INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

VI CURSO DE COMANDO E DIREÇÃO POLICIAL

Trabalho Individual Final

Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre a PSP e o sistema de justiça

Auditor

Paulo Jorge dos Santos Costa

Lisboa, 16 de outubro de 2025

Resumo

A transformação digital da sociedade trouxe novos desafios à investigação criminal, em particular no que respeita à recolha, preservação e apresentação de prova digital em tribunal. A natureza volátil e facilmente manipulável destes elementos probatórios torna a sua gestão especialmente exigente, revelando fragilidades no modelo tradicional da cadeia de custódia, ainda muito dependente de registos manuais e de sistemas centralizados. Neste enquadramento, a tecnologia blockchain apresenta-se como uma alternativa inovadora, capaz de assegurar um registo transparente, imutável e verificável de todas as operações realizadas sobre a prova. A conjugação desta tecnologia com contratos inteligentes permite, adicionalmente, realizar tarefas como o registo inicial da prova recolhida, a validação das transferências de custódia, a gestão de acessos diferenciados e a emissão de notificações processuais. O trabalho analisa as limitações do modelo atualmente em vigor, examina experiências internacionais relevantes e propõe um modelo conceptual de integração entre a PSP e o sistema de justiça assente em blockchain permissionada e contratos inteligentes. Pretende-se, deste modo, contribuir para o reforço da fiabilidade da prova digital, para a interoperabilidade entre instituições e para a confiança dos cidadãos na administração da justiça.

Palavras-chave: Blockchain; cadeia de custódia; contratos inteligentes; investigação criminal; prova digital.

Abstract

The digital transformation of society has introduced new challenges to criminal investigations, particularly regarding the collection, preservation, and presentation of digital evidence in court. The volatile and easily manipulated nature of such evidence makes its management especially demanding, exposing vulnerabilities in the traditional chain of custody model, which still relies heavily on manual records and centralized systems. In this context, blockchain technology emerges as an innovative solution, capable of ensuring a transparent, immutable, and verifiable record of all operations performed on digital evidence. When combined with smart contracts, it additionally enables the automation of key tasks such as the initial registration of collected evidence, the validation of custody transfers, differentiated access management, and the issuance of procedural notifications. This study analyses the limitations of the current model, reviews relevant international practices, and proposes a conceptual framework for integrating a permissioned blockchain and smart contracts between the PSP and the justice system. In doing so, it seeks to strengthen the reliability of digital evidence, enhance institutional interoperability, and foster public trust in the administration of justice.

Keywords: Blockchain; chain of custody; criminal investigation; digital evidence; smart contracts.

Índice

Introdução

A digitalização da sociedade contemporânea transformou profundamente a forma como se comunica, trabalha e acede à informação. Paralelamente, aumentaram também os riscos associados à criminalidade informática, que tem vindo a assumir maior relevância nas investigações criminais e a colocar novos desafios às forças de segurança e ao sistema judicial. Neste contexto, a prova digital assume-se como elemento probatório essencial, embora frágil e vulnerável, exigindo mecanismos que assegurem a sua integridade e autenticidade.

A cadeia de custódia constitui precisamente esse mecanismo, ao garantir a rastreabilidade da prova desde a sua apreensão até à apresentação em tribunal. Qualquer quebra neste processo pode implicar a inadmissibilidade da prova, afetando diretamente a eficácia da investigação e a realização da justiça (Valente, 2020). Contudo, a crescente complexidade técnica e a fragmentação dos sistemas de informação entre entidades policiais e judiciais revelam limitações significativas no atual modelo nacional, nomeadamente no que respeita à interoperabilidade, à auditabilidade e à confiança interinstitucional.

Neste cenário, a tecnologia blockchain, associada a contratos inteligentes, surge como uma solução inovadora. O seu registo imutável e transparente, baseado em *hashing* e carimbos temporais, permite reforçar a integridade e rastreabilidade da prova digital (Gopalan et al., 2019). Projetos internacionais, como o LOCARD, financiado pela União Europeia, demonstram a viabilidade da integração de sistemas descentralizados na preservação da cadeia de custódia digital (União Europeia, 2023). Todavia, a aplicação desta tecnologia ao contexto português, especialmente à realidade organizacional e operacional da Polícia de Segurança Pública (PSP), permanece pouco estudada.

A lacuna de investigação centra-se, assim, na escassez de estudos que articulem a dimensão tecnológica da blockchain com os requisitos operacionais da cadeia de custódia da prova digital em Portugal, explorando simultaneamente as possibilidades de integração entre as forças de segurança e o sistema de justiça. A pertinência deste estudo decorre da necessidade de repensar o modelo de gestão da prova digital, conciliando inovação tecnológica, segurança jurídica e eficiência procedimental.

Com base neste enquadramento, o trabalho tem como objetivos:

- Identificar limitações do atual modelo de cadeia de custódia da prova digital na PSP;
- Estudar o potencial da tecnologia blockchain e dos contratos inteligentes;

- Analisar experiências internacionais relevantes;
- Apresentar um modelo conceptual de integração entre a PSP e o sistema de justiça.

Pretende-se, deste modo, contribuir para a reflexão académica e prática sobre uma problemática emergente, propondo soluções que conciliem exigências tecnológicas e operacionais, assegurando a fiabilidade da prova digital e a eficácia da justiça penal.

1. Estado de arte

1.1. A prova digital e a cadeia de custódia na investigação criminal

1.1.1. Conceito e características da prova digital

A prova digital assume crescente relevância na investigação criminal contemporânea, refletindo a digitalização generalizada das interações humanas. De acordo com o Conselho da União Europeia (2024), cerca de 85% das investigações criminais envolvem hoje elementos digitais, recolhidos em dispositivos como computadores ou telemóveis. Esta realidade impõe desafios quanto à recolha, preservação e apresentação da prova em tribunal, exigindo soluções técnicas e jurídicas que assegurem a sua integridade e admissibilidade.

No ordenamento jurídico português, a prova digital encontra enquadramento no Código de Processo Penal (CPP) e na Lei n.º 109/2009 (Lei do Cibercrime). O artigo 125.º do CPP estabelece que são admissíveis todas as provas não proibidas por lei, enquanto o artigo 126.º define os limites à sua obtenção. Assim, a admissibilidade da prova depende da legalidade dos meios de recolha e do respeito pelas garantias processuais.

A doutrina tem procurado delimitar o conceito de prova digital. Ramos (2014), define-a como "informação passível de ser extraída de um dispositivo eletrónico" (p.86), destacando a fiabilidade técnica. Já Rodrigues (2009) entende-a como "informação com valor probatório, armazenada (…) transmitida em sistemas e redes informáticas" (p.722), sublinhando o seu valor jurídico, enquanto Thamay e Tamer (2020) acentuam a dimensão instrumental e demonstrativa, ao definirem-na como um meio destinado a provar factos ocorridos em ambiente digital.

Apesar das diferenças, a literatura converge quanto às características da prova digital: volatilidade, facilidade de cópia e suscetibilidade à alteração. Rodrigues (2011) descreve-a como "fragmentária, dispersa, frágil, volátil, alterável, instável, apagável e manipulável, invisível e espacialmente dispersa" (p.29). Militão (2012) destaca as dificuldades na sua

identificação, recolha e preservação, enquanto Tsai (2021) chama a atenção para os riscos de alteração e contaminação. Estas vulnerabilidades justificam a adoção de procedimentos rigorosos e normalizados.

O avanço tecnológico trouxe também novos riscos. A Europol (2022) alerta para o uso de técnicas de manipulação audiovisuais, como os *deepfakes*, que permitem criar ou adulterar conteúdos de forma quase indetetável, comprometendo a credibilidade probatória. Assim, a prova digital requer mecanismos adicionais de validação e verificação.

Neste contexto, a literatura identifica dois requisitos essenciais para a eficácia da prova digital: integridade e autenticidade. Segundo Casey (2011), a integridade garante que a informação não foi alterada desde a sua apreensão, enquanto a autenticidade assegura a sua origem e contexto temporal. Técnicas como valores *hash*, assinaturas digitais, metadados e certificados eletrónicos são fundamentais para garantir esses princípios. A norma ISO/IEC 27037:2012 reforça estas orientações, definindo diretrizes internacionais para a identificação e preservação da prova digital (*International Organization for Standardization* [ISO], 2012).

Em síntese, a prova digital é hoje um elemento central da investigação criminal, mas a sua volatilidade e vulnerabilidade exigem mecanismos de custódia que assegurem autenticidade, integridade e fiabilidade perante o contraditório judicial.

1.1.2. Fragilidades do modelo tradicional da cadeia de custódia

A resposta clássica a estas fragilidades encontra-se na cadeia de custódia. Embora o ordenamento jurídico português não a defina expressamente, a sua importância decorre da Constituição da República Portuguesa (CRP) (artigos 20.º e 32.º) e do CPP (artigos 125.º e 126.º), que impõem aos órgãos de polícia criminal (OPC) a preservação dos vestígios do crime.

A doutrina tem procurado clarificar este conceito. Valente (2020) entende a cadeia de custódia como um procedimento jurídico destinado a garantir a identidade e autenticidade da prova. Ramos (2015) sublinha a necessidade de registos detalhados de todo o histórico de manuseamento, enquanto Rubio Alamillo (2016) destaca a preservação da prova tal como foi apreendida. García Mateo (2016) enfatiza a rastreabilidade completa, e Khan et al. (2021) definem-na como o processo de registo e documentação de todo o percurso da prova, assegurando a sua autenticidade e admissibilidade em tribunal.

A jurisprudência portuguesa acompanha esta exigência. O Acórdão do Tribunal da Relação do Porto (2015) reconheceu que quanto maior o cuidado na preservação, mais

robusta será a prova. Já o Tribunal da Relação de Évora (2024) e o Tribunal da Relação de Lisboa (2025) discutiram nulidades relacionadas com falhas na preservação da prova digital, demonstrando que a problemática não é apenas teórica, mas afeta de forma concreta a prática judiciária nacional.

Apesar da sua relevância, o modelo tradicional da cadeia de custódia revela limitações. Casey (2011) alerta para erros humanos e registos incompletos, que comprometem a rastreabilidade. No contexto português, com base em observação profissional direta, verifica-se uma forte dependência de documentação manual e de suportes físicos, como CDs ou DVDs, o que aumenta o risco de perda ou deterioração da informação. Lillis et al. (2016) referem que a vida útil limitada desses suportes compromete a preservação a longo prazo, enquanto Marques (2013) recorda que, até à publicação da norma ISO/IEC FDIS 27037:2012, inexistiam padrões internacionais específicos nesta matéria.

Embora a PSP tenha vindo a adotar práticas alinhadas com normas internacionais, persistem problemas de uniformização e interoperabilidade entre os OPC e o sistema judicial. A prática de criar cópias forenses em duplicado, gravadas em suportes óticos e acompanhada de códigos *hash*, mostra-se cada vez mais insuficiente. Como refere Daniele (2011), as normas e práticas devem adaptar-se ao ambiente digital, e não o contrário. Do mesmo modo, Giova (2011) salienta que não basta conhecer o código *hash*, a localização da prova ou a identidade dos peritos, é indispensável assegurar a assinatura eletrónica de cada objeto, o registo exato das interações, a localização precisa e o controlo de acesso, bem como uma auditoria contínua de todos os registos.

Estas fragilidades reforçam a necessidade de soluções tecnológicas mais seguras e rastreáveis. Khan et al. (2021) sugerem o uso de dispositivos de armazenamento encriptados e servidores seguros com acesso controlado, enquanto estudos recentes apontam a tecnologia blockchain como alternativa inovadora, valorizada pela sua imutabilidade, transparência e descentralização (Gopalan et al., 2019; Bonomi et al., 2018).

1.2. Blockchain e contratos inteligentes: potencialidades

1.2.1. A tecnologia blockchain

A tecnologia blockchain surgiu em 2008, associada à proposta que originou a Bitcoin, a sua primeira aplicação prática (Iansiti & Lakhani, 2017). A publicação do artigo

Bitcoin: A *Peer-to-Peer Electronic Cash System*, sob o pseudónimo de Satoshi Nakamoto (2008), marcou o ponto de partida para a consolidação da blockchain enquanto solução tecnológica inovadora (Martins, 2018). Desde então, o conceito tem vindo a dissociar-se progressivamente das criptomoedas, revelando potencial de aplicação em múltiplos domínios.

Tecnicamente, a blockchain é "uma base de dados distribuída entre diferentes participantes, protegida criptograficamente e organizada em blocos de transações matematicamente interligados (…) que não pode ser alterada" (Preukschat, 2018, p. 29). McFarland (2023) recorre a uma metáfora elucidativa ao afirmar que uma "blockchain é como uma base de dados resultantes do empilhar de folhas de cálculo, só que os blocos, que são como as folhas de cálculos individuais numa pilha maior, estão todos unidos por uma «corrente»" (p. 15). Cada bloco contém um conjunto de informação, um identificador único (*hash*) e o *hash* do bloco anterior, garantindo rastreabilidade e imutabilidade. Qualquer tentativa de alteração compromete toda a cadeia subsequente, tornando a manipulação praticamente impossível (Freire, 2022). Assim, a blockchain é simultaneamente um repositório descentralizado e um mecanismo de confiança partilhada, dispensando uma autoridade central para validar ou controlar a informação armazenada.

A sua fiabilidade assenta em quatro princípios fundamentais: descentralização, transparência, imutabilidade e segurança criptográfica, amplamente descritos na literatura especializada (Casino et al., 2019; Crosby et al., 2016). A descentralização elimina a dependência de uma autoridade única; a transparência permite a verificação dos registos por todos os participantes; a imutabilidade garante que a informação não pode ser alterada sem comprometer a cadeia; e a segurança criptográfica assegura a integridade e autenticidade das transações. Em conjunto, estas características criam um modelo de consenso distribuído, gerando confiança direta entre entidades.

De forma convergente, o relatório técnico do National Institute of Standards and Technology (NIST) descreve a blockchain como um registo distribuído, apenas aditivo e protegido por mecanismos criptográficos, que assegura a integridade e a auditabilidade dos dados (Yaga et al., 2018).

A literatura distingue três tipologias principais de blockchain: públicas, privadas e permissionadas. As primeiras são abertas a qualquer utilizador e baseiam-se em mecanismos de consenso como o *Proof of Work*, podendo colidir com as exigências de proteção de dados pessoais; as privadas são controladas por uma única entidade; e as permissionadas combinam descentralização e controlo de acessos, garantindo proteção de dados sensíveis (Casino et

al., 2019). Estas últimas revelam-se mais adequadas a contextos institucionais, por permitirem maior eficiência e uma gestão controlada e auditável dos acessos à informação (Yaga et al., 2018).

Projetos como o *Hyperledger Fabric*, desenvolvido por Androulaki et al. (2018), demonstram a viabilidade destas redes em consórcios empresariais e governamentais, privilegiando resiliência e confidencialidade. Freire (2022) reforça a utilidade das blockchain permissionadas para organizações que necessitem partilhar informação de forma segura.

Assim, a adequação das blockchain permissionadas é particularmente evidente em contextos policiais e judiciais, onde múltiplas entidades partilham registos auditáveis e imutáveis, assegurando integridade, transparência e confiança interinstitucional.

1.2.2. Contratos inteligentes

Os contratos inteligentes (*smart contracts*) representam uma inovação tecnológica de grande impacto na automação e segurança das transações digitais. Introduzidos por Szabo (1994), consistem em protocolos informáticos capazes de executar automaticamente cláusulas contratuais previamente definidas, sem necessidade de intervenção humana.

A sua integração em redes blockchain permissionadas amplia o seu potencial muito além do setor financeiro, sendo aplicável a domínios que exigem elevados padrões de integridade e rastreabilidade, como a cadeia de custódia da prova digital (Androulaki et al., 2018; Bonomi et al., 2019; Gopalan et al., 2019; Yaga et al., 2018).

Tecnicamente, um contrato inteligente é um programa armazenado numa blockchain, acionado sempre que determinadas condições são verificadas. A sua segurança decorre das propriedades da blockchain: imutabilidade; segurança criptográfica; e auditabilidade, que dificultam a manipulação e reforçam a confiança (Yaga et al., 2018).

Na cadeia de custódia digital, permitem automatizar operações como recolha, transferência de custódia, análise pericial ou apresentação em tribunal, registando cada ação de forma imutável, com carimbo temporal e assinatura digital (Gopalan et al., 2019).

Adicionalmente, podem gerir acessos diferenciados, garantindo que apenas utilizadores autorizados interajam com dados sensíveis. Alyas et al. (2025), salientam que, em arquiteturas multi-blockchain, os contratos inteligentes permitem implementar políticas de acesso e automatizar tarefas como validações entre múltiplas entidades, gestão de prazos ou emissão de notificações processuais, aumentando a eficiência administrativa.

Modelos conceptuais demonstram a viabilidade desta integração. O modelo *Blockchain-based Chain of Custody* (B-CoC), de Bonomi et al. (2019), mostra como a blockchain regista todas as operações sobre a prova digital, enquanto os contratos inteligentes asseguram a validação automática e auditoria contínua. De modo semelhante, o sistema *MF-Ledger*, desenvolvido por Khan et al. (2021), aplica este paradigma à gestão de provas multimédias, evidenciando ganhos significativos na integridade e autenticidade.

1.2.3. Aplicação da blockchain e dos contratos inteligentes à cadeia de custódia da prova digital

Identificadas as fragilidades do modelo tradicional da cadeia de custódia, importa analisar de que forma a tecnologia blockchain, associada aos contratos inteligentes, pode colmatar essas limitações. A sua arquitetura descentralizada e imutável, dotada de carimbo temporal, permite registar de forma transparente todas as operações realizadas sobre a prova, desde a recolha até à apresentação em tribunal. Cada interação é documentada como uma transação verificável, reforçando a credibilidade judicial (Gopalan et al., 2019).

A literatura sublinha que a blockchain não armazena diretamente a prova, mas apenas os seus metadados e valores *hash* (Bonomi et al., 2019; Crosby et al., 2016; Gopalan et al., 2019; Khan et al., 2021). Assim, a prova permanece guardada em base de dados institucionais seguras, enquanto a blockchain assegura um registo imutável e verificável do histórico de interações. Este modelo garante a integridade e autenticidade da prova, preservando a confidencialidade e evitando a exposição indevida de informação sensível.

No contexto policial e judicial português, em que a proteção de dados constitui um imperativo legal e ético, as blockchain permissionadas assumem especial relevância, por poderem ser utilizadas por entidades que valorizam a segurança e a confidencialidade da informação (Yaga et al., 2018, p. 6). Tal modelo permitiria que os OPC, laboratórios forenses, Ministério Público e tribunais partilhassem um registo comum, imutável e auditável, garantindo rastreabilidade e confiança interinstitucional.

Em síntese, a integração da blockchain e dos contratos inteligentes configura uma solução inovadora e promissora para reforçar a integridade, a rastreabilidade e a autenticidade da prova digital. Embora subsistam desafios de ordem tecnológica, organizacional e jurídica, a literatura destaca o seu potencial transformador na gestão e validação da prova em tribunal.

1.3. Projetos e práticas internacionais

A literatura internacional sobre a utilização da blockchain na cadeia de custódia da prova digital tem evoluído, passando de modelos conceptuais para protótipos e projetos experimentais, muitos associados a sistemas judiciais ou iniciativas transnacionais. A análise destas práticas permite identificar padrões comuns e caminhos de implementação.

Entre os primeiros modelos académicos destaca-se o *B-CoC*, proposto por Bonomi et al. (2019). Assente numa arquitetura privada e permissionada, armazena apenas metadados e valores *hash*, detetando automaticamente qualquer alteração. Recorre a contratos inteligentes na plataforma *Ethereum* e ao mecanismo de consenso *Proof of Authority*, assegurando autenticidade e auditabilidade sem necessidade de intermediários.

Em linha com o exposto, Gopalan et al. (2019) sublinham o potencial da blockchain para reforçar a integridade e a rastreabilidade da prova digital, propondo o uso de algoritmos de *hashing* e mecanismo de consenso para proteger os registos contra adulterações. Já o *MF-Ledger*, desenvolvido por Khan et al. (2021) foca-se em provas multimédia, recorrendo ao *Hyperledger Sawtooth*, uma plataforma permissionada, e a contratos inteligentes para automatizar registos e validações em tempo real. Também Tsai (2021) destaca a importância da definição de papéis funcionais (administrador, criador, proprietário e investigador), regulados por contratos inteligentes, garantindo um controlo
rigoroso de acessos.

Em síntese, estes contributos demonstram que a blockchain pode colmatar fragilidades do modelo tradicional da cadeia de custódia, nomeadamente a vulnerabilidade à alteração, a falta de rastreabilidade plena e a dependência de documentação manual.

Para além da investigação académica, vários contextos institucionais têm validado a tecnologia. Nos Estados Unidos, o Estado de Vermont reconhece o valor probatório de registos armazenados em blockchain, desde que certificados (Vermont Legislatura, 2024). Na Europa, o projeto LOCARD, financiado pelo programa Horizonte 2020, utiliza a blockchain para preservar metadados forenses, facilitando a cooperação entre jurisdições e reforçando a confiança na admissibilidade da prova (Comissão Europeia, 2023). De forma complementar, a *European Blockchain Services Infrastructure* (EBSI), desenvolvida pela Comissão Europeia e pelos Estados-Membros, procura criar uma rede descentralizada de serviços públicos digitais, aplicando contratos inteligentes e registos distribuídos para garantir segurança e rastreabilidade (Comissão Europeia, 2025).

