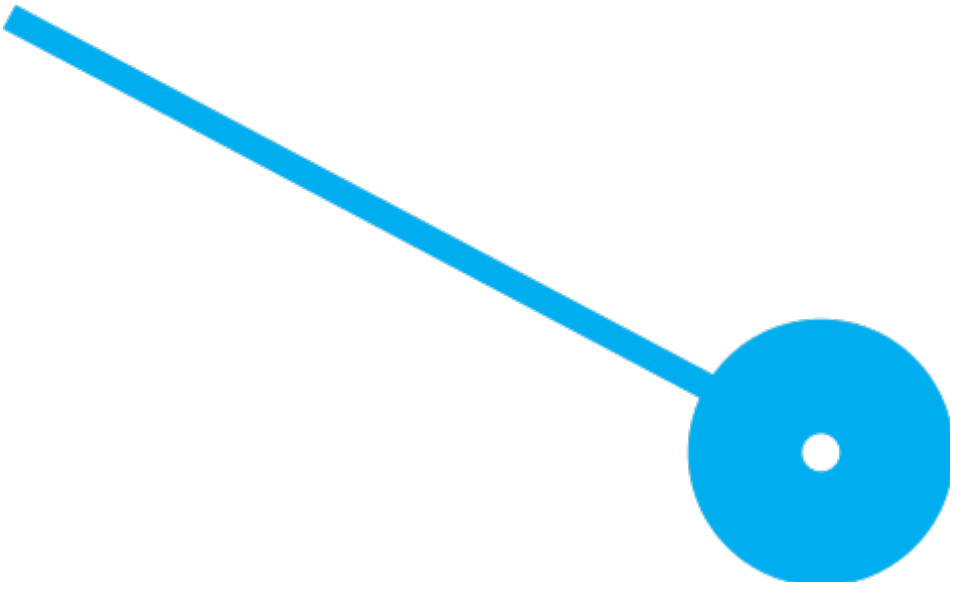
ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

MESTRADO
PRÁTICAS JURÍDICO-DIGITAIS

Desenvolvimento de Procedimento e Ferramenta de Suporte à Análise Forense Digital a Dispositivos Móveis em Portugal

Carla Patrícia de Abreu Teixeira Pinto

OUTUBRO/2025



Este trabalho não inclui as críticas e sugestões feitas pelo Júri

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

MESTRADO
PRÁTICAS JURÍDICO-DIGITAIS

Desenvolvimento de Procedimento e Ferramenta de Suporte à Análise Forense Digital a Dispositivos Móveis em Portugal

Carla Patrícia de Abreu Teixeira Pinto
8180690

Orientador(es)

Prof. Doutora Patrícia dos Anjos Oliveira Nogueira de Azevedo
Prof. Doutor Pedro Filipe Cruz Pinto

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Práticas Jurídico-Digitais pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico do Porto.

OUTUBRO/2025

Este trabalho não inclui as críticas e sugestões feitas pelo Júri

Declaração de integridade

Eu, **Carla Patrícia de Abreu Teixeira Pinto**, estudante nº **8180690**, do Mestrado **Práticas Jurídico-Digitais** da Escola Superior de Tecnologia e Gestão do Instituto Politécnico do Porto, declaro que não fiz plágio nem auto-plágio, pelo que o trabalho intitulado "**Desenvolvimento de Procedimento e Ferramenta de Suporte à Análise Forense Digital a Dispositivos Móveis em Portugal**" é original e da minha autoria, não tendo sido usado previamente para qualquer outro fim. Mais declaro que todas as fontes usadas estão citadas, no texto e na bibliografia final, segundo as regras de referenciação adotadas na instituição.

Agradecimentos

A todos os Professores do Mestrado em Práticas Jurídico-Digitais, expresso o meu sincero agradecimento pelo conhecimento transmitido, pela disponibilidade e pela dedicação demonstrada ao longo deste percurso académico.

Um agradecimento muito especial aos meus orientadores, Professor Doutor Pedro Pinto e Professora Doutora Patrícia dos Anjos, pela orientação, partilha de saber e acompanhamento constante, fundamentais para a concretização deste trabalho.

Aos meus colegas de mestrado, pela ajuda, incentivo e, sobretudo, pela amizade e companheirismo que tornaram esta etapa mais enriquecedora e gratificante.

À Catarina, pelo apoio constante, pela amizade e por ser uma colega de profissão exemplar, cuja presença e incentivo foram essenciais ao longo deste percurso.

Ao Vítor, um grande amigo e exemplo de determinação e resiliência, cuja atitude positiva e força de espírito, mesmo nos momentos mais desafiantes, foram uma inspiração constante ao longo deste percurso.

À minha família, pelo amor, compreensão e apoio incondicional, e em especial ao meu marido, cujo incentivo constante e paciência foram fundamentais para que eu pudesse concluir este mestrado. Sem o seu apoio, esta conquista não teria sido possível.

A todos, o meu profundo e sentido agradecimento.

Abstract

The digital forensic analysis of mobile devices is an emerging and essential area for criminal investigations, given the amount and relevance of the data stored on these devices. This thesis aims to develop a structured and standardized procedure for the forensic analysis of mobile devices in Portugal, in accordance with national and European laws, including the Portuguese Cybercrime Law and the General Data Protection Regulation (GDPR). This research addresses technical and legal challenges, including data encryption, biometric authentication, and the lack of a standardized methodology in Portugal. The practical application of the procedure is to be validated by a case study. This contribution is considered to support professionals in the area, ensuring standardization and compliance with legal and ethical standards.

Keywords: Digital forensics, mobile devices, legal regulation, forensic procedure.

Resumo

A análise forense digital de dispositivos móveis é uma área emergente e essencial para investigações criminais, dada a quantidade e a relevância dos dados armazenados nesses dispositivos. O objetivo desta tese é o de desenvolver um procedimento estruturado e padronizado para a análise forense desses dispositivos móveis em Portugal, em conformidade com legislação nacional e europeia, de que são exemplos a Lei do Cibercrime e o Regulamento Geral sobre a Proteção de Dados (RGPD). São identificados desafios técnicos e legais, incluindo a criptografia de dados, a autenticação biométrica e a ausência de uma metodologia padronizada em Portugal. Considera-se que esta contribuição apoie os profissionais da área, garantindo a padronização e o cumprimento das normas legais e éticas.

Palavras-chave: Forense digital, dispositivos móveis, regulamentação legal, procedimento forense.

Conteúdo

Lista de Figuras

Acrónimos

API Application Programming Interface.

CCTV Closed-Circuit Television.

CDR Call Detail Records.

CNPD Comissão Nacional de Proteção de Dados.

CPP Código do Processo Penal.

DEFR Digital Evidence First Responders.

DES Digital Evidence Specialists.

DFU Device Firmware Update.

ENISA European Union Agency for Cybersecurity.

EPD Encarregado de Proteção de Dados.

EXIF Exchangeable Image File Format.

GPS Global Positioning System.

ICCID Integrated Circuit Card Identifier.

IEC International Electrotechnical Commission.

IMEI International Mobile Equipment Identity.

IMSI International Mobile Subscriber Identity.

INTERPOL International Criminal Police Organization.

iOS iPhone Operating System.

IoT Internet of Things.

ISO International Standards Organisation.

JTAG Joint Test Action Group.

MD5 Message Digest 5.

MMS Multimedia Message Service.

NIST National Institute for Standards and Technology.

PIN Personal Identification Number.

RAM Random Access Memory.

RGPD Regulamento Geral sobre a Proteção de Dados.

ROM Read-Only Memory.

SHA Secure Hash Algorithm.

SIM Subscriber Identity Module.

SMS Short Message Service.

STJ Supremo Tribunal de Justiça.

UE União Europeia.

UICC Universal Integrated Circuit Card.

Capítulo 1

Introdução

Com o advento das tecnologias de comunicação e entretenimento, a perícia forense digital tem crescido progressivamente nos últimos anos, especialmente quando se trata de dispositivos móveis. Esses dispositivos armazenam grandes quantidades de dados, dados estes que podem ser cruciais em investigações criminais. Muito além da investigação com base em listas de chamadas telefónicas recebidas/efetuadas, técnica muito frequente na década de 1990 [4]. Agora, informações como chamadas, mensagens de texto, e-mails, fotos, vídeos e dados de localização são recursos comuns em dispositivos digitais como smartphones, relógios digitais, tablets e muitos outros dispositivos e, portanto, poderão ser de extrema importância na reconstrução de eventos e na recolha de evidências digitais [5, 6, 7]. Um estudo recente mostra que 92,8% da população possui telemóvel e que 99% dos utilizadores portugueses acedem à Internet por meio de dispositivos móveis. Em termos de utilização, ultrapassam-se as 3 horas e 35 minutos por dia, destacando assim a importância destes dispositivos em investigações criminais[1].

1.1 Motivação

A análise forense a dispositivos móveis não está isenta de dificuldades. Cada dispositivo possui características específicas que podem exigir diferentes abordagens técnicas. A diversidade e a constante inovação dos sistemas operativos móveis aumentam a complexidade da análise de dados, o que complica o trabalho de advogados e investigadores. Por exemplo, a encriptação encontrada na maioria dos dispositivos móveis mais recentes, juntamente com medidas de segurança como biometria e códigos Personal Identification Number (PIN), adiciona uma camada de segurança que dificulta o acesso aos dados armazenados e exige técnicas analíticas novas e em constante evolução. Programas de *software*

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

específicos para análise forense digital de dispositivos móveis, como o Cellebrite[2] ou o Magnet AXIOM[3], entre outros, também precisam de estar em constante evolução [5].

A falta de métodos uniformes e aceitáveis para a ciência forense em Portugal é outra razão para a complexidade da área. Embora tenham sido estabelecidas diretrizes internacionais, como as emitidas pelo National Institute for Standards and Technology (NIST), dos Estados Unidos da América, e as diretrizes da International Criminal Police Organization (INTERPOL) para a análise de provas físicas, estas foram adaptadas por diversas instituições portuguesas, como tribunais, autoridades e, frequentemente, investigadores. Isso cria inconsistências que podem prejudicar a integridade das provas digitais, ameaçando sua admissibilidade em juízo e, consequentemente, a eficácia das investigações [8].

Além das questões técnicas e metodológicas, a análise forense encontra-se profundamente envolvida e rodeada de questões legais e éticas. As implicações legais da recolha e análise de dados pessoais são importantes, assim como o cumprimento das leis de proteção de dados. O Regulamento Geral sobre a Proteção de Dados (RGPD) estabelece regras rígidas para o processamento de dados pessoais, determinando que os indivíduos devem ser informados sobre recolhas de dados e que estes devem ser processados de forma transparente, segura e em conformidade com os direitos fundamentais à privacidade desses dados.

1.2 Objetivos

Esta dissertação visa promover o avanço da análise forense em dispositivos móveis no âmbito do enquadramento jurídico português. O seu principal objetivo é desenvolver um procedimento normalizado para a recolha, preservação e análise de provas digitais a partir de dispositivos móveis, garantindo a sua integridade e admissibilidade em contexto judicial. Assim, identificam-se três objetivos específicos:

- Análise de legislação relacionada (nacional e europeia);
- Definição de procedimento para análise forense digital a dispositivos móveis;
- Elaboração de ferramenta digital de apoio à realização do procedimento.

O primeiro objetivo específico consiste em realizar uma investigação sobre a legislação portuguesa e europeia aplicável à investigação forense digital, com destaque para a Lei do Cibercrime (Lei n.º 109/2009 de 15 de setembro), o Código de Processo Penal Código do Processo Penal (CPP), a Lei n.º 58/2019, de 8 de agosto e o RGPD . A análise crítica destes regulamentos visa identificar lacunas e desafios jurídicos que possam afetar a aplicação das técnicas de investigação forense digital, bem como avaliar o impacto da

[2] `https://cellebrite.com/pt/inicio/`
[3] `https://www.magnetforensics.com/products/magnet-axiom/`

regulamentação em matéria de proteção de dados na recolha e tratamento de provas. A partir desta análise, será possível compreender as limitações legais existentes e os requisitos que devem ser cumpridos para garantir a validade das provas em tribunal.

O segundo objetivo consiste em propor um procedimento para análise forense digital a dispositivos móveis, para uso por autoridades judiciais e de investigação. Este procedimento deverá ser adaptável a diversos dispositivos e contextos de investigação, respeitando as normas legais. O procedimento proposto também deverá atender às especificidades dos dispositivos móveis e suas constantes atualizações, considerando as ferramentas e técnicas forenses mais adequadas para cada tipo de dispositivo e sistema operativo.

O terceiro objetivo consiste em desenvolver uma ferramenta digital para auxiliar os profissionais forenses na aplicação do procedimento de forma consistente e eficiente. Esta ferramenta terá como objetivo facilitar a aplicação do procedimento de forma padronizada, acessível e prática, permitindo que os profissionais acompanhem as etapas do processo de análise forense de forma clara e organizada. A ferramenta deverá garantir o cumprimento das melhores práticas e dos requisitos legais, proporcionando uma abordagem eficaz e eficiente para a recolha e análise de dados.

1.3 Contribuições e Resultados

A principal contribuição desta dissertação é a criação de um procedimento forense digital padronizado e adaptado para dispositivos móveis em Portugal, alinhado com as normas jurídicas nacionais e internacionais. Essencialmente, este procedimento visa aprimorar a integridade e a admissibilidade de provas digitais, apoiado por uma ferramenta de suporte digital para orientar os investigadores durante o processo.

O trabalho apresentado na presente dissertação foi submetido a apreciação científica por pares em conferências nacionais e internacionais. Neste contexto, foram alcançados os seguintes resultados:

- Guidelines for Mobile Digital Forensics, Carla Pinto, Patrícia Anjos Azevedo, Pedro Pinto, apresentado na International Student Scientific Conference "Cyber threats as new Challenges for Crisis Management", 12 Dezembro 2024, Universidade Maria Curie-Skłodowska.

- Review of the Regulations Related to Digital Forensics of Mobile Devices, Carla Abreu Teixeira, Patrícia Anjos Azevedo, Pedro Pinto, apresentado no Symposium of Applied Science for Young Researchers (SASYR), 2 Julho 2025, Viana do Castelo, Portugal.

1.4 Estrutura

A presente dissertação encontra-se organizada em capítulos. O Capítulo 2 apresenta a contextualização teórica e jurídica do tema, abordando conceitos como prova digital, metadados e cadeia de custódia, e analisando o enquadramento legal português e europeu, com referência à Lei do Cibercrime, ao RGPD e a outros diplomas. Inclui também a análise de normas e diretrizes internacionais (NIST, INTERPOL e International Standards Organisation (ISO)) e termina com uma discussão sobre questões técnicas e éticas. O Capítulo 3 descreve a metodologia adotada e apresenta o procedimento aqui proposto para a análise de dispositivos móveis, estruturado em quatro fases: apreensão, aquisição, análise e reporte. O Capítulo 4 apresenta a ferramenta informática desenvolvida no âmbito deste trabalho, que assume a forma de uma *checklist* digital e online, elaborada para apoiar os profissionais na apreensão e no tratamento de dispositivos móveis, promovendo rigor e padronização de atuação. O Capítulo 5 apresenta as principais conclusões retiradas deste trabalho e sugere linhas de trabalho futuras.

Capítulo 2

Análise Forense Digital

A análise forense digital consiste num conjunto de métodos técnicos e procedimentos jurídicos destinados à recolha, preservação, exame, análise e apresentação de dados digitais com relevância probatória [9]. Esta análise forense digital aplica-se em investigações criminais, processos civis, auditorias e outros contextos jurídicos, exigindo o cumprimento simultâneo de requisitos legais e técnicos para assegurar a admissibilidade da prova [10].

No que concerne ao enquadramento jurídico português, o artigo 32.º da Constituição da República Portuguesa estabelece as garantias do processo criminal, incluindo a presunção de inocência, o direito ao contraditório, o direito de defesa e a proibição de utilização de provas obtidas por meios ilícitos, enquanto o artigo 18.º determina que restrições a direitos, liberdades e garantias apenas podem ocorrer por via legal e de forma proporcional. Por seu turno, o Código de Processo Penal não define expressamente a prova digital, aplicando-lhe regimes previstos para outros meios de prova, como as comunicações telefónicas, nos artigos 187.º a 189.º, complementando-se com legislação específica [10].

A Lei n.º 109/2009, de 15 de setembro[1], conhecida como Lei do Cibercrime [11], transpõe para o ordenamento jurídico nacional a Convenção sobre o Cibercrime do Conselho da União Europeia [12] e define instrumentos próprios para a obtenção de prova digital. A Lei n.º 32/2008, de 17 de julho[2], regula a conservação e transmissão de dados de tráfego e de localização por operadores de comunicações, destinados à investigação de crimes graves [13].

O processo de análise forense digital pode seguir o modelo proposto pelo NIST [14], que compreende quatro fases:

1. Apreensão – que visa assegurar que os dados recolhidos não são alterados desde a apreensão até à sua análise em laboratório;

[1]Versão mais recente da Lei (alterada pela Lei n.º 79/2021, de 24/11)
[2]Versão mais recente da Lei (alterada pela Lei n.º 18/2024, de 05/02)

2. Aquisição – que consiste no processamento dos dados para detetar e extrair informação relevante, podendo incluir a recuperação de ficheiros apagados, a análise de metadados e a filtragem de grandes volumes de informação;

3. Análise – que implica interpretar os dados obtidos, estabelecer sequências temporais, identificar ações de utilizadores e correlacionar resultados com outros elementos probatórios [9];

4. Reporte – que consiste na elaboração de um documento descritivo de todas as etapas, técnicas utilizadas, resultados alcançados e conclusões, de forma objetiva e compreensível, incluindo a documentação de suporte para eventual auditoria ou repetição do procedimento.

