Universidade do Minho
Escola de Direito

Diogo Nuno Cardoso Miranda de Matos Brandão

A PROVA DIGITAL NO PROCESSO CIVIL: REPENSAR O SISTEMA

outubro de 2019

A PROVA DIGITAL NO PROCESSO CIVIL: REPENSAR O SISTEMA
Diogo Nuno Cardoso Miranda de Matos Brandão
UMinho | 2019

Universidade do Minho
Escola de Direito

Diogo Nuno Cardoso Miranda de Matos Brandão

A PROVA DIGITAL NO PROCESSO CIVIL: REPENSAR O SISTEMA

Dissertação de Mestrado
Mestrado em Direito
Área de Especialização em Direito e Informática

Trabalho efetuado sob a orientação do
Professor Doutor Francisco Andrade
e do
Professor Doutor Victor Fonte

outubro de 2019

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Agradecimentos

Aos meus orientadores, pelo apoio, paciência e interesse com que acompanharam este processo, e pela segurança que me transmitiram naquilo que aquilo me proponho a apresentar.

Aos meus amigos, que sabem quem são, por serem meus companheiros desde que ingressamos na Licenciatura. Mesmo tendo cada um seguido o seu caminho, nunca realmente deixaram de estar lá para me recordar do melhor que estes anos me deram.

À que me deu força e coragem para dar tudo o que tinha a este projeto, e que me deu tanto de si, quer se aperceba quer não. A chegada foi tão mais doce assim.

À minha irmã, pelo ânimo e carinho com que sempre me assegurou que eu seria capaz do que quer que desejasse alcançar e por ser, e pelo orgulho que me dá todos os dias.

Aos meus pais, por me incentivarem a envergar por este Mestrado, que em tanto me enriqueceu e me ajudou a entender o que queria para mim. Obrigado por toda a paciência, apoio e carinho nas alturas mais difíceis e incertas.

Obrigado a todos os que lá estiveram, de uma forma ou outra, enquanto este projeto se materializava. Esta é para mim e para todos vocês.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

A PROVA DIGITAL NO PROCESSO CIVIL: REPENSAR O SISTEMA

Resumo

O presente trabalho tem por objeto o tema da admissibilidade da prova eletrónico-digital no ordenamento jurídico português, no âmbito do processo civil, bem como a consagração de um regime específico e de uma expressa disposição legal em seu torno na lei geral portuguesa.

Realizaremos estudo uma vez que, contrariamente ao que ocorreu com o Processo Penal, e não obstante a recente reforma processual civil (com a Lei 41/2013, de 26 de junho), nenhuma menção específica relativamente a este tipo de prova foi elencada no texto legal do Código de Processo Civil, ficando-se apenas com documentos legais avulsos e transposições de Diretivas Europeias alusivas a valores probatórios de documentos eletrónicos.

Neste sentido, o nosso estudo prender-se-á com a análise da problemática em causa e com a clarificação de vários aspetos jurídicos e científicos relativamente às especificidades da prova eletrónico-digital e ao seu potencial impacto na resolução de vários impasses que afligem o Processo Civil. Teremos como base jurisprudência e doutrina nacional e estrangeira que nos auxiliarão a clarificar quaisquer dúvidas relativamente ao assunto.

Palavras-chave: *Admissibilidade, Processo Civil, prova digital, prova eletrónica.*

DIGITAL EVIDENCE IN CIVIL PROCEDURE: RETHINKING THE SYSTEM

Abstract

This thesis is the product of my research and studies on the issue of the admissibility of digital-electronic evidence in Portugal's legal system, under the scope of its civil procedure; as well as the establishment of a specific base and legal provision for it in Portuguese general law.

Our study was motivated by the fact that, unlike what happened with the Portuguese Criminal Procedure, and in spite of the recent civil procedure reform (with Law 41/2013, of 26 of June), there has been specific mention about this specific type of evidence in the Portuguese Civil Procedure Code, leaving us with loose legal documents and transpositions of European Directives regarding the value of proof found in electronic documents.

As such, our study will focus on the analysis of the issue at hand and on classifying several legal and scientific aspects pertaining the specifics of electronic-digital evidences, and their potential impact in solving several hold-ups that afflict our Civil Procedure. We will base our work in national and international jurisprudence and doctrine, which will help us clarify any doubts regarding the subject.