Alguns países apresentam já aplicações consolidadas. Na Estónia, a *Keyless Signature Infrastructure* (KSI) comprova criptograficamente a integridade e o carimbo temporal de registos públicos, sem expor dados pessoais, constituindo exemplo de utilização da blockchain na gestão de registos estatais (Arm et al., 2019). Nos Emirados Árabes Unidos, a Polícia do Dubai integrou blockchain nos serviços digitais, como a emissão de certificados de passaportes perdidos, demonstrando aplicabilidade em processos administrativos policiais (Government of Dubai Media Office, 2024).

Em síntese, as experiências internacionais confirmam a viabilidade técnica e o reconhecimento jurídico da blockchain na gestão da prova digital, embora a sua adoção dependa de ajustamentos normativos e institucionais. Estes exemplos reforçam a importância de refletir sobre a aplicabilidade ao contexto português e às especificidades da PSP e do sistema de justiça.

1.4. Formulação do problema

A revisão da literatura mostra que, embora a blockchain e os contratos inteligentes sejam reconhecidos como instrumentos capazes de reforçar a integridade, a rastreabilidade e a eficiência da cadeia de custódia da prova digital, a sua aplicação prática no contexto policial e judicial português permanece incipiente. Persistem incertezas quanto ao enquadramento jurídico, à interoperabilidade com sistemas existentes e à aceitação pelos profissionais.

Duas áreas surgem como merecedoras de estudo aprofundado: o impacto jurídico da integração da blockchain no processo penal e as condições técnicas, organizacionais e humanas da sua aplicação prática. Este estudo centra-se nesta última dimensão, privilegiando a perspetiva da PSP e do sistema de justiça, procurando compreender fragilidades, potencialidades e desafios da adoção da tecnologia em contexto real.

É neste quadro que se formula o problema de investigação: de que forma a tecnologia blockchain, complementada por contratos inteligentes, pode contribuir para reforçar a integridade da cadeia de custódia da prova digital, promovendo uma integração eficaz entre a PSP e o sistema de justiça?

2. Método

Em função da natureza e especificidade do problema central a que este trabalho se propõe dar resposta optou-se pela abordagem metodológica seguinte:

2.1. Hipótese de investigação

A investigação foi orientada pela seguinte pergunta de partida formulada na seção anterior, centrando-se na análise de como a tecnologia blockchain, complementada por contratos inteligentes, pode reforçar a integridade da cadeia de custódia da prova digital e promover uma integração eficaz entre a PSP e o sistema de justiça.

Com base nesta problemática, formularam-se as seguintes hipóteses:

H1: O modelo atual da cadeia de custódia da prova digital apresenta fragilidades de natureza procedimental e tecnológica que comprometem a sua credibilidade e eficácia.

H2: A adoção de uma solução baseada em blockchain e contratos inteligentes pode reforçar a integridade, a rastreabilidade e a eficiência operacional da prova digital.

2.2. Amostra/corpus/participantes

A amostra foi definida por conveniência, de forma estratificada, em três grupos: profissionais da PSP; magistrados do sistema de justiça; e académicos. Esta divisão assegurou diversidade de perspetivas (operacional, jurídica e científico-tecnológica). O recrutamento foi efetuado através de contactos institucionais e de redes profissionais, tendo os participantes aceite voluntariamente o convite. De um total de treze contactos efetuados, dois não responderam dentro do prazo estipulado, sendo excluídos da amostra final. Foram realizadas onze entrevistas válidas, com paragem por saturação teórica, entendida como o momento em que novas entrevistas deixam de acrescentar contributos relevantes sob a forma de categorias ou códigos (Van Campenhoudt et al., 2019).

O corpus do estudo foi constituído pelas transcrições das entrevistas (Apêndice D), obtidas maioritariamente por gravação áudio, mediante consentimento informado, e, em três casos, por recolha escrita. As transcrições serviram de base à análise de conteúdo.

2.3. Instrumentos

O instrumento de recolha utilizado consistiu num guião de entrevista semiestruturada (Apêndice C), elaborado a partir da revisão da literatura e do enquadramento teórico. O guião contemplou os tópicos seguintes: (i) fragilidades da cadeia de custódia; (ii) perceção sobre a blockchain e contratos inteligentes; (iii) benefícios esperados e obstáculos identificados; e (iv) perspetivas de articulação entre a PSP e o sistema de justiça.

2.4. Procedimento

As entrevistas foram conduzidas presencialmente ou por videoconferência, nos meses de setembro e de outubro de 2025, consoante a disponibilidade dos participantes, com uma duração média de 20 minutos. Todos foram previamente informados sobre os objetivos do estudo, os procedimentos e os seus direitos. Para salvaguardar a confidencialidade, procedeu-se à pseudonimização dos entrevistados (E1, E2, …), conforme indicado na tabela 3 do Apêndice B e os ficheiros foram armazenados em repositório seguro.

A análise das entrevistas foi conduzida segundo a metodologia de análise de conteúdo proposta por Bardin (2016), em três fases: pré-análise, exploração do material e tratamento dos resultados. As unidades de registo correspondem a trechos de discurso relativo a perceções, vantagens, obstáculos ou desafios. O processo foi apoiado pelo software NVivo 15 (Lumivero, 2025), que permitiu organizar e codificar sistematicamente as categorias, assegurando transparência e rastreabilidade.

A abordagem foi de natureza híbrida, predominantemente dedutiva, uma vez que partiu de categorias teóricas previamente identificadas na literatura, mas também incorporou elementos indutivos emergentes dos discursos dos participantes. As categorias e subcategorias foram sustentadas por evidências empíricas retiradas das entrevistas, sistematizadas na matriz categoria-evidência (tabela 4 do Apêndice E).

Para assegurar a transparência e a qualidade do reporte metodológico, foram considerados os critérios do *Consolidated Criteria for Reporting Qualitative Research* (COREQ), checklist de 32 itens propostos por Tong et al. (2007). A versão adaptada e aplicada ao presente estudo encontra-se na tabela 5 do Apêndice F.

O trabalho beneficiou ainda de uma revisão por pares (*peer debriefing*), realizada por um colega com experiência metodológica, o que reforçou a consistência das interpretações. As transcrições das entrevistas foram devolvidas aos participantes para revisão e confirmação da exatidão do conteúdo, assegurando a fidelidade das declarações recolhidas.

3. Apresentação e discussão dos resultados

A análise de conteúdo das entrevistas permitiu identificar quatro categorias principais que estruturam a apresentação dos resultados (tabela 4 do Apêndice E). Estas categorias refletem as perceções dos participantes acerca das fragilidades do modelo atual e o potencial da tecnologia blockchain na cadeia de custódia da prova digital.

Tabela 1

Categorias e subcategorias resultantes da análise de conteúdo das entrevistas

Categorias	Subcategorias
Contexto e experiência	Experiência
	Perceção sobre a tecnologia
Fragilidades do modelo de cadeia de custódia da prova	Fator humano - falhas processuais
	Heterogeneidade de procedimentos
	Limitações tecnológicas
Adoção da tecnologia blockchain e contratos inteligentes	Vantagens
	Obstáculos
Desafios	Capacitação e formação contínua
	Viabilidade a médio prazo

Fonte: Elaboração própria com base na análise de conteúdo das entrevistas

Tabela 2

Matriz de codificação cruzada (NVivo 15): frequência de unidades de registo por subcategoria e entrevistado

	Experiência	Perceção sobre a tecnologia	Fator humano - falhas processuais	Heterogeneidade de procedimentos	Limitações tecnológicas	Vantagens	Obstáculos	Capacitação e formação contínua	Viabilidade a médio prazo	Total
E1	1	0	0	0	0	2	5	0	0	8
E2	2	3	3	1	0	2	4	0	6	21
E3	1	1	1	0	1	4	3	0	0	11
E4	1	1	1	0	0	2	2	0	2	9
E5	1	1	0	0	4	10	4	1	4	25
E6	1	4	3	3	1	6	5	2	4	29
E7	1	1	0	2	1	6	2	0	3	16
E8	1	1	2	0	2	1	4	0	0	11
E9	1	1	1	2	0	6	6	1	4	22
E10	1	1	0	1	0	1	1	1	2	8
E11	1	1	2	0	1	4	2	2	1	14
Total	12	15	13	9	10	44	38	7	26	174

Nota: A tabela apresenta o número de unidades de registo codificadas em cada subcategoria, resultantes da análise de conteúdos das entrevistas (E1 a E11) com recurso ao software

NVivo 15. Cada valor indica a frequência de referências identificadas por entrevistado em cada subcategoria.

Fonte: Extraído do NVivo 15 (Lumivero, 2025), com adaptação e elaboração própria.

A matriz evidencia maior incidência nas subcategorias vantagens (44) e obstáculos (38), revelando perceções equilibradas entre potencial e constrangimentos. A viabilidade a médio prazo (26) traduz uma atitude cautelosa, porém favorável à adoção da tecnologia, enquanto a capacitação e formação contínua (7) demonstra défice de competências técnicas. As falhas processuais (13) e limitações tecnológicas (10) confirmam vulnerabilidades operacionais, reforçando a necessidade de uniformização e modernização dos procedimentos.

Em conjunto, os dados apontam para um contexto que reconhece o valor estratégico da tecnologia, mas enfrenta barreiras humanas, organizacionais e técnicas cuja superação exige investimento em formação, padronização e infraestrutura tecnológica.

3.1. Categoria 1 – Contexto e experiência

3.1.1. Experiência

Os entrevistados apresentaram percursos profissionais heterogéneos, desde a ausência de contacto prévio (“não tenho qualquer experiência”, E1) até experiência consolidada em contextos operacionais (“trabalho nisto desde 2009”, E2). Alguns participantes referiram experiência relacionada com a atividade profissional, (E7; E9; E10; E11) enquanto outros contribuíram em áreas complementares como cibersegurança (E6), projetos tecnológicos de rastreabilidade (E5) e docência em matérias afins (E4).

Discussão: Esta diversidade de trajetórias favorece a triangulação das perspetivas operacionais, técnico-científicas e judiciais, permitindo uma compreensão integrada dos desafios práticos da cadeia de custódia e das exigências de admissibilidade probatória. A literatura sublinha a necessidade de articular saber operativo, engenharia de segurança e requisitos legais através de modelos processuais normalizados que abranjam todo o ciclo probatório, reduzindo incertezas e contestação em tribunal (Reith et al., 2002).

Os dados corroboram esta perspetiva, revelando um ecossistema com competências complementares, ainda que por vezes compartimentadas.

3.1.2. Perceção sobre a tecnologia

As perceções sobre a tecnologia blockchain variam entre o desconhecimento parcial (E8; E10; E11), noções vagas ("cadeia de informação", E2) e definições tecnicamente consistentes ("registo distribuído e imutável… transparência e rastreabilidade", E6). Verificou-se também a distinção face às criptomoedas (E5) e o reconhecimento da utilidade dos contratos inteligentes na automatização de registos (E6). Ainda assim, alguns participantes, como E9, reconhecem o potencial tecnológico, mas identificam lacunas de formação, evidenciando a necessidade de reforçar a literacia digital.

Discussão: O gradiente de literacia digital surge como variável crítica para a adoção tecnológica: onde a conceptualização é sólida (E6), evidencia-se a associação entre integridade, auditabilidade e governação de acessos; onde a literacia é mais limitada, persistem confusões terminológicas e reservas quanto à aplicação prática. Este padrão confirma Rogers (2003), segundo o qual a adoção depende das perceções de vantagem, compatibilidade e complexidade, mediadas pela formação e pelo conhecimento.

No contexto PSP-sistema de justiça, impõe-se uma estratégia de capacitação progressiva, baseada em caso de uso concreto, linguagem acessível e demonstrações práticas que evidenciem ganhos de integridade e eficiência.

3.2. Categoria 2 – Fragilidades do modelo atual da cadeia de custódia

3.2.1. Fatores humanos e falhas processuais

A análise das entrevistas evidencia fragilidades estruturais no modelo de gestão da prova digital, com impacto direto na credibilidade judicial. O fator humano surge como a vulnerabilidade mais recorrente ("falhas humanas", E2; "dependência de processos manuais", E6), acompanhado de deficiências documentais suscetíveis de contestação (E6) e de riscos de acesso privilegiado por parte de "*malicious insiders*" (E4). A necessidade de mobilizar recursos adicionais para mitigar erros (E3) revela custos organizacionais ocultos e revela a ausência de automatização. Foi ainda referido que "o registo manual" pode originar lapsos ou omissões (E9), ilustrando como o erro humano se materializa na documentação operacional. A observação de que "ainda funcionamos muito com base na confiança" (E11) sintetiza a dependências de práticas assentes em relações interpessoais, em detrimento de sistemas de validação automatizada e transparente.

Discussão: Em consonância com Casey (2011), a autenticidade da prova digital exige uma origem identificável, aquisição completa e conservação inalterada desde a recolha, o que implica documentação robusta e rastreabilidade integral. Neste contexto, as falhas

humanas e a documentação incompleta comprometem a confiança judicial e podem pôr em causa a admissibilidade da prova.

Os resultados reforçam, assim, a necessidade de soluções concebidas desde a origem, que reduzam a intervenção manual e margem de erro humano, assegurando validações automáticas, registos verificáveis e trilhos de auditoria transparentes.

3.2.2. Heterogeneidade de procedimentos

Os entrevistados sublinham a ausência de harmonização entre entidades ("cada um conduz o seu carro", E2), e a rastreabilidade incompleta do percurso da prova (E7). Foi igualmente referido que a falta de integração entre sistemas dificulta a rastreabilidade total e que os intervalos temporais entre a apreensão e a perícia podem ser significativos, ampliando o risco de lacunas na cadeia de custódia (E9).

Discussão: A fragmentação tecnológica e processual constitui um obstáculo estrutural à interoperabilidade. A inexistência de plataformas partilhadas e de perfis de acesso harmonizados potencia redundâncias, atrasos e falhas auditáveis comprometendo a rastreabilidade e a credibilidade judicial da prova.

Em linha com as recomendações da *European Union Agency for Cybersecurity* (2019), impõe-se integrar requisitos de interoperabilidade desde a conceção, promover ferramentas comuns e definir responsabilidades claras entre forças de segurança e sistema de justiça.

3.2.3. Limitações tecnológicas

Persistem práticas baseadas em suportes frágeis (papel, CDs, pen drives), com risco de perda, deterioração ou manipulação indevida (E5; E8; E11) e vulnerabilidades nos sistemas centralizados, como acessos não rastreados e possibilidade de alterações de registo (E5; E6). A dispersão por múltiplas plataformas agrava a morosidade processual e o risco de falhas documentais (E9).

Discussão: O desfasamento entre a volatilidade da prova digital e os mecanismos tradicionais de conservação compromete a integridade e autenticidade probatória (Lillis et al., 2016). Daqui decorre a pertinência de soluções tecnológicas que assegurem redundância distribuída, selagem temporal e registos invioláveis de eventos, princípios intrínsecos à arquitetura da tecnologia blockchain permissionada.

3.3. Categoria 3 – Adoção da tecnologia blockchain e contratos inteligentes

3.3.1. Vantagens

Os participantes antecipam ganhos expressivos em confiança institucional ("reforço da confiança", E1), eficiência processual (redução de morosidade, eliminação de tarefas manuais e interoperabilidade PSP-Ministério Público-tribunais) e integridade probatória ("saber quem acedeu, quando e porquê", E3). Destacam a possibilidade de aceder "facilmente ao histórico das provas" (E11) registar operações e impedir alterações não detetadas (E6). Referem ainda transparência, controlo granular de acessos (E7), rastreabilidade e auditoria automáticas, bem como automação procedimental através de contratos inteligentes.

Esta visão é reforçada por outro entrevistado ao antecipar "maior eficiência e celeridade processual", "redução de contestações formais" e o "aumento da confiança de todos os intervenientes processuais", destacando ainda a blockchain como um "notário digital" que viabiliza o registo inviolável do manuseamento da prova (E9). Outros participantes salientam "maior eficácia do sistema" (E10) e que "permitiria uma análise mais rápida e fiável, evitando atrasos e incertezas" (E11).

Discussão: Estes benefícios estão em consonância com o estado da arte - a imutabilidade dos registos, a rastreabilidade programável e o controlo automatizado de permissões são atributos particularmente adequados à cadeia de custódia digital (Bonomi et al., 2019; Tsai, 2021). A principal vantagem não está na inovação em si, mas na resposta às fragilidades identificadas, nomeadamente a documentação lacunar, a heterogeneidade de procedimentos e a vulnerabilidade de suportes físicos.

A redundância e tolerância a falhas das arquiteturas distribuídas (E5), aliadas à visibilidade de acessos injustificados (E7), configuram mecanismos eficazes de mitigação de risco e de reforço da responsabilização institucional.

3.3.2. Obstáculos

Apesar do potencial identificado, persistem desafios à implementação da tecnologia blockchain na cadeia de custódia digital, designadamente a necessidade de ajustes legislativos e regulamentares (E6); os riscos infraestruturais decorrentes da dependência de

conetividade (E5); e as dificuldades de interoperabilidade entre sistemas heterogéneos (E2; E7).

Enquanto alguns participantes salientaram que um dos principais obstáculos são os custos associados à sua implementação (E3; E9; E10; E11), outros relativizaram esse fator: "os custos não são o problema, objetivamente não" (E5), evidenciando divergências de perceção quanto ao peso financeiro. A resistência à mudança foi igualmente identificada como barreira recorrente (E5; E8; E9; E11), refletindo o impacto das culturas organizacionais na adoção de tecnologia disruptiva.

Discussão: a literatura corrobora esta visão prudente - a eliminação do ponto único de falhas através de *ledgers* distribuídos e verificáveis potencia a dissuasão e deteção de irregularidades, ao criar um registo transparente das operações (Bonomi et al., 2019). Todavia, a eficácia, depende de coerência normativa e técnica, assegurando compatibilidade com os princípios do Estado de Direito, legalidade, proporcionalidade e proteção dos direitos fundamentais.

Do ponto de vista técnico, a prioridade recai sobre a interoperabilidade semântica e funcional, garantindo a integração segura com sistemas processuais e repositórios forenses existentes.

A divergência quanto aos custos revela que estes são percecionados mais como uma questão de governação e vontade política do que de viabilidade técnica.

Assim, a adoção de redes permissionadas com governação interinstitucional e mecanismos de auditoria partilhada constitui a via mais prudente e exequível para o contexto português, equilibrando inovação tecnológica, segurança jurídica e viabilidade operacional.

3.4. Categoria 4 – Desafios e visão de futuro

3.4.1. Capacitação e formação contínua

Os participantes sublinham a necessidade de desconstruir estereótipos que associam a blockchain às criptomoedas "ainda existe o estereótipo de associar blockchain apenas às criptomoedas, mas acredito que isso vai desaparecer gradualmente" (E5).

A transformação digital é considerada um imperativo estratégico: "a transformação digital da justiça e das forças não é um luxo, mas uma necessidade para enfrentar a criminalidade do século XXI" (E6).

Destaca-se ainda a importância da formação e sensibilização, abrangendo não apenas os profissionais operacionais, mas também o poder político e a sociedade civil (E6; E9; E10; E11).

Discussão: os depoimentos convergem na ideia de que a literacia digital e a formação especializada são condições essenciais para uma adoção tecnológica sustentável. O capital humano surge como variável crítica: sem capacitação dirigida, a inovação técnica tende a esbarrar-se na inércia organizacional.

A literatura recente defende estratégias de capacitação progressiva, com programas modulares, guias operacionais claros e promotores internos que assegurem coerência institucional (Alyas et al., 2025).

Em consonância com as orientações da *European Union Agency for Cybersecurity* (2019), a formação técnica e jurídica articulada entre peritos, magistrados e decisores é crucial para alinhar práticas, reforçar a confiança e garantir apropriação gradual da tecnologia.

3.4.2. Viabilidade a médio prazo

Os participantes defendem uma adoção gradual, baseada em projetos-piloto e parcerias interinstitucionais, como via mais prudente: “a médio prazo, vejo a adoção como plausível, desde que exista investimento em infraestrutura, formação e atualização legal” (E6). A colaboração académica é apontada como vetor estratégico: “podemos propor temas de dissertação aos alunos… a tese teria de incluir uma prova de conceito funcional” (E5).

A viabilidade depende, contudo, de decisões políticas e orientações estratégicas conjuntas, ultrapassando resistências corporativas e fragmentação institucional (E2; E6; E9), bem como a existência de uma “estratégia clara e sustentada de modernização tecnológica” (E10).

Os participantes reconhecem ainda limitações de curto prazo, designadamente entraves técnicos, humanos e legais (E2; E6), mas defendem a adoção de redes permissionadas (E4; E5) e a criação de um sistema integrado e transversal que inclua todos os OPC e o sistema de justiça (E2; E7; E9; E10).

Discussão: A prudência expressa é coerente com a literatura internacional, que defende uma adoção faseada e experimental, baseada em projetos-piloto (Alyas et al., 2025). Esta abordagem permite mitigar riscos, reduzir custos e produzir evidência empírica sobre o desempenho e aceitabilidade institucional.

A médio prazo, a viabilidade dependerá da existência de uma estratégia nacional clara, de uma governação tecnológica interinstitucional e integração progressiva com sistemas existentes.

Em síntese, os resultados confirmam a pertinência da integração da tecnologia blockchain na cadeia de custódia da prova digital, evidenciando simultaneamente o seu potencial técnico e os desafios humanos, organizacionais e legais. A diversidade de experiências dos participantes e a convergência das perceções reforçam a necessidade de uma abordagem gradual e sustentada, alicerçada em formação, interoperabilidade e governação partilhada entre a PSP e o sistema de justiça.

Partindo desta análise empírica e em articulação com a literatura especializada, apresenta-se de seguida uma proposta de modelo conceptual, concebida para traduzir essas evidências num quadro tecnológico e organizacional adaptado à realidade da PSP e do sistema de justiça português.

