preservação

A fase de preservação visa proteger a evidência digital contra alteração, degradação ou destruição. Para tal, a norma recomenda o armazenamento seguro em instalações adequadas, bem como a utilização de embalagens antiestáticas, etiquetas invioláveis e condições ambientais controladas, nomeadamente quanto à temperatura, humidade, campos magnéticos e exposição à luz. A preservação não deve ser entendida apenas como armazenamento físico, mas como um conjunto de medidas destinadas a manter a integridade da evidência ao longo de todo o seu ciclo de vida, desde a recolha até à eventual apresentação em tribunal.

Outros Aspetos

A norma atribui especial relevância à cadeia de custódia, entendida como o registo cronológico de todos os movimentos, acessos e intervenções sobre a evidência desde a sua recolha até ao termo do seu ciclo de vida. Este registo é essencial para demonstrar que a prova permaneceu íntegra, devidamente controlada e acessível apenas a pessoas autorizadas. A correta manutenção da cadeia de custódia constitui, assim, uma condição decisiva para a admissibilidade e credibilidade da prova digital.

Em síntese, a ISO/IEC 27037:2012 oferece um enquadramento metodológico robusto para a gestão de evidência digital, permitindo uniformizar procedimentos a nível internacional e facilitar a cooperação transfronteiriça em matéria de cibercrime. Embora não substitua a legislação nacional, funciona como um guia de boas práticas que reforça a confiança no processo de investigação digital e no valor probatório dos vestígios recolhidos. Para além disso, influencia diretamente a formação dos profissionais, ao estabelecer requisitos de competência e ao ajudar a padronizar funções como a do primeiro interveniente forense, do especialista em aquisição, do analista de evidência e do responsável pela validação de métodos.

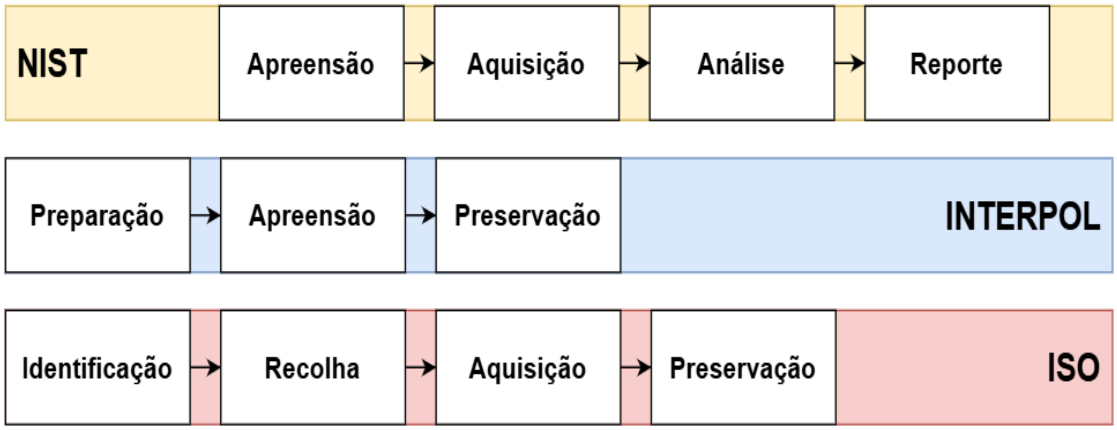
A diversidade de abordagens presentes nestes referenciais internacionais justifica uma análise comparativa das respetivas metodologias, de modo a identificar convergências, diferenças e contributos relevantes para a definição de um procedimento estruturado de análise forense digital. Essa comparação é apresentada na secção seguinte.

2.3. Análise Comparativa

A comparação entre os diferentes referenciais internacionais permite identificar semelhanças metodológicas e diferenças estruturais relevantes para a definição de procedimentos forenses consistentes.

A análise comparativa (ver Figura 2) entre a ISO/IEC 27037:2012, o guia da INTERPOL e a NIST SP 800-101 Revision 1 evidencia diferenças na forma como cada referencial estrutura o processo de análise forense digital, mas também revela pontos de convergência que demonstram a sua complementaridade. A figura mencionada no texto original apresenta, sob a forma de diagrama, a correspondência entre as fases definidas nos três modelos, permitindo visualizar as semelhanças e diferenças na organização metodológica.

Figura 2: Procedimento geral proposto na NIST SP 800-101.



A NIST SP 800-101 Revision 1 adota um ciclo estruturado em quatro fases - apreensão, aquisição, análise e reporte - aproximando-se do modelo clássico da ciência forense. Este referencial distingue-se por incluir explicitamente as fases de análise e de elaboração do relatório, que assumem particular relevância em contexto judicial, uma vez que é nelas que se produzem os relatórios periciais utilizados em sede de julgamento. A inclusão destas etapas evidencia a preocupação do NIST não apenas com a recolha e preservação da evidência, mas também com a sua interpretação técnica e com a sua apresentação formal perante as autoridades judiciais (Ayers et al., 2014).