Keywords: *Admission, Civil Procedure, digital evidence, electronic evidence.*

Índice

Abreviaturas

CAD	Codice dell' Amministrazione Digitale (Itália)
CC	Código Civil
CE	Conselho Europeu
CPC	Código de Processo Civil
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
in fine	*parte final*
in	em
LEC	Ley de Enjuiciamento Civil (Espanha)
PE	Parlamento Europeu
RGPD	Regulamento Geral de Proteção de Dados
UE	União Europeia
Vol.	Volume

Introdução

Com o advento das novas tecnologias e de diferentes meios de apreensão de informação, cada vez mais multimodais e imiscuídos nos mais variados setores de atividade (indústria, comércio, entre outros), torna-se relevante questionar até que ponto não será fulcral os tomar em conta de forma a levar a cabo um funcionamento diligente do nosso Processo Civil e, em particular, da prova.

De facto, é inegável a relevância da prova no Direito e, em particular, do papel que esta ocupa enquanto elemento de demonstração da realidade dos factos contidos nas peças processuais no âmbito do processo. Não se encontraria grande sentido na alegação de factos constitutivos do direito material caso não existissem oportunidades de os comprovar; o que comprometeria o próprio sentido do processo, que gira em torno da busca da verdade.

É precisamente neste âmbito que a discussão da temática da prova digital-eletrónica ganha relevância, uma vez que cada vez mais se recorrem a documentos em formato eletrónico na celebração de negócios jurídicos, ao ponto em que o Comércio Eletrónico já é uma matéria regulamentada. Ainda assim, o valor probatório destes documentos continua a ser um tópico de divergência.

Procurando inserir a necessidade de se prever uma prova digital no elenco de tipos de prova e na sua previsão no Processo Civil, devemos confrontar-nos com duas realidades: em primeiro lugar, no nosso ordenamento jurídico, apenas no âmbito do Processo Penal e do combate ao cibercrime é que se realizaram esforços por consagrar uma funcionalidade e regulamentação das provas digitais; e, em segundo lugar, que a definição de "prova digital" *per si* ainda não se afigura como algo consensual.

Farei minhas as palavras de JOSÉ ESTEVES[1], que entende que *"[o] século XXI apresenta novos desafios para a justiça cível (...) constituindo-se os tempos de hoje num importante momento de reflexão sobre o que se pretende para o direito processual civil, (...) instrumento de procura da verdade material e da realização da justiça, num Estado de Direito Democrático"*.

[1] ESTEVES, José, *"Um novo Mundo, uma nova Racionalidade, um novo processo Civil"*, in *"I Jornadas de processo civil - Olhares transmontanos"*, Valpaços, 2012, p. 11.

Acreditando numa necessidade do Direito acompanhar os tempos, enquanto reflexo da realidade social, o objetivo deste projeto será, primeiramente, de esclarecer possíveis questões e reticências que possam existir relativamente a esta nova *nuance* eletrónica de uma figura tão central ao processo como é a prova; e, de seguida, apontar pontos de melhoria no nosso sistema processual e ordenamento jurídico, no que diz respeito à prova digital-eletrónica e ao seu lugar no Direito português e à própria adaptação às novas tecnologias da informação como forma de mitigar as dificuldades e desafios impostos pela Era Digital, até porque, como dito por CASTELLS[2], *"(...) a tecnologia é condição necessária mas não suficiente para a emergência de uma nova forma de organização social baseada em redes"*.

O trabalho que me proponho realizar nesta tese será desenvolvido ao longo de três Capítulos.

No Primeiro Capítulo, farei uma breve análise da teoria geral da prova, elencando as suas particularidades, o entendimento doutrinário relativamente à sua conceção metodológica, os princípios que a norteiam e a repartição do ónus da prova.

Neste capítulo serão essenciais as teses de vários autores responsáveis por pensarem o Direito na sua índole civilística[3]. Destacamos capítulo a análise dos princípios que norteiam a prova, recolhendo entendimento doutrinário de MANUEL DE ANDRADE[4] e RUI MOREIRA[5] para conseguirmos elencar um leque de princípios que poderão mais tarde ser transpostos e analisados no caso concreto das provas digitais.

Da mesma forma, no que respeita à prova atípica, na qual muitos poderão considerar que se insere a prova eletrónica-digital, recolheremos três possíveis doutrinas relativamente a esta: (i) uma corrente legalista, defendida por autores como LEBRE DE FREITAS[6], que defendem a inadmissibilidade da prova atípica devido a acreditarem no caráter taxativo da enumeração legal dos meios de prova; (ii) uma corrente analógica, defendida por autores como SAMPAIO E

---

[2] CASTELLS, Manuel, "*A Sociedade em Rede: Do Conhecimento à Acção Política*", 2005, p. 17.