4. Proposta de modelo conceptual aplicado à PSP e ao sistema de justiça

A formulação de um modelo conceptual assente na tecnologia blockchain e em contratos inteligentes resulta da articulação entre os resultados da análise empírica e a literatura especializada. As entrevistas revelaram fragilidades no modelo atual de cadeia de custódia, designadamente a dependência de registos manuais (E3), utilização de suportes físicos vulneráveis (E5), a suscetibilidade a falhas humanas (E2) e ausência de uniformização de procedimentos (E3). A doutrina confirma esta perceção, destacando a volatilidade, dispersão e vulnerabilidade à manipulação da prova digital (Rodrigues, 2011; Tsai, 2021). Esta convergência evidencia a necessidade de repensar o sistema vigente, adotando soluções que reforcem a integridade e a rastreabilidade da prova, promovam interoperabilidade e assegurem maior eficiência processual.

A literatura e os entrevistados identificaram as blockchain permissionadas, como a solução mais adequada a contextos regulados e sensíveis. Esta arquitetura permite controlar acessos, proteger dados confidenciais e garantir eficiência operacional (Androulaki et al., 2018; Yaga et al., 2018; E4; E6). O modelo proposto baseia-se, assim, numa rede blockchain permissionada, de uso exclusivo pelas entidades que integram a cadeia de custódia (PSP, Ministério Público e tribunais), funcionando como registo partilhado, imutável e auditável, onde cada operação sobre a prova digital é automaticamente validada e registada. A validação e o consenso entre nós são assegurados por um mecanismo do tipo *Proof of*

Authority (PoA), adequado a redes institucionais em que os validadores são entidades previamente autorizadas e identificadas.

A rede distingue dois tipos de nós operacionais (Figura 1):

- Nós validadores, pertencem às entidades com competência para validar e registar transações, garantindo a integridade e consistência da cadeia. Incluem o Ministério Público e os tribunais.
- Nós de submissão e consulta, correspondem às entidades que introduzem registos ou acedem à informação validada, como a PSP e outros OPC. Estes interagem com a blockchain sem alterar o registo, assegurando transparência e rastreabilidade.

Cada novo elemento probatório é associado a um *hash* criptográfico e a metadados descritivos, armazenados na blockchain, enquanto o ficheiro original permanece fora da cadeia, num repositório seguro. Esta separação reduz os riscos de exposição e assegura a confidencialidade (Crosby et al., 2016; Alyas et al., 2025). A blockchain funciona, assim, como "um registo vivo, onde cada passo da cadeia de custódia ficaria automaticamente validado e registado de forma imutável" (E5).

A proposta integra também contratos inteligentes para automatizar tarefas críticas:

- O registo inicial da prova recolhida;
- A validação das transferências de custódia entre entidades;
- A gestão de acessos com base em perfis diferenciados (investigadores; magistrados; juízes); e
- A emissão de notificações automáticas e controlo de prazos processuais.

Segundo Alyas et al. (2025), a aplicação de contratos inteligentes em sistemas judiciais permite automatizar fluxos de trabalho, reduzir erros, simplificar a gestão processual e aumentar a segurança e a transparência. Os participantes corroboraram esta perspetiva, sublinhando a utilidade destes mecanismos na automatização de regras e na rastreabilidade total (E5); (E6).

A arquitetura conceptual estrutura-se em várias camadas funcionais:

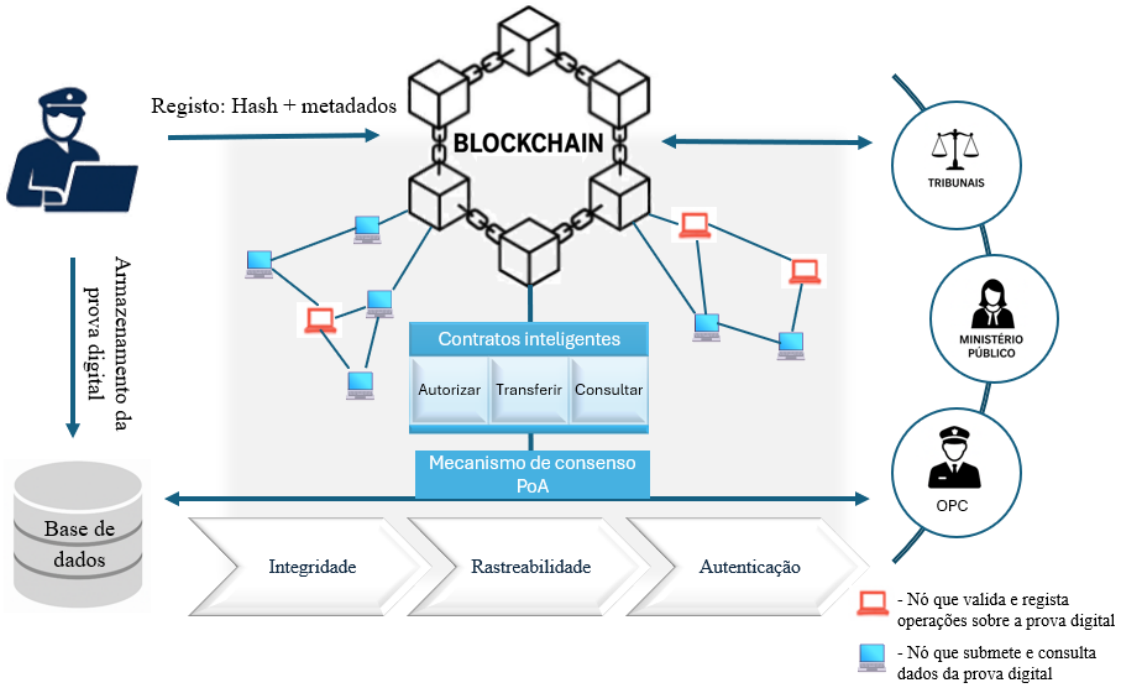
- Identidades e acesso: cada entidade dispõe de perfis institucionais com chaves digitais e permissões atribuídas segundo o princípio da necessidade de conhecer.

- Registo imutável: a blockchain atua como um registo único e partilhado, onde todos os eventos da cadeia de custódia são registados com data, hora e responsável.
- Governação automatizada: os contratos inteligentes aplicam as regras de forma automática; certas operações exigem validação conjunta; e todas as ações são auditáveis.
- Armazenamento: um cofre digital institucional armazena os ficheiros probatórios, enquanto a blockchain guarda apenas a respetiva impressão digital.
- Interoperabilidade: a plataforma integra-se com os sistemas judiciais existentes, como o *Citius*, garantindo continuidade processual.

A operacionalidade do modelo decorre em quatro fases: a aquisição, em que o polícia recolhe a prova, armazena-a numa base de dados segura, gera o respetivo *hash* e procede ao registo inicial na blockchain, onde fiam igualmente associados os metadados relevantes (identificação do policia que recolheu a prova, o local e o momento da recolha), criando assim o primeiro ponto de verificação de integridade; a transferência, onde os contratos inteligentes validam e registam a passagem da custódia entre entidades; a análise, fase em que apenas peritos autorizados acedem à prova mediante autenticação digital; e a apresentação em tribunal, em que o magistrado consulta diretamente a cadeia de custódia, e verifica a integridade do material probatório. Caso seja necessário aceder ao ficheiro original, o sistema gera *tokens* temporários de acesso e recalcula automaticamente o *hash* para confirmar a integridade.

Figura 1

Esquema do modelo conceptual da cadeia de custódia digital baseada em blockchain permissionada para a PSP e o sistema de justiça



Nota: O modelo ilustra o fluxo entre a recolha, armazenamento, registo e validação da prova digital. Os contratos inteligentes automatizam operações de autorização, transferência e consulta, enquanto o mecanismo de consenso *Proof of Authority* assegura a validação e integridade dos registos entre nós autorizados.

Fonte: Elaboração própria com base na literatura.

Em síntese, o modelo conceptual proposto reforça a integridade, autenticidade e rastreabilidade da prova digital, introduzindo ganhos de eficiência processual pela automatização proporcionada pelos contratos inteligentes. Do ponto de vista organizacional, promove interoperabilidade entre PSP, Ministério Público e os tribunais, superando a fragmentação tecnológica e processual vigente. Embora a sua implementação exija ajustamentos legislativos, investimento e formação especializada, constitui uma solução viável e alinhada com as melhores práticas internacionais, contribuindo para o reforço da confiança no sistema de justiça.

Atendendo à complexidade e ao carácter sensível das operações da prova digital, a implementação do modelo poderia iniciar-se através de um projeto-piloto, destinado a testar a arquitetura tecnológica, avaliar a interoperabilidade e identificar constrangimentos operacionais.

Um dos participantes destacou ainda a importância de envolver universidades e centros de investigação, aproveitando a sua capacidade técnica e científica para apoiar o desenvolvimento e a avaliação do sistema. Após a validação dos resultados e o ajustamento

dos procedimentos, o sistema poderá ser progressivamente alargado a todo o sistema de justiça, num processo faseado e sustentável de transformação digital.

5. Conclusão

A presente investigação demonstrou que o modelo tradicional de cadeia de custódia da prova digital, ainda assente em procedimentos manuais, suportes físicos frágeis e sistemas centralizados, apresenta fragilidades que comprometem a sua fiabilidade e credibilidade em sede judicial. As entrevistas realizadas, em consonância com a literatura especializada, evidenciaram riscos significativos associados ao fator humano, à ausência de uniformização de procedimentos e à vulnerabilidade tecnológica das soluções atualmente em vigor.

Face a estas limitações, a tecnologia blockchain, complementada por contratos inteligentes, surge como uma resposta inovadora e robusta. As suas propriedades de imutabilidade, rastreabilidade e auditabilidade permitem garantir a integridade e autenticidade da prova digital, introduzindo simultaneamente ganhos de eficiência processual e reforçando a confiança das instituições e dos cidadãos na justiça. A proposta conceptual desenvolvida neste estudo, baseada numa rede permissionada de acesso restrito às entidades envolvidas, revela-se tecnicamente viável, organizacionalmente desejável e alinhada com boas práticas internacionais.

Contudo, a adoção desta solução exige mais do que inovação tecnológica: requer um enquadramento jurídico adequado, interoperabilidade com sistemas já existentes, investimento em infraestruturas seguras e, sobretudo, um esforço de capacitação humana que minimize resistências à mudança. A experiência internacional indica que a implementação gradual, através de projetos-piloto e parcerias com universidades e centros de investigação, constitui o caminho mais realista para testar e consolidar esta transformação.

Confirma-se, assim, que as hipóteses formuladas neste estudo encontram respaldo nos resultados obtidos: o modelo atual de cadeia de custódia da prova digital apresenta fragilidades estruturais que comprometem a sua credibilidade, e a utilização da tecnologia blockchain, complementada por contratos inteligentes revela potencial para reforçar a integridade, a rastreabilidade e a aceitabilidade judicial da prova digital.

Reconhecendo as limitações deste estudo, de natureza essencialmente exploratória e baseado num número restrito de entrevistas, não abrangendo em profundidade a dimensão jurídico-normativa, importa assinalar linhas de investigação futura. Uma das mais relevantes

consiste na realização de um projeto-piloto em parceria com uma universidade, proposta também mencionada por um dos entrevistados, que permitiria avaliar, em ambiente controlado, a viabilidade técnica e organizacional do modelo conceptual aqui apresentado. Além disso, futuras investigações poderão aprofundar o impacto jurídico da integração da blockchain no processo penal e desenvolver análises comparativas entre diferentes OPC e em contextos internacionais.

Deste modo, este estudo não constitui um ponto de chegada, mas antes um contributo inicial para um debate amplo sobre a transformação digital da cadeia de custódia da prova digital em Portugal. Mais do que uma mera evolução tecnológica, representa um passo estratégico para modernizar a investigação criminal, promover maior interoperabilidade entre a PSP e o sistema de justiça e garantir que a prova digital resiste ao contraditório, preservando a verdade material e a confiança no Estado de Direito.

Referências

Alyas, T., Abbas, Q., Niazi, S., Alqahtany, S. S., Alghamdi, T., Alzahrani, A., Tabassum, N., & Ibrahim, A. M. (2025). Multi blockchain architecture for judicial case management using smart contracts. *Scientific Reports*, *15*(8471), 1–17. https://doi.org/10.1038/s41598-025-92842-8

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Weed Cocco, S., & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *EuroSys '18: Thirteenth EuroSys Conference* (pp. 1–15). ACM. https://doi.org/10.1145/3190508.3190538

Arm, M., Egipt, K., Hansen, R., Harjo, O., Hendrikson, M., Hänni, L., Kaidro, R., Kiirats, A., Krenjova-Cepilova, J., Nyman-Metcalf, K., Ott, A., Pedak, M., Reinsalu, K.,

Rikk, R., Roosna, S., Vahtra-Hellat, A., Vallner, U., & Viik, L. (2019). *E-Estonia: E-Governance in practice* (3rd updated ed.). e-Governance Academy. https://ega.ee/wp-content/uploads/2024/12/e-estonia-egovinpractice.pdf

Bardin, L. (2016). *Análise de conteúdo* (L. A. Reto & A. Pinheiro, Trads., 4.ª ed.). Edições 70.

Bonomi, S., Casini, M., & Ciccotelli, C. (2019). *B-CoC: A blockchain-based chain of custody for evidences management in digital forensics* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.1807.10359

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

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36,* 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Comissão Europeia. (2023). *Lawful evidence collecting and continuity platform development (LOCARD) — Reporting*. CORDIS. https://cordis.europa.eu/project/id/832735/reporting

Conselho da União Europeia. (2024). *Provas eletrónicas (e-evidence).* Conselho da União Europeia. https://www.consilium.europa.eu/pt/policies/e-evidence/

Comissão Europeia. (2025). *What is EBSI?* European Blockchain Services Infrastructure. https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/590447955/What+is+EBSI#infrastructure

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review, 2,* 6–19. https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

Daniele, M. (2011). *La prova digitale nel processo penale*. Rivista di diritto processuale, 66(2), 283–298. https://www.academia.edu/31481406/La_prova_digitale_nel_processo_penale

Decreto-Lei n.º 78/1987, de 17 de fevereiro. *Código de Processo Penal*. Diário da República, I.ª Série, 40. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1987-34570075-50565375

European Union Agency for Cybersecurity (ENISA). (2019). *Roadmap on CSIRT–LE cooperation.* ENISA. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Roadmap%20on%20CSIRT-LE%20Cooperation.pdf

Europol. (2022). *Facing reality? Law enforcement and the challenge of deepfakes: An observatory report from the Europol Innovation Lab*. Publications Office of the European Union. https://doi.org/10.2813/158794

Freire, J. P. (2022). *Blockchain e smart contracts: Implicações jurídicas*. Edições Almedina.

García Mateos, J. A. (2016). Cadena de custodia vs mismidad. In R. Oliva León & S. Valero Barceló (Coords.), *La prueba electrónica: validez y eficacia procesal* (1.ª ed., pp. 130–136). Colección Desafíos Legales.

Giova, G. (2011). *Improving chain of custody in forensic investigation of electronic digital systems*. *International Journal of Computer Science and Network Security,* 11(1), 1–9. https://www.researchgate.net/publication/267400650_Improving_Chain_of_Custody_in_Forensic_Investigation_of_Electronic_Digital_Systems

Gopalan, S. H., Suba, S. A., Ashmithashree, C., Gayathri, A., & Andrews, V. J. (2019). Digital forensics using blockchain. *International Journal of Recent Technology and Engineering, 8*(2S11), 182–184. https://doi.org/10.35940/ijrte.B1030.0982S1119

Government of Dubai Media Office. (2024, 13 de junho). *Dubai Police employs artificial intelligence in police and security operations*. https://mediaoffice.ae/en/news/2024/june/13-06/dubai-police-employs-artificial

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), 118–127. https://www.researchgate.net/publication/341913793_The_Truth_About_Blockchain

International Organization for Standardization. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence* (Norma ISO/IEC n. º 27037:2012). https://www.iso.org/standard/44381.html

Khan, A. A., Uddin, M., Shaikh, A. A., Laghari, A. A., & Rajput, A. E. (2021). MF-Ledger: Blockchain Hyperledger Sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture. *IEEE Access, 9,* 103637–103650. https://doi.org/10.1109/ACCESS.2021.3099037

Lei n.º 109/2009, de 15 de setembro. *Lei do Cibercrime*. Diário da República, I.ª Série, 179. https://diariodarepublica.pt/dr/detalhe/lei/109-2009-489693

Lillis, D., Becker, B. A., O'Sullivan, T., & Scanlon, M. (2016). *Current challenges and future research areas for digital forensic investigation*. In *Annual ADFSL Conference on Digital Forensics, Security and Law, 2016* (pp. 6). ADFSL. https://commons.erau.edu/adfsl/2016/tuesday/6

Lumivero. (2025). *NVivo 15* [Software de computador]. https://lumivero.com/products/nvivo/

Marques, P. P. L. C. (2013). *Informática forense: Recolha e preservação da prova digital* (Dissertação de mestrado, Universidade Católica Portuguesa). Universidade Católica Portuguesa.

Martins, P. (2018). *Introdução à blockchain bitcoin: Criptomoedas, smart contracts, conceitos, tecnologia, implicações*. FCA – Editora de Informática.

McFarland, E. (2023). *O futuro da internet e a revolução blockchain*. Alma dos Livros.

Militão, R. L. (2012). A propósito da prova digital no processo penal. *Revista da Ordem dos Advogados, 72*(1), 247–285.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* https://nakamotoinstitute.org/library/bitcoin/

Preukschat, Á. (2018). Los fundamentos de la tecnología blockchain. In A. Preukschat (Coord.), C. Kuchkovsky, R. Fernández Hergueta, & I. Molero, *Blockchain: La revolución industrial de internet* (2.ª ed., pp. 29-36). Editorial Planeta Colombiana, S.A.

Van Campenhoudt, L., Marquet, J., & Quivy, R. (2019). *Manual de investigação em ciências sociais* (I. Lopes, Trad.; tradução da 5.ª ed. francesa). Gradiva. (Obra original publicada em 2017)

Ramos, A. D. (2014). *A prova digital em processo penal* (1.ª ed.). Chiado Editora.

Ramos, A. D. (2015). *Os meios de prova a partir da internet e das redes sociais no processo penal*. IX Encontro Nacional do IAPI. https://portal.oa.pt/media/119968/os-meios-de-prova-a-partir-da-internet-e-das-redes-sociais-no-processo-penal.pdf

Reith, M., Carr, C., & Gunsch, G. (2002). *An examination of digital forensic models. International Journal of Digital Evidence,* 1(3), 1–12.

Rodrigues, B. S. (2009). *Direito penal: Parte especial. Tomo I. Direito penal informático-digital*. Coimbra Editora.

Rodrigues, B. S. (2011). *Da prova penal: Tomo IV. Da prova eletrónico-digital e da criminalidade informático-digital*. Rei dos Livros.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York, NY: Free Press.

Rubio Alamillo, J. (2016). Conservación de la cadena de custodia de una evidencia informática. *Diario La Ley, 8859*. Wolters Kluwer.

Szabo, N. (1994). *Smart contracts*. Nakamoto Institute. https://nakamotoinstitute.org/library/smart-contracts/

Thamay, R., & Tamer, M. (2020). *Provas no direito digital: Conceito da prova digital, procedimentos e provas digitais em espécie*. Thomson Reuters Revista dos Tribunais.

Tong, A., Sainsbury, P., & Craig, J. (2007). *Consolidated criteria for reporting qualitative research (COREQ): A 32-item checklist for interviews and focus groups*. *International Journal for Quality in Health Care, 19*(6), 349–357. https://doi.org/10.1093/intqhc/mzm042

Tribunal da Relação de Évora. (2024). Acórdão Processo n.º 351/23.6JAFAR.E1. https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/860d36d059c0111680258be20035bfb8

Tribunal da Relação de Lisboa. (2025). Acórdão Processo n.º 379/17.5PCCSC.L1-5. https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/0a9bc8ae58e246c780258c2100437705?OpenDocument

Tribunal da Relação do Porto. (2015). Acórdão *Processo n.º* 367/13.0PAOVR.P1.http://www.gde.mj.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/96176bb8de63445680257e4b0033138d?OpenDocument

Tsai, F. C. (2021). The application of blockchain of custody in criminal investigation process. *Procedia Computer Science, 192*, 2779–2788. https://doi.org/10.1016/j.procs.2021.09.048

Valente, M. M. G. (2020). *Cadeia da custódia da prova* (2.ª ed.). Almedina.

Vermont Legislature. (2024). *12 V.S.A. § 1913*. Vermont Statutes Online. https://legislature.vermont.gov/statutes/section/12/081/01913

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview* (NISTIR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

Apêndices

Apêndice A - Termo de consentimento livre e esclarecido

Por favor, leia com atenção a seguinte informação. Se achar que algo está incorreto ou que não está claro, não hesite em solicitar mais informações. Se concorda com a proposta que lhe foi feita, queira rubricar e assinar este documento.

Título do Estudo: Blockchain e Contratos Inteligentes na Garantia da Cadeia de Custódia da Prova Digital: Uma Proposta de Integração Tecnológica entre PSP e o Sistema de Justiça

Investigador Responsável: Paulo Jorge dos Santos Costa

Instituto Superior de Ciências Policiais e Segurança Interna – VI Curso de Comando e Direção Policial

Objetivo do Estudo:

Este estudo pretende analisar o potencial da tecnologia blockchain e dos contratos inteligentes na cadeia de custódia da prova digital, identificando fragilidades do modelo atual, explorando soluções inovadoras e avaliando a viabilidade da sua integração entre a PSP e o sistema de justiça.

Procedimento:

O(a) participante será convidado(a) a responder a uma entrevista semiestruturada, com a duração aproximada de 30–40 minutos. A entrevista será gravada em áudio (se autorizado) e posteriormente transcrita, sendo todos os dados tratados de forma confidencial.