Em Portugal, a admissibilidade da prova digital depende da conformidade com as normas legais, tais como a Constituição da República Portuguesa, o Código de Processo Penal, a Lei do Cibercrime e a Lei da Conservação de Dados [15], mas também com normas técnicas reconhecidas pela comunidade científica, incluindo mecanismos de verificação de integridade, como funções de hash, e medidas de preservação da autenticidade e confidencialidade [9, 16]. A articulação entre peritos forenses digitais e autoridades judiciárias é essencial para assegurar que a prova seja recolhida, preservada e apresentada de forma válida, relevante e admissível.

2.1 Conceitos Fundamentais

Esta secção examina a prova digital enquanto elemento central na investigação e no processo judicial, abrangendo a sua definição legal e as particularidades técnicas que impõem procedimentos especializados para garantir a sua autenticidade e integridade. Aborda-se igualmente o papel dos metadados como fonte de informação complementar, capaz de contextualizar e validar ficheiros digitais, bem como a importância da cadeia de custódia, que assegura a rastreabilidade e preservação das provas desde a sua recolha até à apresentação em tribunal, salvaguardando a sua admissibilidade jurídica.

2.1.1 Prova Digital

No Direito Penal português, a prova digital compreende a informação eletrónica obtida através de diligências processuais previstas na Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro). Tais diligências incluem a pesquisa informática, o acesso a dados, a injunção para apresentação de dados, a revelação expedita de dados e a apreensão de correio eletrónico [17]. Estes instrumentos foram introduzidos para colmatar lacunas processuais existentes e para adaptar os meios de obtenção de prova ao ambiente digital.

Numa perspetiva internacional, a prova digital corresponde a qualquer dado com valor

probatório armazenado, processado ou transmitido em sistemas informáticos ou redes de comunicações eletrónicas, abrangendo registos de atividades, ficheiros, metadados, mensagens, dados de tráfego e de localização, entre outros [14]. Esta prova apresenta propriedades como intangibilidade, volatilidade, mutabilidade e dispersão geográfica, que exigem a aplicação de procedimentos especializados para garantir a sua autenticidade e integridade [18].

Pedro Dias Venâncio refere que a prova digital é central no Direito Civil, do ponto de vista substantivo e processual, especialmente no contexto do regime consagrado no Decreto-Lei n.º 290-D/99, de 2 de agosto, que atribui valor probatório a documentos, assinaturas e comunicações eletrónicas. No âmbito do direito penal, Venâncio analisa a prova digital à luz da Lei do Cibercrime (Lei n.º 109/2009), destacando o conjunto de medidas processuais destinadas à recolha de prova em suporte eletrónico, como a pesquisa de dados informáticos, a apreensão, a interceção e a preservação de dados [19, 20].

2.1.2 Metadados

Os metadados são dados que descrevem outros dados, funcionando como elementos estruturados que fornecem informação sobre o conteúdo, o contexto e as características técnicas de um ficheiro, registo ou objeto digital. Podem incluir dados como o autor, a data e hora de criação ou modificação, o tipo e formato do ficheiro, a localização geográfica ou lógica e a sua dimensão [21].

A norma ISO 23081-1:2017 classifica os metadados em três categorias, a saber:

- Descritivos – que identificam e caracterizam o recurso;
- Estruturais – que indicam como as partes de um recurso se organizam;
- Administrativos – que contêm informação necessária à gestão e preservação, incluindo direitos de uso e histórico de alterações.

No âmbito jurídico e forense, os metadados têm relevância particular, pois permitem estabelecer a proveniência, a linha temporal e a integridade de um ficheiro [21]. Em investigações criminais, podem ser utilizados para reconstruir eventos, identificar dispositivos usados ou verificar alterações. A sua recolha e preservação devem respeitar procedimentos técnicos e legais que garantam a cadeia de custódia, assegurando a admissibilidade da prova digital em tribunal.

Um exemplo prático aqui relevante é o de uma fotografia digital, que pode conter metadados em formato Exchangeable Image File Format (EXIF), como a data de captura, coordenadas Global Positioning System (GPS) do local onde foi tirada a fotografia, modelo da câmara fotográfica e demais configurações técnicas (exposição, brilho, entre ou-

tros). Estes dados podem ainda ajudar a confirmar a autenticidade do ficheiro ou revelar adulterações [21].

2.1.3 Cadeia de Custódia

A cadeia de custódia na análise forense digital corresponde ao conjunto de procedimentos que documentam, por ordem cronológica, todas as etapas de identificação, recolha, tratamento, transporte, armazenamento, análise e destino final das provas digitais [18]. O objetivo é manter a integridade, autenticidade e fiabilidade dos vestígios digitais, assegurando a sua validade como prova jurídica. Este registo deve identificar a prova, os responsáveis pelo seu manuseamento, as datas, horas e locais de armazenamento, bem como todas as transferências de responsabilidade, garantindo que a prova não sofre alterações que comprometam a sua validade.

No contexto jurídico português, diversas fontes académicas enquadram tais práticas no ordenamento legal nacional. A título de exemplo, Ramos [16] defende que os procedimentos técnicos e jurídicos de identificação, recolha e preservação da prova digital são essenciais para a sua admissibilidade.

2.2 Enquadramento Jurídico

A análise forense digital em dispositivos móveis enquadra-se num conjunto de normas que asseguram simultaneamente a validade da prova e a proteção dos direitos fundamentais. A Lei n.º 109/2009 (Lei do Cibercrime)[11] 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) [22]. O Regulamento (UE) 2016/679 de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados — RGPD)[23] RGPD, complementado pela Lei n.º 58/2019 de 8 de agosto, impõe limites rigorosos ao tratamento de dados pessoais, atendendo à natureza sensível da informação armazenada nestes dispositivos. O Código Penal [24] 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, Rakha [25] salienta que o combate ao cibercrime exige uma abordagem integrada entre os aspetos técnicos da investigação digital e os princípios jurídicos e éticos que a sustentam, sublinhando que a ausência dessa harmonização pode comprometer a admissibilidade e a legitimidade da prova digital. Em conjunto, estes diplomas procuram equilibrar a eficácia da investigação criminal com o respeito pela legalidade processual e pela privacidade dos cidadãos.

2.2.1 Lei do Cibercrime

A Lei n.º 109/2009, de 15 de setembro [11], estabelece o regime jurídico aplicável à criminalidade informática e à recolha de prova digital. Este diploma transpõe para o ordenamento jurídico português a Decisão-Quadro n.º 2005/222/JAI do Conselho [26] e a Convenção sobre o Cibercrime do Conselho da Europa [27], incorporando definições essenciais como "sistema informático" e "fornecedor de serviço". Estas definições constituem a base interpretativa para a aplicação das disposições penais e processuais nele previstas.

No plano penal substantivo, a Lei do Cibercrime tipifica condutas como falsidade informática (artigo 3.º), dano e sabotagem informática (artigos 4.º e 5.º), acesso ilegítimo (artigo 6.º), interceção ilegítima (artigo 7.º) e reprodução não autorizada de programas protegidos (artigo 8.º). O diploma prevê ainda a responsabilidade penal das pessoas coletivas (artigo 11.º) e a perda dos bens utilizados para a prática ilícita (artigo 12.º).

A Lei do Cibercrime articula-se com o Código Penal Português [24], adiante abreviadamente designado por CPP, contendo disposições que replicam ou complementam os tipos legais nela previstos. Entre estas, destacam-se o artigo 221.º (burla informática e nas comunicações), o artigo 262.º-A (dano relativo a programas ou outros dados informáticos), o artigo 262.º-B (dano relativo a dados ou programas informáticos utilizados no funcionamento de infraestruturas críticas), o artigo 264.º-A (sabotagem informática), o artigo 308.º (acesso ilegítimo), o artigo 309.º (interceção ilegítima) e o artigo 310.º (reprodução e uso ilegítimo de programa protegido). A coexistência destes regimes exige a aplicação de critérios como o princípio da especialidade para determinar a norma aplicável a cada caso.

A articulação com o CPP verifica-se no artigo 11.º da Lei do Cibercrime, que determina a aplicação subsidiária do CPP sempre que o diploma não disponha de regime próprio. Esta remissão assegura que as garantias processuais gerais, como a exigência de despacho judicial para a apreensão de comunicações prevista no artigo 179.º do CPP, sejam observadas também nas investigações de criminalidade informática. A tentativa de flexibilizar esta regra, introduzida pela Lei n.º 79/2021 [28] para permitir o acesso a mensagens eletrónicas com validação judicial subsequente, foi considerada inconstitucional pelo Tribunal Constitucional no Acórdão n.º 687/2021 [29], por violação do artigo 34.º, n.º 4, da Constituição.

Do ponto de vista processual, a Lei do Cibercrime estabelece um conjunto de meios especiais de obtenção de prova digital, incluindo a preservação expedita de dados (artigo 12.º), a revelação expedita de dados de tráfego (artigo 13.º), a injunção para apresentação ou concessão de acesso a dados (artigo 14.º), a pesquisa e apreensão de dados informáticos (artigos 15.º e 16.º), a apreensão de correio eletrónico e comunicações similares (artigo 17.º) e a interceção de comunicações (artigo 18.º). Estes mecanismos são relevantes para a

investigação forense digital, permitindo a recolha e conservação de elementos probatórios que, pela sua natureza volátil, podem ser rapidamente alterados ou destruídos.

No contexto do procedimento de forense digital, a Lei do Cibercrime define não apenas o quadro penal substantivo aplicável às condutas ilícitas, mas também os mecanismos processuais específicos para a recolha, preservação e análise de prova digital. A aplicação articulada com o Código Penal e com o Código de Processo Penal assegura que a investigação e a produção de prova em crimes informáticos ocorram dentro de um quadro normativo que combina especialidade e respeito pelas garantias processuais.

2.2.2 Legislação sobre Proteção de Dados

O RGPD, aprovado pelo Regulamento (União Europeia (UE)) 2016/679, estabelece o quadro jurídico aplicável ao tratamento de dados pessoais na União Europeia e em Portugal, sendo reconhecido como direito fundamental no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia [30]. O RGPD define conceitos como dados pessoais, tratamento, titular dos dados, responsável pelo tratamento e subcontratante, e consagra princípios como a limitação da finalidade, a minimização dos dados e a responsabilidade do operador [30]. Em Portugal, a Lei n.º 58/2019 assegura a execução do RGPD no ordenamento jurídico nacional e introduz adaptações necessárias à sua aplicação [31].

A Lei n.º 59/2019 de 8 de agosto transpõe a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e estabelece o regime aplicável ao tratamento de dados pessoais por autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais, bem como da execução de sanções penais [32]. Este regime define autorizações, salvaguardas e limitações específicas destinadas a assegurar um equilíbrio adequado entre as exigências de segurança pública e a proteção dos direitos fundamentais dos titulares dos dados.

A Comissão Nacional de Proteção de Dados (CNPD), criada pela Lei n.º 43/2004 de 18 de agosto [33], é a autoridade de controlo nacional responsável pela supervisão da aplicação do RGPD e da legislação nacional de proteção de dados, com competência para orientar, fiscalizar e aplicar sanções [34, 35, 36].

A doutrina nacional analisa o RGPD como marco legislativo estruturante no domínio da proteção de dados pessoais. Osório [37] examina a sua influência nas políticas de privacidade adotadas por organizações e indivíduos. Estudos internacionais, tais como o de Limberger [38], discutem a aplicação do RGPD a tecnologias emergentes, incluindo dispositivos da Internet das Coisas, com destaque para a exigência de consentimento explícito e a vinculação do tratamento à finalidade inicial da recolha.

O RGPD estabelece a função do Encarregado de Proteção de Dados (EPD), responsável

por supervisionar a conformidade com o regulamento, coordenar auditorias, cooperar com a autoridade de controlo e gerir pedidos dos titulares dos dados [30]. A sua implementação requer a designação formal do responsável, o mapeamento de dados, a organização dos processos, a documentação das medidas aplicadas e a formação das pessoas envolvidas.

A legislação nacional em Portugal prevê a utilização de técnicas de pseudonimização e anonimização como medidas de mitigação de risco, com o objetivo de reduzir a possibilidade de identificação direta dos titulares e, simultaneamente, preservar a utilidade dos dados em contextos .

Estas práticas encontram enquadramento jurídico tanto no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD), que reconhece a pseudonimização como uma medida técnica apropriada para a proteção de dados pessoais, como na Lei n.º 58/2019, de 8 de agosto, que assegura a execução do RGPD na ordem jurídica portuguesa e impõe às entidades responsáveis pelo tratamento a adoção de medidas técnicas e organizativas adequadas à salvaguarda dos direitos dos titulares [39, 31].

A legislação nacional, em Portugal, prevê a utilização de técnicas de pseudonimização e anonimização como medidas de mitigação de risco, com o objetivo de reduzir a possibilidade de identificação direta dos titulares e, simultaneamente, preservar a utilidade dos dados em contextos investigativos [31].

No contexto da análise forense digital de dispositivos móveis, o enquadramento legal português exige que o tratamento de dados digitais, incluindo a recolha, preservação e análise, seja autorizado, fundamentado e documentado, limitado à finalidade específica e realizado sob supervisão do EPD. As técnicas de pseudonimização constituem um mecanismo relevante para proteção da privacidade, assegurando que vestígios digitais sejam tratados de forma compatível com os requisitos legais, preservando a cadeia de custódia e garantindo a sua admissibilidade como prova em processo judicial.

2.2.3 Código Penal

O Código Penal português, aprovado pelo Decreto-Lei n.º 400/82, de 23 de setembro, define os tipos legais de crime e estabelece as respetivas sanções [40]. As alterações legislativas subsequentes introduziram normas adaptadas à criminalidade informática, em articulação com instrumentos internacionais como a Convenção de Budapeste sobre o Cibercrime, ratificada por Portugal pela Resolução da Assembleia da República n.º 88/2009 [41].

A Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, complementa o Código Penal ao tipificar condutas como o acesso ilegítimo, a interceção de comunicações, a

sabotagem informática e a falsidade informática [11]. Estes crimes devem ser interpretados em consonância com os princípios gerais de tipicidade, ilicitude, culpa e punibilidade previstos no Código Penal [40].

A investigação e a prova de crimes informáticos envolvendo dispositivos móveis requerem também a aplicação das normas do Código de Processo Penal, aprovado pelo Decreto-Lei n.º 78/87, de 17 de fevereiro, que estabelece regras para a recolha, preservação e apresentação de prova em juízo [42]. O artigo 174.º prevê a busca e apreensão, enquanto o artigo 178.º regula a perícia, ambos relevantes para a análise forense digital.

A produção de prova digital no contexto penal implica considerar as especificidades dos vestígios eletrónicos, cuja volatilidade e possibilidade de alteração exigem procedimentos técnicos adequados [43]. No caso de crimes como o acesso ilegítimo ou a interceção ilícita de comunicações, a prova extraída de dispositivos móveis deve permitir estabelecer a ocorrência do facto típico, a autoria e a ligação causal, respeitando a cadeia de custódia [43].

A aplicação prática do Código Penal na análise forense digital depende da correta qualificação jurídico-penal dos factos e da utilização de técnicas forenses compatíveis com os parâmetros probatórios exigidos pelo tribunal. Autores como Marques [44] defendem que a prova digital deve ser obtida por peritos devidamente credenciados, utilizando ferramentas reconhecidas e métodos validados, para assegurar que o tribunal possa valorá-la em conformidade com os princípios do processo penal.

2.2.4 Código de Processo Penal

O CPP, aprovado pelo Decreto-Lei n.º 78/87, de 17 de fevereiro, estabelece a estrutura e o funcionamento do processo penal português, regulando as fases de inquérito, instrução, julgamento e recurso, bem como as competências das autoridades judiciárias, os prazos processuais, as garantias de defesa, o estatuto processual dos intervenientes e os meios de obtenção de prova [42].

No contexto da análise forense digital, o CPP define regras aplicáveis à recolha, preservação e apresentação da prova. Estas incluem a prova pericial (arts. 151.º a 163.º), as buscas e apreensões (arts. 174.º a 186.º), a interceção de comunicações (arts. 187.º a 189.º) e o tratamento de documentos e objetos apreendidos. Para dados digitais provenientes de dispositivos móveis, estas normas aplicam-se diretamente ou por remissão da Lei n.º 109/2009 (Lei do Cibercrime), que estabelece procedimentos específicos para pesquisa, apreensão, preservação e revelação expedita de dados informáticos [11].

A disciplina geral da prova no CPP assenta no princípio da livre apreciação (art. 127.º), que permite ao tribunal formar a sua convicção com base na prova produzida, e no

princípio da legalidade dos meios de obtenção de prova, que proíbe a utilização de elementos obtidos com violação de direitos fundamentais ou proibições probatórias [16]. Estes princípios aplicam-se igualmente à prova digital, onde a recolha irregular pode conduzir à sua inadmissibilidade.

