UNIVERSIDADE D
COIMBRA

Andreia Carina Claúdio Hermeiro

A CADEIA DE CUSTÓDIA DA PROVA DIGITAL: O USO DA TECNOLOGIA BLOCKCHAIN COMO FORMA DE PRESERVAÇÃO

VOLUME 1

Dissertação no âmbito do Mestrado em Ciências Jurídico-Forenses orientada pela Professora Doutora Sónia Mariza Florêncio Fidalgo e apresentada à Faculdade de Direito da Universidade de Coimbra

Janeiro de 2023

Andreia Carina Claúdio Hermeiro

A cadeia de custódia da prova digital: O uso da Tecnologia Blockchain como forma de preservação

The chain of custody of digital evidence: The use of Blockchain Technology as a form of preservation

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º Ciclo de Estudos em Ciências Jurídico-Forenses (conducente ao grau de Mestre)

Orientador(a): Professora Doutora Sónia Mariza Florêncio Fidalgo

Coimbra, 2023

À minha família, por todo o amor, sacrifício e apoio incondicional.

Obrigada!

Resumo

O surgimento de recentes avanços tecnológicos tem obrigado à reforma e adaptação da vida em geral, o que se veio a refletir também na área do Direito Penal e no próprio processo. Estes avanços tecnológicos culminaram num novo tipo de prova, a prova digital. É hoje uma realidade inevitável no seio dos processos penais e é, muitas vezes, a única forma de se conseguir comprovar os factos relevantes para a existência ou inexistência de determinado crime.

Para um processo justo e equitativo é necessário pugnar pela manutenção da cadeia de custódia da prova, um procedimento tão importante que vai garantir a preservação da integridade dos meios de prova e que assegura a sua autenticidade, rastreabilidade e confiabilidade. O que se pretende garantir é que a prova recolhida é a mesma que vai ser discutida e posteriormente valorada em tribunal. Quando tal não aconteça, quando haja uma quebra na cadeia de custódia, as consequências são a inadmissibilidade da prova no processo e a proibição da sua valoração, uma vez que os dados aprendidos não transmitem a confiabilidade necessária para um processo justo.

Assim, a necessidade de adaptação às novas tecnologias também se refletiu na matéria da cadeia de custódia, uma vez que obrigou ao surgimento de novos procedimentos e técnicas de preservação para a prova digital. No entanto, em Portugal, se comparado com outros Ordenamentos Jurídicos, carecemos de regulação dos procedimentos a adotar para a preservação da prova digital e para a manutenção da sua cadeia de custódia. Deste silêncio da lei podem advir problemas processuais graves, que seriam evitados se tivéssemos um Manual de Procedimentos, semelhante ao que acontece em outros países.

Como se garante a fidedignidade da prova digital? Face às suas características especialíssimas, como se garante que não houve manipulação da prova por terceiros? Quais são as consequências da quebra da cadeia de custódia? Será a tecnologia Blockchain uma solução mais segura para a preservação da prova digital?

Palavras-chave: Cadeia de custódia, Prova Digital, Blockchain, Processo Penal

Abstract

The emergence of recent technological advances has forced the reform and adaptation of life in general, which has also been reflected in Criminal Law and in the process itself. These technological advances culminated in a new type of proof, the digital proof. It is today an inevitable reality within criminal proceedings and is often the only way to be able to prove the relevant facts for the existence or non-existence of a given crime.

For a fair and equitable process, it is necessary to strive for the maintenance of the chain of custody of the evidence, a procedure that is so important that it will guarantee the integrity's preservation of the evidence and that ensures its authenticity, traceability, reliability and preservation. What is intended to be guaranteed is that the evidence collected is the same that will be discussed and, subsequently, valued in court. When this does not happen, when there is a break in the chain of custody, the consequences are the inadmissibility of the evidence in the process and the prohibition of its valuation since the learned data do not transmit the necessary reliability for a fair process.

Thus, the need to adapt to new technologies was also reflected in the matter of chain of custody since it forced the emergence of new preservation procedures and techniques for digital evidence. However, in Portugal, compared to other legal systems, we lack regulation of the procedures to be adopted for the preservation of digital evidence and the maintenance of its chain of custody. This silence of the law can result in serious procedural problems, which would be avoidable if we had a Manual of procedures, similar to what happens in other countries.

How is the reliability of digital evidence guaranteed? In view of its very special characteristics, how can you guarantee that there was no manipulation of the test by third parties? What are the consequences of breaking the chain of custody? Is Blockchain technology a more secure solution for preserving digital evidence?

Keywords: Chain of Custody, Digital Evidence, Blockchain, Criminal Procedure law

Abreviaturas e Siglas

Ac. – Acórdão

ACPO – Association of Chief Police Officers

ADN – Ácido Desoxirribonucleico

Al. – Alínea

Art. – Artigo

BNP – Banque Nationale de Paris

CPP – Código Processo Penal

CRP – Constituição da República Portuguesa

ENFSI – European Network of Forensic Science Institutes

EUA – Estados Unidos da América

FDIS – Final Draft International Standard

HSBC – Hong Kong and Shanghai Banking Corporation

IEC – International Electrotechnical Commission

IETF – Internet Engineering Task Force

IP – Internet Protocol

ISO – International Organization for Standardization

LC – Lei do Cibercrime

MD 5 – Message-Digest Algorithm 5

MP – Ministério Público

N. º – Número

NIST – National Institute of Standards and Technology

ONU – Organização das Nações Unidas

OPC – Órgãos de polícia criminal

P. – Página

Pp. – Páginas

P2P – Peer-to-peer

PJ – Polícia Judiciária

RAM – Random Access Memory

STC – Sentença do Tribunal Constitucional

STS – Sentença do Tribunal Supremo

SWGDE – Scientific Working Group on Digital Evidence

TIC – Tecnologias da Informação e Comunicação

UNC3T – Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

URL – Uniform Resource Locator

USB – Universal Serial Bus

VOL – Volume

VPN – Virtual Private Network

Índice

Introdução

A sociedade atual está a viver a chamada Quarta Revolução Industrial que nos tem brindado com significativos avanços informáticos, assim como diversas mudanças na vida em geral, na sociedade, mas também no direito. Mudanças estas que, por um lado, vieram tornar o nosso dia a dia mais fácil e agradável, mas que no campo do direito obrigaram a grandes reajustamentos e, muitas vezes, levaram a problemas para os quais ainda não há respostas em muitos ordenamentos jurídicos. A par dos crescentes avanços tecnológicos surgiram também novas formas de criminalidade, de que é exemplo a criminalidade informática, que aumentou exponencialmente nos últimos anos, e que obrigou o direito a adaptar-se a novos tipos de prova, a prova digital. Atualmente, para a investigação da grande maioria dos crimes, é necessário a recolha de prova em formato digital. Para além disso, a prova digital não se cinge a crimes em que o elemento digital integre o tipo legal, mas estende-se a qualquer crime levado a cabo por meios informáticos, ainda que estes tenham sido apenas um instrumento para a prática do crime, não integrando o seu tipo legal.

Com o aparecimento deste tipo de criminalidade, os ordenamentos jurídicos tiveram de se adaptar às novas realidades, quer a nível de recolha da prova, quer ao nível dos procedimentos usados para a sua preservação. Surgiu assim a Lei n.º 109/2009, de 15 de setembro, onde encontramos novos meios de obtenção de prova digital, assim como um conjunto de crimes estritamente informáticos, em que o elemento digital surge como parte integrante do tipo legal ou seu objeto de proteção. Perante tantas inovações, foi também necessário adaptar os procedimentos para a manutenção da cadeia de custódia da prova digital em Portugal, que exigem técnicas especificas da área informática.

O ordenamento jurídico português carece de regulação nesta matéria da cadeia de custódia. A cadeia de custódia tem uma grande importância no processo penal porque são estes procedimentos que evitam que o juiz venha a ter qualquer tipo de dúvida sobre a origem da prova e sobre a sua autenticidade. A validade de determinada prova depende da conservação da cadeia de custódia que, caso seja interrompida, pode causar a inadmissibilidade do seu uso e o comprometimento de todo o processo penal.

Por outro lado, a manutenção da cadeia de custódia depende dos procedimentos usados para a recolha, análise e preservação da prova digital. Em Portugal, os procedimentos

que devem seguir os órgãos de polícia criminal no âmbito de uma investigação em que seja necessária a recolha de prova digital, resultam de recomendações de boas práticas de recolha e armazenamento da prova, feitas por entidades internacionais - o que é criticável, uma vez que outros ordenamentos jurídicos já dispõem de manuais de procedimento sobre a cadeia de custódia que permitem reduzir incertezas sobre o modo como se deve proceder.

Serão as técnicas usadas para a preservação da prova digital as mais adequadas, tendo em conta as especificidades deste tipo de prova? Ou haverá opções mais seguras? Que impacto as tecnologias podem ter no processo judicial?

É na sequência destas questões tão importantes que ousamos sugerir o uso da tecnologia Blockchain aplicado ao sistema de justiça penal. A blockchain é uma tecnologia recente, mas que em poucos anos já mostrou ser confiável e uma mais-valia quando aplicada ao Setor Público, assim como se aplicada aos Tribunais, pelo que já podemos contar com diversos casos de sucesso espalhadas pelo mundo.

Acreditamos que o uso da tecnologia blockchain será uma mais-valia para o processo penal, uma vez que luta pela manutenção da cadeia de custódia. Com o registo da prova na Blockchain, esta tornar-se-ia praticamente imutável, seriam registados o horário e a data em que foi inserida, a pessoa que a inseriu e quem lhe teve acesso, ou seja, fica tudo registado como se de um livro-razão se tratasse. Como é uma tecnologia descentralizada traduz-se numa maior confiabilidade e segurança no armazenamento da prova, possibilita a imutabilidade e integridade dos dados e, consequentemente, uma maior confiança.

Em suma, como ponto de partida, faremos uma breve exposição sobre os princípios mais importantes para o tema, seguida de uma exposição sobre a prova digital, que se revela essencial para que possamos depois passar ao capítulo seguinte, sobre a cadeia de custódia da prova digital e a sua importância para o processo penal. Apenas em último momento é que analisaremos as vantagens da aplicabilidade da tecnologia blockchain no seio dos tribunais, para preservação da prova digital. Antes de terminar esta breve exposição sobre o tema, atrevemo-nos já a afirmar que, pelo menos, esta será uma forma de acompanharmos o desenvolvimento tecnológico dos países que nos rodeiam.

Ciente de que é um tema inovador e complexo, pretendemos com ele trazer possíveis soluções processuais, quer para o panorama atual, quer para o futuro.

1. Princípios constitucionais e processuais penais relativos à prova e à cadeia de custódia

Dando início à investigação sobre a prova digital, entendo ser importante, antes de passar para o tema principal desta dissertação, fazer uma referência aos mais importantes princípios constitucionais e processuais penais relativos à prova e à cadeia de custódia, princípios estes que revelam os valores da nossa comunidade.

Nas palavras de Figueiredo Dias, são estes "princípios gerais do processo penal que dão sentido à multidão das normas, orientação ao legislador e permitem à dogmática não apenas explicar, mas verdadeiramente compreender os problemas de direito processual penal e caminhar com segurança ao encontro da solução"[1].

Para além dos princípios genéricos de processo penal ao nível da prova, iremos também abordar alguns princípios específicos relacionados com a cadeia de custódia da prova digital, são eles o *princípio da não alteração da prova eletrónico-digital no ato de recolha*, o *princípio da especialização ou qualificação do pessoal de investigação forense digital*, o *princípio da documentação de todas as fases de acesso, recolha, armazenamento, transferência, preservação ou apresentação/repetição da prova eletrónico-digital*, o *princípio da pessoalidade do controlo da cadeia de custódia da produção da prova eletrónico-digital* e, por fim, o *princípio da responsabilização repartida dos vários intervenientes na produção da prova eletrónico-digital no respeito dos princípios forenses digitais*[2].

Por uma questão de organização sistemática, os princípios gerais estão divididos em quatro grupos distintos: relativos à promoção processual, onde encontramos os princípios da oficialidade, legalidade e acusação; relativos à prossecução, onde se compreendem os princípios da investigação, contraditoriedade e audiência, suficiência e concentração; nos princípios relativos à forma encontramos os princípios da publicidade, oralidade e imediação

[1] Cf. DIAS, Jorge Figueiredo, *Direito processual penal*, Vol. 1, Coimbra: Coimbra Editora, 2004, p.112
[2] Cf. RODRIGUES, Benjamin Silva, *Direito Penal Parte Especial Tomo I – Direito Penal informático-Digital*, Coimbra: Coimbra Editora, 2009, pp. 726-728

e, por último, os princípios gerais relativos à prova, que compreendem os princípios da investigação, legalidade da prova, livre apreciação da prova e princípio in dubio pro reo[3].

O Direito Processual Penal e a Constituição têm uma estreita relação de proximidade, o que se traduz numa multiplicidade de normas que se referem ao processo penal espalhadas pela Lei Fundamental. Claus Roxin[4] chegou a afirmar que o processo penal é "sismógrafo da constituição de um Estado". Autores como Henkel[5] afirmam que o processo penal é um verdadeiro direito constitucional aplicado, numa dupla dimensão: os fundamentos do direito processual penal são, simultaneamente, os alicerces constitucionais do Estado; a concreta regulamentação de singulares problemas processuais deve ser conformada jurídico-constitucionalmente.

A Constituição atual, de 1976, é o texto constitucional que dispõe de mais artigos dedicados ao processo penal, onde se destacam as normas relativas aos direitos dos sujeitos processuais e ainda princípios constitucionais, desde logo, o princípio da dignidade da pessoa humana logo no artigo 1.º da CRP, o princípio do contraditório, o princípio do juiz legal e o princípio da presunção de inocência, previstos no artigo 32.º da Constituição.

1.1. Princípios constitucionais e processuais penais relativos à prova

O (1) *princípio da investigação ou princípio da verdade material,* é um princípio da prossecução processual penal, mas também um princípio geral da prova porque, como já dissemos anteriormente, esta divisão não é estanque. Está consagrado no artigo 340.º n.º 1 do CPP, segundo o qual o tribunal investiga o facto sujeito a julgamento independentemente dos contributos da defesa e da acusação, constituindo de forma autónoma as bases para a decisão final da causa, de forma a chegar à verdade material, ou seja, a verdade que se obtenha de forma válida no processo[6].

[3] Esta divisão entre os princípios não é rígida, uma vez que há princípios que estão compreendidos em diferentes grupos, como é o caso do princípio da investigação.
[4] Como destaca Claus Roxin, *Strafverfahrensrecht*, München, 1987, citado por ANTUNES, Maria João, *Direito Processual Penal*, Coimbra: Almedina, 2021, p.21
[5] Citado por DIAS, Jorge Figueiredo, *Direito processual penal*..., *cit.*, p.74
[6] Cf. SANTOS, Gil Moreira dos, *Princípios e Prática Processual Penal*, Coimbra: Coimbra Editora, 2014 p.53

Apesar de estar consagrado num dos artigos que se referem à fase da audiência de julgamento e valer para o juiz de julgamento, não se resume exclusivamente a este, vale também para o juiz de instrução, o que podemos confirmar pelo disposto nos artigos 288.º n.º 4, 289.º n. º1 e 290.º n.º 1 do CPP.

A este princípio opõe-se o princípio do dispositivo, de contradição ou discussão, segundo o qual são as partes, a acusação e a defesa, que dispõem do processo. Ou seja, cabe às partes carrear para o processo provas e factos, conduzindo o processo, contradizendo e afirmando, segundo a lógica de um princípio de autorresponsabilidade probatória das partes. O juiz só poderá ter em conta os factos e as provas anexadas pelas partes e tem um papel passivo, em que se limitará a zelar pela observância de normas processuais e, no final, proclamar o resultado obtido[7].

No princípio da investigação, contrariamente à passividade dos juízes do princípio do dispositivo, o juiz tem um verdadeiro poder-dever de investigação, tem um ónus de esclarecer oficiosamente os factos, independentemente das contribuições dos sujeitos processuais[8].

O (2) *princípio da legalidade da prova* está consagrado no artigo 125.º do CPP, onde consta que "são admissíveis as provas que não forem proibidas por lei". Este artigo tem uma estreita ligação com o artigo 32.º n.º 8 da Constituição, onde consta uma lista de provas proibidas – "são nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações" e, também, com o artigo 126.º do CPP quanto aos métodos proibidos de prova.

Este princípio é considerado por alguns autores, como sublinha Castanheira Neves[9], como um limite ao princípio da investigação - "só poderão utilizar-se os meios de prova legalmente admitidos (…), ficando excluídos certos processos porventura eficazes, mas atentatórios de valores fundamentais", constituindo, por vezes, um entrave à descoberta da verdade material.