Garantias ao Participante:

- A participação **é voluntária e** pode ser interrompida a qualquer momento, sem qualquer prejuízo.
- As respostas serão utilizadas apenas para fins académicos e científicos, garantindo-se a anonimização dos dados (nenhum nome ou dado identificativo será divulgado). Cada participante será identificado apenas por um código neutro.
- Os registos (áudio e transcrições) serão armazenados em suporte seguro e eliminados após a conclusão da investigação.

- Não existem riscos previsíveis decorrentes da participação, nem compensações financeiras envolvidas.

Consentimento:
Declaro que fui informado(a) sobre os objetivos e procedimentos do estudo, que compreendi as informações apresentadas e que participo de forma livre e esclarecida.
Local e Data: _____
Assinatura do(a) Participante: _____
Assinatura do Investigador: _____

Apêndice B - Caracterização dos participantes

A tabela seguinte apresenta a caracterização sumária dos entrevistados que integraram a amostra do estudo. Para garantir o anonimato, cada participante foi identificado por um código alfanumérico (E1, E2, …), não sendo revelado nomes. Apenas se indica o grupo profissional de enquadramento, suficiente para evidenciar a diversidade de perspetivas recolhidas.

Tabela 3

Caracterização dos participantes da amostra (códigos e grupos profissionais)

Código	Grupo profissional
E1	PSP
E2	PSP
E3	PSP
E4	Académico
E5	Académico
E6	Académico/Jurista
E7	Magistrado Judicial
E8	Magistrado MP
E9	PSP
E10	Magistrado MP
E11	Magistrado Judicial

Fonte: elaboração própria

Apêndice C - Guião da entrevista

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?

Bloco 2 – Problemas no modelo atual

2. Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?

3. Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?

Bloco 3 – Perceções sobre tecnologia

4. Está familiarizado com o conceito de blockchain e contratos inteligentes?

5. Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?

Bloco 4 – Implementação e desafios

6. Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?

7. Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?

Bloco 5 – Visão de futuro

8. Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?

9. Que vantagens práticas esperaria de um sistema com estas características?

10. Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?

Apêndice D - Transcrição das entrevistas

Entrevista: E1

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. **Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?**

   R: Não tenho qualquer experiência ou contacto.

Bloco 2 – Problemas no modelo atual

2. **Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?**

   R: Não consigo identificar as fragilidades porque não conheço o modelo.

3. **Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?**

   R: Não.

Bloco 3 – Perceções sobre tecnologia

4. **Está familiarizado com o conceito de blockchain e contratos inteligentes?**

   R: Sim.

5. **Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?**

   R: Sim. Porque incutirão maior confiança aos polícias e aos demais intervenientes no processo (criminal).

Bloco 4 – Implementação e desafios

6. **Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?**

   R: Custo de implementação; falta de literacia nas tecnologias em apreço; custo de manutenção.

7. **Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?**

R: investimento estruturado e financeiramente sustentável; integração das várias entidades do sistema judicial no projeto, para corresponder a todas as necessidades e expetativas; alavancagem das competências técnicas e da literacia digital ao nível técnico (TIC) e ao nível de exploração (polícias e demais atores)

Bloco 5 – Visão de futuro

8. **Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?**

R: Sim, desde que cumpridas as condições referidas em 7

9. **Que vantagens práticas esperaria de um sistema com estas características?**

R: digitalização de procedimentos, incremento da segurança na interoperabilidade de informação criminal, melhor serviço público.

10. **Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?**

R: Não

Entrevista: E2

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. **Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?**

R: A minha experiência nesta área já tem uns aninhos — daí também alguns cabelos brancos que se notam. Desde o início, quando se pensou em criar um laboratório na polícia, sempre tivemos presente a importância de considerar todas as questões relacionadas com a prova digital, fosse ela produzida como prova pericial ou, pelo menos, no âmbito de um exame de apreciação técnico-forense. Estas duas vertentes obrigam-nos, desde logo, a refletir sobre todos os aspetos que podem colocar em causa a validade da prova durante o processo, em qualquer das suas fases.

A nossa principal preocupação sempre foi garantir que tudo o que fazemos assenta no princípio da legalidade e no cumprimento rigoroso dos protocolos forenses. A prova que tratamos é disponibilizada a quem, em cada momento processual, tem legitimidade para a conhecer. Esta prática sistemática tem sido fundamental para consolidar uma experiência que se foi alargando ao longo dos anos.

Trabalho nesta área desde cerca de 2009, altura em que surgiram as primeiras preocupações estruturadas com estas matérias. Desde então, fomos todos aprendendo, processo após processo, contacto após contacto com operadores judiciários e magistrados. Muitas vezes houve debate, até divergência, mas nunca deixámos de defender, com firmeza, mas também com abertura, aquilo que entendemos ser a prática correta. E, em muitos casos, as próprias magistraturas acabaram por reconhecer a validade dos nossos procedimentos, precisamente porque a nossa atuação sempre teve como objetivo que a prova produzida fosse robusta, fiável e resistente a qualquer contestação.

Como dizia a Dra. Maria José Morgado, quando estava no DIAP de Lisboa, a prova tem de resistir ao contraditório em julgamento. E quando resiste, é porque foi bem construída. Essa tem sido, em suma, a nossa linha de atuação e o resultado de muitos anos de experiência, que continuam a ser também um espaço constante de aprendizagem.

Bloco 2 – Problemas no modelo atual

2. **Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?**

R: Fragilidades existem sempre, e é precisamente conhecendo as nossas vulnerabilidades que conseguimos corrigi-las, reforçar os procedimentos e evitar erros. Essa

tem sido também a nossa experiência ao longo do tempo: perceber onde podemos melhorar, para que a prova nunca seja contaminada nem sujeita a práticas incorretas.

Assim, quando a prova chega ao Ministério Público, ao juiz de instrução ou, mais tarde, ao tribunal de julgamento, já passou por um processo rigoroso de preservação e tratamento. Isso dá-nos hoje uma maior capacidade de resposta e uma margem cada vez menor de erro.

Isso dá-nos hoje uma maior capacidade de resposta e uma margem cada vez menor de erro. As principais vulnerabilidades que ainda podem subsistir não se prendem tanto com o que está implementado no laboratório — onde considero que as garantias são robustas e todas as portas estão fechadas a qualquer possibilidade de contaminação — mas sobretudo com aspetos externos, que muitas vezes não dependem diretamente de nós.

O que me preocupa é que as vulnerabilidades que possam existir têm a ver muitas das vezes com as falhas humanas. A prova começa essencialmente naquilo que são os cenários de crime que vocês na investigação criminal primeiro abordam. Quem primeiro tem o contacto com aquilo que é um cenário e que não preserva como deve ser pode vir a contaminar tudo aquilo que é posteriormente realizado. E, até, colocar em crise, aquilo que a posteriori pode vir a ser realizado. E, portanto, as vulnerabilidades prendem-se, a meu ver, essencialmente no momento em que há o primeiro contacto com a prova.

Se não forem cumprirmos os protocolos que estão determinados a toda a estrutura da investigação criminal e a toda a rede nacional de polícia técnica e forense e se houver falhas e contaminações logo numa fase inicial, vamos ter muito problema a seguir. Esta é uma vulnerabilidade. Outra vulnerabilidade, embora não esteja diagnosticada no nosso sistema, é o facto de os nossos recursos humanos, sejam eles técnicos, peritos, investigadores criminais, comandantes, subordinados, não estarem capazes e não perceberem qual é que é o melindro do que nós estamos a falar e qual é que é a responsabilidade que nós todos temos que ter naquilo que é a cadeia de custódia da prova.

Portanto, vulnerabilidades verificam-se essencialmente, como em todas os trabalhos e todas as circunstâncias, no procedimento humano, ou seja, naquilo que está obrigado a fazer e que às vezes, por facilitismo há falhas.

Os nossos técnicos forenses, quando abordam um cenário, estão preparados, tem informação específica para isso, estão preparados para abordar todo o tipo de prova, todo o tipo de vestígio e todo o tipo de evidência.

Depois, ela é encaminhada para o setor laboratorial respetivo e é tratada pericialmente por esse mesmo setor ao nível da sua cientificidade. Portanto, todo o

procedimento, desde a sua recolha, entrega e saída do laboratório implica o cumprimento de um protocolo específico.

Se eu tiver uma evidência digital, eu tenho um determinado protocolo que me diz como é que eu devo proceder para não contaminar, porque se eu a contamino, eu já estou a quebrar a cadeia de custódia.

Por isso é que temos de ter uma visão holística do manancial probatório no processo de investigação criminal, temos que ir buscar todos os procedimentos quer dos técnicos forenses, quer dos investigadores, dos peritos e também das autoridades judiciárias.

3. Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?

R: Sim, já houve caso, aliás, temos de estar preparados, por isso é que eu digo que a prova tem de ser realizada sobre todos os pressupostos de legalidade, sobre todos os protocolos forenses que temos em vigor para que ela não possa ser atacada pelo contraditório, quer seja em fase de inquérito ou em fase de julgamento, onde o contraditório tem o verdadeiro músculo.

Como tenho vindo a alertar os meus alunos, temos de preparar todo o processo de inquérito, não para conseguirmos um despacho de acusação, mas para conseguirmos que em sede de julgamento a prova possa ser inatacável, quer ela vá descobrir a verdade no sentido de absolver os arguidos, ou quer ela vá na descoberta da verdade para condenar os arguidos.

O que me interessa é que tudo aquilo que investiguei chegue a julgamento e seja inatacável e resista ao contraditório. Se ela resistir, é porque foi bem feita.

Agora, todos os dias, vemos prova a cair nos nossos tribunais. Não tem a ver connosco, nem com a organização, nem com o laboratório. Felizmente, do nosso lado, não temos tido, mas temos aí grandes operações que são atacadas em julgamento pela forma como se chega à prova. Ao não cumprimos os pressupostos legais a prova é considerada proibida e o processo cai.

E é sobre isso que eu ando há quase vinte anos a dizer que não pode ser por aí. O caminho tem de ser sempre pela legalidade, pela estrita objetividade e por apresentar uma prova cristalina que resista ao contraditório do julgamento.

Bloco 3 – Perceções sobre tecnologia

4. Está familiarizado com o conceito de blockchain e contratos inteligentes?

R: Ora bem, a blockchain é conhecida essencialmente como uma cadeia de informação. Porque ela surgiu no âmbito das criptomoedas e toda a segurança de não acesso a toda essa informação. Portanto, podemos dizer que é um bloco de proteção dessa informação.

5. Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?

R: Nada é garantidamente protegido.

Eu aqui há dois anos tive o prazer de orientar uma tese de mestrado de um aluno sobre a blockchain e sobre a capacidade de quebrar a blockchain. E provou-se, claramente, que é possível quebrar a blockchain. Não vamos agora aqui discutir esse pormenor, mas isso é possível.

Isso leva-nos a pensar que não há garantias absolutas de segurança. Agora, se falarmos de um contrato inteligente ao nível de uma suposta arquitetura que vá buscar características da blockchain para a segurança digital - Perfeitamente. Isso é perfeitamente entendível e será claramente, quando possível, uma mais-valia. Dizer, no entanto, que aquilo que nós fazemos neste momento para assegurar a cadeia de custódia da prova no âmbito digital vai mais além do que aqueles relatórios da cadeia de custódia em formato físico, mas a prova digital não é só isso. Ela tem uma cadeia de custódia bem mais importante que está em ambiente digital.

Nós já podemos falar muitas vezes em encriptação e é isso que nós fazemos. Os processos quando vão para o tribunal, vão encriptados e, portanto, os relatórios periciais vão numa parte física, mas o grosso e o mais importante da prova está em digital e encriptada. Nesses casos tem de haver um processo de desencriptação no destinatário, que pode ser o Ministério Público ou o Juiz de instrução.

E, portanto, nós temos aqui, claramente, uma cadeia de custódia digital. A física, no fundo, é a entrega do suporte físico ao circuito de pessoas que a manuseiam, mas, aquilo que é a informação digital vai claramente bloqueada, ou seja, já tem uma cadeia de segurança.

Agora se me diz, que há aí uns contratos de segurança que vão buscar características da blockchain para a segurança, perfeitamente de acordo.

Uma coisa é a tecnologia forense, com tremendas característica, outra coisa diferente é a tecnologia. Muitas vezes quem produz os equipamentos forenses está atento a essas novas tecnologias e incorpora na tecnologia forense já existente todas essas medidas de novidade ao nível tecnológico. Ou seja, quando vem à nossa procura para nos explicar as novidades,

nós conseguimos perceber que no mesmo equipamento que tínhamos um determinado tipo de segurança há 10 anos, hoje tem uma segurança totalmente diferente e a segurança que comprarmos hoje, daqui a dois meses está a ser atualizada com novas regras de segurança.

Portanto eu considero que todas essas formas novas de cadeia de custódia da prova, nomeadamente em ambiente digital, os próprios equipamentos desde que forenses, eles vão começar a incorporar cada vez mais segurança a esse nível. Portanto será necessário nós isoladamente comprarmos uma ferramenta para garantir a cadeia de custódia da prova em ambiente digital que já foi produzida por um equipamento forense que já tem parte dessa segurança? Vale a pena? Pergunta-me e eu digo que honestamente não sei.

Só analisando. Só verificando se aquilo que é a novidade de uma ferramenta própria só para fazer segurança da informação se justifica e se por acaso não é até mais rudimentar do que aquela que já existe nos equipamentos forenses.

Eu neste momento não tenho essa resposta para lhe dar em concreto porque não a conheço e não sei se é pior ou se é melhor do que a que já existe nos nossos equipamentos forenses. Pode ser mais rudimentar e não seguir os protocolos forenses, que são rígidos e complexos.

Portanto não há qualquer hipótese de manipular a prova em ambiente digital sem deixar rastro. O perito sabe que quando faz e cria os códigos de segurança naquela informação, se ela for acedida, o código quando for acedido já não é o mesmo, já é outro qualquer.

Os comunicados técnicos forenses que são emanados pelo laboratório são de comprimento absoluto. Mesmo quando alguém entrega uma prova digital numa Esquadra, por exemplo um vídeo, ela tem que seguir os protocolos e a partir daí ela está salvaguardada.

Os equipamentos dão garantias de segurança e por isso são caros. Se for atacado eu consigo provar que alguém teve acesso. Com a encriptação que é feita, os ficheiros vão à parte das passwords, vai tudo selado e se alguém desselar tem que justificar porque é que quis aceder e se depois já sabemos que esta prova foi contaminada no dia X às X horas quando ela tinha que estar intacta do dia anterior em Y horas.

Bloco 4 – Implementação e desafios

6. Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?

R: Não lhe posso responder claramente a essa questão por não conhecer a ferramenta.

Imaginando que é uma ferramenta que isoladamente pega na informação a bloqueia, que no fundo lhe dá garantias de segurança para o transporte e é ajustável aos procedimentos forenses sem os pôr em causa, será uma mais-valia.

Relativamente à comunicação com o Ministério Público nós temos aí outro tipo de projetos que estamos a desenvolver precisamente para uma outra visão de século XXI.

7. Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?

R: Dependerá claramente dos requisitos da tecnologia, se é uma tecnologia que trabalha em rede ou se é uma tecnologia que requer uma rede fixa.

Temos como projeto já há mais de 10 anos, por mim proposto, a criação de uma rede interna laboratorial, que na altura custava cerca de 300 mil euros.

Com este projeto conseguíamos ter o laboratório central e todos os laboratórios periféricos a trabalhar em rede e a grande vantagem era maior segurança na informação, mais contacto direto entre a rede nacional de peritos que operam nos vários polos. Outra vantagem era em vez de termos de comprar 7 licenças forenses comprávamos apenas uma ou duas. Estas ficavam no laboratório central e dentro dessa rede dedicada e segura o perito do Porto, de Faro, dos Açores, da Madeira, de Lisboa etc … acedia por uma VPN à ferramenta forense que está aqui no laboratório central.

A dificuldade é implementar um sistema desses, que não trabalhe dentro da RNSI, é a necessidade de criar um sistema em rede que permita que essa e outras ferramentas forenses trabalhem dentro desta segurança e desta característica da Blockchain.

Bloco 5 – Visão de futuro

8. Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?

R: Acredito que sim, mas avaliando aquilo que aconteceu nos últimos 15 anos, 20 anos tenho muita dificuldade em perceber porque aqui ainda não está montado. Se repararmos, cada polícia, o próprio Ministério Público e cada organização gosta de ter a sua própria rede, o seu sistema e depois temos de andar com interoperabilidade entre os sistemas, o que dificulta sempre coisa diferente.

Se tivéssemos um sistema único onde toda a gente pudesse trabalhar de igual forma e por perfis de acesso conseguíamos ter uma maior coordenação com o Ministério Público e todas as outras polícias.

Nós temos um projeto na área forense, para incorporar dentro do PESI 2, vamos ter um módulo forense que permite essencialmente fazer com que o técnico forense com um tablet, num cenário de crime, faça a inspeção judiciária, recolha todos os vestidos que tem a recolher e possa carregar informação, através de um check list no seu tablet. Se houver internet no local a informação é logo carregada no sistema central. Se não houver internet, ela é carregada posteriormente em BackOffice. A grande vantagem deste sistema é que as pessoas da investigação criminal requisitam logo uma inspeção judiciária a um determinado local, dentro do próprio sistema, através de um formulário que é recebido pelas equipas de inspeção. Essas equipas avançam para o terreno, fazem a inspeção e todos os vestígios que elas apreendem são enviados ao laboratório para o setor respetivo e o laboratório já sabe que vai ter trabalho para fazer.

É preciso envolver o Ministério Público neste sistema para que o pedido da ordem de perícia ao procurador, a resposta e o envio da perícia ao Ministério Público seja célere, e sem ninguém andar a entregar nada a ninguém. Isto corre tudo em ambiente digital, com todas as garantias de segurança. Se a prova tiver que ser do conhecimento do Juiz de Instrução ele tem de ser envolvido nisto. Este sistema também devolve relatórios estatísticos como perícias pendentes. No fundo, tem-se um conhecimento de toda a rede forense a nível nacional. Este é o futuro que tem de ser implementado.

9. Que vantagens práticas esperaria de um sistema com estas características?

R: No projeto que temos pensado, *LIMS* laboratorial (labway-lims.) existem muitas vantagens. Desde logo celeridade processual, que é o que todos queremos, por outro lado muito mais segurança e certeza no circuito da prova, na cadeia de custódia. A todo o momento podemos ir ao sistema e vemos o que está a ser feito. No sistema da Blockchain, as vantagens são idênticas. As vantagens do conhecimento simultâneo do Ministério público ou juiz de instrução, no fundo do sistema de justiça (procurador, técnico forense, OPC, Juiz de Instrução e Juiz de Julgamento). E se todos estiverem num sistema e se souberem conduzir aquele carro, é um carro igual para todos, e todos o sabem conduzir. O que nós temos hoje é que temos vários carros e cada um conduz o seu, todos diferentes e ninguém sabe conduzir o carro do vizinho.

Temos de ter um sistema em Portugal que consiga funcionar para todas as polícias em que toda a gente comunica com toda a gente. Isto só tem benefícios para todos. Têm é de todos estar cientes que trabalham todos na mesma máquina ou da mesma maneira. O futuro pode ser melhor se todos alinharem na coordenação entre todos. É colocar o interesse do país à frente e deixar os interesses corporativos.

Com um sistema assim o Ministério Público consegue controlar a morosidade, dar instruções e enviar as ordens de perícia de forma rápida. Isto é sem dúvida uma evolução brutal no sistema de justiça em Portugal.

Quando se diz que a justiça está mal é porque não tem sistemas a funcionar desta maneira. Cada um tem o seu sistema e não comunicam entre eles e quando comunicam, comunicam mal. Tudo o que seja segurança da informação, quer seja das características da blockchain, quer seja envolver todos os operadores do sistema de justiça só pode melhorar a justiça. Isso é uma mais-valia brutal.

10. **Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?**

    R: Mais nada.

Entrevista: E3

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. **Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?**

R: Enquanto Diretor de Departamento, tenho naturalmente contacto com estas matérias. Não trabalho diretamente com a prova digital, mas conheço os procedimentos adotados e a forma como é tramitada dentro da PSP.

Bloco 2 – Problemas no modelo atual

1. **Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?**

R: Existe uma fragilidade relevante que obriga frequentemente a afetar recursos adicionais no terreno. Muitas unidades que realizam apreensões locais não têm capacidade para assegurar a custódia adequada da prova, de acordo com os padrões exigidos. Nessas situações, é necessário mobilizar elementos do laboratório para apoiar as unidades de investigação, garantindo que a custódia é devidamente assegurada desde o início, por peritos especializados.

2. **Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?**

R: Formalmente, nunca tivemos conhecimento de contestação. Ocorrem, sim, algumas dificuldades pontuais, que são normalmente esclarecidas pelos nossos peritos. Trata-se sobretudo de problemas de interpretação. Muitas vezes, o técnico que procede à recolha é o único que compreende a estrutura da informação apreendida. Os informáticos têm capacidade para organizar e armazenar os dados de determinada forma, mas essa lógica nem sempre é facilmente entendida por terceiros. Assim, o técnico que apreende acaba frequentemente por apoiar a autoridade judiciária, mas isto não configura uma contestação da cadeia de custódia, apenas uma dificuldade de interpretação.

Bloco 3 – Perceções sobre tecnologia

3. Está familiarizado com o conceito de blockchain e contratos inteligentes?

R: Apenas na vertente associada às criptomoedas. Não sou investidor, mas acompanho ocasionalmente o tema e sei que se trata de um sistema que permite a rastreabilidade total de todas as operações realizadas sobre esse ativo.

4. Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?

