Áreas de armazenamento em dispositivos móveis com o sistema operativo Android e a sua relevância na análise forense digital

Storage areas on mobile devices with the android operating system and their relevance in digital forensic analysis

10.29073/j2.v9i1.1137

Recebido: 15 de março de 2026.
Aprovado: 05 de abril de 2026.
Publicado: 08 de abril de 2026.

Autor/a 1: João Sousa, ESTG-IPP, Portugal, jsampaiodesousa@gmail.com.
Autor/a 2: Marco Gomes, ESTG-IPP, Portugal, mfg@estg.ipp.pt.
Autor/a 3: Patrícia Azevedo, ESTG-IPP, Portugal, pamv@estg.ipp.pt.

Resumo

A digitalização crescente da sociedade transformou significativamente a comunicação, o trabalho e a interação social, conferindo aos dispositivos móveis, especialmente os que operam com o sistema operativo Android, um papel central na vida quotidiana. Estes equipamentos armazenam grandes volumes de dados pessoais, profissionais e sensíveis, tornando-se alvos frequentes de cibercrime e fontes privilegiadas de prova digital em investigações criminais e cíveis.

O presente artigo visa identificar e analisar as principais áreas de armazenamento em dispositivos Android relevantes para a análise forense digital. Para tal, caracteriza-se a arquitetura do sistema operativo e descrevem-se as partições mais significativas para a recolha de evidência, com destaque para /data e /sdcard. Adicionalmente, é abordado o enquadramento jurídico português aplicável à prova digital, incluindo o Código de Processo Penal, a Lei do Cibercrime e a legislação de proteção de dados, com especial ênfase nos princípios da autenticidade, integridade e cadeia de custódia.

A metodologia adotada combina revisão de literatura técnico-científica e análise normativa com aplicação prática através de um estudo de caso. Este estudo focaliza a recuperação de mensagens eliminadas do WhatsApp em contexto de violência doméstica, demonstrando a importância da perícia digital na reconstrução de factos, proteção das vítimas e responsabilização dos agressores.

Conclui-se que a análise forense em dispositivos Android apresenta elevada complexidade técnica e legal, exigindo ferramentas certificadas, procedimentos rigorosos e conhecimento especializado. A integração entre competências técnicas e enquadramento jurídico é essencial para garantir a admissibilidade, fiabilidade e robustez da prova digital, contribuindo para a eficácia da justiça e para a proteção dos direitos fundamentais na era digital.

Palavras-Chave: Análise Forense Digital; Cadeia de Custódia; Dispositivos Android; Prova Digital; Recuperação de Dados.

Abstract

The increasing digitalization of society has significantly transformed communication, work, and social interaction, making mobile devices, especially those running Android, central to daily life. These devices store large volumes of personal, professional, and sensitive data, making them frequent targets of cybercrime and privileged sources of digital evidence in criminal and civil investigations.

This article aims to identify and examine the main storage areas on Android devices relevant to digital forensic analysis. To this end, the operating system architecture is characterized, and the most significant partitions for

evidence collection are described, with emphasis on /data and /sdcard. Additionally, the Portuguese legal framework relevant to digital evidence is addressed, including the Code of Criminal Procedure, the Cybercrime Law, and data protection legislation, with special emphasis on the principles of authenticity, integrity, and chain of custody. The methodology adopted combines a review of technical and scientific literature and normative analysis with practical use through a case study.

This study centers on the recovery of deleted WhatsApp messages in the context of domestic violence, demonstrating the importance of digital forensics in reconstructing facts, protecting victims, and holding perpetrators accountable.

It concludes that forensic analysis of Android devices is highly complex and requires certified tools, rigorous procedures, and specialized knowledge. The combination of technical skills and the legal framework is essential to guarantee the admissibility, reliability, and soundness of digital evidence, helping ensure the effectiveness of justice and the protection of fundamental rights in the digital age.

Keywords: Android Devices; Android Partitions; Chain of Custody; Digital Evidence; Digital Forensic Analysis.

1. Introdução

A crescente digitalização da sociedade contemporânea tem vindo a transformar, de forma profunda, os modos de comunicação, de organização do trabalho e de interação social. Neste contexto, a Informática assume um papel estruturante, constituindo um meio essencial para a concretização de relações económicas, sociais e culturais à distância, que, de outro modo, não seriam viáveis (Venâncio, 2011). Paralelamente, a massificação dos dispositivos móveis, em particular aqueles baseados no sistema operativo Android, contribuiu para a centralização, nestes equipamentos, de volumes significativos de dados de natureza pessoal, profissional e sensível (Casey, 2011).