No regime de buscas e apreensões, o CPP exige autorização judicial para diligências em locais privados, salvo casos de flagrante delito, e prevê formalidades de documentação e justificação [45]. A Lei do Cibercrime adapta estas regras ao ambiente informático, prevendo que a apreensão de dados (art. 16.º) ou a pesquisa em sistemas (art. 15.º) sigam as formalidades do CPP, incluindo reserva de juiz para situações que envolvam direitos fundamentais.

A jurisprudência do Supremo Tribunal de Justiça (STJ) [3] [4] clarificou que a apreensão de mensagens de correio eletrónico ou de comunicações similares requer despacho do juiz de instrução, independentemente de estarem lidas ou não, aplicando-se o artigo 17.º da Lei do Cibercrime[5] e o artigo 179.º do CPP[6]. O Tribunal da Relação de Lisboa[7] distingue entre interceção de comunicações em trânsito (arts. 187.º e seguintes) e acesso a mensagens armazenadas (arts. 179.º e seguintes), esclarecendo a determinação do regime aplicável e a necessidade de reserva de juiz.

O regime de interceção de comunicações do CPP é restrito a um catálogo de crimes e depende de autorização judicial prévia. Abrange comunicações telefónicas e eletrónicas em trânsito, com prazos máximos, regras para execução, guarda e destruição de registos, e proibições específicas, como as comunicações entre advogado e cliente. A Lei do Cibercrime complementa este regime para dados de tráfego e conteúdos, com previsão autónoma para preservação e revelação expedita [11].

A prova pericial, prevista nos artigos 151.º a 163.º do CPP, aplica-se sempre que a perceção ou a apreciação dos factos exija conhecimentos técnicos, científicos ou artísticos. No domínio digital, a perícia é essencial para validar a aquisição, preservação e análise de dados [46]. O relatório pericial deve indicar o objeto, a metodologia, as operações realizadas e as conclusões, documentando todas as fases do processo para permitir controlo judicial e contraditório [43].

Embora o CPP não utilize a expressão "cadeia de custódia", o conceito decorre das regras

[3] ver `https://juris.stj.pt/28999\%2F18.3T8LSB-B.L1-A.S1/YXWIK-7MTIt2d802J-n3UAaaelU`

[4] `https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/9b1e715fa7cdbceb80258a4b003f6591?OpenDocument`

[5] `https://diariodarepublica.pt/dr/detalhe/acordao-supremo-tribunal-justica/10-2023-224081976`

[6] `https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument`

[7] `https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/8ce57ecb0a16a8e0802585ec0036019a?OpenDocument`

de apreensão, guarda e restituição de objetos, bem como das exigências de documentação das diligências. Na prova digital, a preservação da integridade e autenticidade é garantida por técnicas como o cálculo de valores chamados de resumos criptográficos, ou *secure hash* em inglês, e o registo de metadados [43].

Assim, o CPP fornece o quadro legal de base para a recolha, preservação e utilização da prova digital em processo penal, enquanto a Lei do Cibercrime introduz mecanismos específicos adaptados ao ambiente informático. A jurisprudência assegura a aplicação uniforme destas normas, e a doutrina sublinha que apenas a conjugação de rigor técnico com cumprimento das formalidades processuais assegura a admissibilidade da prova digital em julgamento.

2.3 Normas e Diretrizes Internacionais

A análise forense digital em dispositivos móveis é também orientada por normas e diretrizes internacionais que asseguram a uniformização de procedimentos e a validade da prova em diferentes contextos. Destacam-se as orientações do NIST, em particular a SP 800-101, que define fases e boas práticas para apreensão, aquisição, análise e reporte; as diretrizes da INTERPOL, que promovem a cooperação e harmonização de metodologias entre autoridades; e as normas ISO/International Electrotechnical Commission (IEC), como a número 27037, que estabelecem critérios técnicos de preservação e integridade da prova digital. Estes referenciais complementam a legislação nacional e reforçam a credibilidade da prova em sede judicial.

2.3.1 Publicações NIST

O NIST, organismo norte-americano que se destaca na definição de normas e boas práticas no domínio da segurança da informação e da ciência forense digital, tem publicado uma série de documentos que orientam profissionais, académicos e instituições na implementação de procedimentos rigorosos e tecnicamente sólidos. O NIST tem desempenhado um papel relevante no desenvolvimento de normas e guias técnicos aplicados à segurança da informação e à ciência forense digital, estabelecendo metodologias reconhecidas internacionalmente.

Entre as suas publicações mais relevantes para a área da forense digital, destacam-se:

- *NIST SP 800-86 (2006): Guide to Integrating Forensic Techniques into Incident Response*, que introduz a integração de técnicas forenses em processos de resposta a incidentes.
- *NIST SP 800-72 (2004)*: *Guidelines on PDA Forensics*, voltado especificamente para dispositivos de assistência pessoal digital (antecessores dos smartphones).

- *NIST SP 800-115 (2008): Technical Guide to Information Security Testing and Assessment*, que inclui metodologias de teste e auditoria aplicáveis a contextos forenses.

- *NIST SP 800-101 Revision 1 (2014): Guidelines on Mobile Device Forensics*, documento atualizado que substitui a versão original de 2007 e serve hoje como a principal referência internacional para a recolha, preservação, análise e apresentação de evidências provenientes de dispositivos móveis.

No que respeita à análise forense aplicada a dispositivos móveis, destaca-se a publicação NIST SP 800-101, publicada em 2014, que se consolidou como uma referência central para a prática norte-americana nesta área emergente e em constante evolução. Este documento surge em resposta à transformação tecnológica que fez dos dispositivos móveis, como smartphones e tablets, não apenas ferramentas de comunicação, mas também centros de armazenamento e gestão de informação pessoal e profissional. Os dispositivos móveis atuais integram funcionalidades que vão muito além das chamadas e mensagens, abrangendo sistemas de georreferenciação como o GPS, o correio eletrónico, o acesso a redes sociais, a informação bancária, bem assim como aplicações de produtividade e de entretenimento. A sua ligação constante a serviços em nuvem, em potência, pode possibilitar acesso a um ainda maior conjunto de dados e informação. Esta circunstância transforma os dispositivos móveis em fontes privilegiadas de prova digital, pese embora sejam dispositivos de tratamento complexo no contexto forense, dado o ritmo acelerado de evolução tecnológica e a diversidade de plataformas existentes.

A NIST SP 800-101 define um conjunto de princípios e fases de atuação que visam harmonizar a prática forense, assegurando não apenas a extração do maior volume possível de dados relevantes, mas sobretudo a sua validade, integridade e admissibilidade em tribunal. O guia estrutura-se em torno de quatro grandes fases processuais, que são apresentadas como interdependentes e que devem ser seguidas de acordo com os requisitos técnicos e legais de cada investigação: apreensão, aquisição, exame e análise, e relatório.

Importa salientar, no entanto, que estas fases não devem ser entendidas como etapas estanques e lineares, mas antes como um modelo lógico de referência, sujeito a sobreposições e repetições, consoante as especificidades de cada caso. Por exemplo, durante a fase de aquisição, pode ser necessário realizar um exame preliminar para verificar a consistência dos dados obtidos, criando uma sobreposição entre as duas fases. De igual modo, a necessidade de recuperar informação em falta pode exigir a repetição da aquisição, recorrendo a técnicas mais intrusivas ou complementares. Também em situações em que o dispositivo contém dados voláteis em risco de perda imediata, o perito pode ser forçado a proceder a análises parciais ainda durante a fase de preservação. Esta flexibilidade, longe de comprometer o rigor do processo, reforça-o, uma vez que permite adaptar a metodologia às

condições concretas de cada investigação, assegurando a máxima integridade da evidência e a sua aceitabilidade em tribunal.

A Fig. 2.1 apresenta a triagem recomendada no processo proposto na NIST SP 800-101 [1]. A triagem é apresentada sob a forma de um fluxograma de triagem genérica, utilizado para orientar o processo de decisão durante as fases iniciais de recolha e análise de dispositivos em contextos de investigação forense digital. O diagrama tem como objetivo apoiar o operador na escolha das ações mais adequadas, tendo em conta a urgência da situação, o estado do dispositivo, o nível de bateria e os recursos técnicos disponíveis. O processo inicia-se com a verificação da urgência do caso. Se este for considerado urgente, deve confirmar-se se o dispositivo se encontra desbloqueado e sem danos, e se o operador dispõe das ferramentas e da formação necessárias para proceder. Quando estas condições estão reunidas, aplicam-se técnicas de isolamento, como o modo de voo ou o isolamento de rádio, e realiza-se a extração de dados. Caso, após a extração, sejam necessários dados adicionais, o dispositivo é encaminhado para processamento em laboratório; caso contrário, o processo é dado como concluído. No entanto, se o operador não possuir os meios ou a formação adequados, deve contactar um especialista.

Se a situação não for urgente, o fluxograma orienta a verificar se o laboratório se encontra a menos de duas horas de distância e se a bateria do dispositivo está acima de 50%. Se estas condições forem cumpridas, aplicam-se as técnicas de isolamento adequadas, como o modo de voo, o isolamento de rádio, a remoção da bateria ou o simples desligar do equipamento, e o dispositivo é então enviado para o laboratório. Caso contrário, o operador deve igualmente contactar um especialista, garantindo que o dispositivo é manuseado de forma segura e que a integridade dos dados é preservada.

De forma geral, o fluxograma define uma sequência estruturada de decisões que assegura uma atuação controlada, segura e tecnicamente adequada durante a recolha inicial de dispositivos. Este procedimento reduz o risco de perda, alteração ou contaminação dos dados, contribuindo assim para a fiabilidade e validade das provas digitais recolhidas.

Fase 1: Apreensão

A fase de apreensão constitui o ponto de partida do processo forense e desempenha um papel absolutamente crucial para a validade da evidência digital. O seu objetivo principal é assegurar que os dados recolhidos em dispositivos móveis permanecem inalterados desde o momento da apreensão até à análise em laboratório, garantindo assim a integridade, a autenticidade e a admissibilidade jurídica da prova.

Logo no local da ocorrência, o primeiro passo consiste na documentação inicial do dispositivo e do contexto em que foi encontrado. Devem ser registadas as condições em que o equipamento se encontrava (se estava ligado ou desligado, bloqueado ou desbloqueado,

Figura 2.1: Procedimento geral proposto na NIST SP 800-101 (Obtida de [1])

em rede ou em modo *offline*), bem como informações sobre o ambiente físico da apreensão. Esta documentação deve incluir fotografias, anotações e, sempre que possível, o testemunho de agentes ou peritos presentes, de forma a criar um registo fiável do estado inicial da evidência.

Um dos aspetos mais críticos da apreensão é o isolamento do dispositivo para evitar

Figura 2.2: Exemplo de Bolsa de *Faraday*

qualquer alteração remota dos dados, seja por atualizações automáticas, sincronizações com a cloud, comunicações de rede ou ações deliberadas de terceiros. Para tal, recorrem-se a técnicas e dispositivos específicos, como as bolsas de (ver exemplo na Fig. 2.2), que bloqueiam sinais de rádio, ou a ativação do modo avião, quando operacionalmente viável.

Paralelamente, deve ser garantida a conservação física do dispositivo, com o recurso a invólucros antiestáticos e embalagens seladas, protegendo-o contra humidade, variações de temperatura ou danos mecânicos. O transporte até ao laboratório forense deve ser feito em condições controladas e devidamente documentado para manter a cadeia de custódia.

É essencial que cada ação realizada seja registada em relatórios de ocorrência ou fichas de cadeia de custódia. Esta documentação inclui informações sobre quem apreendeu o dispositivo, em que circunstâncias, quais os procedimentos aplicados e quem teve acesso à evidência em cada momento.

Em suma, a apreensão estabelece as bases de todo o processo forense, funcionando como a garantia inicial de que os dados obtidos são fidedignos, íntegros e legalmente válidos. Sem uma apreensão rigorosa, mesmo a análise mais avançada pode ser comprometida, colocando em risco a admissibilidade da prova em tribunal e a credibilidade da investigação.

Fase 2: Aquisição

A fase de aquisição representa um dos momentos centrais do processo de forense digital em dispositivos móveis, pois dela depende não apenas a quantidade de dados obtidos, mas também a sua qualidade e integridade, aspetos indispensáveis para que a informação

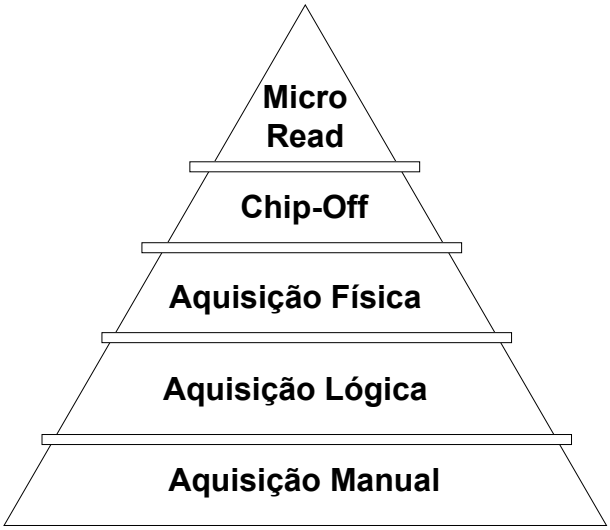


Figura 2.3: Classificação de métodos de aquisição (adaptado de [1])

seja aceite como prova válida. De acordo com a SP 800-101, esta etapa é considerada particularmente crítica, dado que envolve a extração do conteúdo armazenado no dispositivo com a finalidade de o preservar no seu estado original e garantir a possibilidade de replicar em análises futuras. Para orientar este processo, o guia estabelece uma classificação estruturada em cinco níveis, que se distinguem pelo grau de complexidade técnica, pela intrusividade dos métodos aplicados e pela profundidade do acesso à memória do equipamento (ver Fig. 2.3).

O primeiro nível corresponde à aquisição manual, em que o perito interage diretamente com o dispositivo e regista a informação exibida no ecrã. Trata-se de um método simples e não intrusivo, frequentemente utilizado em contextos de urgência ou quando não se dispõe de ferramentas especializadas. O registo pode ser realizado através de fotografias, vídeos ou notas manuais. Apesar da sua utilidade prática em cenários específicos, esta técnica apresenta limitações significativas, já que apenas permite capturar dados visíveis e está sujeita a erros humanos, não possibilitando a recuperação de informação eliminada ou armazenada em áreas ocultas da memória.

O segundo nível é a aquisição lógica e constitui um avanço em relação ao nível anterior, permitindo a extração de objetos de dados a partir do sistema operativo do dispositivo, recorrendo a protocolos de comunicação como USB, *Bluetooth* ou Wi-Fi, bem como às Application Programming Interfaces (APIs) disponibilizadas pelos fabricantes. Este método viabiliza a recolha de elementos como mensagens de texto, registos de chamadas, contactos, emails, ficheiros multimédia e dados de aplicações. A principal vantagem reside no facto de ser um processo relativamente rápido, não intrusivo e amplamente suportado por ferramentas forenses reconhecidas, tais como o *Cellebrite UFED Logical, o XRY Logical ou o Oxygen Forensic Suite*. Contudo, este tipo de aquisição não acede diretamente à

memória física do dispositivo e, por isso, raramente permite recuperar dados apagados ou encriptados.

O terceiro nível é a aquisição física que aprofunda a análise ao proporcionar uma cópia *bit a bit* da(s) memória(s) do dispositivo, de forma semelhante ao que ocorre na criação de imagens forenses de discos rígidos em computadores. Ao duplicar integralmente o conteúdo da memória, esta técnica possibilita o acesso a dados ativos, apagados ou fragmentados. Entre os métodos utilizados destaca-se a exploração de interfaces de depuração via Joint Test Action Group (JTAG) [47] e o recurso a programas de arranque (*bootloaders*) modificados. Ferramentas como o *Cellebrite UFED Ultimate, o XRY Complete ou o EnCase Smartphone Examiner* oferecem suporte para este tipo de aquisição. Embora mais poderosa, a aquisição física é também mais complexa, requerendo equipamento especializado, mais conhecimentos técnicos e apresentando riscos acrescidos para o dispositivo.

O quarto nível, conhecido como *chip-off* (ver exemplo na Fig. 2.4), é um procedimento altamente invasivo que implica a dessoldagem do chip de memória do dispositivo, seguido da sua leitura através de programadores externos. Este método é geralmente reservado para situações em que o equipamento se encontra seriamente danificado ou em que as abordagens anteriores se revelaram infrutíferas. Apesar da sua eficácia na recuperação de dados inacessíveis por outros meios, o *chip-off* apresenta desvantagens já que é um processo destrutivo, por vezes irreversível, e que exige elevado grau de especialização técnica e recursos laboratoriais apropriados.