[3] Como o são ALBERTO DOS REIS (*"Código de Processo Civil Anotado, vol. III"*), ISABEL ALEXANDRE (*"Provas Ilícitas em Processo Civil"*), LEBRE DE FREITAS (*"A ação declarativa comum, à luz do Código de Processo Civil de 2013"*), MANUEL DE ANDRADE (*"Noções elementares de processo Civil"*), MENEZES CORDEIRO (*"Tratado de direito civil português, tomo I"*) e REMÉDIO MARQUES (*"A aquisição e a valoração probatória de factos (des)favoráveis ao depoente ou à parte chamada a prestar informações ou esclarecimentos"*). Da mesma forma, as contribuições sobre a metodologia do Direito de CARNELUTTI (*"La prova civile"*), MARINONI ("*Curso de Processo Civil, Processo Cautelar, vol. 4, 3.ª ed. revista e atualizada"*), PERELMAN (*"Retóricas"*), PISANI (*"Lezioni di diritto processuale civile"*) e TARUFFO (*"Funzione della prova: la funzione dimostrativa"*) serão de grande relevância para explanar o pretendido.

[4] ANDRADE, Manuel A. Domingues de, *"Noções elementares de processo Civil"*, Coimbra Editora, Coimbra, 1993.

[5] MOREIRA, Rui, *"Os princípios estruturantes do processo civil português e o projeto de uma nova Reforma do Processo Civil" in "O Novo Processo Civil: contributos da doutrina para a compreensão do novo Código de Processo Civil"*, 2ª Edição, Centro de Estudos Judiciários, 2013.

[6] LEBRE DE FREITAS, José, *"A confissão no direito probatório: um estudo de direito positivo"*, 2ª Edição, Coimbra Editora, Coimbra, 2013.

NORA[7], e que é flexível na sua aceitação de novos meios de prova, via analogia ao meio de prova enunciado pela lei; e, por fim (iii) uma corrente discricionária, partilhada por autores como ISABEL ALEXANDRE[8], que colocam os meios de prova à admissibilidade criteriosa do juiz.

No segundo Capítulo, tentaremos fazer um esclarecimento teórico relativamente à prova digital-eletrónica e à sua definição, características próprias, integração no regime da prova, limitações e meios de obtenção; sendo, de seguida, feita uma análise comparativa relativamente às perceções de vários ordenamentos relativamente a este tipo de prova[9].

Destaque particular neste capítulo virá no que concerne à perspetiva comparada dos vários ordenamentos jurídicos relativamente à prova eletrónica-digital e à forma como esta se insere no seu sistema, sendo que a obra de ILLÁN FERNANDEZ[10] potenciou um vasto leque exemplificativo das realidades processuais e legais de vários países, tanto do sistema de *"Civil Law"*, como de *"Common Law"*, essencial ao elaborar das nossas conclusões para o seguinte projeto.

Por fim, no terceiro e último Capítulo, ligar-se-ão os temas desenvolvidos nos dois primeiros com aquela que é a realidade processual portuguesa, apresentando não só uma proposta de postura a ser adotada relativamente à prova digital-eletrónica na lei processual, mas também uma comparação com a lei penal (que, entretanto, procurou transpor o tema no âmbito do seu processo), bem como várias sugestões de potenciação e desenvolvimento do processo português em si, por recurso às novas tecnologias (Criptografia, Lógica Formal, *Blockchain* e Portal CITIUS), e de acordo com novas regulamentações em vigor (como o é o Regulamento Geral de Proteção de Dados do Parlamento Europeu e do Conselho).

Na doutrina jurídica portuguesa encontraremos uma grande base de apoio em autores como CONDE CORREIA (*"Prova digital: enquadramento legal")*, COSTA ANDRADE (*"Bruscamente no Verão Passado: A Reforma do Código de Processo Penal — Observações críticas sobre uma Lei que podia e devia ter sido diferente")*, DÁ MESQUITA (*"Processo Penal, Prova e Sistema Judiciário")*, FRANCISCO ANDRADE (*"Comunicações eletrónicas e Direitos*

[7] ANTUNES VARELA, João, MIGUEL BEZERRA, José, SAMPAIO E NORA, *"Manual de Processo Civil: De Acordo com o Decreto-lei 242/85"*, 2ª edição, Coimbra Editora, Coimbra, 2006.

[8] ALEXANDRE, Isabel, *"Provas Ilícitas em Processo Civil"*, Almedina, Coimbra, 1998.

[9] Pelas particularidades do tópico, e pela dificuldade de o definir, a doutrina de DIAS RAMOS (""*A Prova Digital em Processo Penal")*, FRANCISCO ANDRADE (*"Comunicações eletrónicas e Direitos Humanos: O perigo do homo connectus")*, e SILVA RODRIGUES (*"Da Prova Penal, Tomo II, Bruscamente, A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal")*; aliada a conceções internacionais, como o são as de EOGHAN CASEY, ILLÁN FERNANDEZ (*"La prueba eletrónica, eficácia y valoración en el processo civil")*, SENG e MASON (*"Electronic Evidence")* serão particularmente importantes no esclarecimento de quaisquer dúvidas que possam persistir relativamente ao aspeto mais teórico da prova eletrónico-digital.