A ubiquidade dos dispositivos Android, aliada à diversidade e intensidade de utilização de aplicações móveis, confere-lhes uma relevância crescente no domínio da análise forense digital. Estes dispositivos constituem simultaneamente instrumentos potenciais para a prática de ilícitos e repositórios privilegiados de evidência digital, suscetível de ser utilizada em processos de natureza criminal e cível. Neste âmbito, a identificação, caracterização e correta interpretação das diferentes áreas de armazenamento assumem particular importância, na medida em que condicionam diretamente a eficácia dos procedimentos de recolha e análise de prova.

Com efeito, aplicações de comunicação instantânea, amplamente utilizadas no quotidiano, armazenam informação de elevado valor probatório. Em diversos contextos, nomeadamente em situações de violência doméstica, os dados gerados por estas aplicações, como mensagens, ficheiros multimédia ou registos de interação, podem ser deliberadamente eliminados pelos utilizadores, exigindo a aplicação de técnicas forenses especializadas para a sua recuperação e validação (Marques, 2013).

Neste enquadramento, a análise das áreas de armazenamento em dispositivos Android revela-se fundamental não apenas do ponto de vista técnico, mas também jurídico, dado o seu impacto na admissibilidade e fiabilidade da prova digital. A relevância do tema decorre, assim, da sua atualidade e da sua contribuição para a administração da justiça, a salvaguarda de direitos fundamentais e o reforço da eficácia no combate ao cibercrime.

O presente artigo tem como objetivo principal identificar e analisar as principais áreas de armazenamento em dispositivos Android com relevância para a análise forense digital. Em termos específicos, pretende-se descrever a estrutura do sistema de ficheiros Android, identificar as áreas mais relevantes para a recolha e análise de evidência digital, com particular incidência nas partições `/data` e `/sdcard`, analisar a recuperação de dados eliminados em aplicações de comunicação e discutir os principais desafios técnicos e legais associados à análise forense neste tipo de dispositivos, à luz do enquadramento normativo vigente.

A investigação desenvolvida neste trabalho assenta numa abordagem qualitativa, baseada na revisão de literatura científica e técnica relevante no domínio da análise forense digital, bem como na análise do enquadramento jurídico aplicável à prova digital e ao cibercrime. Foram consideradas diversas fontes, incluindo artigos académicos, manuais especializados, relatórios técnicos e documentação oficial, privilegiando-se contributos recentes e amplamente reconhecidos na área. Paralelamente, recorreu-se à análise de metodologias e boas práticas forenses internacionalmente aceites, incluindo a utilização de ferramentas especializadas no contexto da aquisição e análise de dados digitais, permitindo articular uma perspetiva teórica com uma dimensão aplicada.

A análise forense em dispositivos com o Sistema Operativo *Android* assume, atualmente, uma importância crítica, refletindo o papel central destes dispositivos na comunicação interpessoal, nas transações digitais e no armazenamento de informação. A sua ampla disseminação reforça a probabilidade de serem relevantes em investigações de natureza criminal e cível, funcionando frequentemente como fontes primárias de evidência digital. Neste contexto, a capacidade de extrair, preservar e analisar dados provenientes destes dispositivos revela-se determinante, nomeadamente pela possibilidade de recuperar informação eliminada, como mensagens, registos de localização ou conteúdos multimédia, e, assim, reconstruir sequências de acontecimentos e sustentar a verificação de comportamentos ilícitos.

Em particular, em casos de violência doméstica, a prova digital proveniente de aplicações de comunicação pode assumir um papel central, contribuindo para a validação das declarações das vítimas e para a consolidação da base probatória necessária à acusação e eventual condenação dos suspeitos. A análise forense digital constitui, assim, um elemento essencial na construção de decisões judiciais fundamentadas em evidência objetiva.

Todavia, a evolução do sistema operativo Android tem introduzido mecanismos avançados de segurança, como a criptografia baseada em ficheiros (*File-Based Encryption*) e funcionalidades como o *Direct Boot*, que visam proteger os dados dos utilizadores. Embora fundamentais para a salvaguarda da privacidade, estas medidas colocam desafios significativos à atividade forense, exigindo o recurso a técnicas especializadas, como a extração física de dados ou a análise de cópias de segurança, frequentemente dependentes de autorização judicial.

Do ponto de vista jurídico, a recolha e tratamento de prova digital devem respeitar princípios fundamentais, designadamente os da autenticidade, integridade e cadeia de custódia. Em Portugal, a Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), estabelece o quadro normativo aplicável, impondo requisitos rigorosos quanto à obtenção e admissibilidade da prova digital em processo judicial. A utilização de ferramentas forenses validadas contribui para assegurar o cumprimento destes requisitos e a fiabilidade dos resultados obtidos.