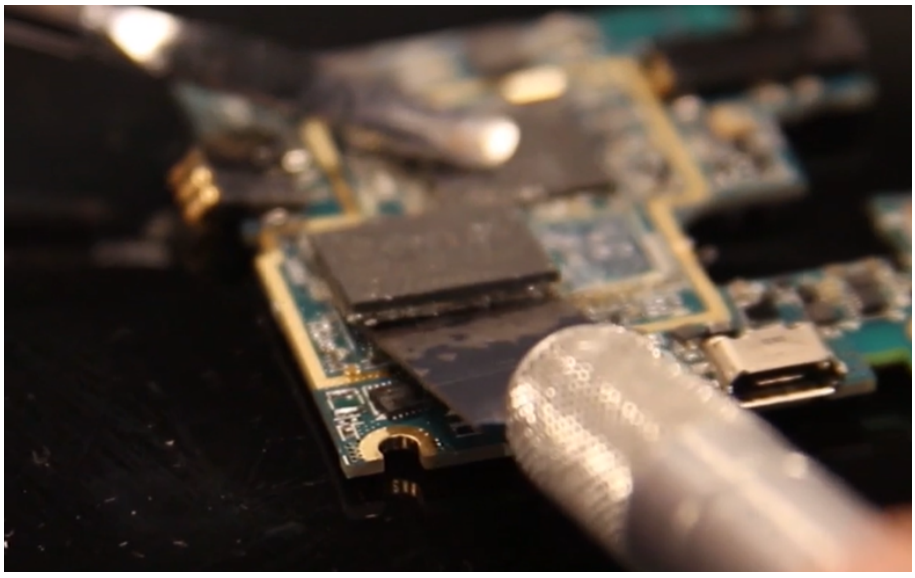


Figura 2.4: Exemplo de Técnica de *chip-off*

Por fim, o quinto nível refere-se à aquisição por micro-read, considerada a técnica mais avançada e especializada. Este método consiste na análise direta das células de memória através de microscopia eletrónica, permitindo a interpretação manual dos padrões binários armazenados. Trata-se de um processo extremamente moroso, oneroso e tecnicamente

exigente, raramente utilizado fora de contextos militares ou governamentais. Apesar do seu potencial em casos de elevado valor estratégico, o micro-read é visto como uma medida de último recurso, apenas aplicável quando todos os outros métodos falharam.

Para além da memória interna do dispositivo, os cartões Subscriber Identity Module (SIM)/Universal Integrated Circuit Card (UICC) representam uma fonte importante de informação forense. Estes cartões armazenam dados essenciais para a identificação e funcionamento do terminal na rede, tais como o International Mobile Subscriber Identity (IMSI), o Integrated Circuit Card Identifier (ICCID), registos de Short Message Service (SMS) e listas de contactos. A sua análise pode fornecer elementos cruciais para investigações relacionadas com comunicações, ligações entre utilizadores e geolocalização. A extração de dados é realizada com ferramentas especializadas (ver exemplo na Fig. 2.5), que permitem ler, clonar e interpretar os conteúdos sem comprometer a integridade do cartão original.

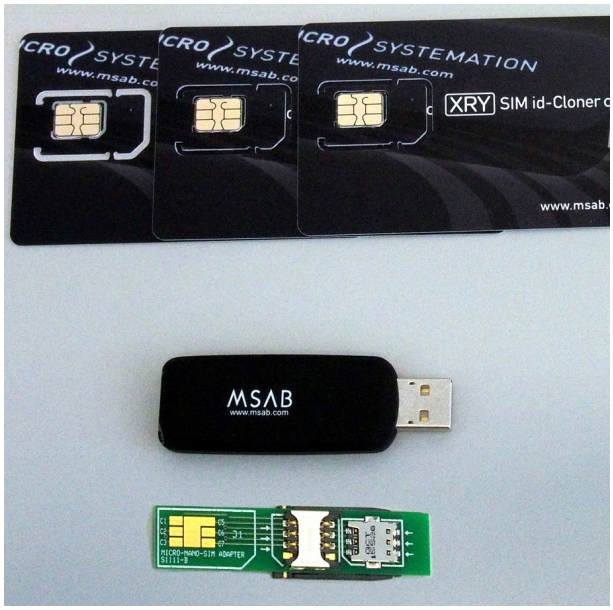


Figura 2.5: Exemplo de Leitor de cartões SIM da MSAB [2]

Os cartões de memória removíveis, como SD ou microSD, que frequentemente armazenam ficheiros multimédia, documentos, bases de dados de aplicações e até sistemas operativos portáteis. Do ponto de vista forense, estes suportes devem ser tratados como discos removíveis e, por conseguinte, clonados de forma bit a bit através de ferramentas forenses tradicionais. Aplicações como o *FTK Imager ou o EnCase* permitem criar cópias forenses fiéis, garantindo a preservação dos dados e a verificação de integridade através do cálculo de resumos criptográficos (*hashes*).

Com a crescente integração entre dispositivos móveis e serviços de armazenamento remoto, a aquisição de dados em *Cloud* tornou-se um elemento essencial das investigações forenses. Muitos sistemas operativos e aplicações móveis realizam cópias de segurança

automáticas para serviços como *iCloud, Google Drive ou OneDrive*, o que significa que a informação de maior interesse pode não estar apenas no terminal, mas também armazenada remotamente. A recolha destes dados requer, contudo, cuidados adicionais de ordem legal e técnica: é geralmente necessária a posse das credenciais do utilizador ou a apresentação de ordens judiciais válidas para acesso aos conteúdos. Ferramentas forenses específicas já integram módulos de extração em *Cloud*, permitindo sincronizar e descarregar informações de contas online de forma controlada e auditável. Este tipo de aquisição amplia significativamente o alcance da investigação, mas exige atenção redobrada à cadeia de custódia e ao enquadramento jurídico da recolha.

Fase 3: Análise

A fase de análise representa o momento em que os dados adquiridos são processados, interpretados e correlacionados, de forma a produzir informação com valor probatório. Se nas fases anteriores (apreensão e aquisição) o objetivo principal é garantir a integridade e a completude da evidência, nesta etapa a ênfase recai sobre a sua interpretação técnica e contextual, permitindo responder a questões de investigação concretas.

Incluí o tratamento inicial da evidência digital, que envolve a organização, a filtragem e a reconstrução de dados a partir da imagem forense obtida. Nesta fase, o perito pode realizar tarefas como a identificação da estrutura do sistema de ficheiros, a extração de bases de dados internas (por exemplo, em formato *SQLite*), a indexação de documentos e a recuperação de dados ocultos ou fragmentados. Técnicas de *parsing* permitem reconstruir o conteúdo de aplicações móveis, como mensagens de *chat*, registos de navegação e histórico de GPS, mesmo quando dispersos em múltiplos ficheiros ou diretórios.

A análise corresponde ainda à interpretação contextual dos dados extraídos, relacionando-os com hipóteses de investigação. Esta etapa pode abranger, por exemplo, a correlação entre registos de chamadas e mensagens, a geolocalização de eventos através de dados GPS ou torres de telecomunicações, a identificação de comunicações em redes sociais, bem como a deteção de software malicioso ou de técnicas de ocultação de atividade. Em casos complexos, é comum recorrer a métodos de validação cruzada, nos quais diferentes ferramentas são aplicadas ao mesmo conjunto de dados, a fim de confirmar a consistência e a fiabilidade dos resultados.

Um dos desafios mais relevantes desta fase é a encriptação dos dados, amplamente utilizada nos dispositivos móveis modernos. A presença de mecanismos de proteção, como PINs, *passwords*, padrões de desbloqueio ou autenticação biométrica, pode limitar ou até impedir o acesso à informação. Nestes casos, o perito pode recorrer a técnicas específicas para ultrapassar estas limitações, incluindo ferramentas de *brute force*, sempre em conformidade com as orientações legais e procedimentais vigentes. Outro obstáculo frequente

é a utilização de formatos proprietários e compressão, que exigem ferramentas forenses atualizadas e compatíveis.

No que respeita a fontes de evidência, os dispositivos móveis oferecem uma diversidade de dados de interesse, entre os quais se incluem: registos de chamadas, mensagens SMS e Multimedia Message Service (MMS), correio eletrónico, histórico de navegação, dados de geolocalização, fotografias e vídeos com metadados embutidos, aplicações de mensagens instantâneas e redes sociais. As bases de dados das aplicações, geralmente em formatos padronizados, como o SQLite, constituem um repositório particularmente rico de informação forense.

A análise forense de dispositivos móveis também deve considerar o contexto temporal e sequencial dos dados. A correlação entre timestamps de ficheiros, registos de chamadas e eventos de GPS permite reconstruir linhas temporais de atividade, que podem ser fundamentais para estabelecer cronologias de incidentes. Técnicas de análise temporal e visualização gráfica são frequentemente aplicadas para facilitar a interpretação e a apresentação dos resultados.

As ferramentas utilizadas nesta fase incluem tanto soluções comerciais robustas, como o *Cellebrite UFED Analytics* [48], o *Oxygen Forensic Detective e o XRY Analyzer* [48], mas também plataformas de código aberto como o *Autopsy* [49], que oferecem flexibilidade na análise e integração com outros sistemas. Independentemente da ferramenta escolhida, é essencial que o processo seja repetível, validado e devidamente documentado, de modo a garantir a admissibilidade legal da prova.

Em síntese, a fase de análise é aquela em que a evidência digital é transformada em conhecimento útil, suportando investigações criminais, auditorias internas ou processos judiciais. A sua eficácia depende não apenas da sofisticação das ferramentas utilizadas, mas também da capacidade interpretativa do perito, que deve combinar rigor técnico com compreensão do contexto de investigação.

Fase 4: Reporte

A fase final corresponde à elaboração do relatório, documento técnico no qual o perito deve apresentar os resultados de forma estruturada, clara, objetiva e passível de auditoria. Este relatório não se limita à exposição dos dados extraídos, devendo incluir também a descrição detalhada dos métodos aplicados, das ferramentas utilizadas, das versões de software envolvidas e dos valores dos resumos criptográficos que comprovam a integridade dos ficheiros obtidos. Os resultados da análise deverão ser sistematizados, interpretados e comunicados de modo a serem compreensíveis tanto por especialistas como por magistrados, advogados ou outros intervenientes processuais. Dado que os relatórios forenses constituem frequentemente a base de avaliação judicial e podem ser objeto de contestação

pela defesa, torna-se indispensável que toda a metodologia seguida seja transparente, replicável e suscetível de validação por terceiros.

Um relatório forense robusto deve incluir, de forma organizada, os seguintes elementos:

- Identificação da evidência analisada: descrição detalhada do dispositivo e dos suportes associados (cartões SIM, cartões SD, cópias de *Cloud*), com menção a características técnicas como fabricante, modelo, número de série, sistema operativo e versão.
- Metodologias aplicadas: exposição das técnicas de preservação, aquisição, exame e análise utilizadas, incluindo o nível de aquisição seguido, os procedimentos técnicos adotados e as justificações para a escolha de determinadas abordagens em detrimento de outras.
- Ferramentas utilizadas: referência às ferramentas forenses utilizadas em cada etapa (com indicação de versões e configurações), bem como às suas limitações conhecidas.
- Resultados obtidos: apresentação dos dados relevantes extraídos e analisados, acompanhada de evidências de suporte, como capturas de ecrã, registos de *hashes* criptográficos e *logs* de ferramentas.
- Limitações encontradas: enumeração de obstáculos técnicos ou jurídicos, como dados inacessíveis devido à encriptação, incompatibilidades de ferramentas ou ausência de credenciais de Cloud.
- Cadeia de custódia: documentação pormenorizada de todas as ações realizadas, identificando quem teve contacto com a evidência e em que circunstâncias, garantindo a rastreabilidade completa do processo.
- Conclusões finais: síntese objetiva dos factos estabelecidos a partir da análise, contextualizados em relação aos objetivos da investigação ou às questões colocadas pela autoridade judicial.

Além da estrutura textual, é recomendada a inclusão de anexos técnicos, contendo informações detalhadas que suportem as conclusões apresentadas, tais como relatórios gerados automaticamente pelas ferramentas forenses, cópias de *logs*, listas de resumos criptográficos e linhas do tempo ou cronologias. Estes anexos permitem assegurar a transparência e a auditabilidade do processo, oferecendo ao leitor especializado a possibilidade de verificar e reproduzir os resultados obtidos.

Outros Aspetos

Para além da estrutura metodológica, o NIST dedica especial atenção a aspetos técnicos específicos que frequentemente constituem obstáculos no trabalho forense.

Um deles é a distinção entre memória volátil (RAM) e não volátil (NAND/NOR flash). A memória volátil, que armazena dados temporários como chaves de sessão ou palavras-passe em uso, perde o seu conteúdo quando o dispositivo é desligado, exigindo que os investigadores adotem procedimentos adequados para a sua captura. A memória não volátil, por seu turno, contém os dados persistentes e, devido a mecanismos como os algoritmos de *wear leveling e garbage collection* [50], pode preservar múltiplas cópias de ficheiros ou fragmentos que representam oportunidades únicas de recuperação de prova.

Outro aspeto de destaque refere-se aos cartões de telemóvel (SIM/UICC), que armazenam identificadores cruciais como o IMSI e o ICCID, para além de poderem também conter registos de chamadas, mensagens de texto e dados de localização de células de rede. É recomendado que estes cartões sejam extraídos e analisados separadamente com leitores especializados, uma vez que podem conter informação não acessível através do dispositivo.

No que respeita às redes celulares, o NIST sublinha o valor dos registos mantidos pelas operadoras, designados os Call Detail Records (CDR), que complementam a análise realizada no dispositivo, permitindo obter dados de localização aproximada, duração de chamadas, volume de tráfego e interações entre utilizadores.

Finalmente, a publicação aborda o tema dos dispositivos obstruídos, protegidos por mecanismos de bloqueio ou encriptação. São descritas abordagens técnicas, como ataques de arranque a frio (*cold boot attacks*) ou o recurso a ferramentas de extração JTAG para contornar bloqueios, mas o documento enfatiza que tais métodos implicam riscos significativos de perda ou alteração de evidência, devendo ser utilizados apenas por peritos altamente especializados e em conformidade com orientações legais.

Em síntese, a NIST SP 800-101 estabelece um quadro metodológico que conjuga rigor técnico com conformidade legal, promovendo práticas que asseguram tanto a eficácia da extração de dados como a sua aceitabilidade em tribunal. Não sendo um manual prescritivo, mas antes um guia de boas práticas, o documento reforça a importância da normalização internacional, constituindo-se como referência essencial para o desenvolvimento de capacidades institucionais na área da análise forense digital de dispositivos móveis.

2.3.2 Diretrizes INTERPOL

A INTERPOL, uma organização policial internacional, tem como missão fomentar a cooperação entre diferentes jurisdições para promover a prevenção e o combate ao crime transnacional. No domínio específico da cibercriminalidade, a organização sentiu a necessidade de definir normas técnicas e operacionais para orientar a atuação dos primeiros intervenientes no local (ou *first responders*, em inglês), isto é, agentes da polícia, investigadores ou peritos enquanto estes são os primeiros a intervir num incidente. Incidente este que poderá incluir dispositivos digitais.

As orientações constantes de [51] resumem o que a INTERPOL considera como melhores práticas forenses internacionais e têm como objetivo harmonizar procedimentos, minimizando o risco de adulteração de evidências, e assegurar que os métodos de recolha se mantêm compatíveis com a realidade tecnológica contemporânea. Tal como outras normas de referência, entre as quais se destacam as publicadas pelo NIST, estas orientações da INTERPOL estabelecem uma estrutura metodológica que visa garantir que os primeiros intervenientes atuem de forma célere, eficaz e juridicamente sólida. Estas orientações consideram as fases desde a preparação de operações de busca e apreensão até aos procedimentos técnicos específicos aplicáveis a diferentes tipos de dispositivos digitais, reforçando a sua pertinência prática e o seu enquadramento no esforço internacional de combate ao cibercrime.

O documento mais relevante no âmbito do trabalho desta dissertação é o *Guidelines for Digital Forensics First Responders – Best Practices for Search and Seizure of Electronic and Digital Evidence* [51], produzido pela INTERPOL, porque se destina a orientar as equipas de policia e os peritos responsáveis pela apreensão e tratamento inicial de dispositivos digitais, com destaque para smartphones e tablets.

Estas orientações partem de um princípio fundamental: a qualidade da evidência digital, pela sua natureza volátil e suscetível de alteração ou destruição, deve ser tratada com um rigor metodológico que assegure a sua integridade, autenticidade e admissibilidade legal. A INTERPOL recomenda que toda a intervenção em campo seja cuidadosamente planeada e documentada, desde a preparação da busca e apreensão até ao transporte do material para laboratório.

Uma ressalta uma diferença significativa entre as orientações propostas pela INTERPOL, quando comparadas com as da NIST, e que é o número de fases consideradas. A norma da NIST considera 4 fases (apreensão, aquisição, análise e reporte), já as orientações da INTERPOL focam-se mais na parte inicial, considerando 2 fases (preparação da apreensão e apreensão).

Fase 1: Preparação da Apreensão

A fase de preparação constitui o alicerce de qualquer intervenção forense em ambiente digital e é considerada pela INTERPOL como um momento determinante para o sucesso da operação. A ausência de um planeamento adequado pode comprometer a recolha da prova, conduzindo à perda de dados voláteis, à contaminação involuntária de evidências ou mesmo à sua rejeição em tribunal por incumprimento dos requisitos legais. Assim, a preparação deve ser entendida como um processo sistemático e multidimensional, que envolve aspetos jurídicos, técnicos, logísticos e humanos.