[10] FERNANDÉZ, J. Mª Illán, *"La prueba eletrónica, eficácia y valoración en el processo civil"*, 1ª Edição, Thomson Reuters, 2009

Humanos: O perigo do homo connectus"), GOMES CANOTILHO (*"Fundamentos da Constituição")*, MILITÃO (*"A propósito da prova digital no processo penal")*, SARMENTO E CASTRO (*"40 anos de 'Utilização da Informática' - o artigo 35.º da Constituição da República Portuguesa")* e VITAL MOREIRA (*"Fundamentos da Constituição"*) constituirão uma grande base de apoio na recolha de informação e de considerações relativamente ao funcionamento do processo português e à forma como este interage com as novas tecnologias no desempenho dos seus objetivos e no desenvolvimento das provas. Em simultâneo, no que concerne aos elementos de melhoria e potenciação a serem tomados em conta[11].

Neste capítulo, destacamos a análise desenvolvida em torno do funcionamento da prova digital no âmbito do Processo Penal, sendo que a análise de MILITÃO[12] se afigurará particularmente útil, em conjunto com a tese de CONDE CORREIA[13], para pintar uma ideia de como é que esta realidade foi transposta para uma realidade processual (ainda que sob forma de diploma legal avulso), bem como os problemas criados por este tipo de provas não terem sido inseridos no âmbito do Código Processo Penal em si; o que facilitará a comparação análoga ao Processo Civil, numa perspetiva de se poder propor a inclusão da prova digital-eletrónica no Código de Processo Civil[14].

[11] BETELLI (*"Agent Technology and On-line Data Protection")*, DIAS VENÂNCIO (*"Lei do Cibercrime: Anotada e Comentada")*, LACAMBRA (*"La lógica como posibilidad del pensamento jurídico")*, PUPO CORREIA (*"Assinatura eletrónica e certificação digital"*) e YUVAL HARARI ("21 Lessons for the 21ª Century") apresentam posições que nos permitem perspetivar os desafios e margens de evolução do Direito em conjugação com as novas tecnologias da informação.

[12] MILITÃO, Renato Lopes, *"A propósito da prova digital no processo penal"*.

[13] CONDE CORREIA, João, *"Prova digital: enquadramento legal"* in *"Cibercriminalidade e prova digital: Jurisdição Penal e Processual Penal"*, Centro de Estudos Judiciários, 2018.

[14] A obra de autores como FRANCISCO ANDRADE ((*"Comunicações eletrónicas e Direitos Humanos: O perigo do homo connectus")*, LARENZ (*"Metodologia da Ciência do Direito")*, KNAPP (*"De l'application de la cybernétique au demaine du droite")*, PAULO NOVAIS (*"Conflict and its Different Dimensions")*, PUPO CORREIA (*"Assinatura eletrónica e certificação digital"* in *"Direito da Sociedade da Informação: Volume VI")*, e YUVAL HARARI ("21 Lessons for the 21ª Century") apresentar-nos-á uma perspetiva relativamente aos desafios colocados pela nova Era Digital, seja pelo elencar das novas realidades tecnológicas que marcam os negócios jurídicos (*cloud computing*, domótica, inteligência artificial), seja pelo esclarecimento da forma como as novas tecnologias poderão ser utilizadas em conformidade com os ordenamentos jurídicos para darem valor probatório aos documentos eletrónicos e automatizarem o processo.

Capítulo I – Teoria Geral da Prova

Todo o sistema jurisdicional existe com o intuito básico de resolver da forma mais eficiente possíveis conflitos (na sua índole subjetiva e objetiva[15]) que possam surgir entre entes coletivos e/ou singulares no desenvolvimento das suas atividades pessoais ou profissionais.

O foco deve então passar a dirigir-se à própria prova e à forma como esta se encontra atualmente perspetivada e regulamentada no âmbito do Processo Civil.

Inserida no âmbito da fase da instrução do processo, na qual se desenvolve a designada atividade instrutória (respeitante à indicação dos meios de prova que as partes pretendem usar em juízo) e a atividade probatória (relativa à utilização desses meios e à concreta produção de prova), sendo certo que, nas palavras de Paulo Pimenta, "uma e outra das atividades não correspondem a momentos estanques e fechados"[16].

Existe um consenso geral em como a prova é imprescindível ao Direito, particularmente ao campo do Direito Processual, no qual se torna particularmente preponderante o ónus de demonstrar factos que alegam a existência de um dado direito material ou uma exceção material. Esta demonstração encontra-se inerentemente dependente daquela que é a prova, trazida ao processo pelas partes, bem como produzida oficiosamente ou requerida pelas partes ao tribunal[17].