O guia da INTERPOL segue uma abordagem mais operacional, orientada sobretudo para a atuação de agentes policiais e primeiros intervenientes. A sua estrutura organiza-se em três fases principais: preparação, apreensão e preservação. Ao contrário do modelo do NIST, não inclui fases autónomas de análise e reporte, concentrando-se nos momentos iniciais da intervenção, isto é, na preparação da operação, na recolha dos dispositivos e na manutenção da cadeia de custódia. Esta opção reflete o objetivo do documento, que é fornecer orientações práticas para o trabalho de campo, garantindo que a evidência digital é recolhida e preservada de forma segura e juridicamente válida (INTERPOL Innovation Centre, 2021).

A ISO/IEC 27037:2012 apresenta uma estrutura metodológica próxima da adotada pela INTERPOL, embora com maior formalização técnica. O processo é dividido em quatro fases: identificação, recolha, aquisição e preservação. Tal como sucede com o guia da INTERPOL, este referencial não inclui fases específicas de análise e reporte, centrando-se na gestão correta da evidência até ao momento em que esta se encontra pronta para ser examinada. A norma tem como principal objetivo assegurar que a evidência digital é identificada, recolhida e preservada de forma adequada, permitindo que etapas posteriores, eventualmente definidas por outros referenciais ou pela legislação nacional, possam ser realizadas sem comprometer a sua integridade (International Organization for Standardization, 2012).

Apesar das diferenças de estrutura, nível de detalhe técnico e público-alvo, os três referenciais partilham um conjunto de princípios fundamentais que constituem a base da prática da análise forense digital. Em primeiro lugar, todos atribuem prioridade absoluta à integridade da evidência digital, reconhecendo que qualquer alteração introduzida durante o processo pode comprometer a sua validade e admissibilidade em tribunal. A preservação do estado original dos dados é, por isso, um requisito comum a todos os modelos.

Outro ponto de convergência é a exigência de uma cadeia de custódia rigorosa. As três normas insistem na necessidade de manter um registo cronológico completo de todas as intervenções realizadas sobre os dispositivos e dados, incluindo a identificação dos intervenientes, as operações efetuadas e as condições em que a evidência foi armazenada ou transferida. Este registo garante a rastreabilidade da prova e permite demonstrar, em sede judicial, que esta não foi adulterada.

Também é comum aos três referenciais a ênfase na documentação detalhada dos procedimentos. Desde a apreensão inicial até às fases posteriores do processo, todas as ações devem ser registadas de forma clara e completa, assegurando transparência, auditabilidade e possibilidade de repetição por outros peritos. Esta exigência está diretamente ligada ao princípio da reprodutibilidade, considerado essencial para a credibilidade da prova digital.

Outro elemento partilhado é a necessidade de que os profissionais envolvidos possuam competência técnica adequada. Tanto o NIST como a INTERPOL e a ISO sublinham que a manipulação de evidência digital deve ser realizada por pessoas qualificadas, capazes de aplicar métodos reconhecidos e de justificar tecnicamente as decisões tomadas durante o processo.

Por fim, todos os referenciais afirmam que a análise forense digital deve respeitar a legislação aplicável na jurisdição onde decorre a investigação. As normas técnicas não substituem o direito processual ou penal, mas funcionam como orientações complementares destinadas a garantir que a recolha e tratamento da prova ocorrem de forma compatível com as exigências legais.

Em síntese, a comparação entre a NIST SP 800-101, o guia da INTERPOL e a ISO/IEC 27037:2012 demonstra que, apesar das diferenças de abordagem, os três referenciais são complementares. A INTERPOL privilegia a atuação inicial no terreno, a ISO fornece um enquadramento metodológico para a gestão da evidência e o NIST apresenta um ciclo completo que inclui análise e reporte. Em conjunto, estes modelos contribuem para a uniformização internacional da prática forense digital e reforçam a fiabilidade e admissibilidade da prova em contexto judicial.

2.4. Desafios Técnicos e Éticos

A análise forense digital de dispositivos móveis compreende o conjunto de procedimentos técnicos e metodológicos destinados à identificação, recolha, preservação, extração, análise e apresentação de dados armazenados ou processados por equipamentos portáteis, como smartphones, tablets e outros dispositivos com capacidades de comunicação e processamento. A evolução tecnológica destes equipamentos, bem como a crescente integração com serviços em nuvem, tem aumentado significativamente a complexidade das investigações forenses, exigindo métodos cada vez mais especializados para garantir a preservação da evidência e a sua validade probatória (Casey, 2011; Arnes, 2018).

Os sistemas operativos móveis dominantes, Android e iOS, apresentam arquiteturas distintas, mecanismos de segurança próprios e diferentes formatos de armazenamento de dados. Esta diversidade obriga à seleção criteriosa dos métodos de aquisição, tendo em conta o modelo do dispositivo, a versão do sistema operativo e as configurações de segurança existentes. Para além destes sistemas, podem também ser alvo de análise forense outros equipamentos, como telemóveis convencionais, dispositivos portáteis de Internet das Coisas, relógios inteligentes ou terminais especializados, como equipamentos de pagamento móvel, que igualmente podem conter informação relevante para a investigação (Casey, 2001).