R: Sim, penso que podem, tanto no âmbito da prova digital como de outros tipos de prova. Num processo-crime é fundamental que, a partir de qualquer interpretação da prova, seja sempre possível regressar à sua posição original. No caso da prova digital, por exemplo, quando um computador é apreendido, é necessário garantir que se conhece exatamente o seu estado no momento da apreensão. A manipulação e a extração de informação deixam naturalmente rastos, pelo que é essencial assegurar a possibilidade de identificar o estado inicial. Esse é, atualmente, o fator mais relevante, pois garante a fiabilidade da prova.

Bloco 4 – Implementação e desafios

5. Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?

R: O principal obstáculo são os custos, que poderão ser significativos. A área da prova digital exige investimentos cada vez maiores e essa tendência tende a agravar-se no futuro. Outro desafio é a necessidade de uniformização de procedimentos. Atualmente, cada OPC trabalha com as ferramentas que consegue adquirir, mas as autoridades judiciárias acabam por lidar com formatos e métodos diferentes. A definição de padrões uniformes para todos os OPC seria fundamental, mas constitui um obstáculo adicional, a par dos custos.

6. Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?

R: Em primeiro lugar, é necessária a uniformização de procedimentos. Além disso, é essencial que as estruturas tecnológicas das forças de segurança, no caso da PSP, tenham consciência da importância do investimento nesta área. Muitos avanços têm sido possíveis graças ao apoio da Direção e da Segurança Interna, mas este investimento deve ser entendido como uma prioridade nacional, e não apenas institucional. Melhorar a justiça e melhorar o serviço prestado pelo Estado ao cidadão. Essa consciencialização ainda não existe de forma plena, mas é fundamental para possibilitar investimentos consistentes nestas ferramentas.

Bloco 5 – Visão de futuro

7. Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?

R: Não sei se especificamente com esta tecnologia, mas uma ferramenta que permita essa partilha terá necessariamente de ser viável. Atualmente já existem algumas ligações entre a PSP e o Ministério da Justiça, mas limitam-se ao envio de informação, e não à partilha de prova digital. O que defendemos há vários anos é a bidirecionalidade: que muitas diligências, ainda feitas em papel e entregues em mão, possam ser transmitidas eletronicamente. A prova digital poderá ser uma dessas áreas. Talvez não na totalidade, devido ao grande volume de dados, mas através de acessos controlados à prova no local onde ela se encontra armazenada. Com registo em blockchain, seria possível saber quem acedeu, quando e porquê.

8. Que vantagens práticas esperaria de um sistema com estas características?

R: A principal vantagem seria a maior fidedignidade da prova, o que é o mais relevante. Além disso, permitiria alguma poupança de trabalho, também essencial.

9. Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?

R: Não tenho mais nada a acrescentar.

Entrevista: E4

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. **Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?**

R: Tenho contacto com o tema apenas teórico: lecionei algumas vezes uma cadeira relacionada com o assunto no Instituto Superior Técnico, no qual sou professor. A cadeira chama-se Ciber Segurança Forense e tem precisamente que ver com recolha, preservação e análise de prova digital. Nessa cadeira tive vários convidados a falar sobre casos práticos, nomeadamente inspetores da Polícia Judiciária.

Bloco 2 – Problemas no modelo atual

2. **Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?**

R: Penso que a pergunta se refere especificamente ao modelo usado em Portugal que eu não conheço em detalhe. Em todo o caso, parece-me que o modelo actual usado quase universalmente pode ser comprometido por pessoas que tenham acesso privilegiado aos dados dessa cadeia ("malicious insiders"), por exemplo modificando dados e os correspondentes hashes. Também existe, obviamente, risco de um ataque externo ("hacking").

3. **Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?**

R: Não

Bloco 3 – Perceções sobre tecnologia

4. **Está familiarizado com o conceito de blockchain e contratos inteligentes?**

R: Sim. Faço investigação, ensino e tenho alguma experiência como consultor/conselheiro na área. há muitos anos. Coordenei o grupo de trabalho que produziu a estratégia nacional de Web 3 (que não foi publicada pelo governo).

5. **Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?**

R: Sim. O uso de contratos inteligentes executados num sistema blockchain permite guardar os hashes dos elementos de prova digital (por exemplo, de cópias bitstream de um disco) de forma a que todas as alterações fiquem registadas e esse registo seja muito difícil de modificar sem existir um conluio de várias pessoas de entidades diferentes. Para a tecnologia ser eficaz, teriam de existir vários nós/réplicas/computadores da blockchain administradas por pessoas diferentes, se possível em organizações diferentes (por exemplo, IGFEJ, informática de várias polícias nacionais, outros ministérios). Ou seja, é importante existir uma descentralização real.

Bloco 4 – Implementação e desafios

6. **Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?**

R: Lendo a última frase que escrevi acima, os obstáculos são óbvios: desafios organizacionais e de custos associados à descentralização organizacional e de administração. Mas essa descentralização também implica governo dessa infraestrutura descentralizada, o que é complexo quando há várias entidades envolvidas.
Outro desafio é o desconhecimento da tecnologia e dos seus potenciais benefícios. As organizações em causa podem ser renitentes em adoptar uma tecnologia que conhecem mal.

7. **Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?**

R: Acabei por responder acima: descentralização organizacional e de administração.

Bloco 5 – Visão de futuro

8. **Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?**

R: Sim, apesar dos desafios que mencionei acima.

9. **Que vantagens práticas esperaria de um sistema com estas características?**

R: A grande vantagem seria a segurança oferecida, ou seja, a redução do risco de comprometimento da cadeia de custódia. Seria preciso um conluio de várias pessoas de diferentes entidades e conhecimentos técnicos avançados para o conseguir.

10. **Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?**

R: Proposta para a PSP e sistema de justiça - Uma blockchain permissioned, p.ex. baseada no software Hyperledger Fabric, Hyperledger Besu ou Canton, com um nó em cada entidade. Essa blockchain executa um ou mais smart contracts que armazenam os metadados da cadeia de custódia, que incluem o hash de cada um dos elementos de prova digital, entre outros metadados. É preciso software cliente para registar e consultar as cadeias de custódia, bem como auditar a sua integridade.

A solução descrita permite detetar quebras de integridade da cadeia de custódia. Para garantir a disponibilidade da cadeia de custódia, é preciso também guardar uma cópia de cada elemento de prova nas diversas entidades.

O uso de tecnologia de identidade digital auto-soberana (SSI), como DIDs e VCs, bem como assinaturas digitais qualificadas, pode também fazer parte da solução, com o fim de identificar as pessoas e entidades envolvidas (p.ex. a pessoa que produziu cada elemento de prova).

Entrevista: E5

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. **Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?**

R: Eu não trabalhei diretamente com provas forenses no âmbito da justiça, mas tive experiência em projetos de desenvolvimento de sistemas de rastreabilidade da cadeia de valor — que é um exemplo semelhante ao que foi referido há pouco.

Um desses projetos em que estive envolvido tinha a ver com a vinha e procurava responder a uma questão simples: quando alguém compra, por exemplo, uma garrafa de Vinho do Porto de 100 ou 150 euros, como é que pode ter a certeza de que as uvas utilizadas provêm, de facto, de uma vinha específica, como a Maria Teresa, da Quinta do Crasto? A realidade é que, normalmente, temos apenas a palavra do produtor.

O objetivo do projeto era criar garantias adicionais. Assim, logo no momento da vindima, as uvas eram pesadas e georreferenciadas no local, tiravam-se fotografias e registava-se a sua classificação. Esse era o primeiro passo da cadeia de valor e funcionava como a primeira prova documental.

Depois, em todas as fases seguintes — transporte, esmagamento, fermentação, estágio em cubas de carvalho, até ao engarrafamento — eram monitorizados automaticamente vários parâmetros, como volume produzido, temperatura ou condições de armazenamento. Todos esses registos eram armazenados em blockchain, garantindo que não podiam ser adulterados.

No final, cada garrafa chegava ao mercado com um QR Code. Ao aceder a esse código, o consumidor podia consultar todo o histórico de produção daquele vinho e verificar, por exemplo, quantas garrafas foram efetivamente produzidas a partir daquele lote. Isso impedia que, se tivessem sido recolhidos 1000 litros de vinho, surgissem de repente 5000.

Resumindo, o sistema criava uma cadeia de evidências digitais que assegurava a autenticidade do processo. O meu envolvimento foi sobretudo neste tipo de soluções, mais ligadas à rastreabilidade e à transparência na cadeia de valor.

Bloco 2 – Problemas no modelo atual

2. **Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?**

   R: Não aplicado

3. **Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?**

   R: Não aplicado

Bloco 3 – Perceções sobre tecnologia

4. **Está familiarizado com o conceito de blockchain e contratos inteligentes?**

R: Sim, fruto da atividade profissional. A implementação de um sistema deste tipo tem um objetivo central: garantir que a informação introduzida no sistema numa determinada data — sejam vídeos, gravações, documentos ou outros elementos digitais — não é alterada em momento algum do processo. Ou seja, assegurar a consistência da prova ao longo de toda a cadeia de custódia.

E aqui a questão é dupla: por um lado, temos de garantir a imutabilidade dessa informação; por outro, temos de definir quem pode aceder a ela. Se a informação tiver de ser pública, uma blockchain aberta poderia ser uma opção. Mas, neste contexto específico, parece-me evidente que estamos a falar de informação sensível, pelo que a solução passaria antes por uma blockchain privada ou de consórcio.

Numa blockchain privada, aquilo que é registado não é a prova em si, mas sim uma chave criptográfica — uma espécie de "marca de água digital" — que corresponde unicamente a essa prova no momento em que foi inserida. As provas em si ficam guardadas num repositório seguro e privado, mas a chave fica gravada na blockchain. Assim, basta que alguém altere um único bit num ficheiro para que a chave já não corresponda ao registo original, permitindo detetar de imediato qualquer adulteração.

A diferença entre uma blockchain privada e uma de consórcio tem a ver com o nível de confiança entre as partes. As blockchains de consórcio são particularmente úteis em cadeias de valor com múltiplos intervenientes que não confiam plenamente uns nos outros — por exemplo, no setor alimentar. Imagine-se o caso do leite: o produtor regista a recolha, depois outra empresa faz a pasteurização, outra transporta e, finalmente, o supermercado coloca o produto à venda. Cada entidade faz registos em momentos distintos e, se houver um problema, como uma quebra de temperatura numa câmara frigorífica, é possível identificar rapidamente onde ocorreu a falha. Neste cenário, faz sentido ter um ledger de consórcio, porque cada parte tem o seu papel e partilha a responsabilidade, mas nenhuma controla o sistema sozinha.

No caso da gestão de provas digitais em contexto de justiça, penso que o enquadramento é diferente. Aqui não há múltiplas entidades privadas com interesses divergentes; a responsabilidade recai sobretudo sobre o Estado, nomeadamente o Ministério da Administração Interna. Por isso, a solução mais adequada seria uma blockchain privada sob gestão do Estado, garantindo segurança, sigilo e, ao mesmo tempo, acesso controlado para quem tiver as credenciais e permissões adequadas.

Naturalmente, este sistema poderia ser complementado com contratos inteligentes que não só regulassem os acessos, mas também permitissem que entidades autorizadas introduzissem nova informação no processo. Assim, não se trataria apenas de um repositório de consulta, mas também de um registo vivo, onde cada passo da cadeia de custódia ficaria automaticamente validado e registado de forma imutável.

5. Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?

R: Eu acho que sim, sem dúvida. A tecnologia blockchain pode contribuir muito para reforçar a gestão e preservação de provas, por várias razões.

A primeira tem a ver com a própria natureza das provas. Muitas vezes, pensamos em toneladas de papel, vídeos ou outros elementos físicos que ocupam espaço, são difíceis de organizar e podem deteriorar-se com o tempo. Quando essas provas passam para formato digital, ganha-se eficiência, mas continua a existir o risco de perda dos dados se usarmos apenas soluções tradicionais. Aí entra a blockchain: é uma tecnologia altamente redundante e tolerante a falhas, porque não existe um ponto único de vulnerabilidade. Cada nó da rede mantém uma cópia integral do registo, o que reduz drasticamente a probabilidade de perda ou alteração não autorizada da prova.

Além disso, há outro aspeto muito relevante: a rastreabilidade. Com os métodos mais clássicos de gestão de provas, especialmente em papel, não conseguimos saber com rigor quem acedeu, quando e de que forma. Com a blockchain, isso muda completamente. Por exemplo, podemos configurar o acesso às provas de forma a que só seja possível através da execução de um smart contract. E sempre que alguém executa esse contrato, fica registado automaticamente quem foi, quando o fez e com que credenciais.

Ou seja, conseguimos ter todo o histórico de acessos e manipulações centralizado num registo imutável, descentralizado e resistente a ataques. Isso aumenta muito a confiança no sistema.

Diria que não vejo grandes desvantagens na aplicação da blockchain à gestão de provas.

Bloco 4 – Implementação e desafios

6. Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?

R: Os custos não são o problema, objetivamente não. Eu falo com alguma experiência: comecei por ser académico, depois estive cerca de uma década na indústria e agora regressei à academia. E o que essa experiência me ensinou é que, na maioria dos casos, o problema nunca é a tecnologia, são sempre as pessoas.

O que quero dizer com isto é simples: se houver recursos disponíveis, desenvolver um sistema destes não é difícil. Há inúmeras plataformas por onde escolher, existe conhecimento técnico e até em Portugal temos competências sólidas nessa área. No âmbito da Agenda Blockchain, por exemplo, temos nove work packages, dos quais seis ou sete são de desenvolvimento, com várias empresas nacionais já a trabalhar ativamente neste campo. Algumas até aplicam conceitos de cadeia de custódia, mas em setores como a saúde. Se falar, por exemplo, com o Pedro Roseiro, ele pode indicar-lhe várias empresas portuguesas que já fazem isso.

Portanto, do ponto de vista tecnológico, não vejo entraves relevantes. O verdadeiro desafio está na adoção. Mudar processos é sempre difícil, existe sempre a resistência típica do "eu já faço isto assim há anos", mas as empresas têm estruturas hierárquicas definidas e podem impor mudanças de forma mais direta. Muitas vezes basta que um detalhe da solução não esteja absolutamente perfeito para ser usado como argumento de que nada funciona.

Mesmo que criemos um sistema ideal, com uma interface simples e intuitiva — onde o utilizador só precise de autenticar-se com um cartão e executar as operações de forma imediata —, o processo de adoção demora sempre muito tempo. Convencer pessoas que usam um sistema há 10, 15 ou 20 anos a mudar não é algo que se faça de um dia para o outro.

Por isso, diria que o grande obstáculo não é tecnológico nem financeiro, mas sim humano: a resistência à mudança. Do ponto de vista técnico, soluções destas já estão a ser implementadas em contextos muito mais complexos do que aquele da justiça.

7. Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?

R: A questão é muito interessante porque, há uns cinco anos, quando se falava em blockchain, a associação imediata era quase sempre às criptomoedas. Hoje, o panorama já é bastante diferente. Em Portugal, começam a surgir várias empresas que vivem destas tecnologias. Um bom exemplo é a Âncoras Digital, que funciona como uma espécie de banco online, já com uma dimensão internacional enorme, escritórios nos Estados Unidos e noutros países, e com capital e know-how essencialmente portugueses. Outra empresa relevante é a Acel Fox, também bastante grande, que tem trabalhado intensamente na área das tecnologias de blockchain.

Eu próprio faço parte de um consórcio ligado ao projeto Blockchain PT, que há pouco referi. Isso mostra que o ecossistema português já está ativo e com vários atores envolvidos, mesmo que a comunicação social não dê grande visibilidade a esta realidade.

É verdade que ainda existe o estereótipo de associar blockchain apenas às criptomoedas, mas acredito que isso vai desaparecer gradualmente. O que vai emergir são os verdadeiros casos de uso desta tecnologia, que vão muito além da moeda digital. As criptomoedas são apenas um produto paralelo; o essencial está nas características da blockchain enquanto tecnologia de registo distribuído, transparente e auditável.

Eu costumo dizer isso mesmo aos meus alunos: imaginem um cenário com várias partes que não confiam totalmente umas nas outras. Como é que garantimos que a informação partilhada é verdadeira e imutável? Neste momento, não há nenhuma outra tecnologia que permita isso de forma tão robusta como a blockchain.

Tenho a convicção de que esta tecnologia vai crescer exponencialmente na próxima década. Aquilo que hoje ainda é visto por alguns como algo "exótico" está, aos poucos, a ganhar reconhecimento. No meu próprio departamento, de eletrónica e telecomunicações, já noto uma mudança de mentalidade e de paradigma.

Bloco 5 – Visão de futuro

8. **Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?**

   R: Acho que é e acho que vai poupar imenso tempo às pessoas.

9. **Que vantagens práticas esperaria de um sistema com estas características?**

R: Eu diria que, se um sistema destes for bem desenvolvido, sobretudo com um grande foco na experiência do utilizador — ou seja, na forma como a interface é desenhada e organizada —, pode poupar imenso tempo e recursos. No fundo, o que acontece "por trás" do sistema não é o mais relevante; o que importa é que, para quem o utiliza, a interação seja simples, intuitiva e eficaz.

Claro que existem riscos, e vemos isso todos os dias: quando falha a internet, estes sistemas deixam de funcionar. É por isso fundamental que, em contextos como os tribunais, exista redundância para garantir aquilo que é absolutamente essencial — eletricidade e acesso à rede.

Ultrapassada essa questão, acredito que um sistema deste tipo teria um impacto muito positivo, especialmente na redução do trabalho manual associado à gestão da prova. Para a PSP, por exemplo, significaria menos tempo gasto em tarefas administrativas e mais eficiência no tratamento da informação.

Outro aspeto muito relevante é a consulta: em vez de depender de suportes físicos como CDs ou DVDs — onde é sempre um desafio perceber em qual disco está determinado vídeo ou documento —, a informação passaria a estar disponível de forma orgânica, estruturada e facilmente acessível.

Se a interface for bem pensada para os diferentes utilizadores — juízes, técnicos ou agentes da PSP —, adaptando-se às necessidades de cada perfil, isso pode reduzir drasticamente a carga de trabalho associada à gestão da prova. E, além disso, resolveria problemas recorrentes como a perda, deterioração ou má catalogação de provas.

Portanto, vejo aqui um grande potencial para melhorar substancialmente todo o processo, desde a recolha até à consulta da prova.

10. Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?

R: Acho que é um projeto muito interessante. Neste momento já estamos um pouco em cima dos prazos, mas vejo bastante potencial para o futuro. Eu sou docente de uma disciplina de mestrado em Cibersegurança chamada Tecnologias de Ledger Distribuído, onde precisamente trabalhamos com blockchain e temas associados.

Nessa disciplina, os alunos começam por ter uma introdução à tecnologia e depois desenvolvem projetos práticos. Claro que, pelo tempo limitado, esses projetos têm sempre

uma ambição mais ajustada, mas servem como um primeiro passo. Posteriormente, muitos desses alunos avançam para teses de mestrado, onde podem aplicar estes conhecimentos de forma mais aprofundada, ligando-os até ao seu contexto profissional.

Nessa fase, já não falamos apenas de projetos exploratórios, mas sim de trabalhos com implementação prática e a criação de *proofs of concept*, ou seja, protótipos que demonstram a tecnologia a funcionar.

Portanto, se no futuro houver interesse em desenvolver esta ideia, podemos perfeitamente propor um ou dois temas de dissertação aos nossos alunos, selecionar candidatos viáveis e tê-los a trabalhar nisto durante um ano. No final, a tese teria de incluir uma prova de conceito funcional, algo que pode ser muito útil até para mostrar a decisores a viabilidade da solução e apoiar o processo de adoção.

Por isso, se no futuro houver interesse em desenvolver projetos ou parcerias nesta área, eu estaria totalmente disponível e com muito gosto até em coordenar um ou dois mestrados em conjunto.

Entrevista: E6

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. **Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?**

R: Na minha atividade profissional em cibersegurança tenho tido contacto com processos de recolha, preservação e análise de prova digital, tanto em incidentes internos como em apoio a investigações. Utilizo metodologias forenses para garantir a integridade da

prova, como a criação de imagens digitais com validação por hash e o registo da cadeia de custódia.

Na fase de análise, foco-me na correlação de eventos, deteção de malware e extração de indicadores de compromisso, sempre com atenção ao enquadramento legal, nomeadamente a Lei do Cibercrime e os princípios do Código de Processo Penal, de forma a assegurar que a prova digital se mantém admissível em tribunal.

Bloco 2 – Problemas no modelo atual

2. Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?

R: Na minha perspetiva, uma das principais fragilidades do atual modelo de cadeia de custódia da prova digital reside na sua forte dependência de processos manuais e da confiança institucional, o que aumenta o risco de erros humanos, falhas na documentação ou mesmo questionamentos em tribunal quanto à integridade da prova. A inexistência de uma normalização transversal e de plataformas integradas entre forças policiais, Ministério Público e tribunais dificulta a rastreabilidade e abre espaço a lacunas na interoperabilidade.

Outra fragilidade relevante é a vulnerabilidade tecnológica dos sistemas em uso: bases de dados centralizadas suscetíveis a intrusões, registos que podem ser alterados sem deixar marcas evidentes e ausência de mecanismos de verificação distribuída e imutável. Estas limitações comprometem a transparência e a confiança no processo judicial, sobretudo em crimes informáticos, onde a credibilidade da prova digital é frequentemente alvo de contestação pelas defesas.

3. Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?

R: Sim, já tive conhecimento de situações em que a cadeia de custódia da prova digital foi contestada em tribunal devido a falhas na documentação ou na ausência de registo claro sobre quem acedeu e quando. Em alguns casos, pequenas inconsistências — como discrepâncias nos relatórios de recolha, ausência de hashes de validação ou transferências de dispositivos sem registo formal — foram suficientes para a defesa levantar dúvidas sobre a autenticidade da prova.