Em síntese, a análise das áreas de armazenamento em dispositivos *Android* constitui um domínio essencial da investigação forense digital, situando-se na interseção entre tecnologia, direito e segurança pública. Neste sentido, o presente artigo encontra-se estruturado de forma a proporcionar uma abordagem progressiva e integrada do tema. Inicialmente, procede-se ao enquadramento legal da análise forense digital em Portugal, destacando os principais normativos e princípios aplicáveis à recolha e admissibilidade da prova digital. Seguidamente, são analisadas as áreas de armazenamento em dispositivos com o sistema operativo Android, com enfoque nas estruturas relevantes para a investigação forense. Posteriormente, apresenta-se a análise de um caso prático, ilustrando a aplicação dos conceitos e técnicas abordados. Por fim, são apresentadas as conclusões, nas quais se sintetizam os principais contributos do estudo e se refletem os desafios e perspetivas futuras neste domínio.

2. Enquadramento Legal da Análise Forense Digital em Portugal

A análise forense digital, entendida como o conjunto de técnicas e procedimentos destinados à recolha, preservação, análise e apresentação de prova digital em contexto judicial, assume um papel central na investigação criminal contemporânea, em virtude da crescente digitalização das interações humanas. Em Portugal, esta atividade encontra-se enquadrada por um sistema normativo complexo, que articula o Código de Processo Penal (CPP), aprovado pelo Decreto-Lei n.º 78/87, de 17 de fevereiro, a Lei do Cibercrime (Lei n.º

109/2009, de 15 de setembro), a Lei n.º 32/2008, de 17 de julho, relativa à conservação de dados de comunicações eletrónicas, bem como o regime de proteção de dados pessoais, designadamente o Regulamento Geral de Proteção de Dados (RGPD) e a Lei n.º 58/2019, de 8 de agosto.

Este enquadramento jurídico visa assegurar a legalidade, autenticidade e integridade da prova digital, conciliando a eficácia da investigação criminal com a proteção dos direitos fundamentais dos cidadãos, como o direito à reserva da vida privada, à proteção de dados pessoais e à inviolabilidade das comunicações (Pereira, 2019). A obtenção de prova digital encontra-se, regra geral, sujeita a autorização judicial, devendo respeitar os princípios constitucionais do devido processo legal e da proporcionalidade.

No âmbito do CPP, a admissibilidade e valoração da prova digital são regidas por princípios gerais aplicáveis a todos os meios de prova. O artigo 125.º consagra o princípio da legalidade da prova, admitindo todos os meios que não sejam proibidos por lei, enquanto o artigo 126.º estabelece a nulidade das provas obtidas por meios ilícitos, nomeadamente com violação de direitos fundamentais, em consonância com o artigo 32.º, n.º 8 da Constituição da República Portuguesa. Por sua vez, o artigo 127.º consagra o princípio da livre apreciação da prova, segundo as regras da experiência e a convicção do julgador.

O CPP regula ainda diversos meios de obtenção de prova particularmente relevantes para a análise forense digital. As perícias (artigos 151.º a 163.º) assumem especial importância, permitindo a intervenção de peritos qualificados na análise de dispositivos, recuperação de dados e verificação da autenticidade de conteúdos digitais. As buscas e apreensões (artigos 174.º e seguintes) constituem instrumentos fundamentais para a recolha de dispositivos e suportes digitais, exigindo, em regra, autorização judicial e o respeito pelas garantias processuais do visado. A apreensão de dados e comunicações digitais (artigos 178.º e 179.º), bem como a interceção de comunicações (artigos 187.º e 188.º), encontram-se igualmente sujeitas a requisitos rigorosos, designadamente a existência de despacho judicial fundamentado, sobretudo em casos de maior gravidade. Acresce o artigo 189.º, que permite o acesso a sistemas informáticos ou suportes de dados mediante mandado judicial, sendo particularmente relevante no contexto da investigação digital.

A Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), que transpõe para o ordenamento jurídico português a Convenção de Budapeste sobre Cibercrime, estabelece um regime específico para a criminalidade informática e para a obtenção de prova digital. Este diploma regula, de forma detalhada, procedimentos como a conservação expedita de dados (artigo 12.º), a obtenção de dados de tráfego e localização (artigo 13.º), o acesso a sistemas informáticos (artigo 15.º), a apreensão de dados (artigo 16.º) e de comunicações eletrónicas (artigo 17.º), bem como a interceção em tempo real (artigo 18.º). Todos estes mecanismos estão sujeitos a controlo judicial e à observância de princípios como a proporcionalidade, a necessidade e a salvaguarda dos direitos fundamentais. A lei impõe ainda a obrigatoriedade de garantir a integridade da prova digital em todas as fases do processo, exigindo a documentação rigorosa das operações realizadas, incluindo a manutenção de registos e a aplicação de mecanismos técnicos que assegurem a rastreabilidade dos dados.