[7] Vide. ANTUNES, Maria João, *Direito Processual Penal*, Coimbra: Almedina, 2011, p.185
[8] Idem.
[9] Cf. NEVES, António Castanheira, *Sumários de processo criminal*: 1967-1968, Coimbra, 1968, p.45

O desrespeito por este princípio vai culminar na nulidade das provas[10], não podendo estas ser utilizadas. Citando Maria João Antunes, "à sanção da nulidade acresce a proibição de valoração da prova obtida através de métodos de prova proibidos"[11].

O (3) *princípio da livre apreciação da prova* está consagrado no artigo 127.º do CPP, segundo o qual "*Salvo quando a lei dispuser diferentemente, a prova é apreciada segundo as regras da experiência e a livre convicção da entidade competente"*, ou seja, a valoração da prova faz-se com base na livre valoração do juiz e a sua convicção pessoal – vigora entre nós um sistema de prova livre, ao qual se contrapõe o sistema de prova legal.

O sistema de prova legal caracteriza-se por haver regras legais que predeterminam o valor a atribuir a cada prova[12]. O facto de o juiz estar obrigado a valorar as provas de acordo com o que está predeterminado pelo legislador, sem ter o poder de apreciar livremente, levou a que este sistema perdesse valor, tanto para a eficácia do processo, como para chegar à verdade[13].

A transição para o sistema atual, o sistema de prova livre, deu-se nas Reformas Judiciárias na primeira metade do séc. XIX[14]. Apesar deste princípio ter maior relevo na fase de julgamento, não deixa de valer para todo o decurso do processo penal e para "todos os órgãos de administração da justiça penal", onde se destacam o juiz de instrução e o MP.

O princípio desdobra-se em dois sentidos enunciados por Figueiredo Dias[15], (1) num sentido negativo, conforme já afirmamos, traduz-se numa ausência de critérios legais que predeterminam o valor da prova; (2) num sentido positivo, a análise da prova deve ser objetivável e motivável. A discricionariedade é sempre marcada por um limite – o dever de perseguir a verdade material.

---

[10] Vide. SILVA, Sandra Oliveira e, LEGALIDADE DA PROVA E PROVAS PROIBIDAS, Revista Portuguesa de Ciência Criminal, Ano 21, n.º 4, 2011, pp. 545 – 591

[11] Cf. ANTUNES, Maria João, *Direito Processual Penal*..., *cit.*, p.188

[12] Idem.

[13] Cf. RIVERA OLARTE, Francisco Javier e ROJAS QUINAYÁ, Lina Fernanda, Estudio interdisciplinario sobre los Sistemas de Valoración y Estándares Probatorios en el derecho procesal colombiano, DIXI, julio-diciembre 2019, pp. 1-49. Disponível em: https://doi.org/10.16925/2357-5891.2019.02.01. Consultado a 10 de dezembro de 2022

[14] Como destaca Eduardo Correia na Revista de Direito e de Estudos Sociais, citado por DIAS, Jorge Figueiredo, *Direito processual penal*, Vol. 1, Coimbra Editora, Coimbra, 2004, p. 201, nota 32

[15] Cf. DIAS, Jorge Figueiredo, *Direito processual penal*..., *cit.*, pp.198-206

Contudo, não podemos deixar de enunciar que este princípio não vale sem quaisquer limitações[16], como é o caso das declarações do arguido quando este confesse crimes puníveis com pena de prisão até 5 anos ou quando se remete ao silêncio, uma vez que este nunca pode ser valorado (arts. 61.º n. º1 alínea d) e 32.º n. º1 CRP) ou o caso das provas periciais (arts. 151.º e 163.º CPP), cujo juízo se presume subtraído à livre convicção do juiz, pois, em princípio releva aquilo que o perito disser[17].

Segundo o (4) *princípio do interesse público na realização da justiça*, esta corresponde a uma das finalidades essenciais que o nosso processo penal visa alcançar – justiça válida e efetiva. Este interesse público na realização da justiça não vale inteiramente, não é absoluto, pelo que podemos apontar alguns limites. Desde logo, como destaca Manuel Monteiro Valente no campo da prova, a intocabilidade da integridade da prova e a legalidade material e formal dos métodos de obtenção de prova, das técnicas jurídicas da sua conservação e manutenção sem quaisquer suspeitas ou presunções da sua manipulação do conteúdo probatório[18].

Em muitas situações este princípio enunciado pode esbarrar com o princípio do respeito dos direitos e interesses fundamentais dos cidadãos, que é, em especial, a defesa e garantia de direitos e liberdades fundamentais pessoais. É no decurso deste conflito que surgem normas que proíbem determinados meios de obtenção de prova e a sua valoração, como é o caso do artigo 126.º do CPP[19] e 32.º da CRP[20]. Por muito que haja interesse público

[16] Vide. ANTUNES, Maria João, *Direito Processual Penal*..., *cit.*, p.190

[17] O julgador tem a possibilidade de discordar do juízo do perito quando ele for também especialista na matéria que foi alvo de perícia. Contudo, tem sempre de fundamentar a sua divergência, como dispõe o n.º 2 do artigo 163.º do CPP,

[18] Cf. Valente, Manuel Monteiro Guedes, *Cadeira de custódia da prova*, Coimbra: Almedina, 2019, p.45

[19] Artigo 126.º CPP - (Métodos proibidos de prova) 1 - São nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas. 2 - São ofensivas da integridade física ou moral das pessoas as provas obtidas, mesmo que com consentimento delas, mediante: a) Perturbação da liberdade de vontade ou de decisão através de maus tratos, ofensas corporais, administração de meios de qualquer natureza, hipnose ou utilização de meios cruéis ou enganosos; b) Perturbação, por qualquer meio, da capacidade de memória ou de avaliação; c) Utilização da força, fora dos casos e dos limites permitidos pela lei; d) Ameaça com medida legalmente inadmissível e, bem assim, com denegação ou condicionamento da obtenção de benefício legalmente previsto; e) Promessa de vantagem legalmente inadmissível. 3 - Ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular. 4 - Se o uso dos métodos de obtenção de provas previstos neste artigo constituir crime, podem aquelas ser utilizadas com o fim exclusivo de proceder contra os agentes do mesmo

[20] Artigo 38.º CRP - (Garantias de processo criminal) N.º 8 - São nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações.

na realização da justiça há um limite inultrapassável que jamais pode ser comprometido – a dignidade da pessoa humana[21].

No processo penal é preciso alcançar prova justa, através de métodos que respeitem a legalidade material e processual e seja processualmente válida e admissível. Só atuando desta forma é que se promove a boa confiança entre Cidadãos – Estado, tão importante num Estado de Direito Democrático.

1.2. Princípios relativos à cadeia de custódia

Segundo o (1) *princípio da identidade e autenticidade da cadeia de custódia*, a cadeia de custódia pode ser definida como um conjunto de diligências que se destinam a assegurar a autenticidade e inalterabilidade das provas. Segundo Manuel Monteiro Valente, é "uma técnica jurídico-processual que garante a identidade e autenticidade da prova ab initio ad finem de todo o processo penal"[22], desde o momento em que se recolhe, através dos meios de obtenção de prova, ao contraditório. Claro está que a cadeia de custódia tem de respeitar os princípios constitucionais e processuais penais relativos à prova, sob pena de a prova contaminada, cuja cadeia de custódia foi violada, ficar inutilizada – o que analisaremos mais à frente.

O (2) *princípio da não alteração da prova eletrónico-digital no ato de recolha* sugere a proibição de alteração da prova digital no ato de recolha e tratamento da prova. Assim, o investigador forense deve, desde o momento de recolha da prova, até ao momento da apresentação dos resultados, ter o máximo de cuidado e zelo para não introduzir modificações nos dados recolhidos, ou seja, para não contaminar a prova recolhida com elementos estranhos ao sistema ou rede informática investigada, o que poderia prejudicar todo o processo penal[23].

[21] Artigo 1.º CRP – (República Portuguesa) - Portugal é uma República soberana, baseada na dignidade da pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária.
[22] Cf. VALENTE, Manuel Monteiro Guedes, *Cadeira de custódia ...*, *cit.*, p.45
[23] RODRIGUES, Benjamin Silva, *Direito Penal Parte Especial..., cit.,* p.726- 728

Segundo o (3) *princípio da especialização ou qualificação do pessoal de investigação forense digital*, o manuseamento da prova digital, ou seja, a sua recolha, análise e conservação da prova tem de ser levada a cabo por pessoas especializadas com os devidos conhecimentos técnico-científicos, sob pena de a prova se perder e não poder ser valorada no processo. Apenas estas pessoas formadas e especializadas estarão aptas para respeitar todas as práticas técnicas definidas internacionalmente, assim como os princípios internacionais em matéria de investigação forense digital[24].

O (4) *princípio da documentação de todas as fases de acesso, recolha, armazenamento, transferência, preservação ou apresentação/repetição da prova eletrónico-digital* está algo relacionado com o princípio anterior. Este princípio decreta que devem ser registadas todas as etapas de produção de prova, em todas as fases, desde o primeiro acesso até à sua apresentação. Apenas a documentação de todas as fases garante a cadeia de custódia da prova, permite-nos saber todos as pessoas que tiveram contacto com a prova e, ainda, a "reversão dinâmica", isto é, a repetição da prova, pelo que os investigadores deverão descrever da forma mais detalhada possível os resultados de cada fase[25].

O (5) *princípio da pessoalidade do controlo da cadeia de custódia da produção da prova eletrónico-digital* levanta a ideia da pessoalidade, ou seja, cada prova (recolhida, analisada e explicada) deve ser manuseada por um único técnico profissional forense ou por um conjunto de técnicos habilitados, que devem ser devidamente identificados e registados no processo[26]. Com isto, não é recomendada a ingerência no processo de terceiros que podem, mesmo sem ter essa intenção, contaminar a prova. O objetivo, mais uma vez, é evitar a perda da cadeia de custódia e a transtorno do processo no qual está a decorrer a investigação.

Por último, mas também de grande importância, é o (6) *princípio da responsabilização repartida dos vários intervenientes na produção da prova eletrónico-digital no respeito dos princípios forenses digitais*, que traduz a ideia de que cada profissional forense envolvido no processo de tratamento de prova deve ser responsável pela recolha, acesso, armazenamento ou transferência da prova que se encontre sob a sua alçada, respeitando os princípios forenses de produção e análise de prova definidos

[24] *Ibidem.*
[25] *Ibidem.*
[26] *Ibidem.*

internacionalmente e, desta forma, colaborar para a manutenção da integridade da prova digital obtida[27].

O respeito por estes princípios é de extrema importância para a validade e, posteriormente, para a valoração da prova em audiência de julgamento.

2. A prova digital no processo penal

2.1. Introdução à cibercriminalidade

Temos assistido, nos últimos anos, a um avanço exponencial nas tecnologias, que muitos apelidam de Quarta Revolução Industrial[28]. O que tem aumentado com estas é, também, a cibercriminalidade. Vivemos num mundo em que a tecnologia e a internet fazem parte do nosso dia a dia em sociedade, desde a administração pública, à atividade económico-financeira, à defesa nacional e até para termos acesso aos mais diversos conteúdos e serviços, quer a nível individual, quer institucional. É inegável que estes avanços tecnológicos nos ofereceram uma melhoria significativa da qualidade de vida, contudo, também é verdade que veio potenciar a prática de atos ilícitos que facilmente ofendem bens jurídicos individuais coletivos e até mesmo a estrutura organizativa da sociedade.

Definir cibercrime nem sempre foi uma tarefa fácil e unânime. O Departamento de Justiça dos EUA, em 1989, definia "computer crime" como sendo qualquer violação da lei criminal que envolvesse conhecimentos de tecnologias de computadores para a sua penetração, investigação ou acusação[29]. Em 2010, no Congresso das Nações Unidas para a Prevenção do Crime e Tratamento das Vítimas, surgiram novos conceitos: Cibercrime em sentido estrito, que corresponderia a "qualquer comportamento ilegal, conduzido através de meios eletrónicos, cujo alvo fosse a segurança de sistemas de computadores e os dados neles alojados" e cibercrime em sentido lato, que "cobriria qualquer comportamento ilegal

[27] *Ibidem.*
[28] Cf. FIDALGO, Sónia. "A utilização de inteligência artificial no âmbito da prova digital - direitos fundamentais (ainda mais) em perigo", in A. M. Rodrigues, *A Inteligência Artificial no Direito Penal,* Coimbra: Almedina, 2020, pp.129-161
[29] Vide. NATÁRIO, Rui, «O combate ao cibercrime: anarquia e ordem no ciberespaço», *Revista Militar*, n.º 2541, 2013, disponível *in*: https://www.revistamilitar.pt/artigo/854

cometido por meio de, ou relacionado com, sistemas ou redes de computadores, incluindo crimes como a posse ilegal e distribuição de informação através de sistemas ou redes de computadores"[30]. Em 2001, a Convenção sobre Cibercrime do Conselho da Europa definiu cibercrime como sendo um "vasto leque de atividade que se enquadram em quatro categorias genéricas de crimes relacionadas com computadores: violações de segurança, fraude e falsificação, pornografia infantil e violação de direitos de autor"[31]. Em Portugal, a Lei n.º 109/2009, de 15 de setembro, conhecida como Lei do Cibercrime (LC), optou por não definir o que é o cibercrime, face à dificuldade de encontrar um conceito uniforme.

De grande contributo é a definição que Pedro Dias Venâncio nos oferece, distinguindo criminalidade informática em sentido amplo, de criminalidade informática em sentido estrito. Num sentido amplo, "englobará toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios"[32]. Por outro lado, em sentido estrito[33], corresponderá aos "crimes em que o elemento digital surge como parte integrador do tipo legal ou seu objeto de proteção", ou seja, recorre-se aos meios informáticos para a prática do crime[34].

Apesar de não haver uma noção estanque para este tipo de criminalidade, podemos identificar algumas características comuns a todas as noções: (1) internacionalização e transnacionalização – um cibercriminoso tem a capacidade de cometer crimes e vitimizar pessoas ou governos que se encontrem em qualquer parte do mundo, porque no mundo cibernético não há fronteiras; (2) anonimato e "cultura de supressão da prova" – na criminalidade informática há uma maior facilidade de manter o anonimato e, consequentemente, uma dificuldade acrescida de recolher prova sobre o crime e sobre o seu autor; (3) utilização e movimentação de maiores materiais e pessoas, nomeadamente o recrutamento de jovens e membros em ambientes marginais – a maioria dos grupos organizados são transnacionais, com membros dispersos por todo o mundo, com uma

[30] *Ibidem.*
[31] *Ibidem.*
[32] Abarca todos os crimes em que há a possibilidade de recorrer aos meios informáticos para a consumação. É disso exemplo uma ofensa à honra ou difamação em redes sociais, blogs ou através de correio eletrónico.
[33] Incluem-se na criminalidade em sentido estrito todos os crimes tipificados na LC.
[34] Cf. VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada*, 1º Edição, Coimbra: Coimbra Editora, 2011, p. 17

tendência para o recrutamento jovem; (4) elevado impacto financeiro, que é incalculável, uma vez que os dados disponíveis fornecidos pelas vitimas não correspondem aos valores reais[35].

Toda a tecnologia envolvida, como as "técnicas de encriptação, esteganografia, a compressão digital e o aumento da literacia computacional"[36] e, por outro lado, o lento desenvolvimento tecnológico dos Estados, incapazes de acompanhar a evolução tecnológica, tem dificultado, tanto em Portugal, como em todo o mundo, o combate a este crime virtual e transfronteiriço que se desenvolve a uma velocidade desmedida.

2.2. A prova digital em Portugal

2.2.1. Conceito da prova digital

Face à colossal progressão dos meios tecnológicos e da criminalidade informática, surgiu a necessidade de alterar o direito, ou seja, alterar e criar nos ordenamentos jurídicos novas leis que acompanhem estes desenvolvimentos e regular figuras como a da prova digital, de forma a combater este tão recente tipo de criminalidade. Com isto, surgiram novas técnicas de investigação, novos métodos de obtenção de prova, novos ramos de especialização e uma nova prova, a prova em suporte eletrónico.

A prova digital é admitida, desde logo, pelo artigo 125.º do CPP, segundo o qual "*são admissíveis as provas que não forem proibidas por lei".*

Não existem muitas definições de prova digital e nem mesmo o legislador português, na LC, nos brindou com um conceito, mas podemos destacar algumas definições relevantes de alguns autores.

O Scientific Working Group on Digital Evidence (SWGDE), definiu, em 1998, "digital evidence" como "qualquer informação com valor probatório que se encontra

[35] Vide. NATÁRIO, Rui, "O combate ao cibercrime..." *cit.* e RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial..., cit.* p. 265.
[36] Cf. VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada..., cit.,* p. 17

armazenada ou é transmitida sob a forma binária"[37]. Armando Dias Ramos definiu prova digital como "toda a informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações". Por outro lado, Benjamin Silva Rodrigues definiu prova digital como "qualquer tipo de informação, com valor probatório, armazenada em repositório eletrónico-digital de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis, sob a forma binaria ou digital"[38], definição que nos parece mais completa.