Também tomei contacto com casos em que a prova foi recolhida corretamente, mas o armazenamento ou transporte não seguiu as melhores práticas forenses, criando vulnerabilidades exploradas em sede de julgamento. Estes exemplos evidenciam que, mesmo quando existe boa-fé e competência técnica, a falta de processos totalmente auditáveis e uniformizados pode fragilizar a credibilidade da prova digital perante o sistema de justiça.

Bloco 3 – Perceções sobre tecnologia

4. Está familiarizado com o conceito de blockchain e contratos inteligentes?

R: Sim, estou familiarizado com o conceito de blockchain e contratos inteligentes, entendendo-os enquanto tecnologias com aplicação muito além do universo das criptomoedas. A blockchain deve ser vista como um registo distribuído e imutável, que garante transparência e rastreabilidade em processos críticos, como a cadeia de custódia da prova digital.

Os contratos inteligentes, por sua vez, são protocolos automatizados que permitem aplicar regras pré-definidas de forma segura e sem intervenção manual, assegurando que operações — como a transferência de prova entre entidades ou a validação de acessos — sejam executadas apenas dentro dos parâmetros autorizados. Importa sublinhar que estes conceitos não estão necessariamente ligados às criptomoedas, podendo ser implementados em blockchains permissionadas e totalmente controladas por entidades estatais ou institucionais.

5. Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?

R: Sim, considero que a utilização de blockchain e contratos inteligentes pode reforçar significativamente a integridade da cadeia de custódia digital. A blockchain, pela sua natureza imutável e auditável, permite registar cada operação relacionada com a prova digital (recolha, transferência, acesso, análise), garantindo que não haja alterações não detetadas e que cada intervenção fique associada a um agente identificado. Desta forma, a prova ganha uma rastreabilidade total, reduzindo a margem para contestações em tribunal sobre a sua autenticidade.

Os contratos inteligentes acrescentam um nível adicional de segurança e eficiência, ao automatizarem regras e permissões no manuseamento da prova. Isto significa que apenas utilizadores previamente autorizados podem aceder ou transferir a prova, sendo cada ação registada de forma automática e transparente. Esta combinação de registo imutável e controlo automatizado permite não só reforçar a confiança no sistema judicial, mas também reduzir erros humanos e falhas processuais, que são atualmente uma das maiores fragilidades do modelo tradicional.

Bloco 4 – Implementação e desafios

6. Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?

R: Na minha perspetiva, a adoção da blockchain e dos contratos inteligentes pela PSP e pelo sistema de justiça seria um avanço natural para reforçar a cadeia de custódia da prova digital, trazendo maior transparência, rastreabilidade e confiança processual. No entanto, qualquer mudança desta natureza enfrenta inevitavelmente resistências e obstáculos que importa analisar de forma crítica.

O primeiro obstáculo é de natureza técnica. A blockchain exige infraestruturas robustas, interoperabilidade entre sistemas já existentes (como o Citius ou bases de dados policiais) e um quadro de cibersegurança capaz de sustentar uma solução desta escala. A PSP, por exemplo, ainda se debate com sistemas desatualizados e fragmentados, o que dificulta a introdução de novas tecnologias sem investimentos estruturais significativos.

O segundo obstáculo prende-se com os recursos humanos. A aplicação prática destas soluções requer equipas altamente qualificadas em cibersegurança, ciência forense digital e programação de contratos inteligentes. A PSP, apesar do esforço e competência dos seus quadros, continua a ter falta de peritos especializados, o que limita a capacidade de absorção tecnológica. Sem um investimento sério na formação e na contratação de especialistas, o risco é criar soluções de difícil utilização prática.

Um terceiro obstáculo está ligado ao quadro legal e regulatório. Embora a blockchain seja compatível com princípios de integridade e auditabilidade, a sua integração no processo penal português exige alterações legislativas e regulamentares, que não são rápidas nem simples. O Código de Processo Penal e a Lei do Cibercrime teriam de ser atualizados para prever explicitamente a admissibilidade e validade de registos em blockchain como prova processual.

Por fim, não podemos ignorar o obstáculo político e orçamental. A adoção destas tecnologias só será possível se o poder político compreender a sua relevância estratégica e disponibilizar meios financeiros adequados. É fundamental que exista uma visão clara de que a transformação digital da justiça e das forças de segurança não é um luxo, mas uma necessidade para enfrentar a criminalidade do século XXI. A polícia precisa de mais meios técnicos e humanos, e cabe ao poder político criar condições para essa evolução, sob pena de ficarmos presos a modelos ultrapassados e vulneráveis à contestação em tribunal.

7. Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?

R: Para que a implementação da blockchain e dos contratos inteligentes na cadeia de custódia da prova digital fosse eficaz, a primeira condição necessária seria a existência de uma infraestrutura tecnológica robusta e interoperável. É essencial que esta tecnologia se integre de forma harmoniosa com os sistemas já utilizados pela PSP, Ministério Público e tribunais, evitando redundâncias ou barreiras de compatibilidade. Isso implica normalização de formatos, APIs seguras e servidores preparados para lidar com elevados volumes de dados.

Em segundo lugar, é indispensável investir em recursos humanos especializados. A blockchain não é apenas uma ferramenta técnica; exige conhecimentos específicos de implementação, manutenção e auditoria. A formação de agentes policiais, peritos forenses e magistrados seria essencial, garantindo que todos compreendem as potencialidades e limitações da tecnologia. Sem quadros devidamente capacitados, qualquer projeto corre o risco de se tornar uma "caixa negra" incompreensível para os próprios utilizadores.

Uma terceira condição prende-se com o quadro legal e normativo. A admissibilidade de registos baseados em blockchain como prova em tribunal tem de estar claramente prevista no Código de Processo Penal e enquadrada pela Lei do Cibercrime. Além disso, seria necessário definir normas técnicas de referência, talvez sob a tutela da ANACOM, do CNCS ou de entidades europeias (ENISA, Comissão Europeia), para garantir que a solução tem reconhecimento oficial e valor probatório inequívoco.

Em quarto lugar, é fundamental assegurar meios financeiros e apoio político. A transformação digital na justiça e nas forças de segurança não é possível sem investimentos estruturais, e cabe ao poder político reconhecer que este tipo de tecnologia não é um "extra", mas um passo essencial para enfrentar a criminalidade digital. O financiamento deve

contemplar não só a aquisição de soluções, mas também a manutenção a longo prazo, evitando o erro de projetos-piloto que ficam pelo caminho.

Por fim, é necessário cultivar uma mudança cultural e organizacional. A adoção da blockchain implica um novo paradigma de trabalho colaborativo entre PSP, Ministério Público, tribunais e até advogados de defesa. A confiança na tecnologia deve ser acompanhada de confiança institucional, transparência e vontade de cooperar. Sem esta mudança de mentalidade, mesmo a melhor tecnologia pode ser subutilizada ou vista como um entrave burocrático em vez de uma ferramenta de reforço da justiça.

Bloco 5 – Visão de futuro

8. Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?

R: Considero que, a curto prazo, a viabilidade de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os Tribunais baseada em blockchain é limitada. Existem entraves técnicos, humanos e legais que ainda não estão resolvidos, desde a interoperabilidade com sistemas já existentes (como o Citius ou as bases de dados policiais) até à ausência de um enquadramento jurídico claro que reconheça formalmente os registos em blockchain como prova admissível em tribunal.

No entanto, a médio prazo, vejo a adoção como plausível, desde que exista um investimento sério em infraestrutura, formação especializada e atualização do quadro legal. Projetos-piloto poderiam ser conduzidos em áreas específicas — como a gestão de prova digital em casos de cibercrime — antes de uma implementação nacional alargada. Isso permitiria testar a tecnologia, ajustar processos e preparar as equipas operacionais e judiciais para um novo modelo de trabalho.

Em última análise, a viabilidade dependerá de uma decisão política e estratégica: reconhecer que a blockchain não é uma moda tecnológica, mas um instrumento capaz de reforçar a confiança na justiça e na investigação criminal. Se o poder político disponibilizar os meios técnicos e humanos necessários, a médio prazo esta integração poderá tornar-se uma realidade sólida e transformadora.

9. Que vantagens práticas esperaria de um sistema com estas características?

R: De um sistema baseado em blockchain e contratos inteligentes esperaria, em primeiro lugar, um reforço inequívoco da integridade e transparência da cadeia de custódia

da prova digital. Cada registo ficaria imutavelmente associado a um momento, a um agente e a uma ação, eliminando dúvidas sobre manipulações ou acessos não autorizados. Isso permitiria reduzir contestações em tribunal e aumentar a confiança de magistrados e advogados na validade da prova apresentada.

Em segundo lugar, destacaria a eficiência operacional. Os contratos inteligentes permitiriam automatizar autorizações de acesso, transferências de prova e geração de relatórios, diminuindo a burocracia e os erros humanos. Além disso, uma plataforma partilhada entre PSP, Ministério Público e tribunais facilitaria a interoperabilidade, acelerando os processos e evitando redundâncias, o que resultaria numa investigação criminal mais célere e numa justiça mais eficaz.

10. Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?

R: Um aspeto relevante que considero importante acrescentar é a necessidade de encarar a transformação digital da justiça e da investigação criminal como um projeto estratégico nacional, e não apenas como uma inovação tecnológica isolada. A blockchain pode ser uma ferramenta poderosa, mas só terá impacto real se for acompanhada por políticas públicas consistentes, investimento sustentado e um compromisso claro em dotar as forças de segurança e os tribunais dos meios técnicos e humanos de que necessitam.

Acrescentaria ainda que, para garantir a eficácia e a aceitação desta tecnologia, seria essencial promover projetos-piloto e parcerias com universidades e centros de investigação, criando um ecossistema colaborativo entre polícia, magistrados, peritos forenses e comunidade científica. Essa abordagem experimental e colaborativa permitiria reduzir riscos, aumentar a confiança institucional e preparar o terreno para uma adoção sólida a médio prazo.

Outro ponto que merece destaque é a importância da sensibilização e formação contínua não apenas dos profissionais diretamente envolvidos, mas também do poder político e da opinião pública. Só através de uma compreensão alargada da utilidade da blockchain será possível ultrapassar resistências culturais e perceções erradas que ainda a associam exclusivamente a criptomoedas. A consciencialização é uma condição essencial para criar aceitação e legitimidade.

Por fim, sublinharia que qualquer solução tecnológica deve estar alinhada com os valores fundamentais do Estado de Direito: legalidade, proporcionalidade e respeito pelos direitos fundamentais. A blockchain, enquanto registo imutável, não deve ser vista como um

substituto do escrutínio judicial, mas como um complemento que reforça a confiança na justiça. É nessa conjugação entre tecnologia, ética e direito que reside a verdadeira mais-valia deste tipo de inovação.

Entrevista: E7

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. **Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?**

R: Não tenho experiência na recolha direta de prova. A minha experiência centra-se sobretudo na preservação, armazenamento, segurança e na análise de prova digital em contexto de inquérito criminal. Trabalho sobretudo com telemóveis e computadores apreendidos: pretendo ser a primeira pessoa a aceder ao conteúdo para selecionar o que é relevante para a investigação e para segregar toda a prova que não interessa ao inquérito — incluindo conteúdos potencialmente ofensivos à honra das pessoas. O material que não for relevante para a investigação determino o seu destino, nomeadamente a sua destruição quando necessário.

Bloco 2 – Problemas no modelo atual

2. **Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?**

R: As principais fragilidades residem sobretudo na falta de visibilidade e de controlo após a saída da prova digital do meu gabinete. Quando recebo a prova, apenas tenho acesso aos relatórios que a acompanham, mas não existe uma rastreabilidade clara sobre como foi manuseada ou preservada antes. A partir do momento em que abro a prova, assumo a responsabilidade da custódia inicial, mas depois não tenho informação detalhada sobre o percurso da prova: para onde vai, como é extraída, quem tem acesso a essa extração e de que forma esse acesso é garantido. Em suma, existe uma fragilidade no controlo do ciclo completo da prova digital, desde a sua saída do meu gabinete até à sua efetiva incorporação no processo.

3. **Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?**

R: Não. Que eu tenha conhecimento nunca ninguém colocou, até hoje, a cadeia de custódia da prova em causa.

Bloco 3 – Perceções sobre tecnologia

4. **Está familiarizado com o conceito de blockchain e contratos inteligentes?**

   R: Conheço, mas não estou familiarizado.

5. **Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?**

   R: Sim, considero que estas tecnologias podem contribuir para reforçar a integridade e a segurança da cadeia de custódia digital. Isto porque permitem registar de forma automática e fiável cada acesso à prova digital, identificando quem acedeu, quando, onde e em que condições. Tal como acontece com sistemas digitais protegidos por credenciais, fica sempre registado o utilizador e o contexto do acesso, o que assegura transparência, rastreabilidade e responsabilização dos intervenientes. Qualquer acesso não justificado ou de natureza não profissional ficaria visível e teria de ser devidamente explicado.

Bloco 4 – Implementação e desafios

6. **Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?**

   R: Um dos principais obstáculos é cada Órgão de Polícia Criminal ter um sistema diferente. Se existisse um sistema único seria melhor.

7. **Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?**

   R: Para que a implementação desta tecnologia fosse eficaz, acho que seria necessário criar uma infraestrutura centralizada e segura, por exemplo um servidor ou plataforma única onde toda a informação relativa à cadeia de custódia pudesse ser armazenada. Essa plataforma deveria estar disponível para todos os Órgãos de Polícia Criminal envolvidos na investigação criminal, garantindo uma interação integrada entre as diferentes entidades.

   No meu entendimento, esse sistema deveria estar sob a tutela de uma entidade com legitimidade transversal, como o Ministério Público ou o respetivo Conselho Superior, assegurando assim que todos os OPC (PSP, GNR, PJ) pudessem aceder com as suas próprias credenciais. Isso permitiria que cada interveniente registasse o seu contacto com a prova, desde a primeira apreensão até à sua utilização em processo.

Dessa forma, cada entidade teria acesso apenas ao que fosse relevante para a sua função, podendo juntar provas e assegurar que a cadeia de custódia fosse preservada de forma uniforme e auditável em todo o sistema de justiça criminal.

Bloco 5 – Visão de futuro

8. **Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?**

R: Sim, acredito que seja viável a curto ou médio prazo, sobretudo considerando a rápida evolução das tecnologias de informação. Cada vez mais, os sistemas digitais caminham para soluções assentes em inteligência artificial e blockchain, reduzindo a dependência de suportes físicos como papel, CDs ou dispositivos externos. Nesse sentido, considero que o futuro passa por esta transformação digital, onde a prova será gerida e partilhada de forma desmaterializada, segura e rastreável.

9. **Que vantagens práticas esperaria de um sistema com estas características?**

R: As principais vantagens seriam a eficiência e a uniformização no manuseamento da prova digital, evitando a dispersão atual em diferentes suportes como CDs, pens ou discos externos, que tornam o processo mais moroso, inseguro e difícil de gerir. Um sistema centralizado e partilhado permitiria acesso mais rápido e controlado à prova digital.
Também facilitaria a coordenação entre os diversos Órgãos de Polícia Criminal e o Ministério Público.

10. **Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?**

R: Não tenho mais nada acrescentar, penso que foi tudo dito.

Entrevista: E8

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. **Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?**

R: Tenho experiência a nível profissional. No que respeita à prova digital, quando é recolhida, é normalmente armazenada numa pen ou num disco rígido, consoante a capacidade necessária, e é aí que permanece guardada. Relativamente à análise dessa prova, o processo não é muito intuitivo, uma vez que temos de percorrer manualmente os elementos, não existindo ferramentas que permitam realizar pesquisas automáticas. Em muitos casos, como já aconteceu num processo em que estive envolvido, devido ao grande volume de informação, recorro à colaboração de técnicos especializados para apoiar na análise.

Bloco 2 – Problemas no modelo atual

2. **Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?**

R: As fragilidades são várias, desde logo porque os suportes utilizados — como pens e discos rígidos — são vulneráveis, podendo desaparecer ou simplesmente deixar de funcionar, dada a sua fragilidade. Muitas vezes, de um dia para o outro, todo o conteúdo de uma pen pode desaparecer sem explicação clara. Por isso, considero que o atual modelo de armazenamento não oferece a segurança necessária; talvez soluções baseadas em bases de dados pudessem assegurar maior fiabilidade.

3. **Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?**

R: Nunca tive essa situação.

Bloco 3 – Perceções sobre tecnologia

4. **Está familiarizado com o conceito de blockchain e contratos inteligentes?**

R: Relativamente ao blockchain, como lhe digo, conheço só de nome, nunca contactei diretamente com a tecnologia, nem sei bem como é que funciona.

5. **Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?**

R: Acho que estas tecnologias podem reforçar a nossa capacidade de resposta e de investigação, o que seria fantástico. Seria igualmente importante que permitissem uma intercomunicação eficaz entre todas as polícias e o Ministério Público, o que representaria

uma grande mais-valia, pois todos trabalhamos com o mesmo objetivo: a defesa da justiça e do cidadão.

Bloco 4 – Implementação e desafios

6. **Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?**

R: Na minha perspetiva, o principal obstáculo é a capacidade para criar uma plataforma deste tipo e garantir que existam pessoas com os conhecimentos necessários para inserir corretamente os elementos nas bases de dados, caso contrário a tecnologia perde sentido. Outro ponto essencial é a segurança: tudo o que está na internet é potencialmente vulnerável, e existe sempre o receio de acessos indevidos.

Costuma dizer-se que "tudo o que cai na internet fica na internet", e isso é preocupante. Já houve situações em que dados foram acedidos com más intenções, o que alimenta alguma resistência em adotar este tipo de soluções, precisamente por dúvidas quanto a quem pode aceder e com que finalidade.

7. **Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?**

R: Dar formação às pessoas para poderem trabalhar com a tecnologia.

Bloco 5 – Visão de futuro

8. **Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?**

R: Sim, acho que sim.

9. **Que vantagens práticas esperaria de um sistema com estas características?**

R: Uma das vantagens seria a possibilidade de o acesso ser limitado. Em regra, deveria ser permitido a todos os agentes da justiça — nomeadamente polícias e Ministério Público —, mas com a possibilidade, em determinadas situações, de restringir o acesso a certos tipos de informação.

10. **Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?**

R: Mais nada a acrescentar.

Entrevista: E9

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. **Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?**

R: A minha experiência profissional nesta área é extensa, tendo desenvolvido atividade essencialmente no domínio da perícia informática. Ao longo dos anos, tenho trabalhado diretamente com a recolha, preservação e análise de prova digital em diversos contextos de investigação criminal. Esta experiência abrange não só os crimes informáticos propriamente ditos, mas também todos os crimes que recorrem a sistemas informáticos para os cometer, bem como aqueles que, independentemente da sua natureza, podem conter dados informáticos importantes para o processo. A realidade é que praticamente todas as investigações criminais, hoje em dia, envolvem alguma componente digital, seja através de telemóveis, computadores, veículos automóveis, sistemas de videovigilância ou outros sistemas informáticos.

Bloco 2 – Problemas no modelo atual

2. **Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?**

R: Na generalidade, o modelo atual de cadeia de custódia funciona normalmente e cumpre os seus objetivos. Contudo, se tivesse de identificar algumas fragilidades, destacaria essencialmente três aspetos. Em primeiro lugar, ainda existe uma componente significativa de registo manual, o que pode originar lapsos humanos ou omissões na documentação. Em segundo lugar, verifica-se uma falta de integração entre sistemas, já que a prova digital passa por diferentes entidades como os Órgãos de Polícia Criminal (OPC), os peritos, o Ministério Público (MP) e os tribunais, que utilizam sistemas informáticos distintos, dificultando assim a rastreabilidade completa. Por último, os intervalos temporais entre a apreensão e a perícia podem ser consideráveis, e qualquer falha no registo desse período pode suscitar dúvidas sobre a integridade da prova.

3. **Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?**

R: Não, que tenha conhecimento. Nos processos em que estive envolvido, a cadeia de custódia nunca foi formalmente colocada em causa. Os procedimentos existentes, quando corretamente aplicados, têm-se revelado capazes de resistir ao escrutínio judicial.

Bloco 3 – Perceções sobre tecnologia

4. **Está familiarizado com o conceito de blockchain e contratos inteligentes?**

R: Sim, embora reconheça que a minha formação e experiência específica em blockchain ainda não é suficiente para uma compreensão profunda de todas as suas potencialidades técnicas. Já tivemos alguns processos-crime relacionados com criptomoedas e tecnologias associadas, o que me permitiu um contacto inicial com estes conceitos, mas sempre numa perspetiva de investigação criminal e não de aplicação tecnológica interna.

5. **Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?**

R: É importante esclarecer que não creio que o blockchain tenha uma relação direta com a integridade da cadeia de custódia no sentido tradicional. O blockchain não impede que uma prova digital seja corrompida ou alterada no momento da sua recolha ou antes de ser registada no sistema.

O que o blockchain pode garantir é a integridade do registo da cadeia de custódia, não da prova em si. Através das suas propriedades de imutabilidade e descentralização, o blockchain pode criar um registo inviolável de quem mexeu na prova, quando e em que circunstâncias. Se alguém tentar alterar uma prova depois de esta estar registada, essa alteração seria facilmente detetável porque o "hash" (assinatura digital) da prova não corresponderia ao registado na blockchain.

Assim, o blockchain funciona como um "notário digital" que certifica o histórico de manuseamento da prova, tornando praticamente impossível falsificar ou alterar os registos da cadeia de custódia sem deixar vestígios.

Bloco 4 – Implementação e desafios

6. Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?

R: Existem algumas dificuldades e entraves significativos à implementação do blockchain na PSP e no sistema judicial. Desde logo, os custos elevados, uma vez que a implementação de uma infraestrutura blockchain exige investimentos consideráveis em tecnologia, formação e manutenção. Depois, existe uma natural resistência à mudança, pois as instituições têm procedimentos estabelecidos há anos e a introdução de uma nova tecnologia implica mudança de mentalidades e adaptação de práticas consolidadas. Acresce ainda a falta de conhecimento técnico, já que a blockchain é uma tecnologia complexa e as competências necessárias são ainda escassas nas forças de segurança e no sistema judicial.