Complementarmente, a Lei n.º 32/2008, de 17 de julho, regula a conservação de dados gerados ou tratados no âmbito de serviços de comunicações eletrónicas, permitindo o acesso a dados de tráfego, localização e identificação, frequentemente utilizados em investigações criminais. Nos termos desta lei, os prestadores de serviços estão obrigados a conservar determinados dados por um período definido, excluindo o conteúdo das comunicações, sendo o seu acesso condicionado a autorização judicial e limitado a investigações de crimes graves. A aplicação deste regime tem, contudo, sido objeto de debate, em particular na sequência da invalidação da Diretiva 2006/24/CE pelo Tribunal de Justiça da União Europeia, no caso *Digital Rights Ireland*, o que tem conduzido a um maior escrutínio judicial na autorização de acesso a estes dados.

A análise forense digital encontra-se igualmente sujeita às normas de proteção de dados pessoais, previstas no RGPD e na Lei n.º 58/2019, de 8 de agosto. Estes diplomas impõem princípios como a proporcionalidade, a minimização de dados e a limitação das finalidades, exigindo que a recolha e tratamento de dados pessoais sejam restritos ao estritamente necessário para a investigação. Exigem ainda a adoção de medidas técnicas e

organizativas adequadas para garantir a segurança, confidencialidade e integridade dos dados, em consonância com as exigências da cadeia de custódia.

A especificidade da prova digital implica a observância de princípios próprios, que complementam os princípios gerais do processo penal. Entre estes destacam-se a autenticidade, que assegura a identificação da origem da prova; a integridade, que garante que os dados não foram alterados desde a sua recolha; e a cadeia de custódia, que consiste no registo contínuo e documentado de todas as operações realizadas sobre a evidência digital. Estes princípios são fundamentais para assegurar a admissibilidade e o valor probatório da evidência, sendo frequentemente suportados por técnicas como a utilização de funções *hash* e por ferramentas forenses certificadas (Casey, 2011; Hermeiro, 2023).

Por fim, importa referir que, em contextos transnacionais, a cooperação internacional assume particular relevância, sendo enquadrada, designadamente, pela Convenção de Budapeste sobre Cibercrime. Este instrumento jurídico facilita a preservação e obtenção de prova digital localizada no estrangeiro, através de mecanismos de assistência mútua entre Estados, contribuindo para a eficácia das investigações em cenários de criminalidade global.

Deste modo, o enquadramento legal da análise forense digital em Portugal caracteriza-se por uma abordagem integrada e exigente, que procura equilibrar a eficácia da investigação criminal com a proteção dos direitos fundamentais, assegurando a validade, fiabilidade e admissibilidade da prova digital em contexto judicial (Correia, 2014).

3. Áreas de Armazenamento em Dispositivos Android

3.1. Estado da Arte

Áreas de Armazenamento em Dispositivos Android

A análise forense de dispositivos Android tem evoluído de forma significativa desde a introdução deste sistema operativo em 2008, acompanhando o aumento da complexidade das suas estruturas internas e dos mecanismos de segurança associados. A crescente fragmentação do ecossistema Android, caracterizada pela existência de milhares de dispositivos distintos e múltiplas versões do sistema operativo em circulação, impõe desafios relevantes à investigação forense, exigindo a adoção de metodologias flexíveis e adaptáveis à diversidade tecnológica (Hoog, 2011; StatCounter, 2020). Neste contexto, a literatura destaca a necessidade de desenvolvimento contínuo de competências especializadas, particularmente em cenários de investigação criminal, onde a heterogeneidade dos dispositivos pode comprometer a uniformidade dos procedimentos (Gomes, 2018).

A evolução do sistema operativo Android introduziu mecanismos avançados de segurança que impactam diretamente a análise forense. Entre estes destacam-se a criptografia baseada em ficheiros (*File-Based Encryption* – FBE), introduzida no Android 7.0, e a funcionalidade *Direct Boot*, que reforça a proteção dos dados mesmo em fases iniciais do arranque do dispositivo. Estas medidas, embora essenciais para a proteção da privacidade dos utilizadores, aumentam substancialmente a complexidade das operações forenses, podendo exigir técnicas especializadas, como a exploração de vulnerabilidades ao nível do *bootloader* ou métodos invasivos, como o *chip-off*, sempre com o cuidado de preservar a integridade da prova digital (Afonin & Katalov, 2016).

Do ponto de vista estrutural, o sistema operativo *Android* assenta numa arquitetura modular, baseada no *kernel* Linux, responsável pela gestão de recursos de *hardware*, processos e mecanismos de segurança. A integração do *Security-Enhanced Linux* (SELinux) introduz um modelo de controlo de acesso mais rigoroso, limitando as interações entre aplicações e o sistema. Sobre esta base, a Camada de Abstração de Hardware (*Hardware Abstraction Layer* - HAL) fornece interfaces normalizadas para a comunicação com componentes físicos, como sensores e câmaras. O ambiente de execução das aplicações é assegurado pelo *Android Runtime* (ART), que substituiu a máquina virtual Dalvik, introduzindo melhorias ao nível do desempenho através de compilação antecipada (*ahead-of-time*).