No caso de dispositivos Android, o processo de arranque ocorre em várias fases, desde o carregamento inicial do firmware até à execução do sistema operativo e dos serviços de utilizador. A obtenção de dados pode ser realizada por aquisição lógica, que extrai apenas informação acessível ao sistema operativo, ou por aquisição física, que consiste na cópia integral da memória interna. A aquisição física é preferível quando se pretende recuperar dados eliminados ou aceder a partições não visíveis ao sistema, mas pode exigir técnicas avançadas e equipamento especializado. Ferramentas forenses comerciais amplamente utilizadas permitem suportar centenas de modelos de dispositivos, oferecendo funcionalidades de desbloqueio, extração e descodificação de dados (Arnes, 2018).

Nos dispositivos Apple, que utilizam o sistema iOS, o processo de arranque inclui uma cadeia de arranque segura, na qual cada etapa é validada criptograficamente antes de ser executada. Este mecanismo dificulta a extração forense direta, obrigando frequentemente ao recurso a métodos alternativos, como a análise de cópias de segurança, acesso a serviços de sincronização remota ou exploração de vulnerabilidades conhecidas. Em

determinados casos, modos especiais de arranque podem permitir acesso ao sistema de ficheiros, embora sujeitos a limitações impostas por mecanismos de encriptação integral do armazenamento interno (Casey, 2011).

Os dados de interesse forense em dispositivos móveis são numerosos e diversificados. Entre os mais comuns encontram-se registos de chamadas, mensagens SMS e MMS, mensagens de aplicações de comunicação, histórico de navegação, dados de localização, fotografias e vídeos, credenciais de acesso, ficheiros de aplicações e artefactos do sistema operativo. Grande parte desta informação é armazenada em bases de dados internas, frequentemente em formato SQLite, que podem conter dados eliminados ainda não sobrescritos. A análise destes registos exige ferramentas capazes de interpretar estruturas de dados específicas de cada sistema e de cada aplicação (Casey, 2001).

A sincronização com serviços de armazenamento remoto introduz novas fontes de evidência, mas também desafios adicionais. Muitos dispositivos mantêm cópias automáticas de dados em serviços de nuvem, o que significa que informação relevante pode não estar presente no equipamento físico. O acesso a estes dados pode exigir credenciais válidas, autorização judicial ou cooperação internacional com os fornecedores de serviços, o que aumenta a complexidade do processo forense (Arnes, 2018).

A encriptação constitui atualmente um dos maiores obstáculos à análise forense de dispositivos móveis. Em versões recentes do Android, a encriptação do armazenamento é frequentemente ativada por defeito, exigindo a chave do utilizador para acesso aos dados. Nos dispositivos Apple, a proteção de dados associa as chaves criptográficas ao hardware e ao código de desbloqueio, dificultando significativamente a extração de informação. Nestes casos, a análise pode limitar-se a dados disponíveis em cópias de segurança ou a informação obtida antes do desligar do dispositivo, quando ainda se encontra em memória volátil (Casey, 2011).

Para além da encriptação, existem técnicas de anti-forense que visam dificultar a investigação. Entre estas incluem-se aplicações concebidas para apagar automaticamente dados sensíveis, utilização de áreas seguras protegidas, sistemas operativos modificados ou mecanismos destinados a impedir a aquisição de dados. A deteção destas alterações exige análise da integridade do sistema, verificação de valores de hash e comparação com imagens de referência conhecidas, de modo a confirmar que o dispositivo não foi alterado de forma a ocultar informação (Casey, 2001).

O desenvolvimento da Internet das Coisas introduziu novas fontes de evidência associadas aos dispositivos móveis. Relógios inteligentes, pulseiras de atividade, veículos conectados, equipamentos médicos e sistemas domésticos inteligentes podem armazenar dados sobre localização, atividade física, comunicações ou interações do utilizador. A análise destes dispositivos exige conhecimento específico dos protocolos utilizados e dos formatos de dados, muitas vezes proprietários, bem como ferramentas adaptadas à sua extração (Arnes, 2018).

A volatilidade dos dados e a rápida evolução tecnológica tornam indispensável a atualização constante das ferramentas e das técnicas utilizadas na análise forense digital. A formação contínua dos peritos, aliada à adoção de procedimentos normalizados, é essencial para garantir consistência, reprodutibilidade e fiabilidade dos resultados obtidos. A aplicação de normas internacionais contribui para uniformizar práticas e reforçar a credibilidade da prova digital em contexto judicial (International Organization for Standardization, 2012).

Em síntese, a análise forense de dispositivos móveis exige a aplicação de métodos técnicos adequados a cada plataforma, respeitando princípios de preservação, documentação e validação da evidência. Este tipo de investigação envolve desafios técnicos e éticos significativos, resultantes do carácter intrusivo das técnicas utilizadas, do volume de informação recolhida e da possibilidade de aceder a dados pessoais sensíveis. A crescente complexidade dos dispositivos e a sua integração em redes e serviços remotos reforçam a necessidade de assegurar que todas as operações respeitam os princípios de legalidade, proporcionalidade e proteção da privacidade (Casey, 2011; Arnes, 2018).