O primeiro passo consiste na definição clara dos objetivos e do âmbito da operação. A

equipa deve compreender a natureza do crime em investigação, os dispositivos digitais que se espera encontrar e o tipo de dados que se pretende privilegiar durante a apreensão. Este exercício de delimitação é fundamental, pois orienta não apenas a escolha das ferramentas adequadas, mas também a constituição da equipa e a forma como serão estabelecidas as prioridades no terreno. A composição da equipa de intervenção deve ser cuidadosamente planeada. Deste modo,para além dos primeiros intervenientes, responsáveis pela execução inicial da diligência, podem ser necessários peritos em forense digital, técnicos de informática especializados em redes ou servidores, agentes de segurança encarregues do isolamento da cena e representantes legais que assegurem a conformidade da operação com as normas jurídicas aplicáveis. A atribuição prévia de papéis e responsabilidades a cada elemento é crucial para evitar sobreposição de tarefas, falhas de comunicação ou perda de informação crítica.

A preparação jurídica é outra dimensão central desta fase. Antes da intervenção, devem ser obtidos todos os mandados de busca e apreensão ou outras autorizações judiciais relevantes, verificando-se a sua validade temporal e territorial. Poderá também ser necessário preparar documentação complementar para solicitar acesso a dados armazenados em servidores remotos ou em serviços de nuvem, o que exige mecanismos de cooperação internacional. Sem esta base legal sólida, a prova recolhida corre o risco de se tornar inadmissível em tribunal, independentemente da sua relevância.

No plano técnico, a preparação passa pela verificação rigorosa dos kits de apreensão digital. Estes devem conter ferramentas indispensáveis, como sacos de *Faraday* para impedir transmissões sem fios, bloqueadores de escrita (ver exemplo na Fig. 2.6) que permitem o acesso a suportes de armazenamento digital[8] sem alterar os dados originais, duplicadores forenses e softwares de aquisição para criação de imagens bit a bit, câmaras fotográficas digitais para registo da cena, blocos de notas e etiquetas invioláveis para assegurar a cadeia de custódia, bem como fontes de energia portáteis e cabos variados que possibilitem a ligação a diferentes dispositivos. Materiais de acondicionamento, como sacos antiestáticos e recipientes resistentes a impactos ou variações de temperatura, são igualmente necessários para garantir a preservação física dos equipamentos.

A par disso, deve ser realizada uma avaliação cuidada dos riscos associados à operação. É necessário considerar a possibilidade de ameaças à segurança física da equipa, como sistemas elétricos defeituosos ou substâncias perigosas no local, bem como riscos de natureza digital, como a existência de mecanismos de autodestruição remota dos dados, sincronização automática com serviços de nuvem ou a ativação de encriptação automática aquando o desligamento do equipamento. Antecipar estas situações permite à equipa preparar-se para decisões críticas no terreno, nomeadamente sobre a necessidade de proceder a uma aquisição em vivo ou optar pela apreensão imediata do dispositivo.

[8]Ex.: Discos de computador, *pens* USB, discos externos, e similares.

Figura 2.6: Exemplo de bloqueador de escrita (Fonte: [3])

A preparação envolve ainda a comunicação e coordenação entre todos os elementos da equipa. Antes da execução, todos devem ser informados sobre o plano detalhado da operação, incluindo a sequência de entrada no local, os procedimentos de isolamento da cena, os responsáveis por cada conjunto de tarefas e as medidas de contingência a adotar em caso de falha técnica ou resistência por parte dos ocupantes do espaço. Esta coordenação prévia reduz a margem de erro, assegura que a intervenção decorre de forma organizada e permite que, mesmo em cenários de elevada pressão, a prova digital seja

recolhida de modo eficiente, preservando a sua integridade e valor probatório.

Fase 2: Apreensão

A fase de apreensão corresponde ao momento em que a operação planeada entra em ação e a equipa de primeiros intervenientes passa a interagir diretamente com a cena e os dispositivos digitais a apreender. Trata-se de uma etapa crítica, em que as decisões tomadas no terreno podem ditar o sucesso ou o fracasso de todo o processo de recolha e preservação da prova digital. A INTERPOL enfatiza que esta fase deve ser conduzida com disciplina, atenção minuciosa ao detalhe e respeito absoluto pelos princípios de integridade, autenticidade e legalidade da evidência.

Ao chegar ao local, é prioridade da equipa o controlo e isolamento da cena; é necessário garantir que nenhum indivíduo não autorizado tenha acesso aos dispositivos digitais, prevenindo qualquer manipulação, apagamento ou transmissão remota de dados. Os primeiros intervenientes devem proceder a uma avaliação rápida da cena. Todos os dispositivos digitais identificados (computadores, *smartphones, tablets*, servidores, consolas, câmaras de vigilância ou equipamentos Internet of Things (IoT)) devem ser registados no estado em que se encontram no momento da apreensão. Antes de qualquer manipulação, deve ser realizada uma documentação fotográfica, complementada por notas descritivas, de forma a preservar o contexto original em que os objetos foram encontrados. Esta documentação inicial servirá para reconstituir a cena em tribunal, garantindo transparência e robustez ao processo.

A manipulação dos dispositivos representa um dos momentos mais delicados desta fase. Os equipamentos podem ser encontrados em diferentes estados: ligados, desligados ou em modo de suspensão. Cada uma destas situações impõe escolhas técnicas específicas. No caso de um dispositivo desligado, a recomendação é evitar qualquer tentativa de o ligar, uma vez que isso poderia alterar dados críticos, desencadear rotinas automáticas de encriptação ou destruir vestígios em memória volátil. Quando o dispositivo se encontra ligado, a equipa deve avaliar cuidadosamente a pertinência de manter o equipamento ativo para preservar informação transitória, como dados em memória Random Access Memory (RAM), ligações de rede ativas ou aplicações em execução. Contudo, essa decisão implica riscos elevados, nomeadamente a possibilidade de acessos remotos não autorizados ou de ativação de mecanismos de autodestruição de dados. A escolha entre desligar ou manter o dispositivo em funcionamento deve ser documentada de forma pormenorizada, incluindo a fundamentação técnica e jurídica que sustentou a decisão.

No caso de equipamentos em suspensão, a situação apresenta complexidade adicional. Ao retomar a atividade, o dispositivo pode executar automaticamente processos de atualização, sincronização com serviços em nuvem ou encriptação, podendo levar à perda

irreversível de informação relevante. Por essa razão, a decisão sobre como proceder deve ser tomada apenas por profissionais qualificados e com base em protocolos previamente estabelecidos.

Outro elemento crítico da fase de apreensão é a documentação em tempo real de todas as ações realizadas. Cada manipulação de um dispositivo deve ser registada, indicando o agente responsável, a hora exata da intervenção e os meios utilizados. Este registo contínuo alimenta a cadeia de custódia, assegurando que a evidência se mantém juridicamente válida e que qualquer questionamento futuro sobre a sua integridade pode ser respondido de forma objetiva e fundamentada.

A execução de uma busca e apreensão em contexto digital deve ainda contemplar a recolha de informação complementar, como a identificação de redes *Wi-Fi* disponíveis no local, ligações *Bluetooth* ativas, cabos conectados e periféricos em uso. Estes elementos, por vezes negligenciados, podem fornecer dados valiosos sobre a utilização dos dispositivos e sobre as conexões estabelecidas entre diferentes equipamentos ou utilizadores.

Fase 3: Preservação

A fase de preservação envolve a criação de cópias forenses completas, recorrendo a imagens bit a bit da memória, acompanhadas de funções de verificação de integridade, como resumos criptográficos[9]. Esta prática permite comprovar que a cópia realizada corresponde fielmente ao original, preservando-o para futuras análises e garantindo a sua aceitação em tribunal.

Para dispositivos móveis, é recomendada a sua imediata colocação em modo de voo, dentro de sacos de *Faraday*, e a extração separada de cartões SIM e cartões de memória, que devem ser analisados de forma independente e documentada. Os cartões SIM contêm dados cruciais como o IMSI, o ICCID e códigos de acesso, enquanto os cartões de memória podem armazenar cópias de fotografias, ficheiros multimédia ou dados de aplicações que não se encontram no dispositivo principal.

O guia dedica uma atenção especial aos dispositivos móveis, reconhecendo que são atualmente centrais na vida quotidiana dos utilizadores e, por conseguinte, fontes de prova particularmente relevantes. Recomenda que se documentem todas as ligações de rede conhecidas, como *Wi-Fi* e *Bluetooth*, que podem fornecer informações sobre os locais frequentados pelo utilizador ou contactos estabelecidos com outros dispositivos. Além disso, alerta para o facto de muitos *smartphones* estarem sincronizados com serviços em nuvem, tais como o *Google Drive* ou a *iCloud*, pelo que a preservação e análise da prova digital não se podem limitar ao equipamento físico, exigindo frequentemente pedidos legais complementares a fornecedores de serviços para acesso a dados armazenados remotamente.

[9]Exemplo: algoritmo SHA-256

Outros Aspetos

As directrizes da INTERPOL têm uma importância acrescida na medida em que criam uma linguagem comum e uma metodologia partilhada por diferentes países, facilitando a cooperação internacional entre polícias, aumentando as probabilidades de que a prova digital seja aceite em tribunal em processos transnacionais. Contudo, a sua aplicação não é obrigatória, devendo ser sempre enquadrada na realidade legal de cada jurisdição. Por essa razão, este documento não substitui normas técnicas nacionais, como as do NIST nos Estados Unidos ou as recomendações da European Union Agency for Cybersecurity (ENISA) na União Europeia, mas funciona como um referencial complementar, particularmente útil em contextos de investigação que envolvam vários países.

Em suma, as directrizes da INTERPOL representam um esforço significativo de harmonização internacional na área da forense digital, assegurando que os primeiros intervenientes em operações de busca e apreensão de dispositivos digitais possam atuar com procedimentos padronizados, reduzindo erros e aumentando a robustez da prova recolhida. No caso específico dos dispositivos móveis, estes princípios revelam-se particularmente relevantes, dada a sua importância crescente como fontes de evidência digital.

2.3.3 Normas ISO

A norma ISO/IEC 27037:2012, elaborada conjuntamente pela ISO e pela IEC, foca-se na gestão de evidência digital. Publicada em 2012, surge no contexto do crescimento exponencial das tecnologias de informação e comunicação e da consequente proliferação de incidentes em que dados digitais assumem valor probatório. O seu propósito é estabelecer linhas orientadoras para a identificação, a recolha, a aquisição e a preservação de evidência digital, assegurando que esta mantém a integridade, a autenticidade e a fiabilidade necessárias à sua admissibilidade em processos judiciais ou disciplinares.

O âmbito de aplicação da norma é vasto, contemplando uma multiplicidade de dispositivos e suportes digitais, que vão desde computadores pessoais, discos rígidos, dispositivos móveis e cartões de memória, até sistemas de navegação, câmaras digitais (incluindo Closed-Circuit Television (CCTV)) e infraestruturas de rede. A sua orientação é dirigida aos que atuam como primeiros intervenientes, aqui chamados de Digital Evidence First Responders (DEFR), e aos peritos, aqui chamados de Digital Evidence Specialists (DES). Ambos devem garantir que as evidências digitais sejam manuseadas de forma sistemática, imparcial e de acordo com a legislação da jurisdição em causa.

A norma estabelece que a evidência digital deve ser sempre tratada à luz de três princípios gerais: relevância, integridade e suficiência:

- Relevância - a sua capacidade para contribuir de forma significativa para provar ou

refutar factos em investigação.

- Integridade - assegurando que os dados correspondem efetivamente ao que se pretende demonstrar, o que exige a utilização de métodos de validação, nomeadamente a aplicação de funções de verificação (*hashes*) como o Message Digest 5 (MD5) ou o Secure Hash Algorithm (SHA).

- Suficiência - necessidade de recolher dados em quantidade e qualidade adequadas para que a análise subsequente seja completa e robusta.

Estes princípios são ainda reforçados por exigências de auditabilidade, repetibilidade e reprodutibilidade, as quais asseguram que os procedimentos adotados podem ser replicados por outros peritos e avaliados de forma independente, promovendo a transparência e a credibilidade do processo. Por fim, a norma enfatiza a necessidade de justificação das decisões tomadas, impondo que cada ação ou método aplicado seja fundamentado e passível de defesa perante instâncias judiciais ou disciplinares.

A norma considera quatro fases: identificação, recolha, aquisição e preservação.

Fase 1: Identificação

A fase de identificação envolve a procura, reconhecimento e documentação de dispositivos ou suportes que possam conter evidência digital, considerando tanto dados voláteis, como a informação presente na memória RAM ou em processos ativos, quanto dados não voláteis, armazenados em discos rígidos ou outros suportes persistentes.

Fase 2: Recolha

A recolha corresponde à remoção e ao transporte dos dispositivos para ambientes controlados, devendo ser executada de forma a preservar o estado original dos sistemas e a garantir que informação complementar relevante, como notas manuscritas com palavras-passe ou periféricos associados, não seja descurada.

Fase 3: Aquisição

A aquisição consiste na criação de cópias forenses da informação, preferencialmente através de imagens bit a bit dos suportes, devidamente validadas por funções de verificação. Esta fase requer a documentação detalhada das ferramentas utilizadas, das versões de software aplicadas, das condições técnicas do processo e de quaisquer limitações ou alterações inevitáveis, como a ocorrência de sectores defeituosos ou a impossibilidade de desligar sistemas críticos.

Fase 4: Preservação

A preservação destina-se a salvaguardar a integridade da evidência recolhida, prevenindo a sua alteração, degradação ou destruição, o que exige não apenas o armazenamento seguro em instalações adequadas, mas também a utilização de embalagens antiestáticas, etiquetas invioláveis e condições ambientais controladas relativamente à temperatura, à humidade, aos campos magnéticos e à exposição à luz.

Outros Aspectos

A norma sublinha a importância da cadeia de custódia, aqui entendida como o registo cronológico de todos os movimentos e acessos à evidência desde a sua recolha até ao final do seu ciclo de vida.

Em síntese, o ISO/IEC 27037:2012 oferece um enquadramento metodológico robusto para a gestão de evidências digitais. A sua aplicação prática permite uniformizar procedimentos a nível internacional, facilitando a cooperação transfronteiriça em matéria de cibercrime, ao mesmo tempo que reforça a credibilidade e a admissibilidade da prova digital em contextos judiciais e disciplinares. A norma não substitui a legislação nacional, mas complementa-a, funcionando como um guia de boas práticas que fortalece a confiança no processo de investigação digital e no valor da evidência recolhida.

As normas também influenciam a formação de profissionais, estabelecendo requisitos de competência e descrevendo papéis específicos na investigação digital. Isto contribui para padronizar funções como a do primeiro respondente forense, do especialista em aquisição, do analista de evidência e do responsável pela validação de métodos.

2.4 Análise Comparativa

A análise comparativa entre a ISO/IEC 27037:2012, o guia da INTERPOL e a SP 800-101 Rev.1 da NIST, evidencia variações na forma como cada procedimento estrutura o processo de análise forense digital, mas também revela pontos de convergência que reforçam a sua complementaridade. A Fig. 2.7 ilustra, através de um diagrama, a comparação entre os conjuntos de fases definidos nos três referenciais analisados.

A NIST SP 800-101 Rev.1 [50] adota um ciclo próximo do modelo clássico da ciência forense, estruturado em quatro fases: apreensão, aquisição, análise e reporte. Esta norma é a única que considera as fases de análise e reporte, as mais importantes do ponto de vista dos Tribunais, pois são as que produzem os relatórios periciais a serem analisados em sede de audiência.

O Guia da INTERPOL [52] segue uma lógica prática e operacional para agentes de forças

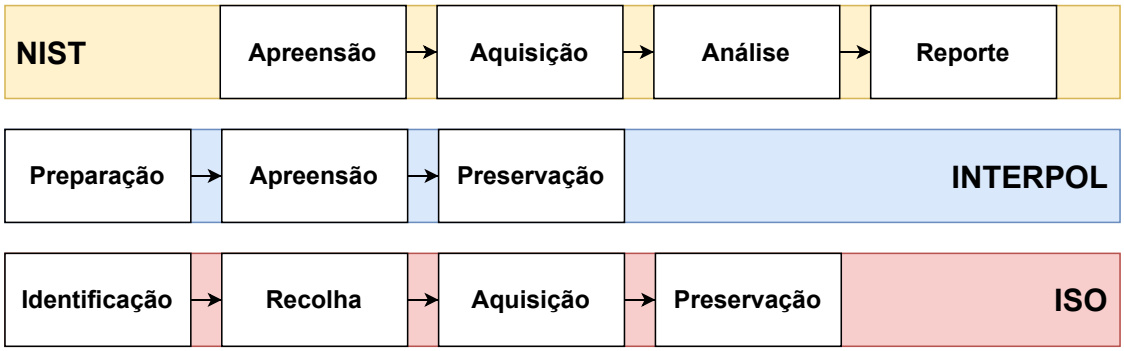


Figura 2.7: Fases NIST, INTERPOL e ISO

policiais, organizada em três fases: preparação, apreensão e preservação. Não estão previstas fases como análise e reporte, focando-se mais nos aspetos de preparação da apreensão dos dispositivos eletrónicos, da sua apreensão e da sua preservação (manutenção da cadeia de custódia).

A ISO/IEC 27037:2012 [53], de forma semelhante ao guião da INTERPOL, adota quatro fases, começando na identificação, passando para a recolha, aquisição e preservação. Esta também não inclui as fases de análise e reporte propostas pela NIST.