No âmbito da presente tese, antes de se desenvolverem matérias relativas à prova digital em si, torna-se necessário compreender o que constitui uma prova, e a forma como esta é analisada legal, jurisprudencial e doutrinalmente, nas suas várias conceções e disposições.

---

[15] *"Subjectively, approaches to define conflict involve attempts to explain it analyzing the ways in which parties understand and behave towards each other. On the other hand, the objective aspects used to define are, roughly, those that are widely independent of the parties' perceptions (...)."* – NOVAIS, P., GOMES, M., "*Conflict and its Different Dimensions"*, p.1.

[16] PIMENTA, Paulo, "*Processo Civil Declaratório",* Almedina, 2015, p. 336.

[17] RANGEL, Rui Manuel de Freitas, *O Ónus da Prova no Processo Civil*, 3.ª ed., Almedina, Coimbra, p. 21., vide TARUFFO, Michele, *"Funzione della prova: la funzione dimostrativa", in "*Rivista Trimestrale di Diritto e Procedura Civile, Anno. 51, n.° 3", Giuffrè Editore, Milão , 1997, p. 553 - 574.

1. A prova

Sendo que o presente trabalho diz respeito à prova digital, tornam-se necessárias algumas clarificações conceptuais daquela que é a prova em si, em todas as suas aceções legais, jurisprudenciais e doutrinárias, antes de passarmos às especificidades da prova digital-eletrónica.

1.1. Definição

Definido como *"aquilo que serve para estabelecer uma verdade por verificação ou demonstração"*, o vocábulo *"prova"* deriva do latim *"proba"*, verbo *"probare"*, devendo ocupar uma dimensão fática e uma dimensão jurídica[18].

De facto, e conforme entendido por PISANI[19], além da tradicional ideia de que "a prova é o resultado da atividade lógica do conhecimento", constata-se que o vocábulo assume, naturalmente, diferentes conotações, podendo referir-se (i) aos instrumentos utilizados por magistrados para o conhecimento dos factos que lhe são apresentados; (ii) ao procedimento de formação desses mesmos instrumentos de cognição e à sua respetiva receção pelo juízo; ou, até mesmo (iii) à atividade lógica celebrada pelo juiz para o conhecimento dos factos.

Numa perspetiva doutrinal nacional, ALBERTO DOS REIS entende a prova como *"o conjunto de operações ou atos destinados a formar a convicção do juiz sobre a verdade das afirmações feitas pelas partes"*[20]. Esta postura parece alinhar-se com as ideias internacionais de autores como LESSONA[21] (que entende que "provar" corresponde a *"fazer conhecidos para o juiz os factos controvertidos e duvidosos, e dar-lhe a certeza do seu modo preciso de ser"*) e LIEBMAN (que define "prova" como os *"meios que servem para dar o conhecimento de um facto e, por isso, para fornecer a demonstração e para formar a convicção da verdade de um facto específico"*[22]).

[18] PIMENTA, Paulo, *Processo Civil Declaratório*, Almedina, 2015, p. 336.
[19] PISANI, Andrea Proto, *"Lezioni di diritto processuale civile"*, Napoli: Jovene, 1994, p.446.
[20] REIS, José Alberto dos, "*Código de Processo Civil* Anotado, vol. III", 3° edição, Coimbra Editora, Coimbra, 2012, p. 238.
[21] LESSONA, Carlos, *"Teoria general de la prueba en derecho civil"*, Madrid: Reus, 1928, p.3.
[22] LIEBMAN, Enrico Tullio, *"Manuale di diritto processuale civile – Principi",* v.1, 5ª edição, Milano: Giuffré, 1992, p. 318.

1.2. Objeto

Partindo do que foi estabelecido, parece justo afirmar que a prova não tem como objeto a reconstrução exata dos factos que irão nortear a aplicação da regra jurídica adequada.

A análise do juiz remete-se a analisar as informações fáticas trazidas pelas partes ao processo, o que não significa que a atividade probatória deverá necessariamente recair sobre tudo o que é alegado, mas sim, apenas sobre os factos controvertidos e pertinentes. Aliás, como o indica PERELMAN[23], as provas referem-se sempre a uma dada proposição, a qual não pode ser única e exclusivamente fundamentada num critério metafísico ou intuitivo, sendo que devem ser expressas de forma percetível, para surtirem o efeito desejado.

Seguindo a ótica de pensamento da MANUEL ANDRADE, parece-nos intuitivo responder que o objeto de uma prova se encontra traduzido num estado, num facto, num dado objeto[24], fazendo algum seguimento com a perspetiva de CARNELUTTI, segundo o qual poderia ser qualquer uma dessas coisas, dependente do ponto de vista em consideração[25].