Podemos concluir que, comparando com outros tipos de prova, a grande diferença que reside entre elas é o formato em que se encontra. No entanto, é o formato digital que vai conseguir responder às crescentes necessidades sentidas na justiça face ao combate à criminalidade informática. Assim como os meios de obtenção previstos na Lei do cibercrime que, de outra forma e com os meios de prova tradicionais, seria impossível de aceder aos dados (tão relevantes para o processo) disponíveis em redes informáticas que nos levam a obter a verdade material.

2.2.2 Diplomas que regulam a prova digital

Temos muita legislação que se debruça sobre a prova digital e a criminalidade informática, mas esta encontra-se dispersa por vários diplomas, o que por vezes pode levantar problemas de harmonização.

Em 2009 surgiu a ainda atual Lei do cibercrime – Lei n. º109/2009, de 15 de setembro – que visou transpor para o ordenamento jurídico português a Decisão-quadro 2005/222/JAI e adaptar o direito interno à Convenção sobre o Cibercrime do Conselho da Europa[39].

---

[37] Vide. WHITCOMB, Carrie Morgan, "An Historical Perspective of Digital Evidence: A Forensic Scientist's View", *International Journal of Digital Evidence*, Spring 2002 Volume 1, Issue 1. Disponível em: https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf. Consultado a 10 de dezembro de 2022

[38] Cf. RODRIGUES, Benjamim Silva*, Direito Penal Parte Especial..., cit.*, p. 722

[39] Art. 1.º da LC - "A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa".

A Lei n.º 109/2009, de 15 de setembro é o diploma base que regula a prova digital. Introduziu e ampliou diversos conceitos jurídico-informáticos[40], revogou a Lei n.º 109/91 de 17 de agosto[41] e alargou os tipos incriminadores, estabeleceu o princípio da competência universal, consagrou regras processuais de obtenção de prova digital, regulou as obrigações de preservação de prova digital para quem tenha a disponibilidade ou o controlo sobre os dados informáticos, ou seja, as operadoras de comunicação e introduziu medidas de cooperação internacional no que alude à obtenção de prova digital[42]. Veio introduzir na ordem jurídica portuguesa novos meios de recolha de prova em suporte eletrónico, que permitem responder aos desafios colocados pela nova criminalidade e suprir lacunas que se colocavam no nosso ordenamento jurídico. Veio ainda alargar a aplicação destas novas normas aos crimes cometidos por meio informático e aos processos em que seja necessário a recolha de prova em suporte eletrónico[43], conforme nos diz o artigo 11.º da LC (que define o âmbito de aplicação das disposições processuais) – ou seja, são aplicáveis, em abstrato, a todos os crimes, pelo que não se entende por que razão não foram introduzidas no CPP. Paulo Dá Mesquita é bastante crítico desta opção do legislador e defende que a integração no Código de Processo Penal seria "a opção mais coerente com a tradição portuguesa, em face da geral inconveniência de ver dispersas em leis extravagantes regras gerais carecidas de enquadramento no código de Processo Penal enquanto diploma estruturante, e a conveniência prática, para os operadores judiciários, de aí ter sistematizados todos os normativos que não são apenas aplicáveis a um setor especifico da criminalidade no Código de Processo Penal"[44]. Antes da entrada em vigor da Lei do Cibercrime, a "investigação dos crimes relacionados com a informática fazia-se recorrendo às regras gerais do Código de Processo Penal"[45].

[40] No art. 2.º da LC encontramos as definições de sistema informático, dados informáticos, dados de tráfego, fornecedor de serviço, interceção, topografia e produto semicondutor.
[41] Também conhecida por Lei da Criminalidade Informática, foi o primeiro diploma em Portugal a debruçar-se sobre prova digital, mas a natureza transfronteiriça cedo levou cedo levantou a necessidade de criar normas internacionais de forma a harmonizar toda a matéria sobre criminalidade informática.
[42] Vide. MILITÃO, Renato Lopes, "A propósito da prova digital no processo penal", *Revista da Ordem dos Advogados*, Lisboa, Ano 72, vol. 1 (Janeiro-Março 2012), p. 247-285
[43] Por exemplo, um crime de ameaça ou difamação cometido em redes sociais ou um homicídio em que haja SMS com o plano do crime.
[44] Cf. MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário,* Coimbra: Wolters Kluwer / Coimbra Editora, 2010, p. 101.
[45] Cf. FIDALGO, Sónia, "A utilização de inteligência artificial...", *cit.*, pp. 129-161

A LC consolidou num único diploma grande parte das normas relativas à criminalidade informática. Como nos diz Pedro Verdelho, "por esta lei são introduzidas na ordem jurídica portuguesa disposições inovadoras, criando novas figuras processuais. Por outro lado, são adaptadas ao ambiente informático, ou digital, institutos de processo penal que, em si mesmos, não conseguiriam adequar-se às novas realidades tecnológicas"[46].

2.2.3. Características da prova digital

Após o estudo do conceito de prova digital, passamos agora a elencar as suas características que a individualizam dos outros meios de prova e a tornam especial. Face à sua natureza e características vimos surgir um novo cenário de recolha, conservação e apresentação de prova em sede de audiência de julgamento, ou seja, uma realidade bastante distinta da que estávamos habituados, porque não é a mesma coisa apreender uma carta ou um email. Algumas destas características que vamos analisar de seguida vão levantar algumas problemáticas e dificuldades que se vão fazer sentir na sua utilização, mais propriamente na sua apreensão, busca e análise. Podemos já afirmar que prova digital exige ser tratada de um modo delicado, sob pena de perder a sua integridade e se tornar inutilizável, comprometendo o êxito da investigação e de todo o processo penal.

Uma das principais características identificados por Benjamin Silva Rodrigues[47] corresponde à imaterialidade ou à inexistência de uma natureza palpável. Neste sentido, a descoberta de provas em ambiente digital exige determinadas técnicas e conhecimentos do investigador forense que, de outra maneira, não se conseguiriam captar porque continuariam invisíveis aos olhos do homem comum. A imaterialidade permite a acumulação de grandes quantidades de informações e de dados nos dispositivos e no próprio ambiente digital o que pode vir a ser um fator dificultador da investigação.

Detém, por vezes, um carácter temporário e efémero, o que obriga os investigadores a terem um trabalho redobrado, exigindo maior celeridade e cuidados na colheita. Pode

[46] Cf. VERDELHO, Pedro, A nova Lei do Cibercrime, *"SCIENTIA IVRIDICA", Revista de Direito Comparado Português e Brasileiro,* outubro – dezembro, 2009, TOMO LVIII, n.º 320, pp. 733-734
[47] Cf. RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial..., cit.*, p.724-726

acontecer que a prova não tenha uma durabilidade bastante que permita a sua congelação para garantir a sua preservação. No entanto, e devido às técnicas de preservação que nos permitem transformar a prova em algo permanente e estável, entendemos que esta característica – o carácter temporário – não deve ser atribuída a toda e qualquer prova digital[48].

A prova digital caracteriza-se também por ser frágil e suscetível de alterabilidade**.** Desta forma, o investigador ao recolher os vestígios da prova terá de identificar de forma precisa e rigorosa o tipo de prova em causa e é esta operação classificatória que garante a inalterabilidade ou até mesmo o possível desaparecimento desta. É muito fácil conseguir fazer desaparecer provas digitais, bastando um clique para todo o material probatório ser eliminado – por vezes basta apagar o histórico de navegação para vermos a investigação comprometida[49].

Para além de frágil, a prova digital é também volátil ou instável, característica que advém da possibilidade da sua alteração ou desaparecimento. Por ser uma prova imaterial e mutável, composta por uma sequência numérica, facilmente se consegue alterar e prejudicar a confiabilidade da prova. Estas alterações podem resultar de um ato propositado ou pode tratar-se de um acidente, por exemplo, pode tratar-se de um descuido por parte do investigador. É muito comum o investigador forense num primeiro momento encontrar uma prova com determinadas características e, num segundo momento, encontrar a mesma alterada, parcialmente ou na sua totalidade, fruto da sua natureza volátil[50].

A recolha de prova digital exige do investigador especiais conhecimentos técnicos e científicos devido à complexidade e à codificação que caracterizam grande parte das provas digitais. O acesso às redes e sistemas informáticos deve ser feita por pessoal qualificado para tal, munido de técnicas de desencriptação e de conhecimentos digitais. É neste sentido que podemos falar do "princípio da especialização ou qualificação do pessoal de investigação forense digital", segundo o qual "o acesso, recolha, conservação e análise da prova forense tem de ser levada a cabo por pessoal especializado, com conhecimentos técnico-científicos, sob pena de a mesma poder ser contaminada ou não corretamente manuseada e, desse jeito,

[48] *Ibidem.*
[49] *Ibidem.*
[50] *Ibidem.*

para sempre perdida para o processo penal"[51]. Os problemas podem surgir na parte da apreciação da prova por parte da entidade competente. Para os técnicos informáticos e os especialistas da área é fácil traçar a relação entre determinado meio de prova, o crime e o seu autor, mas para a grande maioria dos juristas, delinear esta ligação pode vir a tornar-se um verdadeiro desafio. Nem todos os juízes estão familiarizados com os termos tipicamente informáticos, muitos nem receberam formação adequada para lidar com este tipo de criminalidade e os avanços tão acelerados que se registam nas tecnologias não colaboram. Por estas razões é que é tão importante investir em formações nos tribunais para conseguir atualizar os nossos profissionais e, também, sempre que possível, disponibilizar peritos informáticos para os auxiliarem nos processos.

Outra característica que podemos identificar é a dispersão da prova. Por vezes, a prova digital encontra-se dispersa por vários computadores, redes e sistemas informáticos que se estendem além-fronteiras, contrariamente à realidade que nos apresenta a criminalidade no mundo físico. Uma vez que para cometer um crime informático apenas precisamos de um computador ligado à internet, é muito habitual encontrarmos crimes que foram cometidos do outro lado do mundo e a dificuldade acresce quando se usam redes de locais públicos ou cibercafés. Ou seja, é muito raro encontrarmos provas digitais no local exato do crime porque a grande maioria deles são cometidos à distância. Para além disto, podem surgir dificuldades em determinar o momento em que foi cometido o crime, uma vez que muitos dos autores do crime preparam os seus dispositivos antes de os cometerem, instalando nos seus dispositivos uma VPN[52] que vai ocultar a sua verdadeira identidade e, para além de ocultar o verdadeiro IP, ainda fornece outro IP fictício. Com todas estas técnicas conseguem limpar grande parte do rasto que deixam na web ou, pelo menos, atrasar e confundir as investigações[53].

A última característica que Benjamin Silva Rodrigues nos oferece é o dinamismo e mutabilidade da prova, uma vez que a prova digital corresponde a impulsos eletromagnéticos que assumem, momentaneamente e dinamicamente, um papel nas redes e sistemas informáticos. Desta forma, os investigadores terão de realizar uma investigação comparativa

[51] Cf. RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial..., cit.,* p.727
[52] VPN - "Virtual Private Network" (Rede Privada Virtual) - protege os utilizadores ao encriptar os dados e mascarar o endereço IP, deixando o histórico de navegação e a localização impossíveis de controlar.
[53] Vide. RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial..., cit.,* p.727

e temporalmente recortada em distintos espaços para poder perceber e aceder à prova digital mais relevante para a investigação e para o processo[54].

Para além destas, é importante referir ainda outras duas características identificadas por Denise Provasi Vaz. São elas a suscetibilidade de clonagem e necessidade de intermediação.

A clonagem corresponde à elaboração de uma cópia fiel de determinado arquivo digital, contendo exatamente a mesma quantidade de bits que o arquivo original. Por se tratar de um dado digital imaterial, com uma sequência numérica, é fácil a sua transferência integral para outros dispositivos e, consequentemente, facilitar a investigação[55].

Por fim, e no seguimento da característica anterior, uma vez que a prova digital corresponde a um código digital, surge, por vezes, a necessidade de intermediação, isto é, é necessário o uso de softwares, hardwares e equipamentos eletrónicos (como por exemplo, monitores ou impressoras) para processar o código, descodificar a informação e torná-la compreensível ao olho humano[56].

Podemos concluir que dados informáticos e metadados podem ser facilmente corrompidos, alterados ou suprimidos, daí ser necessário um especial cuidado no seu manuseamento, que deve ser feito apenas por profissionais qualificados. Como afirma Armando Dias Ramos, "a rapidez na sua obtenção, aliada a uma correta recolha de prova, são essenciais para o êxito da investigação e imputação dos factos ao suspeito do crime"[57].

2.3. Validade e valoração da prova digital

É inegável que a prova digital é, grande parte das vezes, a única forma de apurar a veracidade dos factos alegados no processo pelos sujeitos processuais e de permitir uma adequada investigação de um crime. É de extrema importância a valoração desta prova,

[54] *Ibidem.*
[55] Vide. VAZ, Denise Provasi, *Provas digitais no processo penal: Formulação do conceito, definição das características e sistematização do procedimento probatório*, Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012, pp.69-70. Tese de doutoramento
[56] Idem.
[57] Cf., Armando Dias, *A prova digital em processo penal: o correio eletrónico*, 1º Edição, Lisboa: Chiado Editora, 2014, p.87

contudo, têm de ser respeitados determinados requisitos para a sua admissibilidade como meio de prova, que analisaremos em seguida.

As provas digitais são admissíveis em tribunal, desde logo, pelo determinado no artigo 125.º do CPP, segundo o qual "são admissíveis as provas que não forem proibidas por lei", o que traduz uma "abertura do sistema" e uma "liberdade das formas aquisitivas"[58] da prova, que advém da consciência do legislador que é incapaz de prever e adiantar todos os desenvolvimentos do mundo quotidiano. Está aqui plasmado o princípio da legalidade já analisado previamente. Esta liberdade funciona a favor da obtenção de prova digital em ambiente digital e exprime a ideia de favorecimento da descoberta material. No entanto, há sempre um limite à descoberta da verdade material que corresponde ao respeito pelos direitos fundamentais do arguido, conforme o disposto no artigo 32.º da Constituição, sob a epigrafe "Garantias do processo criminal".

A prova digital pode ser valorada, e é mesmo necessária, quando não exista outro meio idóneo para formar a convicção do julgador, para alimentar as bases da decisão da causa. A verdade é que para a investigação da grande maioria dos crimes previstos na LC será necessária a recolha de prova digital.

Relativamente à validade e valoração da prova, diz-nos Armando Dias Ramos que a prova digital só poderá ser valorada se estiverem reunidas as seguintes condições: "existir integridade dos dados", "registo da cadeia de custódia da prova", "suporte técnico", "formação profissional" e, por fim, "conformidade com as normas legais em vigor"[59].

A prova digital carece de dois requisitos essenciais de admissibilidade: o (1) cumprimento da lei e o (2) cumprimento das melhores práticas técnicas internacionalmente definidas – é sobre estes que nos vamos debruçar de seguida.

Quanto ao (1) cumprimento da lei, podemos identificar as leis mais relevantes. A LC é o diploma principal e mais relevante, onde se encontra o regime geral da prova digital.

---

[58]Cf. ALBERGARIA, Pedro Soares, "Anotação ao artigo 125.º do CPP – Legalidade da prova", *in*: *Comentário Judiciário do Código de Processo Penal*, Tomo II, Coimbra: Almedina, 2ª ed., 2020, pp. 29-36

[59] Cf. RAMOS, Armando Dias, Os meios de prova a partir da internet e das redes sociais no processo penal, IX Encontro nacional do IAPI, 2015. Obtido de apresentação disponível em: https://portal.oa.pt/media/119968/os-meios-de-prova-a-partir-da-internet-e-das-redes-sociais-no-processo-penal.pdf. Consultado a 10 de dezembro de 2022

Para além do regime geral, há outros diplomas relevantes, como o CPP[60], a Lei n.º 5/2004 – Lei das Comunicações Eletrónicas, a Lei n.º 7/2004 – sobre o Comércio Eletrónico no Mercado Interno e Tratamento de Dados, a Lei n.º 41/2004 – Tratamento de dados pessoais e proteção da privacidade nas telecomunicações e a Lei n.º 59/2019 – Lei de Proteção de Dados Pessoais.

A LC contém o regime geral de obtenção de prova digital e, no artigo 11.º, define que as disposições processuais que se encontram entre os artigos 12.º a 17.º, são aplicáveis em relação aos crimes informáticos em sentido estrito, ou seja, os crimes que se encontram na LC, aos crimes cometidos por meio de um sistema informático e em relação aos crimes em que seja necessário proceder à recolha de prova em suporte eletrónico – podemos já concluir que para a investigação de qualquer crime pode haver necessidade de recolha de prova em suporte eletrónico.