Por outro lado, surgem dificuldades de integração, uma vez que seria necessário garantir que os sistemas da PSP, PJ, GNR, Ministério Público e tribunais comunicassem entre si na mesma rede. Por fim, a falta de enquadramento legal também constitui um obstáculo, pois não existe legislação específica que regule a utilização de blockchain para fins probatórios, o que cria incerteza jurídica.

7. Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?

R: Para que a implementação fosse eficaz, considero essenciais algumas condições fundamentais. A primeira seria garantir formação especializada e contínua, pois todos os intervenientes, desde os agentes que recolhem prova no terreno até aos magistrados, teriam de receber formação adequada sobre o funcionamento, potencialidades e limitações da tecnologia blockchain. A segunda condição passa pela normalização e interoperabilidade dos sistemas, sendo imprescindível a criação de normas técnicas comuns e a garantia de que todos os sistemas informáticos das diferentes instituições, como a PSP, PJ, GNR, MP e tribunais, pudessem comunicar eficazmente através da mesma infraestrutura blockchain. Por último, seria necessário um enquadramento jurídico claro, em que a lei previsse expressamente o valor probatório dos registos blockchain e estabelecesse regras claras sobre a sua utilização, acesso, armazenamento e responsabilidade pela gestão dos dados.

Bloco 5 – Visão de futuro

8. Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?

R: Acredito que a ideia de partilha destas novas tecnologias entre os OPC, nomeadamente a PSP, e entre estes e o MP e os tribunais, será relevante no futuro. Contudo, a curto prazo, vejo essa implementação como pouco realista, dadas as barreiras organizacionais, técnicas e financeiras existentes.

A médio prazo, considerando os avanços tecnológicos e a crescente digitalização dos processos judiciais, esta integração torna-se quase inevitável. A chave está na coordenação entre as diferentes instituições e na criação de um projeto conjunto que beneficie todas as partes envolvidas.

O sucesso desta implementação dependerá da vontade política, do investimento adequado e da capacidade de ultrapassar as barreiras institucionais que tradicionalmente dificultam a colaboração entre diferentes entidades.

9. Que vantagens práticas esperaria de um sistema com estas características?

R: Caso fosse implementado de forma eficaz, um sistema baseado em blockchain poderia trazer várias vantagens práticas. Desde logo, permitiria o rastreio completo e transparente, já que todos os acessos, movimentações e operações realizadas sobre a prova digital ficariam registados de forma imutável e auditável, facilitando a reconstrução da cadeia de custódia judicialmente. Além disso, contribuiria para a redução de contestações formais, pois a existência de um registo público, ou semipúblico, e imutável poderia minimizar o número de contestações sobre a integridade e autenticidade da prova, aumentando a confiança de todos os intervenientes processuais. Por fim, proporcionaria maior eficiência e celeridade processual, uma vez que a automatização de determinados registos e a possibilidade de acesso partilhado e em tempo real por parte das diferentes entidades envolvidas poderiam acelerar procedimentos burocráticos no tratamento da prova digital.

10. Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?

R: Sim, gostaria de salientar que é importante sublinhar que a blockchain deve ser vista como um complemento aos procedimentos existentes, não como substituto. A tecnologia pode melhorar a rastreabilidade e a transparência dos registos, mas não dispensa procedimentos rigorosos, formação adequada e a responsabilidade humana na gestão da

prova. Por mais sofisticada que seja a tecnologia, ela nunca substituirá a necessidade de práticas corretas e de profissionais devidamente preparados para lidar com a prova digital.

Entrevista: E10

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. **Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?**

   R: Alguma experiência relacionada com a atividade profissional.

Bloco 2 – Problemas no modelo atual

2. **Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?**

   R: Nunca lidei com nenhuma situação em que uma prova tivesse sido adulterada ou tivesse sido posta em causa. Contudo, o tratamento das provas por parte dos OPC revela-se, muitas vezes, pouco transparente para quem não está diretamente envolvido no processo. É difícil compreender de forma clara como ocorre esse tratamento, até porque a documentação é frequentemente apresentada numa linguagem técnica pouco acessível apresentada em formato papel.

3. **Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?**

   R: Não tenho conhecimento de que tenha ocorrido qualquer falha nesse âmbito; contudo, à medida que a tecnologia evolui, também as formas de ataque e de adulteração se tornam mais sofisticadas. Nunca tive propriamente nenhuma situação em que tivesse sido confrontada com esse tipo de problema, mas considero que se trata de uma preocupação cada vez mais presente. A criminalidade, seja sob a forma de burlas ou de falsificações de documentos, tende a afastar-se da interação presencial e a recorrer cada vez mais aos meios de comunicação à distância.

Bloco 3 – Perceções sobre tecnologia

4. **Está familiarizado com o conceito de blockchain e contratos inteligentes?**

   R**:** Não estou muito familiarizada com o conceito de blockchain e contratos inteligentes, apesar de já ter ouvido falar deles.

5. **Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?**

R: Considero que seria extremamente interessante, pois caminhamos cada vez mais para uma sociedade em que muitos se refugiam atrás de um computador para a prática de crimes e, muitas vezes, crimes de grande escala. Quando falamos de fenómenos como o branqueamento de capitais em larga dimensão, percebemos que os contactos e as redes envolvidas se expandem ainda mais.

Bloco 4 – Implementação e desafios

6. Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?

R: Uma das principais dificuldades na adoção da tecnologia blockchain prende-se com os custos associados à sua implementação. Pelo que tenho conhecimento, no âmbito do PRR, dos 48 milhões de euros destinados ao sistema de justiça, apenas cerca de um milhão foi aplicado em iniciativas relacionadas com o Ministério Público. Desconheço quanto foi efetivamente atribuído a cada órgão de polícia criminal, mas parece-me evidente que a vontade política e o compromisso com um investimento sério no sistema de justiça não estão, neste momento, particularmente fortalecidos.

Trata-se, no entanto, de um investimento indispensável, pois seria ingénuo acreditar que o crime não se encontra cada vez mais no domínio digital. Para que a implementação desta tecnologia fosse verdadeiramente eficaz, seria necessário garantir condições estruturais, financeiras e organizacionais adequadas, acompanhadas de uma estratégia clara e sustentada de modernização tecnológica.

7. Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?

R: Por um lado, seria importante que o sistema não abrangesse apenas a PSP e a sua ligação direta aos tribunais, mas que fosse alargado a todos os outros órgãos de polícia criminal. Um sistema verdadeiramente integrado e de partilha de dados permitiria cruzar investigações relativas aos mesmos suspeitos, aumentando significativamente a eficácia e a celeridade das investigações criminais.

Por outro lado, para que o sistema pudesse funcionar de forma eficiente, seriam necessárias equipas tecnicamente capacitadas e devidamente formadas. E essa formação não deveria limitar-se apenas aos elementos das forças policiais ou aos que tratam diretamente os dados, mas deveria estender-se também aos magistrados judiciais e ao Ministério Público,

para garantir uma compreensão transversal da tecnologia e de todo o seu potencial no contexto da justiça criminal.

Bloco 5 – Visão de futuro

8. Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?

R: Seria o ideal que a adoção dessa solução tecnológica fosse viável a curto e médio prazo sobretudo porque, pensando nesse horizonte temporal, é quando mais se justificaria a sua implementação. No entanto, essa viabilidade está sempre condicionada por fatores de natureza financeira, que acabam por determinar a capacidade de concretizar o projeto.

9. Que vantagens práticas esperaria de um sistema com estas características?

R: As principais vantagens práticas residem, precisamente, na maior eficácia do sistema no combate ao crime, sobretudo à criminalidade mais organizada, aquela que pode afetar individualmente cada vítima em menor grau, mas que, pela sua dimensão e número de vítimas envolvidas, tem um impacto muito mais amplo e significativo.

10. Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?

R: Mais nada a acrescentar.

Entrevista: E11

Estudo: *Blockchain e contratos inteligentes na garantia da cadeia de custódia da prova digital: uma proposta de integração tecnológica entre PSP e o sistema de justiça*

Esta entrevista integra-se num estudo académico desenvolvido no âmbito do Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

A crescente digitalização da sociedade trouxe novos desafios à investigação criminal, sobretudo no que respeita à recolha, preservação e integridade da prova digital.

Neste contexto, tecnologias emergentes, como a blockchain e os contratos inteligentes, têm vindo a ser estudadas como possíveis ferramentas para reforçar a integridade e a fiabilidade da cadeia de custódia digital.

O trabalho tem como objetivo analisar de que forma a tecnologia blockchain e os contratos inteligentes podem contribuir para reforçar a cadeia de custódia da prova digital, garantindo a sua integridade e fiabilidade desde a recolha pela PSP até à sua apresentação em tribunal.

Pretende-se, em particular:

- identificar as principais fragilidades do modelo atual de cadeia de custódia da prova digital;
- recolher perceções sobre o potencial da tecnologia blockchain e dos contratos inteligentes neste domínio;
- compreender quais seriam os principais desafios e condições necessárias para a sua implementação prática, quer no contexto policial, quer no sistema de justiça;
- explorar a viabilidade futura de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os tribunais.

A sua colaboração permitirá enriquecer a investigação com perspetivas práticas e institucionais, complementando a revisão teórica da literatura.

Bloco 1 – Contexto e experiência

1. **Qual a sua experiência ou contacto com a recolha, preservação e/ou análise da prova digital no contexto das investigações criminais ou no âmbito da sua atividade profissional?**

R: Experiência no âmbito da atividade de Magistrado Judicial.

Bloco 2 – Problemas no modelo atual

2. **Na sua perspetiva, quais considera serem as principais fragilidades do atual modelo de cadeia de custódia da prova digital?**

R: No que respeita às fragilidades parece-me que ainda funcionamos muito com base na confiança. Confiamos naquilo que nos é transmitido pelas polícias, assumindo que as provas não foram adulteradas e que correspondem exatamente ao que foi apreendido na origem. No entanto, na prática, não temos forma de verificar se houve ou não alguma alteração.

Além disso, não dispomos de formação específica para detetar ou lidar com essas situações. A nossa formação de base aborda muito pouco a questão da prova digital. Já no que toca às provas tradicionais, como documentos ou testemunhos, existe preparação adequada. Mas no domínio digital, essa componente ainda é bastante incipiente, e mesmo ao nível da advocacia raramente se levantam questões mais profundas sobre a integridade deste tipo de prova.

3. **Já presenciou ou tomou conhecimento de situações em que a cadeia de custódia digital foi contestada ou colocada em causa?**

R: Pessoalmente, não tenho conhecimento de nenhuma situação concreta em que essa questão tenha sido efetivamente levantada.

Bloco 3 – Perceções sobre tecnologia

4. **Está familiarizado com o conceito de blockchain e contratos inteligentes?**

R: Relativamente ao conceito de blockchain e contratos inteligentes estou pouco familiarizada, apesar de já ter ouvido falar, sobretudo associado às criptomoedas.

5. **Considera que estas tecnologias podem contribuir para reforçar a integridade da cadeia de custódia digital? Porquê?**

R: Estes sistemas baseados em blockchain e contratos inteligentes permitem, de facto, identificar quem acede à informação, mantendo o registo completo, ou seja, o rasto de todas as ações realizadas. Ao contrário das pesquisas convencionais, em que é possível apagar ou alterar dados sem deixar vestígios, aqui tudo fica registado de forma permanente e transparente.

Esta característica é particularmente relevante, não apenas no contexto da cadeia de custódia da prova, mas também noutras situações em que o simples acesso a um processo pode gerar dúvidas ou polémicas. Recordo, por exemplo, casos mediáticos em que se discutiu quem teria acedido a determinados dados e ninguém conseguiu determinar ao certo.

Com a tecnologia blockchain, isso deixaria de acontecer: cada acesso ficaria registado, indicando quem acedeu, quando, onde e a partir de que dispositivo. Seria, portanto, um avanço significativo em termos de transparência e responsabilização, com potencial para ser aplicado no futuro em várias áreas do sistema de justiça.

Bloco 4 – Implementação e desafios

6. Quais seriam, na sua perspetiva, os principais obstáculos à adoção da blockchain pela PSP e pelo sistema de justiça?

R: Conhece o nosso sistema CITIUS. É provavelmente das estruturas mais arcaicas que ainda existem a nível informático. Aliás, a componente tecnológica continua a ser o verdadeiro calcanhar de Aquiles de muitas instituições. Por isso, talvez o primeiro passo devesse ser precisamente a modernização e melhoria dos sistemas atualmente em uso.

Claro que isso exige um investimento muito significativo, não apenas em termos financeiros, mas também humanos.

7. Que condições considera necessárias para que a implementação desta tecnologia fosse eficaz?

R: Uma das condições seria haver uma mudança de mentalidade e uma aposta clara na formação. E isso é um desafio, sobretudo porque há uma certa resistência à mudança, especialmente entre gerações mais antigas, que começaram a trabalhar num contexto totalmente físico e agora enfrentam uma transição para o digital.

A verdade é que esta transformação não depende apenas das polícias: envolve também magistrados, advogados, funcionários judiciais, todo um ecossistema de profissionais com níveis de literacia digital muito distintos. Para que o sistema funcione

realmente, todos precisam de estar capacitados. Caso contrário, de pouco serve termos uma tecnologia avançada se quem a utiliza não estiver preparado para acompanhar a sua implementação e o seu funcionamento diário.

Bloco 5 – Visão de futuro

8. Acredita ser viável, a curto ou médio prazo, uma solução tecnológica partilhada entre a PSP, Ministério Público e Tribunais baseada em blockchain?

R: Acredito e espero que seja possível. Talvez não comecemos de imediato por uma solução baseada em blockchain, mas considero que a nossa comunicação precisa, sem dúvida, de ser muito mais informatizada e integrada. É um passo essencial para modernizar os processos e garantir maior eficiência e transparência no sistema.

9. Que vantagens práticas esperaria de um sistema com estas características?

R: A verdade é que ainda trabalhamos de forma muito dependente do papel, o que torna todo o processo moroso e pouco prático. Uma comunicação mais digital traria inúmeras vantagens, porque facilitaria o trabalho de todos os intervenientes até ao momento do julgamento.

Com um sistema digital integrado, seria possível aceder facilmente ao histórico das provas, verificar se houve alterações e garantir, com segurança, que a prova se mantém intacta. Isso permitiria uma análise mais rápida e fiável, evitando atrasos e incertezas.

Atualmente, ainda lidamos com suportes físicos, como CDs e DVDs, que se tornam obsoletos e de difícil utilização, até porque os computadores fornecidos pelo Estado já nem sequer dispõem de leitores adequados. Muitas vezes temos de recorrer a equipamentos externos apenas para aceder a conteúdos essenciais, como as escutas.

Se todo esse material estivesse armazenado numa base de dados digital segura, o acesso seria imediato, bastaria um clique. Seria, sem dúvida, um avanço enorme, que tornaria o sistema muito mais eficiente e funcional. Neste momento, o acesso à prova é tudo menos prático; o processo é pesado e trabalhoso, e há uma clara necessidade de evoluir para soluções mais modernas e digitais.

10. Há algum aspeto que considere relevante acrescentar e que não tenha sido abordado?

R: De momento não me ocorre mais nada.

Apêndice E - Análise de conteúdo

Tabela 4

Quadro de codificações: categorias, subcategorias, unidades de registo e unidades de contexto

Categoria	Subcategoria	Unidade de Registo	Unidade de Contexto
Contexto e experiência	Experiência	Ausência de experiência prévia	"não tenho qualquer experiência ou contacto" (E1)
		Experiência prática na PSP	"A minha experiência nesta temática, já tem uns aninhos" (E2) "eu trabalho nisto desde 2009" (E2) "tenho naturalmente contacto com estas matérias (…) conheço os procedimentos adotados e a forma como é tramitada dentro da PSP" (E3) "tenho trabalhado diretamente com a recolha, preservação e análise de prova digital em diversos contextos de investigação criminal" (E9)
		Experiência académica (ensino)	"Tenho contacto com o tema apenas teórico: lecionei algumas vezes uma cadeira relacionada com o assunto (…) e tem precisamente que ver com recolha, preservação e análise de prova digital" (E4)
		Experiência em projetos tecnológicos	"tive experiência em projetos de desenvolvimento de sistemas de rastreabilidade da cadeia de valor" (E5)
		Experiência em cibersegurança	"Na minha atividade profissional em cibersegurança tenho tido contacto com processos de recolha, preservação e análise de prova digital" (E6)
		Experiência prática a nível judicial	"A minha experiência centra-se sobretudo na preservação, armazenamento, segurança e na análise de prova digital em contexto de inquérito criminal." (E7)

			“Tenho experiência a nível profissional” (E8) “Alguma experiência relacionada com a atividade profissional” (E10) “Experiência no âmbito da atividade de Magistrado Judicial” (E11)
	Perceção sobre a tecnologia	Desconhecimento parcial sobre blockchain	“não a conheço e não sei se é pior ou se é melhor do que a que já existe nos nossos equipamentos forenses” (E2) “Conheço, mas não estou familiarizado” (E7) “conheço só de nome, nunca contactei diretamente com a tecnologia” (E8) “Não estou muito familiarizada” (E10) “estou pouco familiarizada, apesar de já ter ouvido falar, sobretudo associado às criptomoedas” (E11)
		Conhecimento superficial / difuso	“a blockchain é conhecida essencialmente como uma cadeia, se quiser de informação” (E2) “segurança de não acesso a toda essa informação” (E2)
		Reconhecimento do potencial tecnológico	“acompanho ocasionalmente o tema e sei que se trata de um sistema que permite a rastreabilidade total de todas as operações realizadas sobre esse ativo” (E3) “estou familiarizado com o conceito de blockchain e contratos inteligentes, entendendo-os enquanto tecnologias com aplicação muito além do universo das criptomoedas” (E6)

			"Sim, embora reconheça que a minha formação e experiência específica em blockchain ainda não é suficiente" (E9)
		Definição conceptual clara	"A blockchain deve ser vista como um registo distribuído e imutável, que garante transparência e rastreabilidade em processos críticos, como a cadeia de custódia da prova digital" (E6)
		Explicação sobre contratos inteligentes	"Os contratos inteligentes (…) permitem aplicar regras pré-definidas de forma segura e sem intervenção manual, assegurando que operações (…) sejam executadas apenas dentro dos parâmetros autorizados" (E6)
		Distinção face às criptomoedas	"estes conceitos não estão necessariamente ligados às criptomoedas, podendo ser implementados em blockchains permissionadas e totalmente controladas por entidades estatais ou institucionais" (E6)
		Participação em projetos estratégicos	"Sim. Faço investigação, ensino e tenho alguma experiência como consultor (…) Coordenei o grupo de trabalho que produziu a estratégia nacional de Web 3" (E4) "Sim, fruto da atividade profissional" (E5)
Fragilidades do modelo atual	Fatores humanos - falhas processuais	Erros humanos como vulnerabilidade central	"as vulnerabilidades que podem existir têm a ver muitas das vezes com as falhas humanas" (E2) "erros humanos e falhas processuais, que são atualmente uma das maiores fragilidades do modelo tradicional" (E6)
		Falta de preparação e consciência dos recursos humanos	"o facto de os nossos recursos humanos (…) não estarem capazes e não perceberem qual é que é o melindro do que nós estamos a falar e qual é que é a

		responsabilidade que nós todos temos" (E2)
	Dependência excessiva do procedimento humano	"o procedimento humano" (E2) "forte dependência de processos manuais e da confiança institucional, o que aumenta o risco de erros humanos" (E6) "registo manual, o que pode originar lapsos humanos ou omissões na documentação" (E9) "ainda funcionamos muito com base na confiança. Confiamos naquilo que nos é transmitido pelas polícias, assumindo que as provas não foram adulteradas e que correspondem exatamente ao que foi apreendido na origem" (E11)
	Necessidade de recursos adicionais para compensar falhas	"obriga frequentemente a afetar recursos adicionais no terreno" (E3)
	Risco de acesso privilegiado e manipulação interna (*malicious insiders*)	"pode ser comprometido por pessoas que tenham acesso privilegiado aos dados dessa cadeia (malicious insiders), por exemplo modificando dados e os correspondentes hashes" (E4) "pesquisas convencionais, em que é possível apagar ou alterar dados sem deixar vestígios" (E11)
	Contestação judicial por falhas na documentação da cadeia de custódia	"já tive conhecimento de situações em que a cadeia de custódia da prova digital foi contestada em tribunal devido a falhas na documentação ou na ausência de registo claro sobre quem acedeu e quando" (E6)
Heterogeneidade de procedimentos	Falta de uniformização de procedimentos	"temos vários carros e cada um conduz o seu, todos diferentes e ninguém sabe conduzir o carro do vizinho" (E2)

		“a falta de processos totalmente auditáveis e uniformizados pode fragilizar a credibilidade da prova digital perante o sistema de justiça” (E6)
	Práticas divergentes entre entidades	“A inexistência de uma normalização transversal e de plataformas integradas entre forças policiais, Ministério Público e tribunais dificulta a rastreabilidade e abre espaço a lacunas na interoperabilidade” (E6) “falta de integração entre sistemas, já que a prova digital passa por diferentes entidades (…) dificultando assim a rastreabilidade completa” (E9)
	Divergência entre recolha, armazenamento e transporte da prova	“tomei contacto com casos em que a prova foi recolhida corretamente, mas o armazenamento ou transporte não seguiu as melhores práticas forenses, criando vulnerabilidades exploradas em sede de julgamento” (E6) “intervalos temporais entre a apreensão e a perícia podem ser consideráveis” (E9)
	Falta de rastreabilidade no circuito da prova	“Quando recebo a prova, apenas tenho acesso aos relatórios que a acompanham, mas não existe uma rastreabilidade clara sobre como foi manuseada ou preservada antes” (E7) “A partir do momento em que abro a prova, assumo a responsabilidade da custódia inicial, mas depois não tenho informação detalhada sobre o percurso da prova: para onde vai, como é extraída, quem tem acesso a essa extração e de que forma esse acesso é garantido” (E7)