A organização do sistema de ficheiros segue uma estrutura hierárquica típica dos sistemas Linux, sendo suportada por formatos como *ext4* ou *f2fs*, e sujeita a um controlo rigoroso de permissões, reforçado pelo SELinux (Casey, 2011). A introdução do "Project Treble", no Android 8.0, veio ainda acentuar a modularidade do sistema, separando componentes específicos dos fabricantes na partição, o que tem implicações diretas na análise forense, nomeadamente na identificação de alterações ao sistema e na compatibilidade de ferramentas (Android Open Source Project, 2023).

No contexto da análise forense digital, a compreensão das diferentes partições do sistema de ficheiros *Android* é fundamental para a localização e extração de evidência digital. Entre as áreas de armazenamento mais relevantes destaca-se a partição `/data`, que constitui a principal fonte de informação do utilizador, armazenando dados de aplicações, bases de dados, ficheiros de configuração e cache. É nesta partição que se encontram, por exemplo, os dados associados a aplicações de comunicação, frequentemente determinantes em investigações criminais, incluindo casos de violência doméstica (Tamma et al., 2018).

A par desta, o diretório `/sdcard`, atualmente implementado como armazenamento emulado e tipicamente montado em `/storage/emulated/0`, contém ficheiros acessíveis ao utilizador, como fotografias, vídeos e cópias de segurança de aplicações. Esta área distingue-se dos cartões *Secure Digital* (SD) físicos, embora funcionalmente desempenhe um papel semelhante no armazenamento de dados não críticos do sistema (Hoog, 2011).

Outras partições assumem igualmente relevância no contexto forense. A partição `/system` contém os ficheiros essenciais do sistema operativo e aplicações pré-instaladas, podendo a sua alteração indicar práticas como *rooting* ou modificações maliciosas (Casey, 2011). A partição `/cache` armazena dados temporários e ficheiros associados a atualizações do sistema, podendo fornecer informações úteis para a reconstrução de atividades recentes (Android Open Source Project, 2023). Já a partição `/vendor`, introduzida no âmbito do *Project Treble*, inclui componentes específicos do fabricante, sendo relevante para a análise de personalizações e potenciais vulnerabilidades. Por fim, a partição `/recovery` permite a execução de operações de manutenção e pode ser explorada em contexto forense para a realização de extrações físicas ou lógicas em modos alternativos de arranque (Tamma et al., 2018).

A análise integrada destas áreas de armazenamento permite não só a identificação e recuperação de evidência digital, mas também a compreensão do comportamento do utilizador e das interações com o dispositivo. Assim, o conhecimento aprofundado da arquitetura e das partições do sistema Android constitui um elemento essencial para a condução de investigações forenses eficazes, particularmente num contexto tecnológico em constante evolução.

De seguida na tabela 1 apresenta-se um resumo das ferramentas de extração e análise mais populares.

Tabela 1: Ferramentas de extração.

Ferramenta	Tipo de Extração	Compatibilidade
Cellebrite UFED	Física / Lógica	Android 4.4-13
Magnet AXIOM	Cloud / Backup	WhatsApp, Telegram
ADB + dd	Física	Dispositivos com root
Autopsy (+plugins)	Análise lógica	SQLite, logs do sistema
XRY	Física / Lógica	Android
FTK image	Física	Cartões de memória
SQLiteBrowser	Análise de bases de dados	BD's de aplicações móveis

Ferramentas como o Cellebrite UFED permitem extração física via *Emergency Download Mode* (EDL) em dispositivos bloqueados, enquanto o *Android Debug Bridge* (ADB) é essencial para aceder a partições via comandos como adb pull /data (Cellebrite, 2024). Em Portugal, a Polícia de Segurança Pública (PSP) utiliza

ferramentas forenses para análises de lofoscopia e peritagens em armas, mas está a expandir capacidades em forense digital (Gomes, 2018).

No contexto da análise forense de dispositivos Android, a seleção e aplicação de técnicas adequadas de aquisição e análise de dados constitui um fator determinante para a obtenção de evidência digital fiável e juridicamente admissível. Entre as abordagens mais utilizadas destaca-se a extração lógica, que permite aceder a dados disponíveis através das interfaces do sistema operativo, como mensagens SMS, contactos ou registos de chamadas. Embora menos intrusiva, esta técnica apresenta limitações significativas, nomeadamente a incapacidade de recuperar dados eliminados ou inacessíveis ao nível das permissões do sistema (Hoog, 2011).