Quanto aos meios de obtenção de prova, nos artigos 12.º e 13.º da LC, encontramos medidas cautelares de produção de prova, são elas a preservação expedita de dados e a revelação expedita de dados. Nos artigos que se seguem podemos identificar outras formas de produção de prova digital que conduzem à apreensão (art. 16.º LC), uma vez que sem a apreensão a prova não poderia ser valorada: a injunção para apresentação ou concessão de acesso a dados no artigo 14.º; a pesquisa de dados informáticos no artigo 15.º, que corresponde à figura da busca; no artigo 19.º, está prevista a ação encoberta no decurso da qual também se podem apreender dados informáticos; paralelamente a estes meios, temos a interceção de comunicações prevista no artigo 18.º e que se aplica aos dados em transmissão, ou seja, ocorre em tempo real quanto a dados que estão a ser transmitidos "em direto".

A apreensão de dados informáticos está prevista nos artigos 16.º e 17.º, e podemos fazer a distinção entre quatro regimes. No artigo 16.º, n.º 1 e n.º 2, está previsto o regime geral e apenas se aplica se não estivermos perante um caso de aplicação dos regimes especiais. Quantos aos regimes especiais, podemos distinguir o regime dos dados sensíveis, prevista no artigo 16.º n.º 3, para os casos em que estejam em causa dados cujo conteúdo seja suscetível de revelar dados sensíveis ou íntimos, pondo em causa a privacidade do titular

[60] É de grande relevância o artigo 189.º, n.º 2 - A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo.

ou até de terceiros, o regime dos segredos nos artigos 16.º n. º5 e n.º 6 que remete para o regime do CPP e, por fim, o regime da apreensão de correio eletrónico e registos de comunicações de natureza semelhante no artigo 17.º.

Pedro Dias Venâncio defende que estes meios processuais não devem ser considerados de forma isolada, mas sim de forma anexada, "analisado como um todo, pois em muitos aspetos práticos se relacionam e complementam"[61], uma vez que visam o mesmo objetivo – aceder a dados informáticos indispensáveis à investigação.

O segundo requisito de admissibilidade da prova digital corresponde à (2) obediência das boas práticas técnicas. Estas práticas foram definidas a nível internacional, mas não estão na sua totalidade positivadas na lei portuguesa[62]. No entanto, há casos em que se encontra plasmado na LC, como é o caso da pesquisa e apreensão de dados informáticos[63], em que o cumprimento das melhores práticas tem de ser respeitado, uma vez que a prova recolhida será depois sujeita ao princípio geral de livre apreciação (art. 127.º CPP) e daqui pode advir um problema. Diferentemente do que acontece com os outros meios de prova, dos meios de prova corpóreos, na prova digital as regras da experiência não têm um peso tão significativo, pois não é assim tão fácil perceber que uma prova digital foi manipulada. E também depende da prova digital em questão, porque se se tratar de uma dúvida na integridade de uma imagem pode ser submetida a uma perícia e facilmente descobrimos se se trata de uma imagem manipulada. Mas no caso de a prova se tratar de um ficheiro Excel já não será assim tão fácil perceber se houve manipulação. Por isso é tão importante o cumprimento das melhores práticas técnicas de recolha de prova para que não surjam duvidas ao decisor aquando da valoração da prova. Para além disso, é importante respeitar estas normas internacionais para, nos casos de investigações transnacionais, o que é muito comum neste tipo de criminalidade, se possa valorar a prova em distintos países, pugnando pelo cumprimento dos artigos 20.º e seguintes da LC, relativos à cooperação internacional.

Em Portugal, a prevenção, deteção e investigação criminal dos crimes informáticos compete à Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

[61] Cf. VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada..., cit.* p. 99

[62] Por não estarem positivadas na lei pode questionar-se se é um verdadeiro requisito de admissibilidade.

[63] No artigo 16.º n.º 7 estão previstas as formas para se preceder à apreensão de dados informáticos: apreensão do suporte físico; realização de uma cópia dos dados; preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; eliminação não reversível ou bloqueio do acesso a dados. No entanto, apenas as duas primeiras são verdadeiras formas de apreensão de prova, uma vez que as segunda é apenas uma forma de preservação de prova e a última uma forma de restringir e ocultar conteúdos.

(UNC3T) da Polícia Judiciária, pelo que tem sido esta a responsável por garantir as melhores práticas técnicas no manuseamento da prova digital. Muitas destas diretrizes e recomendações foram emitidas pela Europol[64] e Interpol[65], integradas na PJ e, tais documentos, "têm permitido criar um standard de boas práticas que é seguido por todos os países", por isso é que "ao analisarmos os manuais de diversos países, encontramos grandes semelhanças ou até recomendações que parecem decalcadas umas das outras"[66], daí haver tanta uniformidade nesta matéria.

Em Portugal seguimos a Norma ISO/IEC FDIS 27037:2012 - Diretrizes para identificação, recolha, apreensão e preservação de prova digital (Termo de Adoção em Portugal N.º 1252/2016, 2016-10-12), uma norma publicada em novembro de 2012, mas que não tem força de lei. Contém as diretrizes para a correta identificação, recolha, apreensão, e preservação de prova digital nos seguintes dispositivos: telemóveis, computadores e dispositivos de rede, sistemas de navegação móvel, cartões de memória, discos rígidos e dispositivos de armazenamento de dados com funções semelhantes, câmeras fotográficas e de vídeo e outros dipositivos com funções semelhantes a estas[67].

A norma baseia-se em quatro princípios de tratamento. O primeiro é a "aplicação de métodos", segundo a qual a prova deve ser recolhida da forma menos intrusiva e de forma a procurar e a manter a originalidade da prova, isto é, de forma que não se altere, daí que para a sua recolha se usem métodos e ferramentas especiais que permitem a recolha da prova sem a modificação daquilo que existe no suporte que está a ser analisado. Para além disto, o processo deve ser "aditável", ou seja, os procedimentos devem ser validados e verificados pelas boas práticas éticas e profissionais. O processo deve ainda ser "repetível", registados

---

[64] A Europol é um serviço europeu de polícia, incumbido do tratamento e intercâmbio de informação criminal. Tem por missão contribuir significativamente para a aplicação das leis da União Europeia no âmbito do combate à criminalidade organizada, colocando a tónica nas organizações criminosas envolvidas. O seu objetivo consiste em melhorar a eficácia e a cooperação entre os Estados Membros no domínio da prevenção e do combate a formas graves de criminalidade organizada de dimensão internacional. Disponível em: https://www.policiajudiciaria.pt/wp-content/uploads/2016/12/UNE.pdf.
Consultado a 12 de novembro de 2022

[65] A Organização Internacional de Polícia Criminal - INTERPOL é uma organização mundial de cooperação policial. Disponível em: https://www.policiajudiciaria.pt/wp-content/uploads/2016/12/GNI.pdf Consultado a 12 de novembro de 2022

[66] Cf. MARQUES, Pedro, *Informática Forense: Recolha e preservação da prova digital*, Universidade Católica Portuguesa, 2013, p.15. Dissertação de Mestrado.

[67] Esta lista não é exaustiva. Vide: ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence., 2022) Disponível em: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27037:ed-1:v1:en; https://www.iso.org/standard/44381.html

os passos dados e os resultados obtidos, para permitir depois, caso necessário, a sua repetição e lhe seja conferida credibilidade. Por fim, o processo deve ser "defensável", melhor dizendo, as ferramentas usadas devem estar mencionadas no processo, para que se possa notar a sua validade e adequação técnica para aquele fim visado.

Para que possa haver garantias da sua autenticidade, a norma estabelece ainda, para cada tipo de dispositivo, formas de atuação distintas que se baseiam em três processos: identificação, que corresponde ao processo de identificação das provas e consiste em localizar e identificar informações potenciais ou elementos de prova nos seus dois estados possíveis, o físico e o lógico, conforme o caso de cada tipo de prova; recolha e aquisição, que se define como sendo o conjunto de dispositivos e documentos recolhidos que podem conter provas ou as cópias das informações existentes nos dispositivos alvos; por fim, a conservação/preservação, de forma a garantir a originalidade para que seja admissível como prova completa e seja também garantida a cadeia de custódia.

Outro exemplo das boas práticas técnicas é o guia "Eletronic Evidence Guide" do Conselho da Europa, onde estão plasmados alguns princípios de tratamento da prova digital e critérios técnicos gerais de admissibilidade[68].

Os princípios de tratamento da prova[69] são a integridade de dados, para que não haja dúvidas de que os dados apreendidos são os originais; o registo de auditoria para que posteriormente possam ser auditadas em julgamento caso se suscitem duvidas; o apoio especializado, a formação adequada dos intervenientes e, por fim, a legalidade. Relativamente aos critérios técnico-gerais de admissibilidade[70], podemos identificar cinco: a autenticidade, com isto significa que a prova deve representar o seu estado original; a completude, isto é, devem ser completas e não devem estar manchadas de pré-juízos dos especialistas que procederam à sua apreensão; confiabilidade, o que significa que não deve levantar dúvidas sobre a sua autenticidade; o que levará à credibilidade, para que os decisores possam confiar nelas como verdadeiras e, por fim, os métodos utilizados devem ser proporcionais e justos aos interesses em causa.

[68] Cf. Electronic Evidence Guide – A Basic Guide for Police Officers, Prosecutors and Judges, Cybercrime Division - Directorate General of Human Rights and Rule of Law, Version 3.0, Strasbourg, France, 4 April 2022, p. 15
[69] *Ibidem.*
[70] *Ibidem.*

Concluindo, para a valoração da prova digital, há que respeitar sempre o positivado na lei e as boas práticas técnicas anteriormente analisadas e, sempre que necessário, recorrer ao apoio de perícias e de consultores técnicos-especializados, conforme o disposto nos artigos 151.º a 155.º CPP.

3. Cadeia de custódia da prova digital

A cadeia de custódia é o tema central desta dissertação e sobre o qual nos vamos debruçar de seguida. Muito se fala em todos os ordenamentos jurídicos da cadeia de custódia e da sua importância. No entanto, nem todos os ordenamentos se debruçaram da maneira devida sobre ela e sobre a sua regulamentação, como é o caso de Portugal. Em Portugal não está regulada na lei, muito menos estão positivados os procedimentos de como devem atuar os funcionários que a recolhem, analisam e armazenam as provas, que são cruciais para a prova poder vir a ser posteriormente valorada em tribunal, uma vez que qualquer interrupção/quebra na cadeia de custódia pode resultar na inadmissibilidade da prova. É inegável que Portugal carece de regulação nesta matéria, que apenas refere no artigo 249.º n.º 2 alínea a) do CPP que compete aos OPC "proceder a exames dos vestígios do crime (...) assegurando a manutenção do estado das coisas, dos objetos e dos lugares", ou seja, assegurar a manutenção da cadeia de custódia. Contrariamente a Portugal, há países que se debruçaram afincadamente sobre a cadeia de custódia, a regularam nas suas leis e possuem um manual de procedimentos, como é o caso do Chile, Colômbia, Equador e Perú[71].

Vamos ver que a cadeia de custódia tem grande importância no processo penal porque é o procedimento que assegura que a prova que é apresentada em tribunal é exatamente a mesma que foi obtida em determinado dia e da qual se extraíram dados relevantes para o processo[72].

[71] Cf. MARINHO, Girlei Veloso, *Cadeia de custódia da prova pericial*, Fundação Getúlio Vargas, Escola Brasileira de Administração Pública e de Empresas, Rio de Janeiro, 2011 – Dissertação de Mestrado

[72]Vide. GARCIA MATEOS, José Aurélio, "Cadena de custódia vs mismidad", In: *La prueba electrónica: validez y eficacia Procesal,* Colección Desafios Legales, 1º edición - Septiembre de 2016, p. 130-136

3.1. Conceito da cadeia de custódia

No ordenamento jurídico português não há uma definição de cadeia de custódia positivada na lei, e mesmo as referências doutrinarias são escassas, mas tal não nos impede de a definir e de analisar a sua importância.

Ainda que exista uma escassez conceitual, vamos destacar alguns autores que nos ofereceram um conceito.

Desde logo, Geraldo Prado, que muito se tem debruçado sobre este tema, diz-nos que cadeia de custódia consite no "método por meio do qual se pretende preservar a integridade do elemento probatório e assegurar sua autenticidade"[73].

Manuel Monteiro Valente diz-nos que a cadeia de custódia é "uma técnica jurídico-processual que garante a identidade e autenticidade da prova ab initio ad finem de todo o iter processualis – desde o meio de obtenção da prova (busca e apreensão), a submissão a meio de prova (perícia) que termina a ser submetida à apreciação do Tribunal e ao contraditório, próprio das jurisdições processuais de estrutura acusatória (prova como resultado)", ou seja, está presente em todas as fases importantes do instituto da prova[74].

Javier Rubio Alamillo dá-nos uma definição mais simples – diz-nos que é o "procedimento que permite conservar, desde a recolha até à análise, que a prova tal como ela é", uma definição simples, mas que traduz na integra o que a cadeia de custódia é, uma vez que qualquer alteração, mesmo que feita acidentalmente, distorce a prova e esta já não poderá ser usada[75].

No ordenamento jurídico espanhol, assim como no português, esta matéria carece de regulação, uma vez que não há nada que disponha como se deve garantir e conservar a cadeia de custódia da prova. No entanto, identificamos na jurisprudência uma definição bastante completa. O Supremo Tribunal Espanhol, na Sentença "STS 1190/2009, de 3 de

[73] Cf. PRADO, Geraldo, Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital, "A interface entre o Direito Digital e o Processo Penal", Lisboa, janeiro 2021 - Texto correspondente à palestra proferida pelo professor Geraldo Prado intitulada "A interface entre o Direito Digital e o Processo Penal", no Ciclo Permanente de Palestras com o tema "Consequências do Uso da Inteligência Artificial no Processo Penal"

[74] Cf. VALENTE, Manuel Monteiro Guedes, *Cadeira de custódia...*, *cit.*, p.45

[75] Cf. RUBIO ALAMILLO, Javier, "Conservación de la cadena de custódia de una evidencia informática", *Diario LA LEY*, n.º 8859, Editorial Wolters Kluwer, 2016

deciembre"[76] definiu a cadeia de custódia como sendo "uma figura retirada da realidade que se tinge de força jurídica para, se for o caso, identificar determinado objeto, uma vez que tendo este de passar por diferentes lugares para que se façam exames, é necessário ter a segurança de que o que é transferido e analisado é o mesmo em todos os momentos, desde o momento em que se recolheu do local do crime, até ao momento em que é analisado e, se for o caso, o momento em que se destrói" (tradução minha), e é este processo que garante a "mismidad de la prueba", termo que tende a ser traduzido para português por "mesmidade". Geraldo Prado diz-nos que a "Lei da mesmidad" é "princípio pelo qual se determina que "o mesmo" que se encontrou na cena do crime é o "mesmo" que se está a utilizar para tomar a decisão judicial"[77] assim, vemos que está intimamente relacionado com o *Princípio da identidade e autenticidade da cadeia de custódia* já analisado anteriormente. O facto de se garantir a *mesmidad* é de grande importância porque permite aferir às partes se aquela prova foi obtida respeitando os trâmites legais e se pode vir a ser valorada no processo.

Também de grande relevância é a Sentença do Tribunal Constitucional Espanhol - STC 170/2003 de 23 de octubre de 2003 - relativa à incorporação de suportes informáticos ao processo penal, onde o tribunal nos diz que a incorporação se deve realizar "com o cumprimento das exigências necessárias para garantir a identidade plena e integridade do conteúdo (...) e que não sejam manipulados" (tradução minha)[78].

Por fim, para Robert Doran, "a cadeia de custódia é um processo usado para manter e documentar a história cronológica da evidência. Este processo deve resultar num produto: a documentação formal do processo" (tradução minha)[79].

Podemos identificar várias notas comuns em todas as definições e traçar uma definição própria. Assim, a cadeia de custódia é o procedimento ou processo, que tem de ser adotado desde o momento da sua recolha, até ao momento do trânsito em julgado, para garantir a rastreabilidade, autenticidade, confiabilidade e preservação da prova. O que se

---

[76] Vide. STS 1190/2009, 3 de Diciembre de 2009, disponível em: https://vlex.es/vid/211686183. Consultado a 7 de dezembro de 2022

[77] Cf. PRADO, Geraldo, *A cadeia de custódia da prova no processo penal*, 1.º edição, São Paulo: Marcial Pons, 2019, p. 95

[78] Vide. STC 170/2003 de 23 de octubre de 2003. Disponível em: https://www.boe.es/boe/dias/2003/10/23/pdfs/T00045-00053.pdf Consultado a 7 de dezembro de 2022

[79] Cf. DORAN, Robert A., Exploring the links in the chain of custody, Artigo apresentado na Conferência Anual de Treinamento da Nebraska Association for Property and Evidence (NAPE), 2005. Disponível em: https://pt.scribd.com/document/66568187/Exploring-the-Links-in-the-Chain-of-Custody. Consultado a 7 de dezembro de 2022

pretende garantir é que a prova que foi recolhida é a mesma que vai ser depois valorada e discutida em audiência de julgamento.