Contudo, apesar de existirem diferenças de âmbito, detalhe técnico e público-alvo, as três normas partilham um tronco comum de princípios que sustentam a prática da análise forense digital. Todos atribuem prioridade absoluta à integridade da prova digital, reconhecendo que qualquer alteração introduzida durante o processo pode comprometer a sua admissibilidade em tribunal. De igual modo, convergem na exigência de uma cadeia de custódia rigorosa, que documente de forma clara e contínua todas as intervenções realizadas sobre os dispositivos e dados. Outra dimensão partilhada é a ênfase na documentação exaustiva de procedimentos: todas as ações, desde a apreensão inicial até à análise laboratorial ou ao reporte, devem ser registadas em detalhe, de forma a assegurar transparência e reprodutibilidade. Também se verifica consenso quanto à necessidade de que os profissionais envolvidos possuam competência técnica adequada. Finalmente, todas as normas defendem que o processo deve respeitar a legislação em vigor na jurisdição.

2.5 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 dispositivos portáteis com funcionalidades de comunicação e processamento [43]. A evolução constante destes equipamentos, o aumento das suas capacidades e a integração com serviços em nuvem têm introduzido complexidade crescente

na recolha e preservação de evidências digitais [54].

Os sistemas operativos móveis dominantes, Android e iOS, apresentam arquiteturas distintas, mecanismos de segurança próprios e usam formatos de armazenamento de dados diferentes. Esta diversidade obriga à seleção criteriosa de métodos de aquisição, adaptados ao tipo de dispositivo, à versão do sistema operativo e às configurações de segurança presentes [55]. Além destes dois sistemas, outros equipamentos como *feature phones*, dispositivos IoT portáteis e terminais especializados (por exemplo, terminais de pagamento móveis) podem ter de ser alvo de análise forense.

No caso de dispositivos Android, o arranque (*boot*) decorre em várias fases, desde o *Boot Read-Only Memory (ROM)* ao carregamento do kernel e dos serviços de sistema. O acesso aos dados pode ser obtido através de aquisição lógica, que extrai apenas dados acessíveis pelo sistema operativo, ou física, que consiste na cópia bit a bit da memória interna [54]. A aquisição física é preferível quando se pretende recuperar dados apagados ou aceder a partições ocultas, mas pode exigir técnicas avançadas (ver Secção 2.3.1). Ferramentas forenses comerciais, como *Cellebrite UFED, XRY ou Oxygen Forensic Detective*, disponibilizam suporte para centenas de modelos, com métodos de desbloqueio, extração e descodificação de dados.

O sistema iPhone Operating System (iOS), presente em dispositivos da Apple, incorpora um processo de arranque seguro (*secure boot chain*) que valida criptograficamente cada etapa, desde o *Boot ROM* até ao sistema operativo. A extração de dados pode ser realizada através de *backups* encriptados no *iTunes*, acesso ao *iCloud* ou, em contexto forense, utilizando ferramentas capazes de explorar vulnerabilidades para acesso ao sistema de ficheiros [43]. O modo Device Firmware Update (DFU) pode permitir alterações no processo de arranque para fins de extração, embora sujeito a limitações impostas por mecanismos como a encriptação integral do suporte de armazenamento interno do equipamento.

Os dados de interesse forense em dispositivos móveis incluem registos de chamadas, mensagens SMS e MMS, mensagens de aplicações (como por exemplo, *WhatsApp, Signal, Telegram*), registos de localização GPS, histórico de navegação, ficheiros multimédia, credenciais, dados de aplicações e artefactos de sistema [55]. Bases de dados internas, como SQLite[10], armazenam grande parte desta informação e podem conter dados apagados que permanecem acessíveis até serem sobrescritos. A análise destes registos requer ferramentas capazes de interpretar estruturas de dados específicas de cada aplicação e versão de sistema.

A sincronização com serviços em nuvem introduz fontes adicionais de dados, mas também limitações jurídicas e técnicas. A obtenção de dados em nuvem pode exigir pedidos de co-

[10] `https://sqlite.org/`

operação internacional ou acesso autorizado pelo utilizador. Serviços como *Google Drive, iCloud ou OneDrive* podem conter cópias de mensagens, fotografias e outros ficheiros não presentes localmente no dispositivo [54].

A encriptação é um desafio central. Em dispositivos Android recentes, a encriptação é muitas vezes ativada por padrão, exigindo a chave do utilizador para acesso aos dados. Em dispositivos Apple, no iOS, a encriptação de disco e a proteção de dados (Data Protection API) associam chaves criptográficas ao hardware e ao código de desbloqueio, dificultando o acesso forense. Nestes casos, a análise pode limitar-se a dados disponíveis em backups ou a informações em memória volátil, se recolhidas antes do desligar do dispositivo [43].

Os dispositivos móveis estão também sujeitos a técnicas de anti-forense, como aplicações que destroem dados sensíveis, utilização de áreas seguras (*secure containers*) e sistemas operativos modificados (*custom ROMs*). A deteção destas alterações requer análise da integridade do sistema, verificação de *hashes* e comparação com imagens de referência [55].

No contexto de Internet das Coisas, ou IoT, associada a dispositivos móveis, surgem novos vetores de recolha, como *wearables* (relógios inteligentes, pulseiras de *fitness*), veículos conectados, equipamentos médicos e sistemas domésticos inteligentes. Estes dispositivos podem armazenar registos de atividade, geolocalização e interações do utilizador. A sua análise forense requer conhecimento dos protocolos e formatos de dados específicos, muitas vezes proprietários, e métodos de extração adaptados [54].

A volatilidade dos dados e a rapidez de atualização tecnológica obrigam a constante atualização das ferramentas e técnicas utilizadas. A formação contínua dos peritos e a integração de procedimentos normalizados são essenciais para garantir consistência e fiabilidade dos resultados [53].

Em suma, a análise forense a dispositivos móveis implica a aplicação de métodos técnicos adequados a cada plataforma, respeitando princípios de preservação e documentação da prova.

Esta análise apresenta diversos desafios técnicos e éticos relacionados com a recolha, tratamento, preservação e apresentação de dados digitais. Estes desafios decorrem da natureza intrusiva das técnicas utilizadas, do volume e da diversidade dos dados recolhidos e da possibilidade de aceder a informação pessoal de elevada sensibilidade [43]. A crescente complexidade dos dispositivos e a sua integração em redes e serviços remotos agravam as questões associadas à privacidade, proporcionalidade e legalidade das operações [54].

Capítulo 3

Procedimento para a Análise Forense Digital

Este capítulo descreve o procedimento para a análise forense digital proposto, elaborado com base na análise de normas e diretrizes internacionais, nomeadamente a NIST SP 800-101, as recomendações da INTERPOL e as normas ISO/IEC 27037, articuladas com o enquadramento jurídico português, bem assim como a metodologia utilizada na sua elaboração.

3.1 Metodologia

A metodologia adotada consistiu, numa primeira fase, na identificação da legislação aplicável à análise forense digital no enquadramento jurídico nacional e europeu. Após análise, constatou-se a inexistência da definição de um procedimento para o efeito, tanto na legislação nacional como europeia.

Alargando-se o espectro de regulamentação a analisar, passou-se de seguida à análise de orientações, diretrizes e normas promovidas por entidades de renome internacional que promovam a normalização de procedimentos de investigação digital forense. Aqui, surgiram vários documentos mais concretos e com recomendações sobre a forma de atuação dos agentes judiciais/policiais em situações de análise forense digital (ver Capítulo 2), designadamente a NIST SP 800-101, as orientações da INTERPOL e a norma ISO/IEC 27037.

A análise comparativa destas normas (ver Secção 2.4) permitiu constatar que mesmo estas três normas, mais dirigidas para o procedimento de análise forense digital a dispositivos móveis, tinham objetivos diferentes, cobrindo diferentes partes do procedimento. Esta constatação levou à elaboração e proposta do procedimento de análise forense digital

proposto na secção seguinte.

3.2 Procedimento Proposto

A definição de um procedimento estruturado e metodologicamente consistente é importante para uniformizar a atuação dos vários intervenientes da análise forense digital. Sendo certo que, em Portugal, quer agentes do Ministério Público, quer agentes da Polícia Judiciária, serão os atores mais prováveis em processos de investigação digital criminal, outros poderão surgir. Em particular, peritos contratados por sociedades de advogados, empresas ou entidades lesadas, ou até mesmo peritos atuando no âmbito de protocolos com a Procuradoria Geral da República, poderão liderar atividades inseridas num procedimento de análise forense. Assim, a definição e documentação de um procedimento de análise forense esperam-se socialmente útil.

O procedimento aqui proposto resulta da integração de três referências de reconhecida autoridade: a abrangência metodológica do NIST, a robustez normativa da ISO/IEC 27037:2012 e as boas práticas internacionais promovidas pela INTERPOL. A Figura 3.1 relaciona o procedimento agora proposto com as fases constantes das normas previamente descritas (ver Secção 2.3). Analisando a figura, constata-se que apenas a publicação do NIST e o procedimento aqui proposto consideram as fases de análise e de reporte. Estas fases, melhor descritas à frente, são de extrema importância. Na fase de análise é onde se avaliam as evidências e se formulam hipóteses sobre o que aconteceu. Na fase de reporte, elaboram-se os relatórios periciais que seguirão para análise por magistrados e pelo tribunal. As fases de apreensão e de aquisição são comuns a todas as propostas, sendo que algumas dão mais relevo aos aspetos de preparação da atividade de apreensão do dispositivo móvel (INTERPOL), outras à identificação dos dispositivos apreendidos (ISO).

O diagrama apresentado na Fig. 3.2 organiza, de forma sequencial, as atividades de cada fase, garantindo rastreabilidade, replicabilidade e rigor técnico. Este procedimento estrutura-se em quatro fases: Apreensão, Aquisição, Análise e Reporte.

3.2.1 Fase 1: Apreensão

A primeira fase do processo corresponde à apreensão do dispositivo, etapa inicial em que o dispositivo é retirado do seu contexto original e colocado sob custódia da autoridade investigadora. De acordo com a ISO/IEC 27037, é indispensável proceder à correta identificação do equipamento, registando elementos como o modelo, o número de série e, no caso de dispositivos móveis, o código International Mobile Equipment Identity (IMEI). Estes identificadores funcionam como referências únicas, assegurando a associação inequívoca

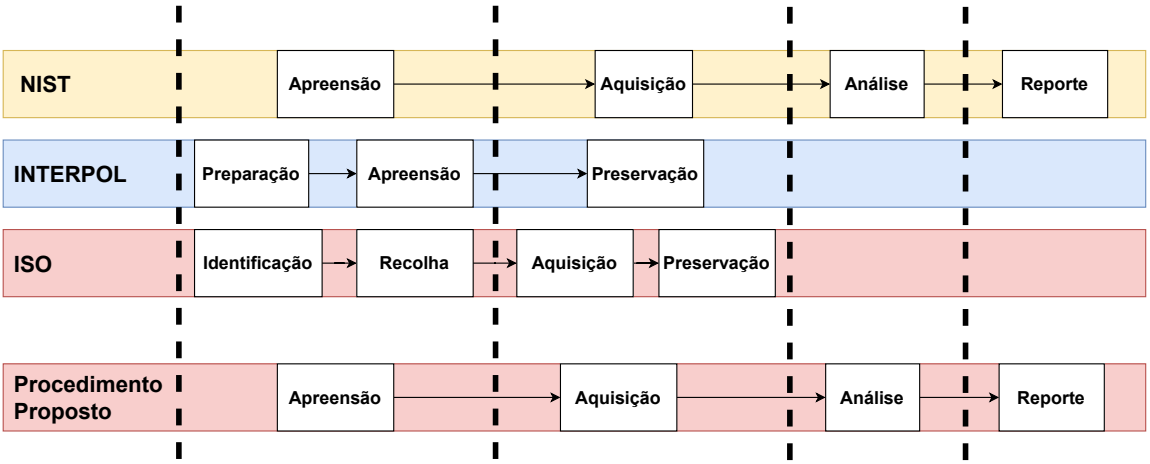


Figura 3.1: Comparação do procedimento proposto com as demais normas.

entre o artefacto e o caso em análise. Paralelamente, e em conformidade com as orientações da INTERPOL, torna-se essencial isolar o dispositivo de qualquer rede de comunicação, com o objetivo de prevenir manipulações remotas que possam comprometer a integridade dos dados. Este isolamento é geralmente realizado através da utilização de bolsas de *Faraday* ou pela ativação do modo avião.

Nesta mesma fase, o investigador deve ainda documentar o estado do dispositivo, registando se este se encontra ligado ou desligado e se apresenta danos físicos, sendo recomendável a realização de registos fotográficos que reforcem a credibilidade da cadeia probatória. A apreensão deve culminar com o registo formal na cadeia de custódia, mecanismo processual que garante a rastreabilidade da prova desde a sua recolha até à eventual apresentação em tribunal.

A condição operacional do equipamento define os procedimentos subsequentes. Caso o dispositivo se encontre ligado, a ISO/IEC 27037 recomenda que não seja desligado, uma vez que tal ação pode desencadear bloqueios ou encriptação automática, inviabilizando o acesso à informação. Nestas situações, em conformidade com a NIST, deve ser efetuado o registo detalhado das informações visíveis no ecrã, preferencialmente através de notas complementadas com registos fotográficos. Se, por outro lado, o dispositivo se encontrar desligado, este deve permanecer nessa condição, dado que uma inicialização pode modificar o sistema de ficheiros ou sobrescrever dados voláteis, comprometendo a integridade da prova.

Nos casos em que o equipamento esteja bloqueado por palavra-passe ou outro mecanismo de segurança, o recurso a ferramentas forenses específicas pode permitir o desbloqueio sem comprometer a integridade da evidência. As ferramentas utilizadas, bem assim como as suas versões, devem ser registadas e, mais tarde, documentadas no relatório final.

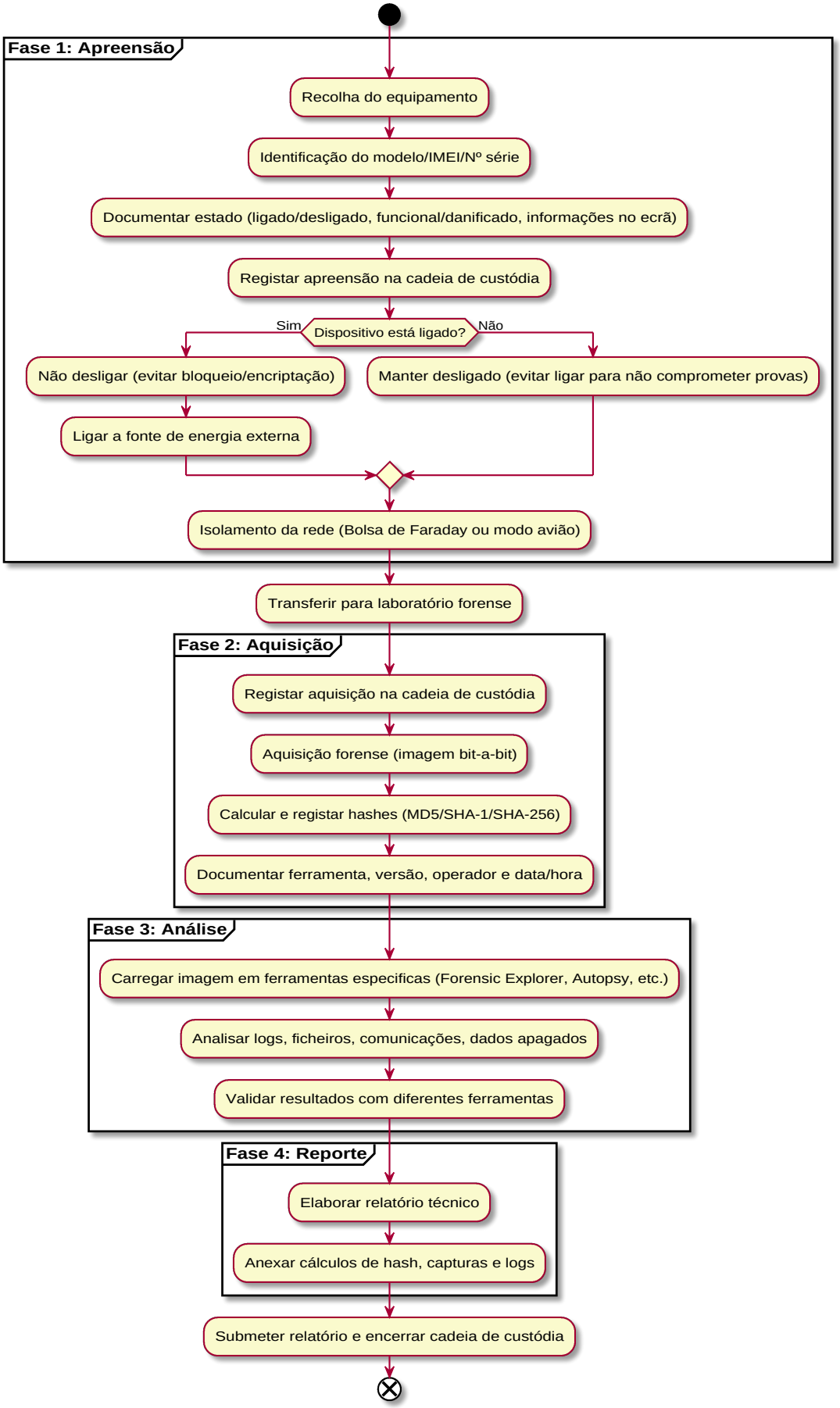


Figura 3.2: Procedimento proposto

3.2.2 Fase 2: Aquisição

A fase de aquisição inicia-se após a apreensão e transporte seguro do dispositivo para o laboratório forense. De acordo com a ISO/IEC 27037:2012, a aquisição tem como objetivo central a criação de uma imagem forense, uma cópia bit a bit da informação constante do equipamento apreendido na fase anterior. A cópia *bit a bit* é uma cópia integral e fiel de todo o conteúdo armazenado, incluindo ficheiros ativos, dados eliminados e espaço não alocado. Este método distingue-se de uma mera cópia de ficheiros por abranger todas as áreas de armazenamento de dados do equipamento. Para assegurar a autenticidade da imagem obtida, tanto a norma ISO quanto a NIST SP 800-101 Rev.1 recomendam o cálculo de resumos criptográficos (ou *hashes*) antes e após a aquisição. Estes funcionam como assinaturas digitais que permitem verificar a invariabilidade da evidência. Note-se que as funções de resumo MD5 e SHA-1 já não são consideradas seguras [56, 57], pelo que se deve optar por funções mais recentes, como a SHA-256 ou a SHA-512. A INTERPOL, por sua vez, reforça a importância de registar não apenas os valores de *hash*, mas também as ferramentas e os métodos utilizados, garantindo a verificação do processo.