Por sua vez, a extração física possibilita a criação de imagens completas das partições do dispositivo, através de cópias *bit-a-bit*, recorrendo a ferramentas como *dd* ou *dc3dd*. Esta abordagem permite uma análise mais aprofundada, incluindo a recuperação de dados apagados; contudo, requer frequentemente privilégios elevados, como acesso *root* ou utilização de modos alternativos de arranque, como o *recovery*. A implementação de mecanismos de segurança, como a criptografia baseada em ficheiros (*File-Based Encryption*), pode, no entanto, limitar o acesso direto a determinadas partições, nomeadamente à `/data` (Afonin & Katalov, 2016).

A análise de bases de dados SQLite assume igualmente um papel central, sobretudo no contexto da recuperação de dados provenientes de aplicações. Técnicas de *data carving* permitem extrair informação eliminada de bases de dados, incluindo mensagens de aplicações de comunicação, mesmo quando estas se encontram cifradas, mediante o uso de ferramentas especializadas (Casey, 2011). Complementarmente, a *live forensics* permite a recolha de dados voláteis, como conteúdos em memória RAM ou processos ativos, antes do desligamento do dispositivo, sendo particularmente útil em cenários onde a informação pode ser perdida de forma irreversível (Gomes, 2018).

Em situações em que o acesso lógico ou físico convencional não é possível, podem ser utilizadas técnicas mais invasivas, como *chip-off* ou *JTAG*, que permitem a leitura direta da memória do dispositivo. Contudo, estas metodologias apresentam riscos elevados, tanto do ponto de vista técnico como jurídico, exigindo uma avaliação criteriosa da sua admissibilidade no ordenamento jurídico português.

A par da seleção das técnicas forenses, a adoção de boas práticas é essencial para garantir a integridade e fiabilidade da prova digital. Entre estas destaca-se o isolamento do dispositivo através de meios de bloqueio de sinais de radiofrequência, como sacos de Faraday, prevenindo alterações remotas aos dados. A documentação rigorosa de todas as operações realizadas, incluindo a identificação do dispositivo, estado do *bootloader* e cálculo de valores *hash* constitui igualmente um requisito fundamental para assegurar a rastreabilidade da evidência (ISO/IEC 27037, 2012; Casey, 2011).

A preservação de registos do sistema, como *logcat* e *dmesg*, permite reconstruir cronologias de eventos e identificar atividades relevantes, como comunicações ou ligações de rede (Gomes, 2018). Adicionalmente, a realização das operações em ambientes forenses controlados reduz o risco de contaminação ou alteração inadvertida dos dados, garantindo a fiabilidade dos resultados obtidos.

Neste contexto, a cadeia de custódia assume um papel central, exigindo o registo detalhado de todas as interações com a evidência digital, desde a sua recolha até à apresentação em tribunal. Este processo inclui a identificação dos intervenientes, a marcação temporal das operações e o armazenamento seguro das cópias forenses em ambientes controlados, assegurando a sua integridade ao longo do tempo (Casey, 2011; ISO/IEC 27037). A conformidade com os requisitos legais e normativos, incluindo o RGPD, é igualmente indispensável no tratamento de dados pessoais.

A integridade da prova digital é, por sua vez, garantida através da utilização de mecanismos técnicos específicos, como funções hash criptográficas, designadamente SHA-256 ou SHA-3, que permitem verificar se os dados permanecem inalterados ao longo do processo forense (Casey, 2011). A utilização de dispositivos de *write-*

blocking durante a aquisição física impede a modificação acidental dos dados originais, reforçando a fiabilidade da evidência (Hoog, 2011).

Por fim, a validação dos procedimentos forenses à luz do enquadramento legal vigente, nomeadamente da Lei n.º 109/2009, de 15 de setembro, é essencial para assegurar a admissibilidade da prova em tribunal. O recurso a ferramentas forenses reconhecidas e amplamente utilizadas em contexto profissional contribui para garantir a conformidade dos procedimentos com os padrões técnicos e legais exigidos (Gomes, 2018).

A análise forense de dispositivos Android é tecnicamente complexa devido à fragmentação do ecossistema e às medidas de segurança como a criptografia FBE. A correta identificação das áreas de armazenamento (e.g., /data, /sdcard) e a utilização de ferramentas especializadas são essenciais para garantir a integridade da prova, em conformidade com a legislação portuguesa. A cadeia de custódia e a certificação ISO/IEC 27037 reforçam a credibilidade da prova perante os tribunais, assegurando justiça em casos sensíveis como a violência doméstica.

4. Análise de Caso Prático

No âmbito da aplicação prática dos conceitos e metodologias de análise forense digital em dispositivos com o sistema operativo *Android*, considera-se o caso de Maria, vítima de violência doméstica, que apresentou queixa formal contra o seu marido, António, junto das autoridades policiais. A vítima alegou ter sido alvo de ameaças e agressões, sustentando que parte relevante da prova se encontrava em mensagens trocadas através da aplicação WhatsApp, entretanto eliminadas do seu dispositivo móvel. Com o objetivo de recuperar essa informação e utilizá-la em contexto judicial, o dispositivo foi entregue às autoridades para análise forense.