Após esta análise, estamos capazes de perceber a importância da "chain of custody" para o processo e é sobre isso que nos debruçaremos de seguida.

3.2. Relevância da cadeia de custódia para o processo penal

A conservação da cadeia de custódia das provas digitais é de grande importância nos processos penais, uma vez que, atualmente, devido à digitalização da vida, para a investigação da grande maioria dos crimes é necessária a recolha prova digital, por exemplo em telemóveis ou tablets, computadores ou discos duros, cartões de memória ou até mesmo redes sociais. Diria até que a garantia da cadeia de custódia da prova digital, face às suas características, por ser uma prova complexa, imaterial, suscetível de alterabilidade, volátil e muitas vezes dispersa em redes e sistemas, tem uma importância acrescida. No entanto, determinar uma alteração neste tipo de prova é uma "questão matemática y dicotómica, isto é, ou a prova não foi alterada, ou a prova foi alterada" (tradução minha)[80].

A grande finalidade da cadeia de custódia da prova informático-forense é manter a força probatória da prova que foi apreendida para poder ser usada no processo penal para a formação da convicção do julgador. No entanto, para que os vestígios encontrados possam constituir prova e demonstrar a veracidade dos factos, é crucial demonstrar a sua genuinidade e integridade material. Com isso, o objetivo é garantir que a prova oferecida cumpra as exigências do processuais, "devendo garantir a rastreabilidade: humana (determinação de responsabilidades no tratamento da prova, desde a sua deteção e recolha até ao final do processo), física (incluindo a totalidade das equipas locais ou remotas envolvidos, seja no armazenamento, processamento ou comunicações) e lógica (descrição dos locais ou redes e informações acedidas)"; e, por outro lado, deve garantir a "confiabilidade (integridade, autenticidade, confidencialidade)" (tradução minha)[81].

[80] Cf. RUBIO ALAMILLO, Javier, "Conservación de la cadena de custódia...", *cit.*
[81] Cf. ARELLANO, Luis Henrique; Castañeda, Carlos Mario, "La cadena de custódia informático-forense", *Revista ACTIVA*, ISSN 2027-8101, N.º 3, enero-junio 2012, pp. 67-81, Tecnológico de Antioquia, Medellín (Colombia)

Por fim, a cadeia de custódia tem uma grande relevância porque, como nos diz Emma Calderón Arias, "os elementos probatórios obtidos inicialmente no local do facto ou em outros locais relacionados com o crime, servem para que no momento em que as autoridades competentes se pronunciam, o consigam fazer da forma mais precisa e justa possível, demonstrando que isso é imprescindível para o acompanhamento, segurança, confiabilidade de que as amostras, vestígios ou provas cheguem à audiência de julgamento de acordo com os factos, respeitando os direitos dos arguidos, a Constituição, assim como os princípios processuais penais" (tradução minha)[82]. Serão tutelados os direitos fundamentais à garantia da confiabilidade e integridade dos sistemas de tecnologias da informação, que o Tribunal Constitucional Federal Alemão entendeu estarem abrangidos pelo direito geral da personalidade[83]. A cadeia de custódia irá ainda tutelar o "direito à proteção do entorno digital, da identidade digital, do domicílio digital e, por óbvio, da privacidade associada ao direito de decidir o que tornar público ou não relativamente à esfera da vida da pessoa"[84].

3.3. Procedimentos de recolha, análise e preservação da prova digital

Após o cometimento de um crime através de um sistema ou rede informática ficam nestes uma série de vestígios e provas que vão ser essenciais para a punição do seu agente, para se imputar o facto a um agente determinado, mas, antes disso, para se conseguir identificar o agente do facto. Para tal, importa saber como devemos tratar as provas digitais, como as recolher, preservar, analisar e depois apresentar. Só com o respeito destes passos é que é possível valorarmos a prova em tribunal. Seguimos o mesmo pensamento de

---

[82] Cf. CALDERÓN ARIAS, Emma, "Fundamentos teóricos de la cadena de custódia en el proceso penal cubano", *MISIÓN JURÍDICA - Revista de Derecho y Ciencias Sociales*, N.º 12, Año 2017, Enero - Junio, Bogotá, D.C. (Colombia), pp. 241-253

[83] "1. The general right of personality (Article 2.1 in conjunction with Article 1.1 of the Basic Law (*Grundgesetz – GG*)) encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems. (…) ALEMANHA. Bundesverfassungsgericht (Tribunal Constitucional Federal da Alemanha). BVerfGE 120, 274. 1 BvR 370/07; 1 BvR 595/07. Decisão. Data: 27 de fevereiro de 2008. Ementa. Versão em inglês disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html. Consultado a 15 de novembro de 2022

[84] Vide. PRADO, Geraldo, Notas sobre proteção de dados, prova digital e o devido processo penal Disponível em: https://geraldoprado.com.br/artigos/notas-sobre-protecao-de-dados-prova-digital-e-o-devido-processo-penal/. Consultado a 7 de dezembro de 2022. Trata-se da comunicação do autor no painel VI do Seminário Internacional da Comissão de Juristas: "Proteção de dados pessoais na segurança pública e investigação criminal", promovido pela Câmara dos Deputados do Congresso Nacional Brasileiro de forma online e transmitido pelo canal oficial da Câmara dos Deputados na plataforma YouTube, disponível na íntegra em https://www.youtube.com/watch?v=J4m5yiQnLbI. Consultado a 7 de dezembro de 2022

Fernandez Martinez, quando afirma que o primeiro passo para que se possa valorar uma prova digital é zelar para que a sua integridade e autenticidade não seja questionada, "uma vez que todos conhecemos a facilidade da sua manipulação, assim como da sua volatilidade" [85] (tradução livre).

A prova digital, face às suas características que analisamos anteriormente, não pode ser recolhida e analisada com os meios convencionais, exige para tal técnicas próprias de análise forense que, segundo Pedro Marques, corresponde à "aplicação de técnicas científicas a questões de interesse legal" e "a inspeção sistemática e tecnológica de um sistema informático e dos seus conteúdos, para a obtenção de provas de um crime ou qualquer outro uso que seja investigado", sendo hoje a "peça chave para a investigação criminal"[86].

Relativamente aos procedimentos, em Portugal seguimos as recomendações de boas práticas de recolha e armazenamento de prova digital da Norma ISO/IEC FDIS 27037:2012 e do "Eletronic Evidence Guide – A basic guide for police officers, prosecutors and judges" do Conselho da Europa e que exige o registo de todos os passos e fases de recolha da prova. Para além disso, esta exigência de documentação de determinados passos e fases também decorre de outros órgãos internacionais[87] como a Association of Chief Police Officers (ACPO)[88], o National Institute of Standards and Technology (NIST) e o Internet Engineering Task Force (IETF)[89].

O primeiro passo para a apreensão de dados informáticos, como dispõe a LC no seu artigo 16º, é haver um despacho das autoridades competentes (MP ou juiz), a ordenar a apreensão dos dados ou documentos informáticos relevantes. Também pode ser apreendido

---

[85]Cf. FÉRNANDEZ MARTÍNEZ, Juan Carlos. "Especialidades de la prueba cuando, esta, es tecnológica". In: Ortega Burgos, Enrique. *Actualidad: Nuevas Tecnologías*. Valencia: Tirant lo Blanch, 2020, p. 333

[86] Cf. MARQUES, Pedro, *Informática Forense: Recolha..., cit.,* p.13.

[87] Vide. Quilling, Chelsea, The Future of Digital Evidence Authentication at the International Criminal Court, *Journal of Public and International Affairs*, 2022. Disponível em: https://jpia.princeton.edu/news/future-digital-evidence-authentication-international-criminal-court Consultado a 20 de dezembro de 202

[88] Vide. Good Practice Guide for Computer-Based Electronic Evidence, Official release version 4.0. Disponível em:https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf Consultado a 20 de dezembro de 202

[89] Outros exemplos: European Network of Forensic Science Institutes (ENFSI), Best Practice Manual for the Forensic Examination of Digital Technology, 2015; o National Institute of Justice (USA), Forensic Examination of Digital Evidence: A Guide for Law Enforcement, 2004 e o Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, 2007; do Scientific Working Group on Digital Evidence (SWGDE).

pelos órgãos de polícia criminal, neste caso a Polícia Judiciária, sem a prévia autorização da autoridade judiciaria, no decurso de uma pesquisa de dados legitimamente ordenada, nos casos em que haja urgência ou perigo na demora. Deverão ser apresentadas no prazo máximo de 72 horas às autoridades judiciárias competentes para que esta as possa validar, conforme exige o disposto no n.º 4 do artigo 16.º da LC. A LC oferece-nos no n.º 7 do mesmo artigo, algumas práticas técnicas, ou melhor dizendo, formas de apreensão disponíveis. Temos, desde logo, a possibilidade de apreensão do suporte onde está instalado o sistema ou a apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respetiva leitura. Por exemplo, podemos, desde logo, idealizar a situação de apreensão de computadores ou apreensão de CDs, em que será necessário apreender também um leitor de CDs, uma vez que é um dispositivo "necessário à respetiva leitura"[90]. Por outro lado, está também prevista outra forma de apreensão, que corresponde à realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo. Existe esta possibilidade expressamente prevista na lei, porque há situações em que, em termos de logística, é inconcebível apreender centenas de computadores de uma empresa, por exemplo. Nestes casos, a cópia tem de ser feita em duplicado e uma cópia é selada e confiada ao secretario judicial dos serviços onde o processo correr os seus termos e, se os dados assim o permitirem, são certificados por meio de assinatura digital, precisamente para garantir a autenticidade da prova. Nas perícias da prova digital os originais devem ser preservados, e o trabalho pericial deve ser realizado em cópias idênticas realizadas com ferramentas específicas, para evitar futuras alegações de adulteração[91].

É a partir da apreensão que se inaugura o processo de uma análise forense. Segundo Pedro Marques, o processo encontra-se distribuído em quatro fases: "identificação da origem da prova digital; preservação da prova (pode implicar a duplicação da prova[92]); análise e investigação das provas; e a apresentação de relatórios ou resultados"[93].

---

[90] Art. 16.º n.º 7 al. a) "Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura."

[91] Cf. MACHADO, Michelle Moreira, "Importância da cadeia de custódia para a prova pericial", *Revista Criminalística e Medicina Legal*, N.º 1, V.º 2, 2017. Disponível em: http://revistacml.com.br/wp-content/uploads/2018/04/RCML-2-01.pdf. Consultado a 8 de dezembro de 2022

[92] Há casos em que não se faz duplicação da prova porque se apreendem os suportes físicos, como por exemplo, a apreensão de um computador onde estão armazenados os dados.

[93] Cf. MARQUES, Pedro, *Informática Forense: Recolha..., cit.,* p.13

Assim sendo, o primeiro passo é "deteção, identificação e registo da prova"**,** em que se deve "identificar a totalidade de elementos informáticos alvo, como computadores, rede de computadores, computador portátil, telemóveis, tablets"[94] e "registá-los detalhadamente no relatório da operação, que ficheiros foram identificados pelo alvo como importantes e porquê, quais foram copiados e caso o alvo refira que nada de importante há a copiar, tal também deve ser registado e assinado pelo alvo"[95]. Deve proceder-se à documentação de todo o cenário envolvente, recorrendo a uma reportagem fotográfica; assim como seguir todas as etapas de etiquetagem dos objetos alvo de investigação, para que possam vir a ser admissíveis em tribunal. Pedro Marques, anuncia-nos uma série de etapas a executar para a recolha da prova digital[96].

O segundo passo passa pela preservação da prova digital, onde é crucial empregar um conjunto de técnicas que não modifiquem a prova, técnicas essas que devem ser sempre realizadas por pessoas especializadas, por peritos, que possam vir mais tarde, em tribunal, explicar e testemunhar os passos que foram realizados desde a recolha da prova digital até aos resultados.

Uma das técnicas que é utilizada para garantir a integridade e autenticidade dos dados recolhidos é o código Hash. O código hash "é o resultado da aplicação de um procedimento matemático a um conjunto de dados, que podem estar contidos num ficheiro (como um documento ou uma fotografia), numa Pen Drive, num disco rígido, num DVD, etc. O código é o "resumo único atribuído ao conjunto de informação sobre a qual se aplicou o algoritmo, obtendo-se um resumo completamente distinto, para o mesmo algoritmo, com a mínima alteração que se produza nos dados originais"[97]. Funciona como se fosse uma impressão digital de um dado, de uma quantidade de bites. Para garantir a integridade da prova deve ser feita uma cópia integral dos dados, como nos sugere o artigo 16.º, n.º 7 alínea b), que será feita em duplicado e deverá ser calculado o código hash de ambas. Para efeitos de investigação, apenas se deve trabalhar com uma das cópias, "preservando a primeira como fonte, para o caso de ser preciso fazer uma nova cópia. No entanto, sempre que seja preciso

[94] Cf. ARELLANO, Luis Henrique; Castañeda, Carlos Mario, "La cadena de custódia informático-forense", *Revista ACTIVA*, ISSN 2027-8101, N.º 3, enero-junio 2012, pp. 67-81, Tecnológico de Antioquia, Medellín (Colombia)
[95] Cf. MARQUES, Pedro, *Informática Forense: Recolha..., cit.,* p.24.
[96] Idem. p. 33
[97] Cf. RUBIO ALAMILLO, Javier, "Conservación de la cadena de custódia...", *cit.*

fazer uma nova cópia haverá que calcular o código hash, para se ter a certeza que se está a trabalhar com o mesmo que dispúnhamos no início, com a prova original[98].

Conforme o Acórdão da Relação de Lisboa[99], "a prova eletrónica em ambiente digital caracteriza-se pela volatilidade, instabilidade, diversidade de tecnologias utilizadas e o anonimato oferecido pelas Tecnologias da Informação e da Comunicação (TIC); o Message - Digest Algorithm 5 (MD 5), utilizado na assinatura digital certificada, gera uma mensagem com um código de identificação único e irrepetível, a que se denomina função "hash", sobre determinado conteúdo de mensagem de correio eletrónico; o valor MD5 é, assim, o equivalente ao DNA digital, na medida em que é univocamente identificada uma determinada informação de carácter digital, pois só assim, se garante que a informação transmitida tem as características necessárias para produzir os efeitos legais pretendidos, ou seja, características de integridade, de molde a assegurar que o conteúdo da informação produzida e transmitida a Juízo não foi alterado de forma propositada ou acidental; e características de autenticidade, de molde a permitir identificar inequivocamente o responsável pela produção da informação eletrónica, o propósito e em que termos esta foi produzida e o controlo exclusivo por parte do possuidor ou possuidores dessa informação". Concluindo, o código hash é o que garante que a prova digital não foi alterada, uma vez que se se alterar um bit, o código hash será distinto do original, o que terá consequências irreversíveis para o processo uma vez que a sua integridade foi violada.

Todos os passos de que falamos anteriormente, de recolha e de preservação da prova, devem ser documentados, assim como os resultados obtidos. É este registo que nos vai garantir que não houve a quebra da cadeia de custódia. O registo é também importante para possibilidade de a autoridade judiciaria competente determinar que deve ser feita uma nova perícia ou renovada a perícia anterior a cargo de outro ou outros peritos, conforme está previsto no artigo 158.º do CPP, pois a nova perícia deverá obter os mesmos resultados que o relatório anterior apresentou - "Uma entidade externa deve poder chegar aos mesmos resultados executando os mesmos procedimentos. Não respeitar esta regra pode comprometer irremediavelmente a validade da prova"[100].

---

[98] Cf. GARCIA MATEOS, José Aurélio, "Cadena de custódia...", *cit*., p. 130-136

[99] Vide. Acórdão do Tribunal da Relação de Lisboa de 13-12-2016, processo: 4069/13.0TACSC-5. Disponível em:http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/4fdb60ca67ced178802580c2003de80b?OpenDocument

[100] Cf. MARQUES, Pedro, *Informática Forense: Recolha..., cit.,* p.117

Após a apreensão e preservação da prova digital há lugar à análise forense da mesma. O trabalho forense deverá ser realizado nas cópias para evitar que venham a alegar adulteração da prova - "A fim de não comprometer a integralidade da prova digital, o seu conteúdo original, juntamente com seus *hashes* (assinatura digital) devem ser preservados e efetuada a análise na cópia"[101]. Por fim, devem ser elaborados os relatórios com os resultados obtidos, que devem estar redigidos numa linguagem simples e adequada à compreensão dos juristas e de todos os que intervêm no processo. Os peritos podem ainda vir a ser convocados ao processo pela autoridade judiciária para prestarem esclarecimentos (artigo 158.º do CPP), mais uma vez aqui se vê a importância do registo de todos os passos para que o perito consiga explicar todos os passos para a realização da prova aquando do julgamento. Para além disso, importa ainda referir que o relatório dos procedimentos da cadeia de custódia deve ser mantido até a trânsito em julgado[102].