3.2.3 Fase 3: Análise

Concluída a aquisição, inicia-se a fase de análise, a qual deve incidir exclusivamente sobre a cópia forense e nunca sobre o dispositivo original, conforme explicitamente referido pela ISO/IEC 27037:2012 [53]. Nesta etapa, a imagem é examinada através de ferramentas especializadas, como o *Forensic Explore*r, o *Autopsy*, o *X-Ways Forensics* ou o *Magnet AXIOM* [48, 49], capazes de identificar e interpretar elementos relevantes, incluindo logs de sistema, ficheiros apagados, registos de comunicações, histórico de navegação, dados de geolocalização e metadados associados. Oferecem elevada flexibilidade e capacidade de integração com outros sistemas, permitindo uma análise mais abrangente e eficiente da evidência digital [49, 48]

A NIST SP 800-101 Rev.1 enfatiza a importância da validação cruzada dos resultados, recomendando a utilização de múltiplas ferramentas para mitigar falhas metodológicas e reduzir a dependência de um único software. Esta prática encontra respaldo também nas orientações da INTERPOL, que destacam a necessidade de que a análise seja objetiva, reprodutível e passível de auditoria externa, garantindo a credibilidade das conclusões. A documentação minuciosa de cada ação realizada durante a análise é, portanto, um requisito para preservar a transparência e a legitimidade dos resultados.

3.2.4 Fase 4: Reporte

A fase final corresponde ao reporte, no qual os resultados da investigação são consolidados num relatório técnico-científico. De acordo com a ISO/IEC 27037:2012, este relatório

deve apresentar uma descrição detalhada dos procedimentos executados, a fundamentação técnica das escolhas metodológicas, os resultados obtidos e quaisquer limitações encontradas ao longo do processo. O relatório deve ser redigido em linguagem clara e acessível, de modo a que possa ser compreendido não apenas por peritos, mas também por autoridades judiciais e decisores legais. Devem ser anexados elementos de suporte, como os cálculos de *hash*, capturas de ecrã e registos de *logs*, de forma a corroborar a integridade e a autenticidade da evidência analisada.

Recomenda-se ainda que o relatório identifique as ferramentas utilizadas, incluindo as suas versões e certificações reconhecidas, reforçando a fiabilidade dos resultados. O processo encerra-se com a formalização da cadeia de custódia, garantindo que toda a prova recolhida e analisada pode ser apresentada em tribunal de forma admissível, tecnicamente sustentada e em conformidade com padrões internacionais de qualidade e legalidade.

Capítulo 4

Ferramenta de Suporte à Análise Forense Digital

A ferramenta digital de suporte ao procedimento de análise forense digital a dispositivos móveis consiste numa lista de verificação, *checklist* em inglês, com indicação de ajuda em cada um dos passos. A *checklist* tem o propósito de guiar e apoiar os agentes judiciais/-policiais na prossecução das investigações a dispositivos móveis.

Em particular, considerando que as Fases 2, 3 e 4 do procedimento proposto nesta dissertação têm de ser forçosamente elaboradas por peritos, não se considera útil elaborar uma *checklist* de apoio para estas fases. Caso contrário, consta-se na Fase 1, pois esta poderá ser encetada por vários intervenientes com diferentes formações de base, onde se inclui a formação em Direito.

4.1 Características

O formulário digital apresentado corresponde a uma *checklist* destinada a apoiar o procedimento de apreensão de dispositivos móveis no âmbito da análise forense digital. Estruturado em diferentes fases, o formulário permite o registo de dados essenciais, incluindo a identificação do processo e do investigador responsável, a caracterização do dispositivo apreendido (marca, modelo, número de série/IMEI, estado de conservação, estado de funcionamento), bem como a documentação fotográfica do equipamento. Complementarmente, orienta o utilizador quanto aos procedimentos a adotar quando o dispositivo se encontra ligado, designadamente a sua colocação em modo de voo ou a utilização de saco de *Faraday*. Após o preenchimento e submissão, o registo da apreensão fica concluído, prosseguindo-se com a transferência do dispositivo para o laboratório forense, onde decorrem as fases subsequentes da análise.

A ferramenta escolhida para a construção do formulário justifica-se por um conjunto de fatores relacionados com a sua adequação às necessidades operacionais e académicas do projeto. Em primeiro lugar, trata-se de uma solução compatível com dispositivos móveis e computadores, o que garante acessibilidade em diferentes contextos de utilização. Em segundo lugar, a edição do formulário é simples e intuitiva, não exigindo conhecimentos técnicos avançados de informática, o que permite a sua utilização por investigadores com diferentes perfis. Acresce ainda o facto de se tratar de uma plataforma online, o que facilita a partilha e submissão da informação em tempo real.

Do ponto de vista da segurança, a escolha encontra respaldo adicional na certificação atribuída pelo Gabinete Nacional de Segurança à infraestrutura da *Microsoft*, nomeadamente ao *Azure* e ao *Office 365*, que inclui também o *Azure OpenAI*. Esta certificação reforça a confiança na utilização da plataforma, assegurando que os dados recolhidos e processados cumprem requisitos de proteção e integridade compatíveis com as exigências da análise forense digital (Microsoft, 2024).[1]

4.2 Funcionamento

A ferramenta assume a forma de uma *checklist* de fácil utilização, online (*Microsoft Forms*). A Figura 4.1 apresenta o ecrã inicial da *checklist*. Depois do título principal em destaque, segue-se uma breve descrição que informa o utilizador que se trata de uma *checklist* de apoio a ações de apreensão de dispositivos móveis no contexto da análise forense digital. No final, encontra-se um botão com a designação "Seguinte" para avançar no formulário.

A secção apresentada na Figura 4.2 corresponde à Identificação do Processo, onde são solicitados dois elementos obrigatórios: o número do processo e a identificação do investigador (nome e/ou número). Na parte inferior, estão disponíveis dois botões de navegação: "Anterior", que permite regressar à etapa anterior, e "Seguinte", que possibilita avançar para a fase seguinte do formulário.

Nesta etapa do formulário (ver Figura 4.3) são recolhidas informações relativas ao equipamento apreendido, nomeadamente a marca e modelo do dispositivo e os números de identificação (série/IMEI), ambos de preenchimento obrigatório. É também registado o estado de conservação do dispositivo móvel, com possibilidade de escolha entre "bom estado de conservação" ou "danos visíveis". Adicionalmente, pode ser carregada uma fotografia do dispositivo através da função de anexar ficheiros, sendo permitido um máximo de quatro ficheiros, com limite de 10 MB cada e formatos compatíveis como *Word, Excel, PPT, PDF*, imagem, vídeo e áudio. Por fim, é solicitado o registo do estado do dispo-

[1] https://news.microsoft.com/pt-pt/2024/09/23/microsoft-recebe-certificacao-de-seguranca-para-azure-e-office-365-incluindo-azure-open-ai/

Figura 4.1: Checklist - ecrã inicial

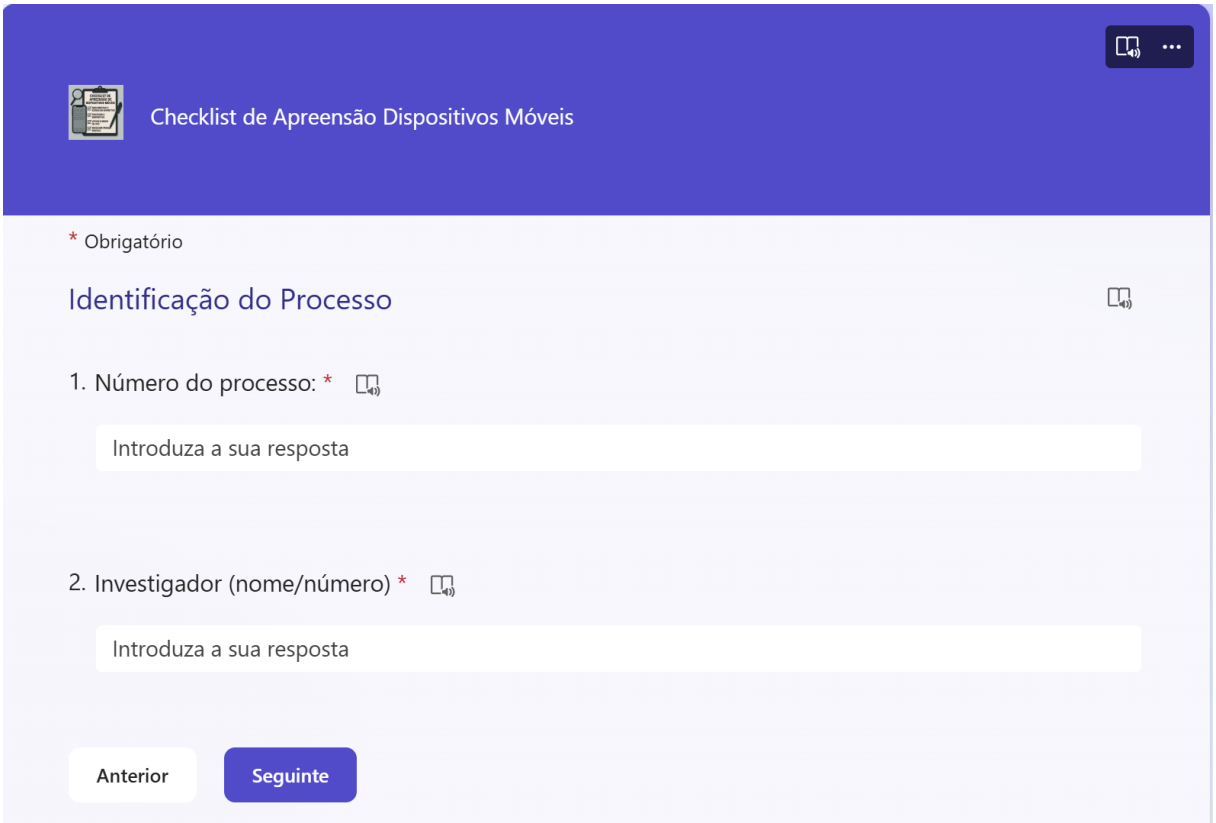


Figura 4.2: Checklist - passo 2

sitivo móvel, com as opções "ligado" ou "desligado". Aqui foi inserida uma ramificação no formulário, conforme consta no diagrama do procedimento proposto (ver Figura 3.2),

avançando para a etapa "Dispositivo ligado"(ver Figura 4.4) ou a etapa "Dispositivo desligado"(ver Figura 4.5), respetivamente. Na parte inferior da página estão disponíveis os botões de navegação: o botão "Anterior", que permite regressar à fase anterior, e o botão "Seguinte", que possibilita o avanço para a fase seguinte do formulário.

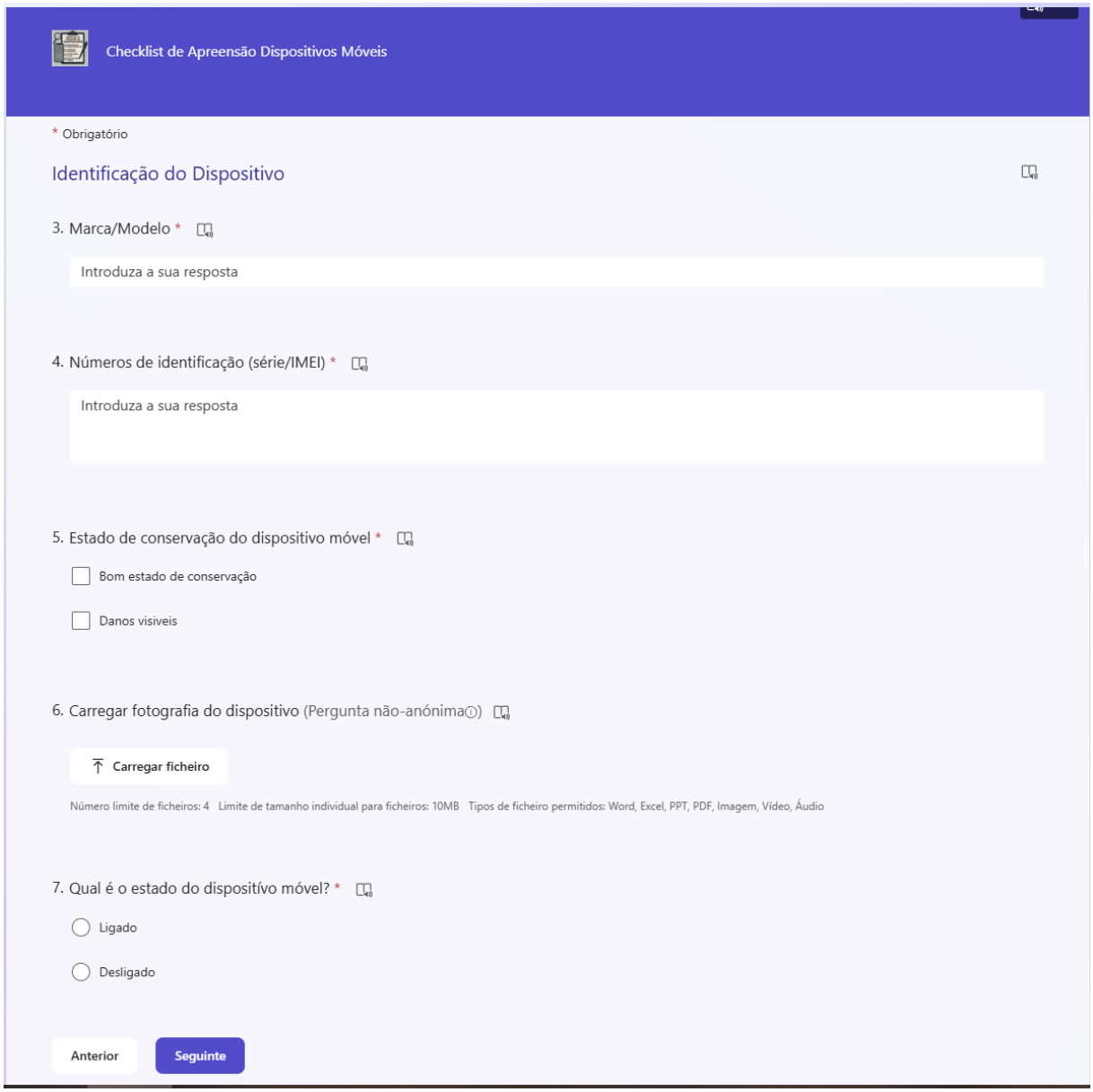


Figura 4.3: Checklist - passo 3

Nesta etapa do formulário (ver Figura 4.4) é apresentada a instrução relativa ao procedimento a adotar quando o dispositivo móvel se encontra ligado. O utilizador é orientado a não desligar o dispositivo, a ligá-lo a uma fonte de energia externa (*powerbank*), sempre que possível, e a colocá-lo em modo de voo ou, em alternativa, a guardá-lo num saco de *Faraday*. Em seguida, é solicitada a confirmação de que o dispositivo se encontra ligado e em modo de voo, mediante a seleção das opções "Sim" ou "Não". Tal como no procedimento anterior, na parte inferior da página estão disponíveis os botões de navegação: o botão

"Anterior", que permite regressar à fase anterior, e o botão "Seguinte", que possibilita o avanço para a fase seguinte do formulário.