CARNELUTTI entende ainda ser impossível tomar como objeto da prova apenas factos, ou pessoas e coisas, no sentido em que o objeto das provas são *"uma e outra dessas coisas conforme o ponto de vista por que foram consideradas"*.

1.3. Função

Numa aceção jurídica, e bebendo do direito substantivo, uma breve leitura do Código Civil, no seu artigo 341º, permitir-nos-á inferir que *"as provas têm por função a demonstração da realidade dos factos".* Com base neste artigo, é possível entender que a prova funciona como um meio para um fim, neste caso, a demonstração da realidade de um dado facto, numa verdadeira concretização do *"narra mihi factum, dabo tibi ius" ("narra-me os factos, e dar-te-ei o Direito"*).

A principal e imediata relevância desta função, quer para juristas, quer para leigos, surge com a clara questão que se coloca ao juiz, quando este é confrontado com um conjunto de factos que as partes trazem ao processo, sem nunca os ter efetivamente presenciado: como é que os conhece e com que base é que os julga? A prova fornece ao juiz os elementos

[23] PERELMAN, Chaïm, *"Retóricas"*, tradução de Maria Ermantina Galvão G. Pereira, São Paulo: Martins Fontes, 1997, p.164.
[24] ANDRADE, Manuel A. Domingues de, *"Noções elementares de processo Civil"*, Coimbra Editora, Coimbra, 1993, p. 194
[25] CARNELUTTI, Francesco, *"Teoria Geral do Direito"*, tradução de A. Rodrigues Queiró e Artur Anselmo de Castro, Armênio Amado Editor, Coimbra, 1942, p. 493.

necessários para controlar a veracidade desses factos[26], pelo que se apresenta como resposta a este dilema básico.

Sublinhe-se que utilizámos a palavra "controlar" de forma intencional, fruto da diferença clara entre o ramo da ciência jurídica e o ramo das ciências puras/exatas e da natureza das verdades a serem nestas comprovadas. De facto, e longe de procurar uma demonstração lógica e absoluta dos factos, a prova jurídica assume uma natureza altamente probabilística[27], cuja efetividade está dependente, acima de tudo, do grau de convicção que é capaz de exercer sobre o juiz, como inclusive o prescreve o artigo 341º do Código Civil.

Fazendo seguimento a esta importância intuitiva, existe um consenso geral em como a prova é imprescindível ao Direito, particularmente ao campo do Direito Processual, quer numa ótica de concretização jurisdicional daquele que é o direito substantivo[28], quer como forma de canalizar o dinamismo da sucessão dos atos processuais[29] para a criação e desenvolvimento de normas jurídicas.

Inserida no âmbito da fase da instrução do processo, na qual se desenvolve a designada atividade instrutória (respeitante à indicação dos meios de prova que as partes pretendem usar em juízo)[30] e a atividade probatória (relativa à utilização desses meios e à concreta produção de prova), sendo certo que, nas palavras de Paulo Pimenta, *"uma e outra das atividades não correspondem a momentos estanques e fechados"*[31], a prova apresenta-se como elo de ligação entre estes dois momentos na busca pela verdade material.

Seguindo essa lógica, e uma vez que o Direito Processual existe como garante do cumprimento das normas jurídicas materiais e na garantia do direito substantivo, é natural que o ónus de demonstrar factos que alegam a existência de um dado direito material ou uma exceção material se assuma como fulcral a tal objetivo. Esta demonstração[32] encontra-se inerentemente dependente daquela que é a prova, trazida ao processo pelas partes, produzida oficiosamente, ou requerida pelas partes ao tribunal[33].

---

[26] ANDRADE, Manuel A. Domingues de, "*Noções elementares (...)".*, Coimbra Editora, Coimbra, 1993, p.190.
[27] VARELA, Antunes, BEZERRA, J. Miguel e NORA, Sampaio E., *"Manual de processo Civil"*, 2.ª ed. (Reimpressão), Coimbra Editora, Coimbra, 2004, p. 407-408.
[28] FREITAS, José Lebre de, "*Introdução ao Processo Civil - Conceito e Princípios Gerais à Luz do Novo Código"*, 3.ª ed., Coimbra Editora, Coimbra, 2013, p. 13.
[29] VARELA, Antunes, *"Manuel de Andrade e o ensino do processo Civil"*, in Boletim da Faculdade de Direito de Coimbra, Vol.35, Coimbra.
[30] RANGEL, Rui Manuel de Freitas, *O Ónus da Prova no Processo Civil*, 3.ª ed., Almedina, Coimbra, 2006 p.23.
[31] PIMENTA, Paulo, *Processo Civil Declaratório*, Almedina, 2015, p. 336.
[32] TARUFFO, Michele, *"Funzione della prova: la funzione dimostrativa" in "Rivista Trimestrale di Diritto e Procedura Civile, Anno. 51, n.º 3"*, Giuffrè Editore, Milão, 1997, p. 553 - 574.
[33] RANGEL, Rui Manuel de Freitas, "*O Ónus da Prova (...)*" p. 21.