Resumidamente, "as medidas tomadas não devem modificar as provas e todas as pessoas envolvidas devem ser competentes para os procedimentos forenses. Todas as atividades realizadas devem ser documentadas e as provas conservadas, de modo que estejam disponíveis para a repetição de exames em que seja possível obter o mesmo resultado"[103].

Em síntese, a validade da prova da prova digital está dependente do respeito por estes procedimentos, que se aplicam tanto às provas materiais como virtuais. Desta forma, será conservada a cadeia de custódia da prova digital, que garantirá que a prova não foi contaminada ou destruída.

---

[101] Cf. DOMINGOS, Fernanda Teixeira Souza, "As provas digitais nos delitos de pornografia infantil na internet". In: Salgado, Daniel de Resende; Queiroz, Ronaldo Pinheiro (orgs.), *A prova no enfrentamento à macrocriminalidade*, 3.º edição, Salvador: Juspodvim, p. 197.

[102] ART. 188.º n.º 12 do CPP - Os suportes técnicos referentes a conversações ou comunicações que não forem transcritas para servirem como meio de prova são guardados em envelope lacrado, à ordem do tribunal, e destruídos após o trânsito em julgado da decisão que puser termo ao processo. n.º 13 - Após o trânsito em julgado previsto no número anterior, os suportes técnicos que não forem destruídos são guardados em envelope lacrado, junto ao processo, e só podem ser utilizados em caso de interposição de recurso extraordinário.

[103] Cf. MARQUÉS ARPA, Tomás; SERRA RUIZ, Jordi, Cadena de custódia en el análisis forense. Implementación de un marco de gestión de la evidencia digital, Universidad de Alicante, Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información: celebrado del 5 al 8 de septiembre 2014, Alicante, pp. 167-172

3.4. A problemática das contaminações da prova digital

A prova digital, face as suas características, pode ser facilmente alterada, de onde podem advir consequências gravíssimas para o processo. Depois de estudarmos os procedimentos de manutenção da cadeia de custódia, sabemos que uma simples alteração vai invalidar a prova, pondo em causa o processo penal. E, por isso, é que é tão importante seguir os procedimentos e os princípios para a recolha de prova.

A contaminação das provas pode acontecer de várias formas, dependendo se a prova alvo é objeto físico, como um computador ou um telemóvel ou se nos estamos a referir a um documento digital.

Por exemplo, é muito fácil perder a cadeia de custódia de um telemóvel. Pelo simples facto de ligar o telemóvel antes do momento programado e adequado pode invalidar a prova, uma vez que quando se liga um telemóvel o sistema operativo começa a funcionar, o que vai alterar a memória interna do dispositivo e é possível que este receba e envie informações para o exterior, alterando os dados que continha. O mesmo funciona para os computadores e outros dispositivos, nunca se devem ligar quando estes se encontram desligados, assim como se o computador se encontrar ligado não se deve desligar porque pode ser ativado algum mecanismo de bloqueio assim como não se deve tocar em qualquer tecla do teclado. Também não se deve remover a corrente de um computador ligado porque tal afeta os programas que estão a ser executados, limpar a memoria RAM, quebrar as ligações à internet e a drives remotas e encriptadas[104].

Uma forma muito fácil de contaminar a prova é conectar a um computador uma Pen USB, um cartão de memória ou um disco duro sem antes ativar um bloqueio de escrita/leitura, já que será registado o acesso ao dispositivo e isto alterará a prova e o código Hash que foi calculado no início já não será o mesmo aquando da valoração da prova[105].

Uma coisa é certa, quando interagimos com prova em processo penal, jamais uma ação deve provocar uma alteração.

[104] Vide. MARQUES, Pedro, *Informática Forense: Recolha..., cit.,* pp.130-131
[105] Cf. RUBIO ALAMILLO, Javier, "Conservación de la cadena de custódia...", *cit.*

3.5. Quebra da cadeia de custódia e consequências para o processo

A quebra da cadeia de custódia vai resultar na proibição da utilização da prova cuja cadeia de custódia foi alterada. Seguindo os exemplos mencionados no ponto anterior, quando o código Hash calculado inicialmente não corresponde com o código calculado no momento da valoração da prova, significa que essa prova sofreu alterações, pelo que já não transmite confiabilidade e, consequentemente, já não poderá ser valorada em tribunal. Por esta razão é que é tão importante respeitar todos os procedimentos indicados[106], para que não se prejudique a verdade, para que não se absolvam culpados, mas, principalmente, para que não se condenem inocentes. No entanto, para além de terem de ser respeitados todos os procedimentos, há ainda que respeitar os princípios supracitados e o disposto na lei.

Citando Amanda Costa das Almas, "A aplicação da cadeia de custódia acarreta a redução da possibilidade de ocorrência de erros jurídicos, os quais podem ensejar uma condenação criminal revestida por nulidades**,** razão pela qual qualquer eventual quebra dessa cadeia de custódia compromete a fiabilidade do material colhido ao curso da investigação criminal"[107]**.**

Para Geraldo Prado, "quando verificada a quebra da cadeia de custódia, o que há é a impossibilidade do exercício efetivo do contraditório pela parte que não tem acesso à prova íntegra. Os elementos remanescentes sofrem com a lacuna criada pela supressão de outros elementos que poderiam configurar argumentos persuasivos em sentido contrário à tese deduzida no processo e por essa razão estão contaminados e igualmente não válidos"[108]. Assim, se a prova não fosse invalidada estaríamos a pôr em causa princípios jurídicos como o princípio do contraditório, princípios da lealdade, da boa-fé e da confiança, assim como o direito à autodeterminação informativa.

---

[106] O valor das provas pode ser perdido se os procedimentos não forem adequadamente constituídos. Cf. MACHADO, Michele Moreira, "Importância da cadeia de custódia...", *cit.*

[107] ALMAS, Amanda Costa das, "A Aplicabilidade da cadeia de custódia em dados digitais utilizados como prova no processo penal brasileiro", *IBCCRIM - Laboratório de Ciências Criminais de Porto Alegre/RS*. Disponível em: https://www.ibccrim.org.br/media/documentos/doc-07-10-2021-11-44-50-262499.pdf. Consultado a 8 de dezembro de 2022

[108] Cf. PRADO, Geraldo, *A Cadeia de Custódia da Prova no Processo Penal*, São Paulo: Marcial Pons, 2019, p.128

As consequências da quebra da cadeia de custódia são, na ótica de Manuel Monteiro Valente[109], desde logo, a ilicitude da prova, que é a mais grave das consequências jurídico-processuais penais: uma nulidade qualificada - proibição total de admissibilidade e de valoração da prova por se terem violado regras processuais tão importantes, assim como direitos fundamentais. Para além disso, será ainda instaurado um processo administrativo disciplinar ou um processo-crime[110] contra o agente que levou à ilicitude da prova[111]. A destruição da cadeia de custódia é um processo irreversível que não oferece outra alternativa senão a proibição da sua valoração. Michelle Machado destaca a importância da cadeia de custódia com um caso paradigmático da justiça americana, "o caso de O. J. Simpson, ex-jogador de futebol americano dos Estados Unidos, em que mesmo diante de provas que demonstravam o envolvimento do jogador em um duplo homicídio, a defesa conseguiu a absolvição devido à preservação do local inadequada, aos procedimentos de coleta de vestígios incorretos em que ficaram evidentes falhas na cadeia de custódia"[112].

A nulidade das provas obtidas por meios ilícitos está prevista na Constituição no artigo 32º, n.º 8, desde logo por lesarem bens jurídicos carentes de tutela penal, tais como a vida, integridade física, a reserva da intimidade da vida privada e familiar, a inviolabilidade das comunicações e do domicílio. Se a consequência da destruição da quebra da cadeia de custódia não fosse a invalidade estaríamos a descredibilizar a confiança dos cidadãos no Estado de Direito Democrático. Seguindo as palavras de Manuel Monteiro Valente[113], "o Estado e os seus operadores da justiça devem ser o rosto da dignidade da justiça e não da sua indignidade que se sujeita a ser, em qualquer momento, maquiada com pós mágicos doutrinários de purificação e expiação da ilicitude, da ilegalidade e da ilegitimidade do processo-crime, que vive do instituto da prova".

Concluindo, a cadeia de custódia é um procedimento com extrema importância que deve ser rigorosamente seguido, quando tal não aconteça as consequências são a inadmissibilidade da prova no processo e a proibição da sua valoração, uma vez que os dados

[109] Cf. VALENTE, Manuel Monteiro Guedes, *Cadeira de custódia..., cit.*, pp. 78-81
[110] *Idem.* p. 80
[111] Deve sempre averiguar-se, em cada caso em concreto, se existe ou não uma causa de justificação que levará à extinção do procedimento criminal ou disciplinar.
[112] Cf. MACHADO, Michelle Moreira, "Importância da cadeia de custódia...", *cit.*
[113] Cf. VALENTE, Manuel Monteiro Guedes*, Cadeira de custódia..., cit.,* p.83

aprendidos não transmitem a confiabilidade necessária para um processo justo e democrático.

4. Aplicabilidade da tecnologia blockchain na manutenção da cadeia de custódia

4.1. O que é a tecnologia blockchain

A blockchain surgiu pela primeira vez em 2008 associada à criptomoeda Bitcoin. Rapidamente foi mais além e, atualmente, está a causar expetativas tão elevadas que já pode ser encontrada em diversas áreas como a saúde, negócios, e até mesmo no setor público. Há cada vez mais países a investir nesta recente tecnologia com o objetivo último de melhorar os seus serviços públicos.

A tecnologia blockchain refere-se a uma cadeia de blocos de dados encadeados – um sistema de registo que contém todas as transações processadas. Segundo Alexander Preukschat, traduz-se numa "base de dados distribuída por diferentes participantes, protegida criptograficamente e organizada em blocos de transações matematicamente relacionados entre si" – é uma base de dados descentralizada que não pode ser alterada. Assim, uma blockchain pode traduzir-se num conjunto de computadores conectados que utilizam o mesmo sistema de comunicação e vão validar e armazenar a mesma informação numa rede peer-to-peer[114]. Permite o registo de todas as transações, organizadas cronologicamente, na qual todos os integrantes detêm a responsabilidade de armazenar e manter a base de dados[115].

Baseia-se num algoritmo matemático que, através de uma corrente de blocos, identifica a transação realizada. A cadeia de blocos gerada após a operação é registada e seguidamente replicada em outros servidores que vão ser reesposáveis pela sua validação e

[114] Cf. PREUKSCHAT, Alexander, *Blockchain: la revolución industrial de internet*, Barcelona: Gestión 2000, 2017, p. 14

[115] Vide, LUCENA, Antônio de, Estudo de Arquiteturas dos blockchains de Bitcoin e Ethereum, IX Encontro de Alunos e Docentes do DCA/FEEC/UNICAMP (EADCA), Universidade Estadual de Campinas, Campinas, SP, Brasil, 2016

registo. É exatamente isto que torna a tecnologia tão segura – uma vez que as cópias se encontram descentralizadas é difícil de alterar os blocos[116].

É uma tecnologia que se apoia numa chave criptografada, uma sequência de blocos, em que cada um detém um número pré-definido e a sua união com outros blocos dá-se a partir de uma lógica matemática. Cada bloco representa uma operação, assegurada por assinaturas digitais criptografadas, permitindo a proteção de quem recebe e emite a transação, assim como o registo e, consequentemente, a transparência. Conta também com uma rede distribuída para a verificação da autenticidade da operação[117].

Assim, a blockchain é uma tecnologia composta por blocos criptografados e, como nos explica Edgar Taveira, as "cadeias de blocos compreendem registos ou blocos de dados. À medida que cada transação ocorre, ela é colocada num bloco. Cada bloco é conectado ao bloco anterior e posterior, sendo adicionado ao próximo numa ordem irreversível e as transações são armazenadas juntas. Depois dos blocos serem guardados e validados para armazenamento no ledger, não podem ser alterados ou excluídos por um único ponto/nó da rede. Este sistema funciona com base numa estrutura descentralizada, ou distribuída, onde cada ponto/nó possui uma cópia integral ou parcial de todo o blockchain ledger. Qualquer alteração ao ledger pressupõe uma aceitação coletiva, não havendo a possibilidade de alterar ou acrescentar novos blocos sem que todos os pontos/nós pertencentes à rede aprovem a transação"[118].

As redes de Blockchain podem ser públicas ou privadas. A blockchain pública é um sistema aberto, em que qualquer pessoa pode ter acesso à consulta, programação e leitura dos dados armazenados sem precisar de autorização para tal; é uma rede descentralizada e distribuída; a identidade de quem realiza transações é pseudoanónima, uma vez que é

---

[116] Vide, Government Office for Science, Distributed ledger technology: Beyond block chain, 2016. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf Consultado a 29 de dezembro de 2022

[117] Vide. MOURA, Luisa; BRAUNER, Daniela e JANISSEK-MUNIZ, Raquel, "Blockchain e a Perspectiva Tecnológica para a Administração Pública: Uma Revisão Sistemática", *Revista de Administração Contemporânea*, vol. 24, núm. 3, pp. 259-274, 2020, Associação Nacional dos Programas de Pós-graduação em Administração. Disponível em: https://www.redalyc.org/journal/840/84062698006/html/#B59 Consultado a 29 de dezembro de 2022

[118] TAVEIRA, Edgar, *Uma Visão Sobre A Tecnologia Blockchain: Domínios De Aplicação E Especificidades Na Cadeia De Abastecimento,* 2020, p.39. Relatório elaborado para satisfação parcial dos requisitos da Unidade Curricular de Tese/Dissertação do Mestrado em Engenharia Eletrotécnica e de Computadores, Departamento de Engenharia Eletrotécnica Mestrado em Engenharia Eletrotécnica e de Computadores Área de Especialização em Sistemas e Planeamento Industrial

possível rastrear o movimento, mas a sua identidade pessoal é anónima[119]. Por outro lado, as blockchain privadas caracterizam-se por serem "centralizadas, fechadas e distribuídas"[120]. Estão sob o controlo de uma única entidade e é esta que autoriza e permite o acesso de alguém à rede. Assim, aqui o acesso não é livre e só pode participar quem for convidado[121] – apenas os utilizadores que sejam pré-validados podem entrar na rede e ver os dados. A identidade dos participantes é conhecida previamente às transações, contrariamente ao que acontece numa blockchain pública. Dependendo do uso e do destino que quiserem dar ao sistema será eleita ou uma ou outra, mas tendo sempre como base a tecnologia de cadeia de blocos de dados encadeados.

4.2. Características da tecnologia blockchain

É possível identificar algumas características arquiteturais[122], como a descentralização das operações, ou seja, a informação está armazenada em diversos locais permitindo uma maior transparência[123] e dificultando a fraude; segurança nos armazenamentos dos registos, possibilitando a imutabilidade de transações e, com isso, uma maior confiança e controlo; integridade de dados, uma vez que os dados são armazenados em blocos distintos e praticamente imutáveis[124]. Existe a possibilidade de reverter as

[119] Cf. LEÓN TORRES, Alberto de, *Blockchain: características y estado actual. Posible efecto sobre la auditoría*, Trabajo especial de grado em Contabilidad y finanzas, Facultad de economia, empresa y turismo, Universidad de La Laguna, 2020. Disponível em: https://riull.ull.es/xmlui/bitstream/handle/915/20593/Blockchain%20caracteristicas%20y%20estado%20actual.%20Posible%20efecto%20sobre%20la%20auditoria.%20.pdf?sequence=1 Consultado a 2 de janeiro de 2023

[120] Idem.

[121] Vide. JAYACHANDRAN, Praveen, "The difference between public and private blockchain", *IBM*, 2017 Disponível em https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/. Consultado a 8 de dezembro de 2022

[122] SIMÕES, Maervelym Pâmella de Andrade et al, "Benefícios do uso da tecnologia Blockchain como instrumento para a auditoria contábil", *Revista Ambiente Contábil*, Vol.13, n.º 1, jan./jun., 2021

[123] A transparência não se traduz na "transparência dos dados" que são registados na blockchain. A transparência refere-se ao processo que é enviado para os vários participantes da rede para que seja validado. Relativamente aos dados inseridos no bloco, a informação é protegida porque está criptografada, pelo que aqueles que a validam não têm acesso ao conteúdo que aquele bloco contém. Desta forma, não há qualquer violação de privacidade porque só tem acesso ao conteúdo dos dados quem possui a chave para os desencriptar.