3. Discussão sobre o Atual Enquadramento e suas Lacunas

A comparação entre os diferentes referenciais internacionais permite identificar semelhanças metodológicas e diferenças estruturais relevantes para o desenvolvimento de procedimentos forenses

A metodologia adotada iniciou-se com a identificação e análise da legislação aplicável à análise forense digital no enquadramento jurídico nacional e europeu. Esta fase teve como objetivo determinar se existia, no ordenamento jurídico vigente, um procedimento formalmente definido para a recolha, preservação e análise de prova digital, em particular no contexto de dispositivos móveis. Após a análise dos diplomas legais relevantes, verificou-se que, embora exista regulamentação sobre obtenção de prova, proteção de dados e investigação criminal, não se encontra definido um procedimento técnico-operacional específico para a realização de análise forense digital, quer na legislação nacional, quer na legislação europeia.

Face a esta lacuna normativa, o estudo foi alargado à análise de orientações, diretrizes e normas técnicas produzidas por entidades internacionais reconhecidas, com o objetivo de identificar modelos de referência que pudessem contribuir para a normalização de procedimentos de investigação forense digital. Nesta fase foram analisados documentos técnicos amplamente utilizados na comunidade forense, nomeadamente a NIST SP 800-101, as diretrizes da INTERPOL para primeiros intervenientes e a norma ISO/IEC 27037, por constituírem referenciais internacionais relevantes na definição de boas práticas para a gestão de evidência digital.

A análise destes documentos permitiu verificar que, embora todos apresentem orientações estruturadas, cada um deles possui um âmbito e objetivos distintos. A NIST SP 800-101 apresenta um modelo completo que inclui apreensão, aquisição, análise e reporte, enquanto as diretrizes da INTERPOL se concentram sobretudo nas fases iniciais da intervenção, com especial enfoque na preparação e apreensão. Por sua vez, a ISO/IEC 27037 define um enquadramento metodológico para identificação, recolha, aquisição e preservação da evidência, privilegiando a gestão adequada dos vestígios digitais antes da fase de análise.

A comparação entre estes referenciais evidenciou que, apesar de partilharem princípios comuns, nenhum deles cobre de forma integral todas as etapas necessárias à realização de uma análise forense digital de dispositivos móveis no contexto jurídico considerado. Esta constatação justificou a necessidade de propor um procedimento próprio, que integre os contributos das normas analisadas e que seja compatível com as exigências legais aplicáveis.

Assim, com base na análise da legislação e na comparação das normas internacionais, foi elaborado o procedimento de análise forense digital apresentado na secção seguinte, procurando estabelecer uma metodologia estruturada, tecnicamente fundamentada e juridicamente conforme, aplicável à investigação forense em dispositivos móveis.

Assim, a inexistência de um procedimento claramente definido para a análise forense de dispositivos móveis justifica o desenvolvimento de um modelo estruturado que integre boas práticas internacionais e respeite o enquadramento jurídico aplicável.

4. Proposta de Procedimento para Análise Forense Digital a Dispositivos Móveis

Com base na análise da legislação aplicável e na comparação das normas internacionais anteriormente discutidas, foi desenvolvido um procedimento estruturado para a análise forense digital de dispositivos móveis. O modelo proposto integra contributos das orientações do NIST, das diretrizes da INTERPOL e da norma ISO/IEC 27037, procurando adaptar estas boas práticas ao contexto jurídico português.