Em suma, o conhecimento relativamente à detenção do direito material, a demonstração dos factos apresentados e a determinação da convicção do julgador estariam inevitavelmente comprometidos, juntamente com o próprio Direito Processual, perante a ausência da figura da prova. Sem as provas, o processo seria inexistente, o que se traduz no facto de que as provas são a base do processo.

1.4. Meio de Prova

Os meios de prova podem ser definidos como sendo *"as diversas modalidades pelas quais a constatação sobre a ocorrência ou inocorrência dos factos chega até ao juiz"*[34], de forma a que se alcance um resultado probatório**.** Exemplos claros de meios de prova são, por exemplo, a prova testemunhal (que resulta num depoimento), a prova pericial (que resulta num relatório pericial) e a prova documental. As decisões dos tribunais partem, conforme dito, de elementos como estes, sendo que a prova é apreciada segundo as regras da experiência e a livre convicção da entidade julgadora competente.

Nesse sentido, não devemos confundir os meios de prova com meios de obtenção de prova, que correspondem aos mecanismos destinados a aceder às fontes de prova e obter as informações necessárias para a formação da convicção do julgador sobre a matéria de facto e, naturalmente, trazê-las ao processo. No âmbito do processo penal temos, por exemplo, os exames, as revistas e buscas, as apreensões e as escutas telefónicas.

1.5. Fonte de Prova

Por fonte da prova entendemos o elemento a partir do qual o juiz chega ao conhecimento de um facto, seja esse elemento uma pessoa (como ocorre no caso da prova testemunhal, na qual um terceiro capaz depõe como testemunha [artigo 495º CPC]) ou uma coisa (como ocorre na prova documental, na qual a fonte da prova é uma coisa, planta, objeto, etc. [artigo 423º e seguintes do CPC]).

Posto isto, o valor da fonte de prova depende dos factos relevantes revelados para o processo. Assim, conforme dito por NGONGO BARNABÉ, *"torna-se necessário que os documentos sejam lidos, que as pessoas sejam ouvidas, que os filmes sejam exibidos, que as*

[34] WAMBIER, Luiz Rodrigues, TALAMINI, Eduardo, *"Curso Avançado de Processo Civil, Teoria Geral do Processo e Processo de Conhecimento, Vol. 1"*, 12.ª ed., Editora Revistas dos Tribunais - RT, São Paulo, 2012, p. 495.

gravações sejam reproduzidas, as coisas sejam inspecionadas, que os factos sejam bem narrados"[35].

1.6. Conteúdo

Por conteúdo da prova, entendemos o resultado probatório conseguido através do uso dos diversos meios de prova dotados de previsão legal, e que partem de uma fonte de prova.

Não se pode negar que a prova será condicionada de acordo com os componentes culturais, políticos, económicos e sociais dos vários sujeitos que envolvem o processo[36], da mesma forma que o julgador será influenciado por essas mesmas realidades, como o indica FOUCAULT[37].

2. Ónus da Prova

Num panorama mais conceitual e geral, e conforme definido por ANTUNES VARELA, por ónus (de prova, de alegação, etc.), entende-se uma *"necessidade de observância de determinado comportamento (...) como pressuposto da obtenção de uma vantagem para o próprio, a qual pode inclusivamente cifrar-se em evitar a perda de um benefício antes adquirido"*.

Torna-se pertinente delinear que "ónus" não se confunde com "dever" (associado a uma norma de conduta, impositiva ou proibitiva) nem com "obrigação" (que surge do não cumprimento de um dever jurídico, ligado a um direito subjetivo de alguém). A figura do ónus tem uma natureza facultativa (ou seja, implica uma vantagem ou desvantagem perante o seu cumprimento ou não cumprimento) nunca traduzida numa sanção coativa (como ocorre no dever) e não pressupõe a existência de um direito subjetivo (como ocorre na obrigação), sendo o onerado quem tem interesse em cumprir ou não o ónus, de acordo com esta lógica de incentivo/peso, definida por MENEZES CORDEIRO como uma situação jurídica passiva[38].