[124] Vide. ALCANTARA, Lucas Teles de et al. "Uso da tecnologia Blockchain como instrumento de governança eletrônica no setor público" In: Congresso Internacional de Contabilidade Pública, 2., 2019, Lisboa: Ordem dos Contabilistas Certificados, 2019. Disponível em: https://repositorio.unb.br/bitstream/10482/34651/1/EVENTO_UsoTecnologiaBlockchain.pdf Consultado a 29 de dezembro de 2022

alterações, mas traduz-se numa operação que exige uma quantidade avulta de recursos informáticos.

Há uma característica que alguns autores[125] identificam como a mais inovadora e importante – o facto de permitir que diferentes organismos realizem transações entre si sem precisarem da validação de uma estrutura central. Contudo, na opinião de Jan Veuger[126], e com a qual concordo, uma das características mais inovadoras é a possibilidade de rastreamento de transações, mesmo em bases de dados descentralizadas e públicas, permitindo assim reduzir a possibilidade de fraude e corrupção. Para além desta, a segurança, aliada a "um histórico inalterável, transparente e rastreável"[127] é, sem dúvida, a característica mais importante. A segurança decorre da imutabilidade dos dados que foram validados por cada bloco e, para que haja lugar à adição de um novo bloco, é exigido o consenso entre os participantes da rede.

Depois de analisar as características podemos, desde já, afirmar que a tecnologia blockchain poderá vir a ser uma mais-valia para o setor público, nomeadamente se aplicada à área da justiça e do processo penal. Oferece um conjunto de novas oportunidades para os Governos: maior controlo contra a fraude, transparência, fácil acesso a informação, maior qualidade de dados, eficiência, segurança e uma maior confiança na Administração Pública.

Como referido anteriormente, a tecnologia blockchain, atualmente, já encontra aplicabilidade prática em diversos setores, como o caso da indústria, comunicações e instituições públicas. Apesar do setor financeiro ter sido o que mais investiu nesta tecnologia, pelo facto de ser um setor altamente centralizado e consequentemente suscetível a ataques, é também no seio de muitos governos espalhados pelo Mundo que está a ser alvo de

[125] Cf. HORIUCHI, Felipe Seiti, *Ratreabilidade de um modelo de cadeia produtiva agrícola generalizado de uma rede blockchain.* 2018, Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação da Universidade Estadual de Londrina para obtenção do título de Bacharel em Ciência da Computação

[126] VEUGER, Jan, "Trust in a viable real estate economy with disruption and blockchain", *Facilities* Vol. 36 N. º 1/2, pp. 103-120. Disponível em: https://doi.org/10.1108/F-11-2017-0106 Consultado a 29 de dezembro de 2022

[127] TAVEIRA, Edgar, *Uma Visão Sobre A Tecnologia Blockchain..., cit.,* p.42

experiências – destacando-se a Estónia[128], Holanda[129], França[130] e o Dubai, países que investiram fortemente na digitalização do setor público. No entanto, não é só no seio dos governos que esta tecnologia tem avançado, também organizações internacionais têm apostado cada vez mais no uso da blockchain, nomeadamente a Organização das Nações Unidas (ONU), aplicando-a a projetos de ajuda humanitária[131].

No âmbito do processo penal também podemos apontar alguns exemplos a nível mundial. Nos EUA, em 2016, no Estado de Vermont foi criada uma lei, a Lei 12 V.S.A. § 1913[132], com a finalidade de enquadrar a tecnologia blockchain nos processos jurídicos e para que os dados armazenados por aquela possam ser usados como meio de prova. A Lei define o que é blockchain, indica os procedimentos e requisitos que têm de ser adotados para que os dados armazenados na blockchain possam ser valorados. Desde que se possa verificar a data e a hora em que o documento se registou na blockchain, a conduta se possa considerar regular e, ainda, se se fizer acompanhar de uma declaração de uma pessoa qualificada, feita sob juramento, onde declara a sua qualificação para certificar aquelas informações, a informação é considerada autêntica, a menos que algo indique falta de confiabilidade.

Na China, o Supremo Tribunal Chines, após uma decisão do Tribunal da Internet de Hangzhou[133] a 27 de outubro de 2018, onde foi usada como meio de prova o conteúdo de uma página de internet, um "printscreen" que foi inserido e armazenado numa blockchain,

---

[128] A Estónia foi pioneira na introdução do uso usa da blockchain no setor público, sendo o país que mais investimentos fez na área. Segundo dados recolhidos do site do Governo da Estónia, 99% dos serviços públicos estão disponíveis online ininterruptamente. Trata-se de um sistema digital onde prima a transparência pública, a segurança e a integridade dos dados. Vide. https://e-estonia.com/wp-content/uploads/2020mar-nochanges-faq-a4-v03-blockchain-1-1.pdf Consultado a 8 de dezembro de 2022

[129] A Holanda criou a Dutch Blockchain Action, uma agenda para o desenvolvimento da blockchain que tem como pilares "a Identificação Digital; as Condições para o uso da Blockchain; e a Capacitação para o desenvolvimento e uso da tecnologia". Disponível em https://dutchblockchaincoalition.org/ Disponível em https://www.government.nl/topics/ict/ict-and-economy

[130] A França testou em 2021 um projeto piloto liderado por um consórcio de instituições financeiras (BNP Paribas, Crédit Agricole CIB, HSBC e Sociéte Générale), que se baseia na utilização da tecnologia blockchain na área das obrigações, o que permite o "pagamento de juros, liquidação de transações e recompra de títulos". Disponível em https://expresso.pt/economia/2021-10-19-Franca-usa-blockchain-e-moeda-digital-para-comprar-e-vender-divida-soberana-em-projeto-piloto-e2c18928

[131] O projeto "Building Blocks", em que através da tecnologia Blockchain controlam as transferências de ajudas monetárias para refugiados no Líbano, na Jordânia e em Bangladesh, conseguindo rastrear, coordenar e fornecer assistência, incluindo dinheiro, medicação, alimentação e WASH (água, saneamento e higiene). Disponível em https://innovation.wfp.org/project/building-blocks

[132] Vide. The Vermont Statutes Online, Vermont General Assembly, 2022, disponível em: https://legislature.vermont.gov/statutes/section/12/081/01913 Consultado a 8 de dezembro de 2022

[133] O Tribunal da Internet de Hangzhou foi criado em 2017 e tem apenas competências específicas para litígios que decorram na internet, sejam eles contratos de compra e venda de produtos, serviços, direitos de propriedade intelectual ou difamações em redes sociais.

veio admitir, a 7 de setembro de 2019, que os dados armazenados pela blockchain possuem um elevado valor probatório e pode ser usado nos processos judiciais[134].

No Brasil foram usados num processo penal meios de prova armazenados na blockchain[135], nomeadamente publicações de redes sociais como o Facebook, Instagram e Twitter. Através do projeto da OriginalMy[136] o autor providenciou a preservação de todo o conteúdo das provas na plataforma Blockchain, para que as ofensas que circulavam nas redes sociais pudessem ser removidas sem que tal prejudicasse o processo penal. A introdução numa blockchain foi uma forma de comprovar a veracidade e a existência daquelas publicações sem prejudicar a justiça. A OriginalMy[137] usa a extensão PACWeb que, quando instalada no navegador, gera automaticamente um relatório em formato PDF daquilo que se está a visualizar, sejam mensagens no Telegram, Whatsapp, Facebook, email; além do relatório também grava em vídeo o mesmo conteúdo. De seguida os dados são inseridos numa blockchain para se comprovar que a prova não sofreu alterações e mesmo se o conteúdo for eliminado da internet, há esse registo com a hora e data em que ocorreu. Outro projeto que se dedica à conservação de provas para a sua posterior utilização no processo é a plataforma HashCool[138] que tem como finalidade o registo de documentos e arquivos digitais ou digitalizados, assim como informações contidas em URL´s, garantindo a sua imutabilidade e autenticidade. Por fim, o UProov é um serviço que certifica fotos, vídeos ou ficheiros de áudio com data e hora para que sejam considerados autênticos; após ser criada uma chave com indicação da hora e data, é inserida na blockchain e há um bloqueio daquele ficheiro, que caso seja alterado, caso ocorra a alteração de um simples pixel, a chave criada no início já não corresponderá à criada posteriormente à modificação[139].

[134]Decisão de 7 de setembro de 2019 do Supremo Tribunal Chinês. Disponível em: https://www.court.gov.cn/zixun-xiangqing-116981.html (na língua original).
[135] Tribunal de Justiça de São Paulo TJ-SP - Agravo de Instrumento: AI XXXXX-77.2018.8.26.0000 SP XXXXX-77.2018.8.26.0000. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/661192846/inteiro-teor-661192900
[136] Cf. MILAGRE, José António, "O uso da infraestrutura Blockchain na realização de negócios jurídicos", The tenth international conference on forensic computer science and cyber law, São Paulo, Brasil, 2018
[137] Vide. https://originalmy.com/pacweb Consultado a 12 de dezembro de 2022
[138] Vide. https://hash.cool/ Consultado a 12 de dezembro de 2022
[139] Cf. MILAGRE, José António, "O uso da infraestrutura Blockchain..." *cit.*

4.3. Vantagens da aplicabilidade da tecnologia blockchain na preservação da prova

A blockchain pode ser usada como meio de preservação de dados, de prova digital, tendo em conta a sua máxima segurança e autenticidade, que caracterizam esta tecnologia. É um sistema que mantém os registos de forma segura, inalteráveis e imutáveis.

A grande vantagem de utilizarmos a blockchain para preservação de dados é a confiabilidade no armazenamento da prova, ou seja, a garantia de que a cadeia de custódia da prova não é quebrada e de que aquela prova não é alterada. O facto de a prova armazenada na blockchain ser validada por vários nós que integram a rede garante que a prova não será manipulada, porque uma parte sozinha não consegue modificar os dados conservados.

Face ao que já analisamos, a blockchain já mostrou ser uma oportunidade para o acondicionamento da prova, para preservar alterações posteriores ao seu registo. Como já referimos anteriormente, a técnica usada pelos órgãos de polícia criminal para garantir a integridade das provas é o cálculo do código Hash, que não podemos deixar de afirmar que é um meio seguro e fiável. Apesar de o reconhecermos, vimos fazer a sugestão de ser criada uma blockchain para a inserção dessas provas.

Relativamente ao registo de documentos, imagens ou vídeos, ou seja, de provas digitais, na blockchain, teríamos de continuar a criar o seu código Hash e, após a criação da assinatura digital, teríamos de a inserir na blockchain, onde "cada bloco de informações possui referência ao bloco anterior (daí o termo "cadeia de blocos") e, por isso, nenhum bloco anterior pode ser alterado sem que modifiquem os blocos posteriores"[140]. Desta forma, uma determinada informação criptografada (qualquer dado, como uma imagem, um vídeo, um documento) seria inserida no primeiro bloco e, a partir daí, seria criado o código hash que identifica esse primeiro bloco. No bloco seguinte já seria armazenada outra informação criptografada, por exemplo, outro documento e, também, o hash que foi calculado para o bloco anterior. "A partir desse conjunto (da informação inserida no novo bloco e do código hash do bloco anterior) é extraído o hash desse segundo bloco"[141], e assim

[140] Cf. ROQUE, André Vasconcellos, A tecnologia blockchain como fonte de prova no processo civil, 2018. Disponível em: http://genjuridico.com.br/2018/10/15/tecnologia-blockchain-fonte-de-prova/ Consultado a 8 de dezembro de 2022

[141] *Idem.*

consecutivamente. André Vasconcellos Roque[142] diz-nos que "mínimas alterações na informação original (...) modificam completamente o *hash*. Assim, se alguém tentar adulterar a informação armazenada no bloco A (o primeiro bloco), isso irá modificar o Hash A, que é gravado no bloco B, de maneira que toda a cadeia de informações nos blocos subsequentes se tornará inconsistente". É isto que torna esta tecnologia tão segura e confiável que, para "além da formação de cadeia de blocos, esta é armazenada de maneira descentralizada em várias máquinas ao mesmo tempo", o que se denomina rede Peer-to-peer (P2P). Com o uso desta tecnologia é possível aumentar a eficiência, a transparência, o acesso à informação e a confiança de que a cadeia de custódia não foi alterada.

Para além desta tecnologia poder ser usada pelos OPC para a preservação da prova, poderia ser também utilizada pelos sujeitos, quer pelo assistente que, segundo o artigo 69.º, n.º 2, alínea a), tem o dever de oferecer provas, quer pelo arguido que tem também o direito de oferecer provas, segundo o artigo 61.º, n.º 2, alínea g). Com a criação de um projeto em que os sujeitos pudessem inserir as provas que detêm sobre determinado crime numa blockchain, conseguiriam garantir que aquela prova é autêntica. Basta pensarmos num crime de difamação nas redes sociais em que o ofendido tira printscreens das publicações em que é difamado. Com um simples clique aquela publicação pode ser apagada pelo seu autor e daqui podem advir problemas. No entanto, se a imagem for inserida numa blockchain vai ficar registada a sua data, hora e quem a inseriu, transmitindo transparência e autenticidade necessárias para que seja considerada uma prova válida no processo. Contudo, se seguido este esquema, ainda se poderia questionar a credibilidade daquela imagem, daquele printscreen, porque pode ter sido alvo de alterações, como por exemplo, pode ter ocorrido uma manipulação da imagem depois de tirado o printscreen e antes de ser introduzido na blockchain. Este fenómeno de manipulação de imagens, vídeos ou áudios é conhecido pelo termo "deepfake" que, segundo Robert Chesney e Danielle Citron corresponde "à manipulação digital de som, imagens ou vídeo para imitar alguém ou fazer parecer que a pessoa fez alguma coisa – e fazer isso de uma maneira que seja cada vez mais realística, ao ponto de não se conseguir detetar a falsificação" (tradução livre)[143]. Estas manipulações são

[142] *Idem.*
[143] Cf. Robert Chesney e Danielle Citron, Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?, citado por MEDON AFFONSO , F. J., "O direito à imagem na era das deep fakes". *Revista Brasileira De Direito Civil*, *27*(01), p.251, 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/438 Consultado a 10 de janeiro de 2023

realizadas através de "técnicas computacionais avançadas", recorrendo a Inteligência Artificial, "que faz com que seja quase impossível detetar a fraude"[144]. Desta forma, para que a conservação de provas em blockchain pelos sujeitos fosse permitida na prática jurídica, seria também importante haver uma gravação de todos os passos de recolha de prova para não haver dúvidas da sua autenticidade e não haver o risco de esta ter sido manipulada. Ou seja, recorrendo à gravação do browser onde se encontra a prova relevante para o processo, por exemplo numa rede social como o Twitter ou o Whatsapp. Desta forma, conseguir-se-ia atentar todos os passos dados desde o momento em que se recolheu a prova, ou seja, desde que se tirou o printscreen, até ao momento em que é inserido na blockchain, semelhante ao que acontece com o programa PACWeb[145], já anteriormente referido. Seguidos estes passos não haveria dúvidas quanto à autenticidade das provas preservadas pelos sujeitos na blockchain.

Citando Ana Dias Meireles, "tornar a blockchain uma realidade, quase que inata e umbilical com a pegada digital, seria facilitar a prova para todos"[146].

[144] Medon Affonso, F. J., "O direito à imagem...", *cit*.

[145] Já houve decisões judiciarias onde se cita esta solução como um meio seguro e económico para a apresentação das provas em Tribunal. Vide. Processo 2237253-77.2018.8.26.0000 do Tribunal de Justiça de São Paulo e Processo 1000708-05.2019.5.02.0481 do Tribunal Regional do Trabalho da 2.º Região

[146] Cf. MEIRELES, Ana Isa Dias, *A prova digital no processo judicial*, Escola de Direito, Universidade do Minho, 2022, p.194. Tese de Doutoramento em Ciências Jurídicas – Especialidade em Ciências Jurídicas Privatísticas

Conclusão

Chegados aqui, e após o longo caminho percorrido, estamos finalmente capazes de responder às questões que levantamos e ao que nos propusemos analisar inicialmente.

Com os grandes avanços tecnológicos e com o aumento da criminalidade informática, o uso e a necessidade de recorrer a provas digitais nos processos penais é cada vez mais necessário e até mesmo inevitável, uma vez que é esta prova que vai permitir responder às crescentes necessidades sentidas na justiça penal face ao combate ao cibercrime.

A natureza complexa deste tipo de prova, que se caracteriza por ser uma prova imaterial, de carácter temporário ou efémero, frágil, suscetível a alterabilidade, volátil e instável, levou ao surgimento de legislação especifica, que no nosso caso é a Lei n.º 109/2019 de 15 de setembro, também conhecida por Lei do Cibercrime, e é este o diploma base que regula a prova digital em Portugal.