A primeira etapa do procedimento consistiu na preservação da prova digital, assegurando o cumprimento rigoroso da cadeia de custódia. Para o efeito, procedeu-se ao registo detalhado das características do dispositivo, incluindo marca, modelo, IMEI, número de série e estado geral. O equipamento foi colocado em modo avião e isolado de redes externas, preferencialmente através da utilização de uma bolsa de Faraday, com o intuito de evitar acessos remotos ou alterações aos dados. Todas as operações foram devidamente documentadas, incluindo registos fotográficos e descrição pormenorizada das ações realizadas, garantindo a rastreabilidade da evidência.

Seguidamente, procedeu-se à aquisição forense dos dados, recorrendo a ferramentas reconhecidas e amplamente utilizadas no contexto profissional, como o Cellebrite UFED, Magnet AXIOM ou Oxygen Forensic Detective. Sempre que possível, optou-se pela aquisição física, permitindo a obtenção de uma cópia integral das partições do dispositivo, incluindo dados eliminados. Em alternativa, foi considerada a aquisição lógica, nos casos em que o acesso físico se revelasse inviável. A criação de uma imagem forense da partição `/data` assumiu particular relevância, uma vez que esta contém os dados associados às aplicações instaladas, incluindo o WhatsApp. Após a aquisição, foram gerados valores *hash*, nomeadamente através do algoritmo SHA-256, com o objetivo de garantir a integridade da cópia obtida.

A fase seguinte consistiu na localização e extração dos ficheiros relevantes da aplicação WhatsApp. Em particular, foram identificados o ficheiro de base de dados de mensagens, geralmente designado por *msgstore.db.crypt15* e a respetiva chave de encriptação (*key*), armazenados em diretórias específicas do sistema, como `/data/data/com.whatsapp/` ou, em alguns casos, no armazenamento emulado (`/sdcard/WhatsApp/Databases/`). A obtenção destes ficheiros é essencial para possibilitar a posterior desencriptação dos dados.

Com base nos ficheiros extraídos, procedeu-se à desencriptação do conteúdo, recorrendo a ferramentas especializadas, como WhatsApp Viewer, WADB Extractor ou scripts desenvolvidos em Python. Este processo permitiu converter o ficheiro cifrado num formato legível, nomeadamente uma base de dados SQLite (*msgstore.db*), possibilitando a sua análise detalhada.

A análise da base de dados incidiu na identificação e recuperação de mensagens eliminadas. Importa referir que, em muitos casos, os registos apagados não são imediatamente removidos da base de dados, permanecendo

armazenados até serem sobrescritos. Assim, através da utilização de ferramentas forenses avançadas e técnicas de *data carving*, foi possível recuperar mensagens relevantes, incluindo informação associada como data, hora, remetente, destinatário e conteúdo. Estes elementos revelaram-se potencialmente determinantes para a reconstrução dos factos e para a comprovação das alegações apresentadas pela vítima.

Todo o processo foi acompanhado de uma documentação rigorosa, incluindo o registo detalhado das etapas realizadas, das ferramentas utilizadas (e respetivas versões) e dos resultados obtidos. A análise foi sempre conduzida sobre cópias forenses, preservando a integridade dos dados originais. Com base nos resultados, foi elaborado um relatório técnico estruturado, contendo a descrição dos procedimentos, a evidência recolhida e a sua interpretação, de forma a garantir a sua compreensão e admissibilidade em contexto judicial.

Do ponto de vista legal, o procedimento respeitou os princípios estabelecidos no enquadramento jurídico aplicável, nomeadamente no que se refere à proteção de dados pessoais e à admissibilidade da prova digital. Em conformidade com o RGPD, a análise limitou-se aos dados estritamente relevantes para o caso em apreço, assegurando o princípio da minimização. Paralelamente, foram observadas as disposições do Código de Processo Penal e as boas práticas internacionais, como as definidas na norma ISO/IEC 27037, garantindo a legalidade, autenticidade e integridade da prova produzida.

6. Conclusão

A análise forense de dispositivos Android afirma-se, no contexto da sociedade digital contemporânea, como uma área indispensável à investigação criminal e cível, em virtude da ampla disseminação destes dispositivos e da natureza sensível dos dados que neles se encontram armazenados. O presente estudo permitiu identificar e caracterizar as principais áreas de armazenamento com relevância forense, com especial destaque para as partições `/data` e `/sdcard`, evidenciando simultaneamente os desafios decorrentes da fragmentação do ecossistema Android e da crescente implementação de mecanismos avançados de segurança, como a criptografia baseada em ficheiros.