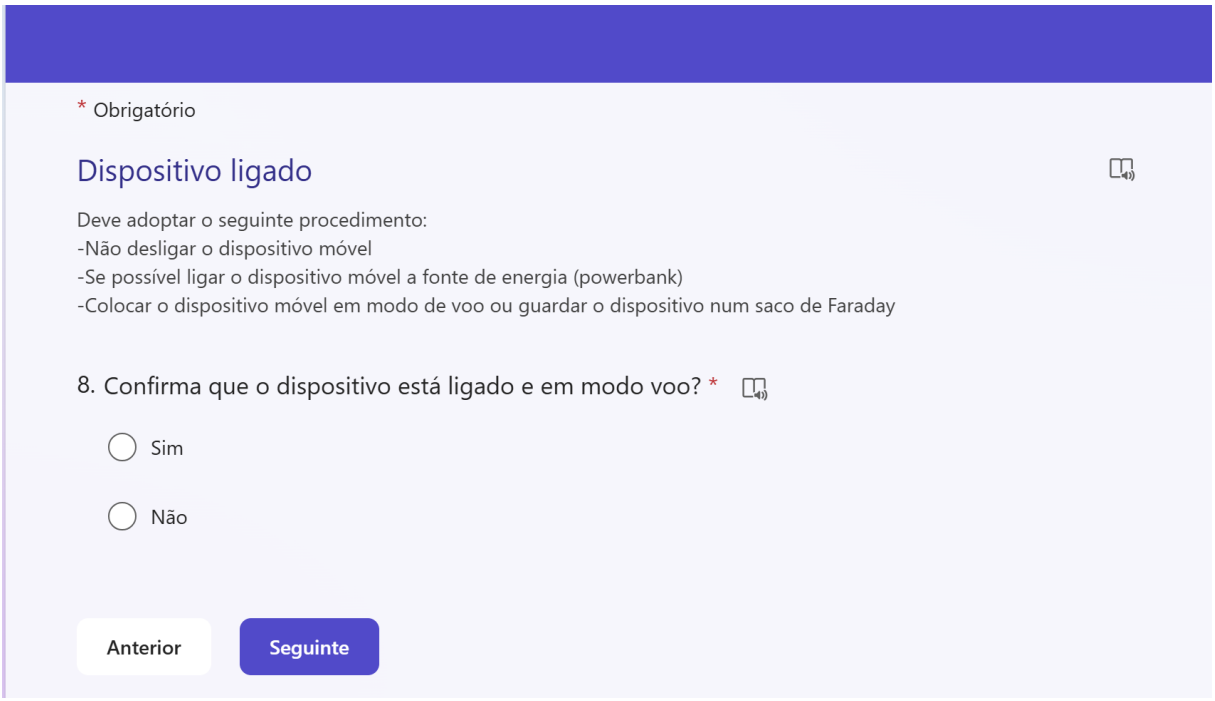


Figura 4.4: Checklist - passo 4 (ligado)

Nesta etapa do formulário (ver Figura 4.5) é apresentada a instrução relativa ao procedimento a adotar quando o dispositivo móvel se encontra desligado. O agente não deve, em nenhum momento, ligar o equipamento. Sempre que possível, o dispositivo deve ser armazenado num saco de *Faraday*, de modo a impedir comunicações externas e preservar a integridade dos dados. A confirmação explícita de que o dispositivo se encontra desligado assegura a correta documentação do estado inicial do equipamento e constitui uma medida preventiva contra a alteração ou perda de informação potencialmente relevante.

Nesta etapa do formulário (ver Figura 4.6) é apresentada a conclusão da Fase 1 – Apreensão. O sistema informa que o registo da apreensão será realizado no momento da submissão do formulário. Após este procedimento, o investigador responsável deve proceder à transferência do dispositivo móvel para o laboratório forense, de forma a dar continuidade às fases seguintes da análise forense digital. Tal como no procedimento anterior, na parte inferior da página estão disponíveis os botões de navegação: o botão "Anterior", que permite regressar à fase anterior, e o botão "Seguinte", que possibilita o avanço para a fase seguinte do formulário.

Figura 4.5: Checklist - passo 4 (desligado)

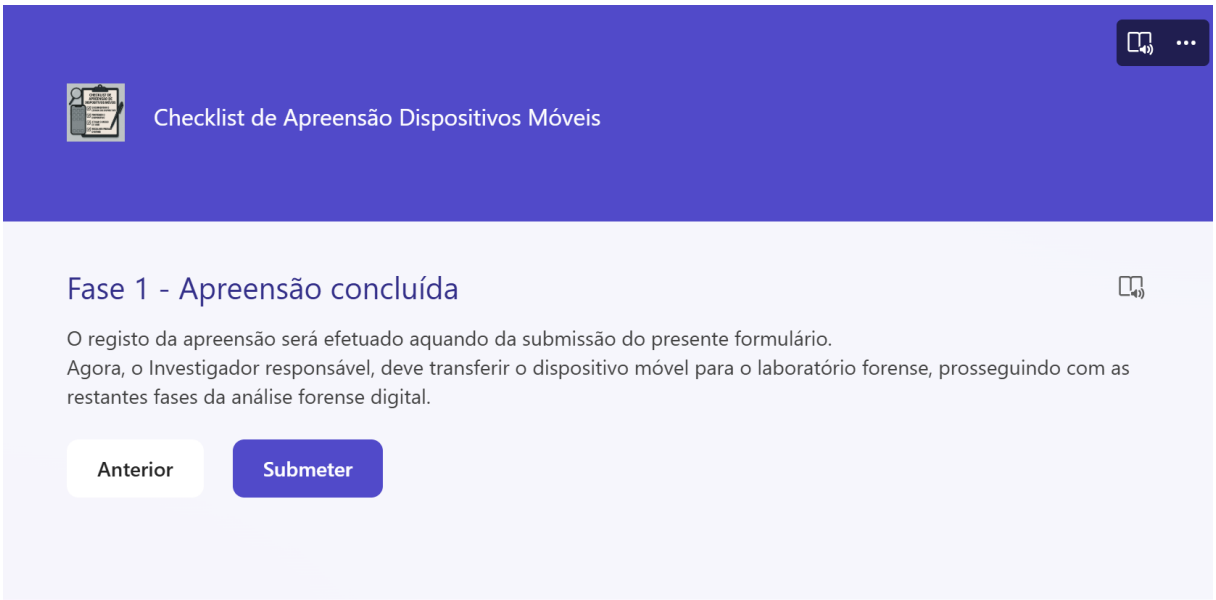


Figura 4.6: Checklist - passo 5

Capítulo 5

Conclusões

O presente trabalho teve como objetivo propor um procedimento estruturado e adaptado à realidade portuguesa para a análise forense digital de dispositivos móveis. Partindo da revisão da legislação aplicável (nacional e europeia) e de normas internacionais mais relevantes — ISO/IEC 27037, diretrizes da INTERPOL e guia NIST SP 800-101 — foi possível constatar a ausência de um modelo padronizado aplicável em Portugal, situação que pode gerar inconsistências na recolha e tratamento da prova digital.

Como resposta, foi desenvolvido um procedimento forense dividido em quatro fases — apreensão, aquisição, análise e reporte — articulado com o enquadramento legal português e europeu, em especial a Lei do Cibercrime, o Código de Processo Penal e o Regulamento Geral sobre a Proteção de Dados. Para reforçar a aplicabilidade prática do modelo, foi criada uma ferramenta digital de apoio em formato de *checklist*, que auxilia profissionais no registo sistemático e documentado das suas ações, promovendo a integridade da prova e a rastreabilidade da cadeia de custódia.

A mais-valia do trabalho reside, assim, na conjugação entre a análise teórica e jurídica e a componente prática operacionalizada através da ferramenta digital, garantindo uma aproximação entre normas internacionais e necessidades nacionais. Pretende-se com este contributo dar apoio às entidades judiciárias e de investigação criminal.

Numa perspetiva de continuidade, propõe-se o alargamento da *checklist* às fases de aquisição, análise e reporte, garantindo a cobertura completa do procedimento forense digital. Paralelamente, considera-se relevante explorar a integração da ferramenta com sistemas de gestão de prova digital e com soluções baseadas em *blockchain*, de modo a reforçar a rastreabilidade e a fiabilidade da cadeia de custódia.

Bibliografia

[1] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on Mobile Device Forensics," NIST Special Publication 800-101 Revision 1, National Institute of Standards and Technology, 2014.

[2] MSAB. Disponível em `https://www.msab.com/`, Oct 2025.

[3] N. Bodla, "Nauman Ashraf Bodla expert in Cybercrime & Digital Forensics Investigation_2025." Disponível em `https://www.naumanbodla.com/`, Apr 2025.

[4] X. Xu, *Impacts of Mobile Usage and Experience in Contemporary Society*. Hershey, PA: IGI Global, 2019.

[5] S. Kiran, J. Sanjana, and N. J. Reddy, "Mobile Phone Addiction: Symptoms, Impacts and Causes — A Review," in *International Conference on Trends in Industrial Value Engineering and Business and Social Innovation (ICTIVBSI)*, vol. 2019, pp. 81–86, Mar. 2019.

[6] L. F. C. Santos, "Dynamic Analysis Techniques for Android Applications," master's thesis, Polytechnic Institute of Leiria, School of Technology and Management, 2024.

[7] M. M. Cruz-Cunha and N. R. Mateus-Coelho, *Handbook of Research on Cyber Crime and Information Privacy*. IGI Global, 2020.

[8] D. S. Ramalho, "The use of malware as a means of obtaining evidence in criminal proceedings," *Journal of Competition and Regulation*, vol. 4, no. 16, pp. 195–243, 2013.

[9] F. Cohen, "Digital forensics," in *Information Security Management Handbook* (H. Tipton and M. Krause, eds.), pp. 1491–1506, Auerbach Publications, 6 ed., 2012.

[10] D. J. Kist, *Prova Digital no Processo Penal*. Brasil: JH Mizuno, 1 ed., 2019.

[11] Assembleia da República (Portugal), "Lei n. 109/2009, de 15 de setembro – Aprova a Lei do Cibercrime." Diário da República, Série I, n.º 180, setembro 2009. Transpõe para a ordem jurídica interna a Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques a sistemas de informação.

[12] Conselho da União Europeia, "Convenção sobre o cibercrime (Budapeste, 23 de novembro de 2001)." Jornal Oficial da União Europeia C 326/1, 2001.

[13] Conselho da União Europeia, "Diretiva 2013/40/ue relativa a ataques contra sistemas de informação." Jornal Oficial da União Europeia L 218/8, 2013.

[14] National Institute of Standards and Technology, "Guide to Integrating Forensic Techniques into Incident Response," Tech. Rep. Special Publication 800-86, U.S. Department of Commerce, 2006.

[15] "Lei n.º 32/2008, de 17 de julho." Diário da República n.º 136/2008, Série I, 17 de julho de 2008, 2008.

[16] A. D. Ramos, *A Prova Digital em Processo Penal. O Correio Eletrónico - 2ª edição.* Chiado Books, 2014.

[17] M. F. d. S. Queirós Colaço, "Buscas informáticas e subsequente apreensão de dados informáticos como métodos de obtenção de prova digital em Processo Penal," dissertação de mestrado, Universidade Católica Portuguesa, Lisboa, Portugal, Março 2023. Consultado em: 9 de agosto de 2025.

[18] National Institute of Justice, "Electronic crime scene investigation: A guide for first responders," tech. rep., U.S. Department of Justice, 2008.

[19] P. D. Venâncio, *Lei do Cibercrime – Anotada e Comentada (atualizada).* Editora D'Ideias, 2023.

[20] P. D. Venâncio, "Regime geral dos atos eletrónicos – um regime esquecido," *Revista Electrónica de Direito*, Outubro 2020.

[21] A. J. Gilliland, "Setting the Stage," in *Introduction to Metadata* (M. baca, ed.), Getty Research Institute, 2016. Consultado em: 9 de agosto de 2025.

[22] C. of Europe, "Convention on cybercrime (ets no. 185)." Treaty document, Council of Europe, 2001. Budapeste, 23 de novembro de 2001.

[23] P. E. e Conselho da União Europeia, "Regulamento (ue) n.º 679/2016, de 27 de abril — regulamento geral sobre a proteção de dados (rgpd)." Diário Oficial da União Europeia, 2016. Versão consolidada.

[24] Diário da República, "Código Penal Português, com as alterações até 2023." Disponível em `https://dre.pt/legislacao-consolidada/-/lc/115629080/202308011938/73475592/diploma`, 2023.

[25] N. A. Rakha, "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations," *Mexican Law Review*, pp. 23–54, 2024.

[26] União Europeia, "Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra sistemas de informação," 2005.

[27] Conselho da Europa, "Convention on Cybercrime (Budapest, 23 November 2001)." Disponível em `https://rm.coe.int/16802fa428`, 2001. European Treaty Series No. 185; texto disponível em formato PDF no sítio do Conselho da Europa.

[28] "Lei n.º 79/2021, de 24 de novembro (alteração à Lei do Cibercrime)," 2021.

[29] Tribunal Constitucional, "Acórdão n.º 687/2021," 2021. Diário da República, 1.ª série, n.º 185.

[30] "Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados." Disponível em `https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679`, 2016. Acedido em: 2025-08-10.

[31] "Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679." Disponível em `https://dre.pt/dre/detalhe/lei/58-2019-123815466`, 2019. Acedido em: 2025-08-10.

[32] "Lei n.º 59/2019, de 8 de agosto, que transpõe a Diretiva (UE) 2016/680, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais." Disponível em `https://dre.pt/dre/detalhe/lei/59-2019-123815467`, 2019. Acedido em: 2025-08-10.

[33] "Lei n. 43/2004, de 18 de agosto: Lei de organização e funcionamento da comissão nacional de protecção de dados," 2004. Diário da República n.º 194/2004, Série I-A, pp. 5251-5257.

[34] "Lei n.º 43/2004, de 18 de agosto, que regula a organização e funcionamento da Comissão Nacional de Proteção de Dados." Disponível em `https://dre.pt/dre/detalhe/lei/43-2004-256063`, 2004. Acedido em: 2025-08-10.

[35] "Lei n.º 5/2010, de 24 de fevereiro, que procede à primeira alteração à Lei n.º 43/2004." Disponível em `https://dre.pt/dre/detalhe/lei/5-2010-671321`, 2010. Acedido em: 2025-08-10.

[36] "Lei n.º 3/2019, de 9 de janeiro, que procede à segunda alteração à Lei n.º 43/2004." Disponível em `https://dre.pt/dre/detalhe/lei/3-2019-117706979`, 2019. Acedido em: 2025-08-10.

[37] P. G. S. Osório, "A proteção de dados na internet: enfoque no RGPD," Master's thesis, Universidade de Lisboa, Faculdade de Letras, 2023.

[38] T. Limberger, G. d. S. Santanna, and D. B. d. S. Giannakos, "Internet das coisas (IoT) e os direitos à privacidade e à proteção de dados do cidadão: uma necessária aproximação," *Revista Brasileira de Políticas Públicas*, 2023. Acedido em: 2025-08-10.

[39] "Manual de Implementação do RGPD." Funções do Encarregado de Proteção de Dados e fases de implementação.

[40] "Decreto-Lei n.º 400/82, de 23 de setembro, Código Penal." Disponível em `https://dre.pt/dre/detalhe/decreto-lei/400-1982-345109`, 1982. Acedido em: 2025-08-10.

[41] "Resolução da Assembleia da República n.º 88/2009, Aprova a Convenção sobre o Cibercrime." Disponível em `https://dre.pt/dre/detalhe/resolucao-da-assembleia-da-republica/88-2009-500917`, 2009. Acedido em: 2025-08-10.

[42] "Decreto-Lei n.º 78/87, de 17 de fevereiro, Código de Processo Penal." Disponível em `https://dre.pt/dre/detalhe/decreto-lei/78-1987-457346`, 1987. Acedido em: 2025-08-10.

[43] E. Casey, *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press, 2011.

[44] J. R. M. Branco, *Prova Digital os Meios de Obtenção de Prova Digital e a Restrição de Direitos do Arguido*. Universidade Coimbra, 2021.

[45] J. d. Figueiredo Dias, *Direito Processual Penal*. Coimbra Editora, 2004.

[46] M. A. V. Veríssimo, "Prova Pericial e Processo Penal Português: Questões Fundamentais," dissertação de mestrado, Universidade Católica Portuguesa, Faculdade de Direito, 2023. Disponível online via repositório institucional UCP.

[47] Joint Test Action Group, "IEEE Standard for Test Access Port and Boundary-Scan Architecture," *IEEE Std 1149.1-2013 (Revision of IEEE Std 1149.1-2001)*, pp. 1–444, 2013.

[48] T. Sutikno, "Mobile forensics tools and techniques for digital crime investigation: a comprehensive review," *International Journal of Informatics and Communication Technology (IJ-ICT)*, 2024. Open access under CC BY-SA 4.0 license.

[49] P. H. G. C. Ferreira, "Autopsy – Enhanced Distributed Forensic Analysis," relatório de estágio de mestrado em cibersegurança e informática forense, Politécnico de Leiria,

Escola Superior de Tecnologia e Gestão, Leiria, Portugal, July 2020. Orientação de Marisa da Silva Maximiano e supervisão de João Mota.

[50] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on Mobile Device Forensics," Tech. Rep. 800-101r1, National Institute of Standards and Technology (NIST), May 2014.

[51] I. I. Centre, "Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence," 2021. Práticas recomendadas para primeiros intervenientes na recolha de prova digital.

[52] "INTERPOL Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence." Disponível em `https://www.interpol.int/en/Crimes/Cybercrime/Guidelines-for-Digital-Forensics-First-Responders`, 2021.

[53] "ISO/IEC 27037:2012 – Guidelines for identification, collection, acquisition and preservation of digital evidence," 2012.

[54] A. Arnes, *Digital Forensics*. Wiley, 2018.

[55] E. Casey, *Handbook of computer crime investigation: forensic tools and technology*. Elsevier, 2001.

[56] T. Xie, F. Liu, and D. Feng, "Fast collision attack on MD5," *Cryptology ePrint Archive*, 2013.

[57] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, "The first collision for full SHA-1," in *Annual international cryptology conference*, Springer, 2017.