Também ao nível da cadeia de custódia foi necessário fazer mudanças. Uma vez que os procedimentos para a manutenção da cadeia de custódia de uma recolha de um perfil de ADN não são os mesmos que são usados para a manutenção da cadeia de custódia de uma prova digital. Foi necessário adaptar meios de obtenção de prova, atualmente regulados na Lei do Cibercrime, a apreensão e recolha, assim como as técnicas de manutenção e preservação da prova. Contudo, na nossa opinião, Portugal não se debruçou da melhor maneira possível sobre a regulamentação destes procedimentos. Ao contrário do que acontece em outros ordenamentos jurídicos, não temos positivado na lei uma definição de cadeia de custódia, não possuímos um manual de procedimentos, há uma escassez quer jurisprudencial, quer doutrinaria, de artigos em que se aborde este tema, o que se traduz numa grande lacuna. Face a esta ausência temos de nos socorrer de recomendações de boas práticas emitidas por entidades internacionais, como é o caso da Norma ISO/IEC FDIS 27037:2012 e do Eletronic Evidence Guide do Conselho da Europa. A regulamentação da cadeia de custódia das provas digitais resultaria numa maior segurança e fiabilidade dos meios de prova apreendidos no decorrer de uma investigação, era a forma de garantir que as provas que estão a ser valoradas no processo estão livres de contaminações e subsequentemente de ilicitudes.

A carência de regulamentação e até de doutrina sobre a cadeia de custódia não é proporcional à importância que esta detém no processo penal. A cadeia de custódia é o procedimento que tem de ser adotado desde o momento da recolha da prova, até ao momento do trânsito em julgado, para garantir a rastreabilidade, a autenticidade, a confiabilidade e a preservação da prova digital. A grande finalidade desde procedimento é manter a força probatória da prova que foi apreendida para que o julgador possa formar a sua convicção com material autêntico e genuíno, livre de contaminações.

Para a garantia da cadeia de custódia é necessário respeitar procedimentos específicos de recolha, análise e preservação da prova digital, que exigem técnicas especificas de análise forense e que vão permitir manter a integridade das provas alvo.

A técnica usada para garantir a preservação da prova e a sua integridade é o cálculo do código hash, que vimos ser o resultado da aplicação de um algoritmo matemático a uma determinada informação, mais propriamente a determinada prova. O código hash vai funcionar como sendo a impressão digital daquela prova, que vai garantir que o conteúdo da prova analisada é igual ao conteúdo da prova original. Se a cópia da prova que foi usada para investigação detiver um código hash diferente do código da prova original, ou seja, se os códigos não corresponderem, significa que houve uma alteração na prova e o valor probatório foi quebrado. Esta técnica é tão segura porque uma mínima alteração que se faça, mesmo a alteração de um simples bit, vai produzir um código completamente distinto. A quebra da cadeia de custódia levará à proibição total da admissibilidade e à proibição de valoração daquela prova no processo.

Face ao já analisado, podemos, desde já, concluir que é inegável a grande importância que detém a cadeia de custódia. Temos também de realçar que a técnica forense do cálculo do código hash é uma técnica segura que garante a confiabilidade das provas digitais. No entanto, se aliarmos esta técnica à introdução da prova digital na recente tecnologia blockchain, teríamos um cenário ainda mais seguro, confiável e que permitiria resolver problemas processuais ao nível da prova.

Na parte final desta dissertação, venho responder à última e grande questão que coloquei inicialmente – se será a tecnologia blockchain adequada para a preservação da prova digital.

Sendo a blockchain um sistema que regista de forma imutável os dados de forma segura, inalterável, que regista o horário e a data em que determinada prova foi registada na rede, quem a inseriu e quem lhe acedeu, poderemos aceitar que seria uma vantagem que pugnaria pelo aumento da eficiência, da transparência e da confiança dos cidadãos em geral no sistema de justiça.

Para além de se mostrar uma vantagem para a manutenção da cadeia de custódia, mais precisamente para a preservação da prova digital pelos OPC, acabamos por fazer uma última sugestão que evitaria muitos problemas de justiça. Esta sugestão passa pela aceitação como meio de prova válido de informações inseridas e preservadas em blockchain pelos sujeitos processuais, como o arguido e o assistente, o que já decorreu em alguns tribunais de outros ordenamentos jurídicos. Chegado ao final deste estudo, podemos concluir que a blockchain seria vista como uma forma segura de preservação de prova.

É inegável que esta tecnologia veio para ficar e o setor público não se deve manter alheiro, muito menos resistir. Esta é uma solução para acompanhar a Quarta Revolução Industrial que está a decorrer e, também, para acompanhar o progresso dos países à nossa volta.

Termino com a plena noção de que é uma sugestão ambiciosa, mas que espero que venha um dia a vigorar no nosso ordenamento jurídico, que permitirá solucionar vários problemas, respeitar os princípios relacionados com a prova e com a cadeia de custódia ou, pelo menos, que pugnará pela digitalização dos nossos tribunais.

Bibliografia

ALBERGARIA, Pedro Soares, Anotação ao artigo 125.º do CPP - Legalidade da prova, in *Comentário Judiciário do Código de Processo Penal*, Tomo II, Coimbra: Almedina, 2020

ALCANTARA, Lucas Teles de et al., Uso da tecnologia Blockchain como instrumento de governança eletrônica no setor público, In: Congresso Internacional de Contabilidade Pública, Lisboa: Ordem dos Contabilistas Certificados, 2019

ALMAS, Amanda Costa das, A Aplicabilidade da cadeia de custódia em dados digitais utilizados como prova no processo penal brasileiro, *IBCCRIM - Laboratório de Ciências Criminais de Porto Alegre/RS*, 2020

ANTUNES, Maria João, *Direito Processual Penal*, Coimbra: Almedina, 2021

ARELLANO, Luis Henrique, CASTAÑEDA, Carlos Mario, La cadena de custodia informático-forense, *Revista ACTIVA*, 3, pp.67-81, 2012

CALDERÓN ARIAS, Emma, Fundamentos teóricos de la cadena de custodia en el proceso penal cubano, *MISIÒN JURÍDICA - Revista de Derecho y Ciencias Sociale*s, n.º 12, pp.241-253, (enero-junio de 2017)

CHELSEA, Quilling, Journal of Public and International Affairs, May de 2022 Obtido de *The Future of Digital Evidence Authentication at the International Criminal Cour*t: https://jpia.princeton.edu/news/future-digital-evidence-authentication-international-criminal-court

DIAS, Jorge Figueiredo, *Direito Processual Penal*, Coimbra: Coimbra Editora, 2004

DOMINGOS, Fernanda Teixeira Souza, "As provas digitais nos delitos de pornografia infantil na internet", In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro, *A prova no enfrentamento à macrocriminalidade, 3º Edição,* Salvador: Editora Juspodvim, p.197, 2015

DORAN, A. Robert, Exploring the links in the chain of custody, Nebraska Association for Property and Evidence (NAPE), 2005

Electronic Evidence Guide - a basic guide for police officers, prosecutors and judges. Cibercrime Division - Directorate General of Human Rights and Rule of Law, Strasbourg, France, 04 de April de 2022

FÉRNANDEZ MARTÍNEZ, Juan Carlos, "Especialidades de la prueba cuando, esta, es tecnológica". In: ORTEGA BURGOS, Enrique, *Actualidad: Nuevas Tecnologías,* Valência: Tirant lo Blanch, p. 333, 2020

FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital - direitos fundamentais (ainda mais) em perigo", In A. M. Rodrigues, *A Inteligência Artificial no Direito Penal*, Coimbra: Almedina, pp. 129-161, 2021

GARCIA MATEOS, José Aurélio, "Cadena de custódia vs mismidad", In: *La prueba electrónica: validez y eficaria procesal*, Colección Defasio Legales, 1º Edicción, pp.130-136, septiembre de 2016

HORIUCHI, Felipe Seiti, *Ratreabilidade de um modelo de cadeia produtiva agrícola generalizado de uma rede blockchain*, Londrina, 2018

ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence, 7 de dezembro de 2022. Obtido de ISO: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27037:ed-1:v1:en

JAYACHANDRAN, Praveen, The difference between public and private blockchain, 2017. Obtido de *IBM*: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

LEÓN TORRES, Alberto de, *Blockchain: características y estado actual, Posible efecto sobre la auditoría*, Universidad de la Laguna, 2020

MACHADO, Michele Moreira, "Importância da cadeia de custódia para a prova pericial", *Revista Criminalística e Medicina Legal*, N.º1, V.º2, 2017

MARINHO, Girlei Veloso, *Cadeia de custódia da prova pericial*, Fundação Getúlio Vargas, Escola Brasileira de Administração Pública e de Empresas, Rio de Janeiro, 2011

MARQUÉS ARPA, Tomás; Serra Ruiz, Jordi, Cadena de custodia en el análisis forense, Implementación de un marco de gestión de la evidencia digital, Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información, pp. 167-172, Alicante: Universidad de Alicante, 2014

MARQUES, Pedro, *Informática Forense: Recolha e preservação da prova digital*, Universidade Católica Portuguesa, 2013

MEDON AFFONSO, Filipe José, "O direito à imagem na era das deep fakes", *Revista Brasileira De Direito Civil*, 27(01), p.251, 2021

MEIRELES, Ana Isa Dias, *A prova digital no processo judicial*, Tese de Doutoramento, Escola de Direito, Universidade do Minho, 2022

MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Wolters Kluwer Portugal - Coimbra Editora, 2010

MILAGRE, José António, "O uso da infraestrutura Blockchain na realização de negócios jurídicos", The tenth international conference on forensic computer science and cyber law, 2018

MILITÃO, Renato Lopes, "A propósito da prova digital no processo penal", *Revista da Ordem dos Advogados*, Lisboa, Ano 72, Vol.1, pp.247-285, 2012

MOURA, Luisa; BRAUNER, Daniela e JANISSEK-MUNIZ, Raquel, "Blockchain e a Perspectiva Tecnológica para a Administração Pública: Uma Revisão Sistemática", *Revista de Administração Contemporânea*, Vol. 24, N.º3, pp.259-274, 2020

NATÁRIO, Rui, "O combate ao cibercrime: anarquia e ordem no ciberespaço", *Revista Militar* n.º 2541, 2013

NEVES, A. Castanheira, Sumários de processo criminal: 1967-1968, 1968

PIMENTA, José da Costa, *Introdução do Processo Penal*, Coimbra: Almedina, 1989

Prado, Geraldo, *A cadeia de custódia da prova no processo penal*, São Paulo: Marcial Pons, 2019

PRADO, Geraldo, Notas sobre proteção de dados, prova digital e o devido processo penal, Proteção de dados pessoais na segurança pública e investigação criminal, 2020

PRADO, Geraldo, Breves notas sobre o funcionamneto constitucional da cadeia de custódia da prova digital, A interface entre o Direito Digital e o Processo Penal, Lisboa, 2021

PREUKSCHAT, Alexander, *Blockchain: la revolución industrial de internet*, Barcelona: Gestión 2000, 2017

RAMOS, Armando Dias, *A prova digital em processo penal*: o correio eletrónico, Lisboa: Chiado Editora, 2014

RODRIGUES, Benjamin Silva, *Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital*, Coimbra: Coimbra Editora, 2009

RIVERA OLARTE, Francisco; ROJAS QUINAYÁ, Lina, Estudio interdisciplinario sobre los Sistemas de Valoración y Estándares probatorios en el Derecho Procesal colombiano, DIXI, pp. 1-49, julio-deciembre 2019

ROQUE, André Vasconcellos, A tecnologia blockchain como fonte de prova no processo civil, 2018

RUBIO ALAMILLO, Javier, "Conservación de la cadena de custodia de una evidencia informática", *Diario LA LEY*, n.º 8859, 2016

SANTOS, Gil Moreira, *Princípios e prática Processual Penal*, Coimbra: Coimbra Editora, 2014

Government Office for Science, Distributed Ledger Technology: beyond block chain, 2016. Obtido de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

SILVA, Sandra Oliveira, "LEGALIDADE DA PROVA E PROVAS PROIBIDAS", *Revista Portuguesa de Ciência Criminal*, Ano 21, N.º4 pp545-591, 2011

SIMÕES, Maervelym Pâmella, "Benefícios do uso da tecnologia Blockchain como instrumento para a auditoria contábil", *Revista Ambiente Contábil,* Vol.13, N.º1, janeiro-junho 2021

TAVEIRA, Edgar, *Uma Visão Sobre A Tecnologia Blockchain: Domínios De Aplicação E Especificidades Na Cadeia De Abastecimento*, 2020

VALENTE, Manuel Monteiro, *Cadeia de custódia da prova*, Coimbra: Almedina, 2019

VAZ, Denise Provasi, *Provas digitais no processo penal: Formulação do conceito, definição das características e sistematização do procedimento probatório*, Faculdade de Direito da Universidade de São Paulo, 2012

VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada*, Coimbra: Coimbra Editora, 2011

VERDELHO, Pedro, "A nova Lei do Cibercrime", *Scientia Ivridica, Revista de Direito Português e Brasileiro*, Tomo LVIII, n.º 320, pp.733-734, outubro - dezembro 2009

VEUGER, Jan, "Trust in a viable real estate economy with disruption and blockchain, Facilities", Facilities, Vol.36, N.º1/2, pp.103-120, 2018

WHITCOMB, Carrie Morgan, "An Historical Perspective of Digital Evidence: A Forensic Scientist´s View", *International Journal of Digital Evidence*, Vol. 1, Issue 1, Spring 2002

Jurisprudência

Sentencia do Supremo Tribunal Espanhol n.º 1190/2009, de 3 de deciembre. Disponível em: https://vlex.es/vid/211686183

Sentencia do Tribunal Constitucional Espanhol n.º 170/2003 de 23 de octubre. Disponível em: https://www.boe.es/boe/dias/2003/10/23/pdfs/T00045-00053.pdf

Acórdão do Tribunal da Relação de Lisboa n.º 4069/13 de 3 de dezembro 2016. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/4fdb60ca67ced178802580c2003de80b?OpenDocument

Decisão do Supremo Tribunal Chinês n.º 16 de 7 de setembro de 2018. Disponível em: https://www.court.gov.cn/zixun-xiangqing-116981.html

Acórdão do Tribunal de Justiça de São Paulo, Agravo de Instrumento: AI XXXXX-77.2018.8.26.0000 SP XXXXX-77.2018.8.26.0000, de 19 de dezembro de 2018. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/661192846/inteiro-teor-661192900

Acórdão Tribunal Constitucional Alemão – Bundesverfassungsgericht - Zitiervorschlag: BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 -, Rn. 1-333. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html

Web

Best Practice Manual for the Forensic Examination of Digital Technology. Disponível em: https://enfsi.eu/about-enfsi/structure/working-groups/documents-page/documents/best-practice-manuals/

Building Blocks - Blockchain network for humanitarian assistance - Graduated Project. Disponível em: https://innovation.wfp.org/project/building-blocks

Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. Disponível em: https://nij.ojp.gov/library/publications/digital-evidence-courtroom-guide-%20law-enforcement-and-prosecutors

Dutch Blockchain Coalition: Disponível em: https://dutchblockchaincoalition.org/

Estonian blockchain Technology. Disponível em: https://e-estonia.com/wp-content/uploads/2020mar-nochanges-faq-a4-v03-blockchain-1-1.pdf

Europol. Disponível em: https://www.policiajudiciaria.pt/wp-content/uploads/2016/12/UNE.pdf

Expresso. França usa "blockchain" e moeda digital para comprar e vender dívida soberana em projeto piloto. Disponível em: https://expresso.pt/economia/2021-10-19-Franca-usa-blockchain-e-moeda-digital-para-comprar-e-vender-divida-soberana-em-projeto-piloto-e2c18928

Good Practice Guide for Computer-Based Electronic Evidence, Official release version 4.0. Disponível em: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf

Government Office for Science, *Distributed ledger technology: Beyond block chain.* Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

HashCool. Disponível em: https://hash.cool/

Lei 12 V.S.A. § 1913 - The Vermont Statutes Online, Vermont General Assembly. Disponível em: https://legislature.vermont.gov/statutes/section/12/081/01913

National Institute of Justice (USA), Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Disponível em: https://nij.ojp.gov/library/publications/forensic-examination-%20digital-evidence-guide-law-enforcement

Organização Internacional de Polícia Criminal – INTERPOL. Disponível em: https://www.policiajudiciaria.pt/wp-content/uploads/2016/12/GNI.pdf

PACWeb. Disponível em: https://originalmy.com/pacweb

Scientific Working Group on Digital Evidence (SWGDE): https://www.swgde.org/documents/published

The Dutch Digital Agenda, Government of the Netherlands. Disponível em: https://www.government.nl/topics/ict/ict-and-economy