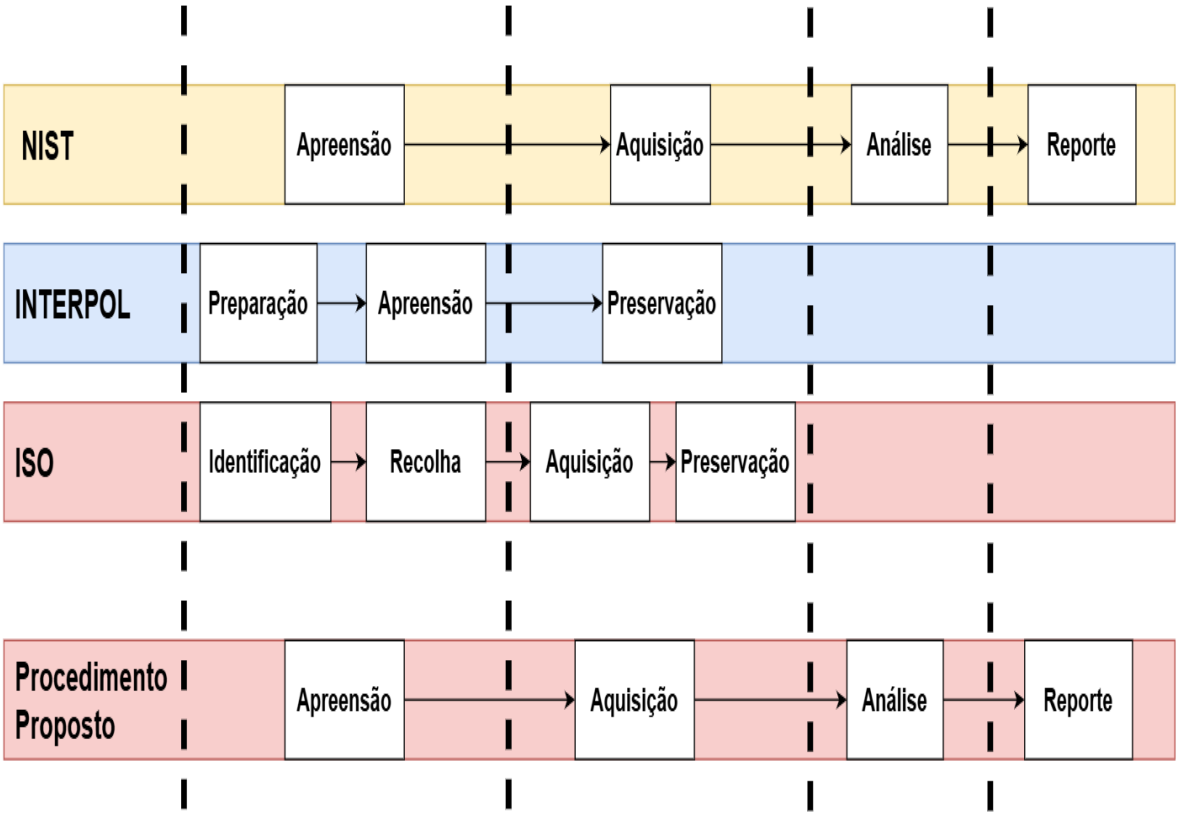
A definição de um procedimento estruturado e metodologicamente consistente revela-se fundamental para uniformizar a atuação dos diferentes intervenientes na análise forense digital. Em Portugal, embora os principais atores em processos de investigação criminal digital sejam habitualmente magistrados do Ministério Público e inspetores da Polícia Judiciária, podem igualmente intervir outros profissionais. Entre estes incluem-se peritos contratados por sociedades de advogados, especialistas ao serviço de empresas ou entidades lesadas, bem como

peritos que atuem no âmbito de protocolos com a Procuradoria-Geral da República. Neste contexto, a existência de um procedimento formalmente definido e devidamente documentado assume utilidade prática e relevância jurídica, contribuindo para maior consistência, transparência e credibilidade das investigações.

O procedimento aqui proposto resulta da integração de três referenciais de reconhecida autoridade internacional: a abrangência metodológica das orientações do NIST, a robustez normativa da ISO/IEC 27037:2012 e as boas práticas operacionais promovidas pela INTERPOL. A Figura 3 apresenta a correspondência entre o procedimento proposto e as fases previstas nas normas anteriormente analisadas.

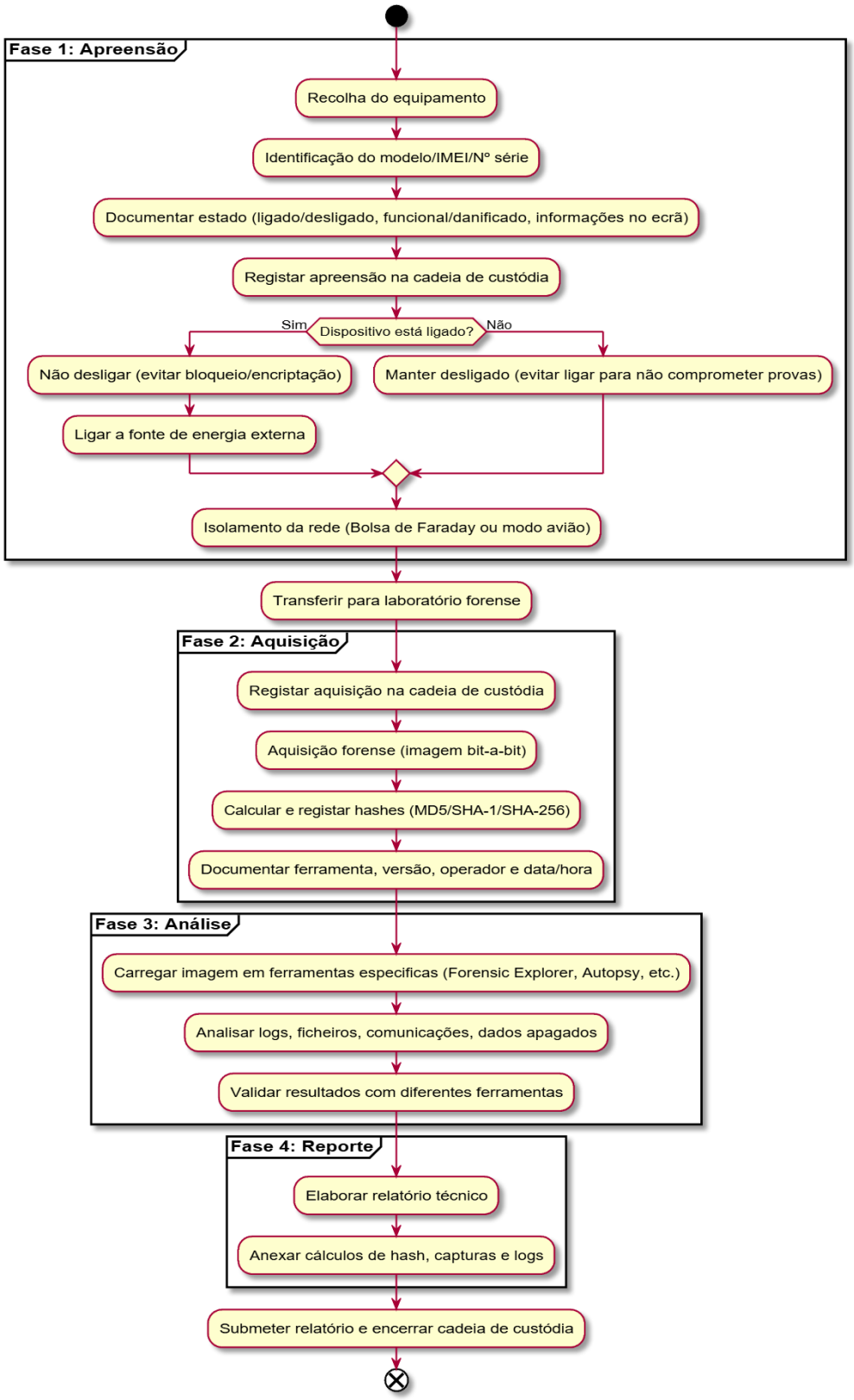
Da observação do diagrama verifica-se que apenas o modelo do NIST e o procedimento agora proposto incluem explicitamente as fases de análise e de reporte. Estas fases assumem particular relevância, pois é na análise que se avaliam as evidências e se formulam hipóteses sobre os factos investigados, e é no reporte que se elaboram os relatórios periciais que serão apreciados por magistrados e tribunais. As fases de apreensão e de aquisição são comuns a todos os referenciais, embora alguns atribuam maior importância à preparação da apreensão, como sucede nas orientações da INTERPOL, enquanto outros enfatizam a identificação dos dispositivos, como acontece na norma ISO.