A abordagem adotada, assente na revisão de literatura técnico-científica e na análise do enquadramento jurídico português, demonstrou que a admissibilidade e a fiabilidade da prova digital dependem do cumprimento rigoroso de princípios fundamentais, nomeadamente a autenticidade, a integridade e a cadeia de custódia. Estes princípios, consagrados no Código de Processo Penal, na Lei do Cibercrime e em normas internacionais como a ISO/IEC 27037, constituem pilares essenciais para garantir a validade probatória da evidência digital. Neste sentido, a utilização de ferramentas forenses certificadas e a documentação exaustiva dos procedimentos realizados revelam-se determinantes para assegurar a conformidade legal e técnica das análises efetuadas.

A análise do caso prático apresentado evidenciou, de forma concreta, a relevância da perícia forense digital na recuperação de informação eliminada, designadamente em aplicações de comunicação, e o seu impacto na produção de prova em contexto judicial. Em particular, no domínio da violência doméstica, a possibilidade de reconstruir interações e recuperar mensagens apagadas pode revelar-se decisiva para a proteção das vítimas e para a responsabilização dos agentes, contribuindo para uma justiça mais eficaz e sustentada em evidência objetiva.

Em síntese, a análise forense em dispositivos com o sistema operativo Android exige uma articulação sólida entre competências técnicas especializadas, conhecimento jurídico aprofundado e respeito pelos direitos fundamentais. Perante a constante evolução tecnológica e o aumento da complexidade dos sistemas digitais, torna-se essencial investir na formação contínua dos profissionais, na atualização de ferramentas e metodologias e na adaptação do quadro legal. Estes fatores constituem elementos-chave para reforçar a eficácia, a credibilidade e a sustentabilidade da prova digital no contexto do sistema de justiça em Portugal.

Referências

Afonin, O., & Katalov, V. (2016). *Mobile forensics: Advanced investigative strategies*. Packt Publishing.

Android Open Source Project. (2023). *Android Open Source Project*. https://developer.android.com

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

Cellebrite. (2024). *UFED user manual*. https://cellebrite.com

Código de Processo Penal. Decreto-Lei n.º 78/87, de 17 de fevereiro. (1987). *Diário da República*, I Série-A, n.º 40.

Convenção sobre o Cibercrime. (2001). Conselho da Europa, ETS n.º 185, Budapeste.

Correia, J. (2014). Prova digital: As leis que temos e a lei que devíamos ter. *Revista do Ministério Público*, 139, 101–124. https://rmp.smmp.pt/wp-content/uploads/2014/04/3_RMP_139_Joao_Correia.pdf

Gomes, T. (2018). Investigação criminal e ciências forenses: Novas competências da Polícia de Segurança Pública. In ISCPSI (Ed.), *Repositório Comum (RCAAP)*. http://hdl.handle.net/10400.26/25013

Hermeiro, A. (2023). A cadeia de custódia da prova digital: O uso da tecnologia blockchain como forma de preservação. In Faculdade de Direito da Universidade de Coimbra, *Repositório Científico da UC*. Universidade de Coimbra. https://hdl.handle.net/10316/107063

Hoog, A. (2011). *Android forensics: Investigation, analysis, and mobile security for Google Android*. Elsevier.

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

Lei n.º 32/2008, de 17 de julho. (2008). Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas. *Diário da República*, 1.ª série, n.º 138.

Lei n.º 58/2019, de 8 de agosto. (2019). Execução do Regulamento Geral de Proteção de Dados. *Diário da República*, 1.ª série, n.º 151.

Lei n.º 109/2009, de 15 de setembro. (2009). Lei do Cibercrime. *Diário da República*, 1.ª série, n.º 180.

Marques, P. (2013). Informática forense: Recolha e preservação da prova digital. In Universidade Católica Portuguesa, *Repositório UCP*. http://hdl.handle.net/10400.14/13191

Pereira, M. (2019). Prova digital: Problemas de compatibilização entre as Leis n.º 32/2008, n.º 109/2009 e o Código de Processo Penal. In Faculdade de Direito da Universidade de Coimbra (Ed.), *Repositório Científico da UC*. Universidade de Coimbra. https://hdl.handle.net/10316/90256

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. (2016). Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial da União Europeia*.

StatCounter. (2020). *Mobile operating system market share worldwide*. https://gs.statcounter.com

Tamma, R., Skulkin, O., Mahalik, H., & Bommisetty, S. (2018). *Practical mobile forensics: A hands-on guide to mastering mobile forensics for the iOS, Android, and Windows Phone platforms* (3rd ed.). Packt Publishing.

Venâncio, P. (2011). *Lei do Cibercrime: Anotada e comentada*. Coimbra Editora.

Declaração Ética

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