		“pouco transparente para quem não está diretamente envolvido no processo” E10
Limitações tecnológicas	Persistência de suportes físicos frágeis	“muitas diligências, ainda feitas em papel e entregues em mão” (E3) “toneladas de papel, vídeos ou outros elementos físicos que ocupam espaço, são difíceis de organizar e podem deteriorar-se com o tempo” (E5) “depender de suportes físicos como Cds ou DVDs” (E5) “os suportes utilizados — como pens e discos rígidos — são vulneráveis, podendo desaparecer ou simplesmente deixar de funcionar, dada a sua fragilidade” (E8) “dispersão atual em diferentes suportes como CDs, pens ou discos externos, que tornam o processo mais moroso, inseguro e difícil de gerir” (E7) “ainda lidamos com suportes físicos, como CDs e DVDs, que se tornam obsoletos e de difícil utilização, até porque os computadores fornecidos pelo Estado já nem sequer dispõem de leitores adequados.” (E11)
	Risco de perda ou deterioração da prova	“perda dos dados” (E5) “o atual modelo de armazenamento não oferece a segurança necessária” (E8)
	Vulnerabilidade de sistemas centralizados	“Com os métodos mais clássicos de gestão de provas, especialmente em papel, não conseguimos saber com rigor

			quem acedeu, quando e de que forma" (E5) "vulnerabilidade tecnológica dos sistemas em uso: bases de dados centralizadas suscetíveis a intrusões, registos que podem ser alterados sem deixar marcas evidentes e ausência de mecanismos de verificação distribuída e imutável. Estas limitações comprometem a transparência e a confiança no processo judicial, sobretudo em crimes informáticos, onde a credibilidade da prova digital é frequentemente alvo de contestação pelas defesas" (E6)
Adoção da tecnologia blockchain e contratos inteligentes	Vantagens	Reforço da confiança institucional	"Porque incutirão maior confiança aos polícias e aos demais intervenientes no processo (criminal)" (E1) "Melhorar a justiça e melhorar o serviço prestado pelo Estado ao cidadão" (E3) "esta combinação de registo imutável e controlo automatizado permite não só reforçar a confiança no sistema judicial, mas também reduzir erros humanos e falhas processuais" (E6) "redução de contestações formais" (E9) "aumentando a confiança de todos os intervenientes processuais" (E9)
		Melhoria da eficiência processual	"digitalização de procedimentos, incremento da segurança na interoperabilidade de informação criminal, melhor serviço público" (E1) "Com um sistema assim o Ministério Público consegue controlar a morosidade, dar

		instruções, enviar as ordens de perícia de forma rápida" (E2) "permitiria alguma poupança de trabalho" (E3) "se um sistema destes for bem desenvolvido (…) pode poupar imenso tempo e recursos." (E5) "a informação passaria a estar disponível de forma orgânica, estruturada e facilmente acessível." (E5) "uma plataforma partilhada entre PSP, Ministério Público e tribunais facilitaria a interoperabilidade, acelerando os processos e evitando redundâncias" (E6) "maior eficiência e celeridade processual" (E9) "maior eficácia do sistema" E10 "facilitaria o trabalho de todos os intervenientes até ao momento do julgamento" (E11) "permitiria uma análise mais rápida e fiável, evitando atrasos e incertezas" (E11)
	Garantia de imutabilidade e integridade da prova	"seria a maior fidedignidade da prova" (E3) "Com registo em blockchain, seria possível saber quem acedeu, quando e porquê" (E3) "O uso de contratos inteligentes executados numa blockchain permite guardar os hashes dos elementos de prova digital (…) de forma que todas as alterações fiquem registadas e esse registo seja muito difícil de modificar" (E4)

		"garantir que a informação introduzida no sistema numa determinada data — sejam vídeos, gravações, documentos ou outros elementos digitais — não é alterada em momento algum do processo. Ou seja, assegurar a consistência da prova ao longo de toda a cadeia de custódia." (E5) "Como é que garantimos que a informação partilhada é verdadeira e imutável? Neste momento, não há nenhuma outra tecnologia que permita isso de forma tão robusta como a blockchain" (E5) "A blockchain (…) permite registar cada operação (…) garantindo que não haja alterações não detetadas" (E6) "considero que a utilização de blockchain e contratos inteligentes pode reforçar significativamente a integridade da cadeia de custódia digital" (E6) "considero que estas tecnologias podem contribuir para reforçar a integridade e a segurança da cadeia de custódia digital" (E7) "Através das suas propriedades de imutabilidade e descentralização, o blockchain pode criar um registo inviolável de quem mexeu na prova, quando e em que circunstâncias" (E9)
	Redução de vulnerabilidades e riscos	"A grande vantagem seria a segurança oferecida, ou seja, a redução do risco de comprometimento da cadeia de custódia" (E4)

		“resolveria problemas recorrentes como a perda, deterioração ou má catalogação de provas” (E5) “a blockchain: é uma tecnologia altamente redundante e tolerante a falhas, porque não existe um ponto único de vulnerabilidade” (E5) “A tecnologia blockchain pode contribuir muito para reforçar a gestão e preservação de provas, por várias razões.” (E5) “funciona como um "notário digital" que certifica o histórico de manuseamento da prova, tornando praticamente impossível falsificar ou alterar os registos da cadeia de custódia sem deixar vestígios” (E9)
	Eficiência e automatização por contratos inteligentes	“um contrato inteligente ao nível de uma suposta arquitetura que vá buscar características da blockchain para a segurança digital. Perfeitamente” (E2) “Os contratos inteligentes acrescentam um nível adicional de segurança e eficiência, ao automatizarem regras e permissões no manuseamento da prova” (E6) “a eficiência operacional. Os contratos inteligentes permitiriam automatizar autorizações de acesso, transferências de prova e geração de relatórios, diminuindo a burocracia e os erros humanos” (E6) “eficiência e a uniformização no manuseamento da prova digital” (E7)

	Transparência e controlo de acessos	“cada entidade teria acesso apenas ao que fosse relevante para a sua função (…) de forma uniforme e auditável” (E7) “a possibilidade, em determinadas situações, de restringir o acesso a certos tipos de informação” (E8) “aspeto muito relevante: a rastreabilidade (…) sempre que alguém executa esse contrato, fica registado automaticamente quem foi, quando o fez e com que credenciais” (E5) “Qualquer acesso não justificado (…) ficaria visível e teria de ser devidamente explicado” (E7)
	Automação de tarefas e redução de erros manuais	“acredito que um sistema deste tipo teria um impacto muito positivo, especialmente na redução do trabalho manual associado à gestão da prova” (E5) “Se a interface for bem pensada (…) pode reduzir drasticamente a carga de trabalho associada à gestão da prova” (E5)
	Rastreabilidade e auditoria	“permitem registar de forma automática e fiável cada acesso à prova digital” (E7) “identificando quem acedeu, quando, onde e em que condições” (E7) “rastreio completo e transparente, já que todos os acessos, movimentações e operações realizadas sobre a prova digital ficariam registados de forma imutável e auditável” (E9) “identificar quem acede à informação, mantendo o registo completo, ou seja, o rasto de todas as ações realizadas” (E11)

			“seria possível aceder facilmente ao histórico das provas, verificar se houve alterações e garantir, com segurança, que a prova se mantém intacta” (E11)
	Obstáculos	Custos de implementação e manutenção	“custo de implementação; (…) custo de manutenção” (E1) “O principal obstáculo são os custos” (E3) “custos associados à descentralização organizacional e de administração” (E4) “A adoção destas tecnologias só será possível se o poder político compreender a sua relevância estratégica e disponibilizar meios financeiros adequados” (E6) “custos elevados” (E9) “investimentos consideráveis em tecnologia, formação e manutenção” (E9) “custos associados à sua implementação” E10 “investimento muito significativo, não apenas em termos financeiros, mas também humanos.” (E11)
		Divergência de perceções quanto ao peso financeiro	“investimento estruturado e financeiramente sustentável” (E1) “Os custos não são o problema, objetivamente não. Eu falo com alguma experiência” (E5)
		Falta de literacia tecnológica	“falta de literacia nas tecnologias em apreço” (E1) “alavancagem das competências técnicas e da literacia digital” (E1) “Dar formação às pessoas” (E8)

	Resistência à mudança	"O verdadeiro desafio está na adoção. Mudar processos é sempre difícil, existe sempre a resistência típica do 'eu já faço isto assim há anos'" (E5) "alguma resistência em adotar este tipo de soluções, precisamente por dúvidas quanto a quem pode aceder e com que finalidade" (E8) "o grande obstáculo não é tecnológico nem financeiro, mas sim humano: a resistência à mudança" (E5) "Muitas vezes basta que um detalhe da solução não esteja absolutamente perfeito para ser usado como argumento de que nada funciona." E5 "existe uma natural resistência à mudança" (E9) "resistência à mudança, especialmente entre gerações mais antigas" (E11)
	Necessidade de equipas qualificadas	"O segundo obstáculo prende-se com os recursos humanos. A aplicação prática destas soluções requer equipas altamente qualificadas em cibersegurança, ciência forense digital e programação de contratos inteligentes" (E6) "garantir que existam pessoas com os conhecimentos necessários para inserir corretamente os elementos nas bases de dados" (E8)

	Necessidade de alterações legislativas	"Embora a blockchain seja compatível com princípios de integridade e auditabilidade, a sua integração no processo penal português exige alterações legislativas e regulamentares" (E6) "qualquer solução tecnológica deve estar alinhada com os valores fundamentais do Estado de Direito: legalidade, proporcionalidade e respeito pelos direitos fundamentais" (E6) "temos que ver até que ponto é que isso depois é ajustável aos procedimentos forenses" (E2) "falta de enquadramento legal" (E9)
	Limitações técnicas e infraestruturais	"Claro que existem riscos, e vemos isso todos os dias: quando falha a internet, estes sistemas deixam de funcionar" (E5) "O primeiro obstáculo é de natureza técnica. A blockchain exige infraestruturas robustas, interoperabilidade entre sistemas já existentes (…) e um quadro de cibersegurança capaz de sustentar uma solução desta escala" (E6) "o principal obstáculo é a capacidade para criar uma plataforma deste tipo" (E8) "falta de conhecimento técnico" (E9)
	Interoperabilidade com sistemas existentes	"dependerá claramente dos requisitos da tecnologia (…)" (E2) "cada polícia, o próprio Ministério Público, cada organização, gosta de ter a sua rede e o seu sistema e depois faz-se aqui uma interoperabilidade

			entre os sistemas, o que dificulta sempre" (E2) "Um dos principais obstáculos é cada Órgão de Polícia Criminal ter um sistema diferente" (E7) "dificuldades de integração" (E9)
		Fragmentação tecnológica entre entidades	"necessidade de uniformização de procedimentos (…) cada OPC trabalha com as ferramentas que consegue adquirir, mas as autoridades judiciárias acabam por lidar com formatos e métodos diferentes" (E3) "integração das várias entidades do sistema judicial no projeto, para corresponder a todas as necessidades e expetativas" (E1) "Se existisse um sistema único seria melhor" (E7)
		Necessidade de investimento estratégico e institucional	"é essencial que as estruturas tecnológicas das forças de segurança, no caso da PSP, tenham consciência da importância do investimento nesta área" (E3) "nós temos como projeto já há mais de 10 anos (…) criação de uma rede interna laboratorial (…) todos os laboratórios periféricos a trabalhar em rede traz vantagem, mais segurança na informação e mais contacto direto" (E2)
Desafios e visão de futuro	Capacitação e formação contínua	Necessidade de desconstruir estereótipos sobre blockchain	"ainda existe o estereótipo de associar blockchain apenas às criptomoedas, mas acredito que isso vai desaparecer gradualmente" (E5)
		Transformação digital como necessidade estratégica	"É fundamental que exista uma visão clara de que a transformação digital da justiça e das forças de segurança não é um luxo, mas uma necessidade para enfrentar a criminalidade do século XXI" (E6)

		Importância da sensibilização e formação contínua	"a importância da sensibilização e formação contínua não apenas dos profissionais diretamente envolvidos, mas também do poder político e da opinião pública" (E6) "garantir formação especializada e contínua" (E9) "seriam necessárias equipas tecnicamente capacitadas e devidamente formadas" (E10) "haver uma mudança de mentalidade e uma aposta clara na formação" (E11) "de pouco serve termos uma tecnologia avançada se quem a utiliza não estiver preparado para acompanhar a sua implementação" (E11)
	Viabilidade a médio prazo	Adoção gradual e através de projetos-piloto	"todas essas formas novas de cadeia de custódia da prova, nomeadamente em ambiente digital, os próprios equipamentos desde que forenses, eles vão começar a incorporar cada vez mais segurança a esse nível." (E2) "Sim, apesar dos desafios" (E4) "a médio prazo, vejo a adoção como plausível, desde que exista um investimento sério em infraestrutura, formação especializada e atualização do quadro legal. Projetos-piloto poderiam ser conduzidos em áreas específicas (…) antes de uma implementação nacional alargada" (E6) "para garantir a eficácia e a aceitação desta tecnologia, seria essencial promover projetos-piloto e parcerias com universidades e centros de investigação" (E6)

	"Portanto, se no futuro houver interesse em desenvolver esta ideia, podemos perfeitamente propor um ou dois temas de dissertação aos nossos alunos, selecionar candidatos viáveis e tê-los a trabalhar nisto durante um ano. No final, a tese teria de incluir uma prova de conceito funcional, algo que pode ser muito útil até para mostrar a decisores a viabilidade da solução e apoiar o processo de adoção. Por isso, se no futuro houver interesse em desenvolver projetos ou parcerias nesta área, eu estaria totalmente disponível e com muito gosto até em coordenar um ou dois mestrados em conjunto." (E5) "Sim, acredito que seja viável a curto ou médio prazo, sobretudo considerando a rápida evolução das tecnologias de informação" (E7) "A médio prazo, considerando os avanços tecnológicos e a crescente digitalização dos processos judiciais, esta integração torna-se quase inevitável" (E9) "Acredito e espero que seja possível. Talvez não comecemos de imediato por uma solução baseada em blockchain, mas considero que a nossa comunicação precisa, sem dúvida, de ser muito mais informatizada e integrada." (E11)
Dependência da decisão política e estratégica	"a viabilidade dependerá de uma decisão política e estratégica: reconhecer que a blockchain não é uma moda tecnológica, mas um instrumento capaz de reforçar a

		confiança na justiça e na investigação criminal" (E6) "É colocar o interesse do país à frente e deixar os interesses corporativos" (E2) "O sucesso desta implementação dependerá da vontade política, do investimento adequado e da capacidade de ultrapassar as barreiras institucionais" (E9) "necessário garantir condições estruturais, financeiras e organizacionais adequadas, acompanhadas de uma estratégia clara e sustentada de modernização tecnológica." (E10)
	Potencial técnico já demonstrado noutras áreas	"Do ponto de vista técnico, soluções destas já estão a ser implementadas em contextos muito mais complexos do que aquele da justiça" (E5) "Tenho a convicção de que esta tecnologia vai crescer exponencialmente na próxima década. Aquilo que hoje ainda é visto por alguns como algo "exótico" está, aos poucos, a ganhar reconhecimento. No meu próprio departamento, de eletrónica e telecomunicações, já noto uma mudança de mentalidade e de paradigma." (E5)
	Limitações a curto prazo	"a curto prazo, a viabilidade de uma solução tecnológica partilhada entre a PSP, o Ministério Público e os Tribunais baseada em blockchain é limitada. Existem entraves técnicos, humanos e legais (…)" (E6) "Acredito que sim mas avaliando aquilo que aconteceu nos últimos

		15 anos, 20 anos tenho muita dificuldade em perceber" (E2) "barreiras organizacionais, técnicas e financeiras existentes" (E9)
	Propostas de implementação em contexto nacional	"Proposta para a PSP e sistema de justiça – Uma blockchain permissioned (…) com um nó em cada entidade" (E4) "neste contexto específico (…) a solução passaria antes por uma blockchain privada (…) complementada com contratos inteligentes" (E5) "Para que a implementação desta tecnologia fosse eficaz, acho que seria necessário criar uma infraestrutura centralizada e segura (…)" (E7)
	Integração entre entidades do sistema de justiça	"Temos como projeto já há mais de 10 anos, por mim proposto, a criação de uma rede interna laboratorial" (E2) "Se tivéssemos um sistema único onde toda a gente pudesse trabalhar de igual forma e por perfis de acesso conseguíamos ter uma maior coordenação com o Ministério Público e todas as outras polícias (E2) "Temos de ter um sistema em Portugal que consiga funcionar para todas as polícias" (E2) "plataforma deveria estar disponível para todos os Órgãos de Polícia Criminal envolvidos na investigação criminal, garantindo uma interação integrada entre as diferentes entidades" (E7) "normalização e interoperabilidade dos sistemas" (E9)

	"seria importante que o sistema não abrangesse apenas a PSP e a sua ligação direta aos tribunais, mas que fosse alargado a todos os outros órgãos de polícia criminal" (E10)

Fonte: Elaboração própria com base nas entrevistas, segundo o modelo de codificação de Bardin (2016), operacionalizado no NVivo 15 (Lumivero, 2025).

Apêndice F - Checklist COREQ

Tabela 5

Checklist COREQ – Síntese do desenho e condução do estudo qualitativo

1. Entrevistador	**Quem conduziu as entrevistas?**	**O próprio investigador**
2. Qualificações	Quais as credenciais do investigador?	Investigador do VI Curso de Comando e Direção Policial (ISCPSI).
3. Ocupação	Qual era a ocupação do investigador?	Oficial da Polícia de Segurança Pública.
4. Género	Qual o género do investigador?	Masculino.
5. Experiência e formação	Que experiência ou formação possuía o investigador?	Formação académica em ciências policiais e experiência profissional na PSP.
6. Relação estabelecida	Foi estabelecida relação prévia com participantes?	Não houve relação prévia formal com os entrevistados.
7. Conhecimento dos participantes	O que sabiam os participantes sobre o investigador?	Foram informados dos objetivos do estudo e do enquadramento académico.
8. Características do entrevistador	Foram reportadas características pessoais, motivações ou interesses?	Motivado em compreender fragilidades e soluções para a cadeia de custódia da prova digital.
Domínio 2: Desenho do estudo		
9. Orientação metodológica	Qual o enquadramento teórico-metodológico?	Análise de conteúdo (Bardin, 2016), abordagem híbrida, predominantemente dedutiva.
10. Amostragem	Como foram selecionados os participantes?	Amostra de conveniência, estratificada por grupo profissional.
11. Método de contacto	Como foram abordados os participantes?	Por contactos institucionais e redes profissionais.

12. Dimensão da amostra	Quantos participantes participaram?	11 entrevistas realizadas (4 PSP, 2 académicos, 1 académico/jurista, 4 magistrados).
13. Não participação	Houve recusas ou desistências?	Sim, houve duas ausências de resposta.
14. Contexto da recolha	Onde foi realizada a recolha de dados?	Presencial ou por videoconferência e e-mail, em setembro-outubro 2025.
15. Presença de não participantes	Alguém além dos participantes esteve presente?	Não.
16. Descrição da amostra	Quais as características da amostra?	Diversidade de perspetivas: operacional, jurídica e científico-tecnológica.
17. Guião de entrevista	Foi usado guião de entrevista?	Sim, guião semiestruturado (Apêndice C).
18. Repetição de entrevistas	Foram feitas entrevistas repetidas?	Não.
19. Gravação áudio/visual	Foi realizada gravação?	Sim, gravação áudio, com consentimento.
20. Notas de campo	Foram feitas notas de campo?	Sim, notas analíticas registadas no NVivo.
21. Duração	Qual a duração média?	20 minutos.
22. Saturação	Foi discutida saturação?	Sim, paragem por saturação teórica.
23. Devolução de transcrições	Foram devolvidas transcrições?	As transcrições das entrevistas foram devolvidas aos participantes para revisão e confirmação da exatidão do conteúdo, assegurando a fidelidade das declarações recolhidas (*member checking)*
Domínio 3: Análise e resultados		

24. Número de codificadores	Quantos investigadores codificaram os dados?	Codificação realizada pelo investigador, com revisão por pares.
25. Árvore de códigos	Foi descrita a árvore de códigos?	Sim, matriz categoria-evidência no Apêndice E.
26. Derivação de temas	Os temas foram pré-definidos ou emergentes?	Híbrido: categorias dedutivas da literatura e categorias indutivas emergentes.
27. Software	Foi usado software para análise?	Sim, NVivo 15 (Lumivero, 2025).
28. Validação pelos participantes	Participantes validaram resultados?	Não.
29. Citações apresentadas	Foram apresentadas citações ilustrativas?	Sim, excertos identificados por código (E1, E2, …).
30. Consistência dados-resultados	Há consistência entre dados e resultados?	Sim, categorias suportadas por evidências empíricas.
31. Clareza dos temas principais	Os temas principais estão claros?	Sim, quatro categorias principais identificadas.
32. Clareza dos temas secundários	Foram relatados casos divergentes ou subtemas?	Sim, foram identificados e descritos subtemas, tais como as limitações tecnológicas e a heterogeneidade de procedimentos, bem como perspetivas divergentes relativamente a fatores como os custos de implementação e a resistência à mudança.

Fonte: Adaptado de Tong et al. (2007). Elaboração própria com base na aplicação ao presente estudo.