Figura 3: Procedimento geral proposto na NIST SP 800-101.



O diagrama apresentado na Figura 4 organiza, de forma sequencial, as atividades associadas a cada fase, garantindo rastreabilidade, replicabilidade e rigor técnico. O procedimento estrutura-se em quatro fases principais: apreensão, aquisição, análise e reporte.

Figura 4: Procedimento proposto.



Fase 1: Apreensão

A primeira fase corresponde à apreensão do dispositivo, momento inicial em que o equipamento é retirado do seu contexto original e colocado sob custódia da autoridade investigadora. De acordo com a ISO/IEC 27037:2012, é indispensável proceder à correta identificação do equipamento, registando elementos como o fabricante, o modelo, o número de série e, no caso de dispositivos móveis, o código IMEI. Estes identificadores permitem estabelecer uma ligação inequívoca entre o dispositivo apreendido e o processo em investigação.

Em conformidade com as orientações da INTERPOL, o dispositivo deve ser imediatamente isolado de qualquer rede de comunicação, de modo a impedir manipulações remotas ou sincronizações automáticas que possam comprometer a integridade dos dados. Este isolamento pode ser realizado através da utilização de bolsas de Faraday ou pela ativação do modo de voo, sempre que tecnicamente possível.

Nesta fase deve ainda ser documentado o estado do equipamento, registando se se encontra ligado ou desligado, bloqueado ou desbloqueado, e se apresenta danos físicos. Recomenda-se a realização de registos fotográficos, complementados por notas descritivas, de forma a reforçar a credibilidade da cadeia probatória. A apreensão deve terminar com o registo formal na cadeia de custódia, mecanismo que assegura a rastreabilidade da prova desde a recolha até à sua eventual apresentação em tribunal.

O estado operacional do dispositivo condiciona os procedimentos seguintes. Se o equipamento se encontrar ligado, a ISO/IEC 27037 recomenda que não seja desligado, pois tal pode desencadear bloqueios ou encriptação automática. Nestas situações, em conformidade com o NIST, devem ser registadas as informações visíveis no ecrã, preferencialmente através de notas e fotografias. Se o dispositivo estiver desligado, deve manter-se nessa condição, uma vez que a sua inicialização pode alterar o sistema de ficheiros ou sobrescrever dados voláteis.

Quando o dispositivo se encontra protegido por palavra-passe ou outro mecanismo de segurança, podem ser utilizadas ferramentas forenses específicas que permitam o desbloqueio sem comprometer a integridade da evidência. Todas as ferramentas utilizadas, bem como as respetivas versões, devem ser registadas para posterior inclusão no relatório pericial.

Fase 2: Aquisição

A fase de aquisição inicia-se após o transporte seguro do dispositivo para o laboratório forense. Segundo a ISO/IEC 27037:2012, o objetivo principal desta fase é a criação de uma imagem forense, isto é, uma cópia bit a bit de todo o conteúdo do equipamento apreendido. Esta cópia inclui ficheiros ativos, dados eliminados e espaço não alocado, distinguindo-se de uma simples cópia de ficheiros por preservar integralmente o conteúdo do suporte.

Para garantir a autenticidade da imagem obtida, tanto a ISO/IEC 27037 como a NIST SP 800-101 recomendam o cálculo de resumos criptográficos antes e após a aquisição. Estes valores funcionam como assinaturas digitais que permitem verificar que a evidência não sofreu alterações. Funções antigas como MD5 ou SHA-1 deixaram de ser consideradas seguras, devendo ser utilizadas funções mais robustas, como SHA-256 ou SHA-512 (Xie, Feng, & Lai, 2013; Stevens et al., 2017).

As orientações da INTERPOL reforçam ainda a necessidade de documentar detalhadamente todo o processo, incluindo as ferramentas utilizadas, as configurações aplicadas e as condições técnicas da aquisição, de modo a permitir a verificação posterior por outros peritos.

Fase 3: Análise

Concluída a aquisição, inicia-se a fase de análise, que deve ser realizada exclusivamente sobre a cópia forense e nunca sobre o dispositivo original, conforme indicado na ISO/IEC 27037:2012. Nesta etapa, a imagem obtida é examinada através de ferramentas especializadas capazes de identificar e interpretar dados relevantes, como

registos de sistema, ficheiros eliminados, histórico de comunicações, dados de navegação, informação de geolocalização e metadados.

Entre as ferramentas frequentemente utilizadas encontram-se aplicações forenses comerciais e de código aberto, que permitem analisar diferentes formatos de dados e integrar resultados provenientes de várias fontes. A utilização de múltiplas ferramentas é recomendada pelo NIST, que enfatiza a importância da validação cruzada para reduzir a probabilidade de erro e aumentar a fiabilidade das conclusões (Ayers et al., 2014).

As orientações da INTERPOL sublinham igualmente que a análise deve ser objetiva, reprodutível e passível de auditoria externa. Por essa razão, todas as operações realizadas devem ser documentadas de forma detalhada, garantindo que o processo pode ser revisto e validado por terceiros.

Fase 4: Reporte

A última fase corresponde ao reporte, em que os resultados da investigação são consolidados num relatório técnico-científico. De acordo com a ISO/IEC 27037:2012, este relatório deve incluir a descrição detalhada dos procedimentos executados, a fundamentação das opções metodológicas, os resultados obtidos e as limitações encontradas durante a análise.

O relatório deve ser redigido de forma clara e compreensível, permitindo a sua leitura não apenas por peritos, mas também por magistrados, advogados e outros intervenientes processuais. Devem ser incluídos elementos de suporte, como valores de hash, capturas de ecrã, registos de operações e cronologias, de modo a demonstrar a integridade e autenticidade da evidência.

Recomenda-se igualmente que sejam indicadas as ferramentas utilizadas, incluindo versões e certificações, reforçando a credibilidade do trabalho realizado. O procedimento conclui-se com a formalização completa da cadeia de custódia, assegurando que toda a prova recolhida pode ser apresentada em tribunal de forma admissível, tecnicamente fundamentada e conforme os padrões internacionais de qualidade e legalidade.

6. Conclusão

O presente trabalho teve como objetivo propor um procedimento estruturado e adaptado à realidade portuguesa para a análise forense digital de dispositivos móveis. A partir da revisão da legislação nacional e europeia aplicável, bem como da análise de normas e orientações internacionais relevantes, nomeadamente a ISO/IEC 27037, as diretrizes da INTERPOL e o guia NIST SP 800-101, foi possível verificar a inexistência de um modelo padronizado especificamente aplicável ao contexto português. Esta lacuna pode originar inconsistências na recolha, preservação e análise da prova digital, com potenciais consequências na sua admissibilidade em tribunal.

Com base nesta constatação, foi desenvolvido um procedimento forense estruturado em quatro fases — apreensão, aquisição, análise e reporte — concebido de forma a articular as boas práticas internacionais com o enquadramento jurídico português e europeu. O procedimento proposto foi definido tendo em consideração, em particular, as exigências da Lei do Cibercrime, do Código de Processo Penal e do Regulamento Geral sobre a Proteção de Dados, assegurando que as operações técnicas realizadas no âmbito da análise forense digital respeitam os princípios de legalidade, proporcionalidade, integridade e proteção da privacidade.

A principal mais-valia do trabalho reside na conjugação entre a análise teórica, jurídica e normativa e a definição de um procedimento técnico aplicável à prática forense, permitindo aproximar as recomendações internacionais das necessidades específicas do ordenamento jurídico português. Este contributo pretende servir de referência para magistrados, órgãos de polícia criminal e peritos envolvidos em investigações que incluam evidência digital proveniente de dispositivos móveis, promovendo maior uniformidade de atuação e maior segurança jurídica na utilização da prova digital.

Numa perspetiva de trabalho futuro, considera-se relevante aprofundar e validar o procedimento proposto através da sua aplicação em contextos reais de investigação, permitindo avaliar a sua eficácia e identificar eventuais melhorias. Poderá igualmente ser explorada a integração do procedimento com sistemas de gestão de prova digital, de forma a automatizar o registo das operações e reforçar os mecanismos de controlo e rastreabilidade.

Adicionalmente, a utilização de tecnologias baseadas em blockchain constitui uma linha de desenvolvimento promissora, na medida em que pode contribuir para reforçar a imutabilidade, a transparência e a fiabilidade da cadeia de custódia. A aplicação destas soluções poderá aumentar o grau de confiança na prova digital apresentada em tribunal e favorecer a harmonização de procedimentos em investigações que envolvam múltiplas entidades ou diferentes jurisdições.

Referências

Arnes, A. (2018). *Digital forensics*. Wiley.

Assembleia da República (Portugal). (2009). *Lei n.º 109/2009, de 15 de setembro: Aprova a Lei do Cibercrime*. *Diário da República, Série I*(180).

Casey, E. (2001). *Handbook of computer crime investigation: Forensic tools and technology*. Academic Press.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3.ª ed.). Academic Press.

Cohen, F. (2012). Digital forensics. In H. Tipton & M. Krause (Eds.), *Information security management handbook* (6.ª ed.). Auerbach Publications. https://doi.org/10.1201/b11819-107

Conselho da União Europeia. (2001). *Convenção sobre o cibercrime (Budapeste, 23 de novembro de 2001)*. *Jornal Oficial da União Europeia*.

Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185)*.

Cruz-Cunha, M. M., & Mateus-Coelho, N. R. (2020). *Handbook of research on cyber crime and information privacy*. IGI Global.

Diário da República. (2023). *Código Penal português (com as alterações até 2023)*.

European Union. (2016, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Gilliland, A. J. (2016). Setting the stage. In M. Baca (Ed.), *Introduction to metadata*. Getty Research Institute. https://www.getty.edu/publications/intrometadata/setting-the-stage/

International Organization for Standardization. (2012). *ISO/IEC 27037:2012 – Guidelines for identification, collection, acquisition and preservation of digital evidence*.

International Organization for Standardization. (2017). *ISO 23081-1:2017 – Information and documentation – Records management processes – Metadata for records – Part 1: Principles*.

Kiran, S., Sanjana, J., & Reddy, N. J. (2019, March). Mobile phone addiction: Symptoms, impacts and causes—A review. In *International Conference on Trends in Industrial Value Engineering and Business and Social Innovation (ICTIVBSI)* (pp. 81–86).

Kist, D. J. (2019). *Prova digital no processo penal*. JH Mizuno.

Lei n.º 32/2008, de 17 de julho. (2008). *Diário da República*.

Limberger, T., Santanna, G. da S., & Giannakos, D. B. da S. (2023). Internet das coisas (IoT) e os direitos à privacidade e à proteção de dados do cidadão. *Revista Brasileira de Políticas Públicas*. https://doi.org/10.5102/rbpp.v13i3.8536

National Institute of Justice. (2008). *Electronic crime scene investigation: A guide for first responders* (2.ª ed.). U.S. Department of Justice.

National Institute of Standards and Technology. (2006). *Guide to integrating forensic techniques into incident response (Special Publication 800-86)*.

Portugal. (2019). *Lei n.º 58/2019, de 8 de agosto: Assegura a execução do RGPD na ordem jurídica nacional*. https://dre.pt/dre/detalhe/lei/58-2019-123815466

Queirós Colaço, M. F. dos S. (2023). *Buscas informáticas e subsequente apreensão de dados informáticos como métodos de obtenção de prova digital em processo penal* [Dissertação de mestrado, Universidade Católica Portuguesa].

Ramalho, D. S. (2013). The use of malware as a means of obtaining evidence in criminal proceedings. *Journal of Competition and Regulation, 4*(16), 195–243.

Ramos, A. D. (2014). *A prova digital em processo penal: O correio eletrónico* (2.ª ed.). Chiado Books.

República Portuguesa. (1987, fevereiro 17). *Código de processo penal (Decreto-Lei n.º 78/87)*. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1987-34570075

Santos, L. F. C. (2024). *Dynamic analysis techniques for Android applications* [Dissertação de mestrado, Polytechnic Institute of Leiria]. https://iconline.ipleiria.pt/bitstream/10400.8/9768/1/Te%CC%81cnicas%20de%20ana%CC%81lise%20dina%CC%82mica%20a%20aplicac%CC%A7o%CC%83es%20Android_cf.pdf

Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. (2017). The first collision for full SHA-1. In *Advances in Cryptology – CRYPTO 2017*.

Venâncio, P. D. (2020). Regime geral dos atos eletrónicos – Um regime esquecido. *Revista Electrónica de Direito*.

Venâncio, P. D. (2023). *Lei do cibercrime: Anotada e comentada*. Editora D'Ideias.

Xie, T., Feng, D., & Lai, X. (2013). Fast collision attack on MD5. *Journal of Cryptographic Engineering*.

Xu, X. (2019). *Impacts of mobile usage and experience in contemporary society*. IGI Global.

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.