Se as provas têm por função a demonstração da realidade dos factos, torna-se pertinente saber a quem cabe fazer a sua prova, sempre que se alegue um dado direito, sejam

[35] NGONGO BARNABÉ, Augusto, *"Direito Probatório"*, Tese de Mestrado pela Universidade de Coimbra, 2014, p. 20.
[36] MARINONI, Luiz Guilherme e ARENHART, Sérgio Cruz, "Prova e Convicção", 4ª Edição, Thomson Reuters, pp.63-67
[37] FOUCAULT, Michel, *"Vigiar e punir: história da violência nas prisões"*, 32ª Edição, Tradução de Raquel Ramalhete, Petrópolis: Vozes, 1987, p.106.
[38] MENEZES CORDEIRO, *"Tratado de direito civil português, tomo I"*, 3.ª edição, 2005, p. 358

esses factos constitutivos, impeditivos, modificativos ou extintivos do direito invocado. Nisto se insere o ónus probatório.

Orientado no sentido de assegurar uma justa repartição do ónus probatório e de alcançar a verdade material, o critério geral de repartição do ónus da prova, encontra-se consagrado no artigo 342º e seguintes do CC.

Posto isto, torna-se claro, pelo artigo 342º do CC, que ao demandante cabe fazer provas dos factos constitutivos[39] (que levam ao surgimento de um dado direito, como por exemplo, o de propriedade), enquanto que ao demandado cabe a prova dos factos impeditivos[40] (que se opõem a que o direito do autor tenha eficazmente surgido ou que, segundo MANUEL DE ANDRADE, tenha tido o seu nascimento atrasado[41]), modificativos[42] (que alteram o direito do autor validamente constituído[43]) ou extintivos[44] (que determinam a extinção do direito do autor, assumindo que este surgiu validamente).

Estando o autor da ação incumbido de provar os factos constitutivos alegados, sob pena de julgarem contra si e de o processo ser improcedente, há um incentivo para a sua diligência e iniciativa processual[45]. Por sua vez, o autor encontra-se protegido de situações tendencialmente de prova difícil para si nos casos de factos impeditivos, modificativos ou extintivos de diretos, pois o ónus de prova é da contraparte[46], a qual tem de provar a ausência de tais factos, o que por sua vez lhe confere uma oportunidade de defesa contra as alegações contra si feitas.

Entende-se que, em Portugal, o Juiz e o Tribunal não podem encerrar um processo nem deixar de conhecer a questão de mérito perante provas insuficientes ou inconclusivas, alegando *non liquet*[47] e evitando proferir uma decisão de mérito favorável a uma parte[48].

---

[39] Caso de empréstimos, testamentos, entre outros.

[40] Casos de incapacidade, coação, simulação, erro, dolo, condição suspensiva, entre outros.

[41] Com a ressalva de admissão da existência de autênticas exceções ao invés mera negação indireta dos factos constitutivos invocados pelo autor, como por exemplo, o réu afirmar ter recebido como doação o que o autor assevera ter-lhe emprestado. Estaríamos aqui perante uma impugnação, e não perante uma exceção.

[42] Casos da mudança do local de servidão e concentração de objeto da prestação, entre outros.

[43] Há doutrina que não considera os factos modificativos como uma categoria, como é o caso de NUNO PINTO DE OLIVEIRA que, em *"Estudos sobre o não cumprimento das obrigações"*, 2ª edição, Coimbra, Almedina, 2009, p. 116, considera que os factos modificativos são tratados como impeditivos (caso de moratórias a devedores) ou extintivos (caso da concentração de objeto) consoante o sentido da modificação, não devendo por isso ser considerados autónomos.

[44] Casos de condição resolutiva, pagamento, novação, compensação, prescrição, entre outros.

[45] Em *Die Beweislas*t, editada em 1990, p. 2, ROSENBERG demonstra exemplo prático ao enunciar as dúvidas que dominam o magistrado em face de um caso concreto e a sua necessidade de definir as regras que o orientem no julgamento, concluindo que a resposta se encontra nas regras que formam o ónus da prova, pois é na indicação ao juiz do conteúdo da decisão que há de proferir em casos de incerteza da veracidade que residem a essência e o valor destas regras.

[46] VAZ SERRA, em "*Provas: direito probatório material"*, Lisboa, 1962, p. 70, aponta para a necessidade de se atender a um critério de normalidade, considerando não fazer sentido o autor ter de provar a falta do que é "normal", ou seja, das causas que extinguem, modificam ou impedem o direito em causa.

[47] *"Ao 'non liquet' no domínio dos factos, corresponde ou deverá sempre corresponder um 'liquet' jurídico"* - DE CASTRO, Anselmo, *"Lições de processo civil, vol. IV",* Atlântida, Coimbra, 1969,

Tudo o que foi exposto supra torna claro que, no ordenamento jurídico português, a posição das partes no litígio perde relevância perante o direito a ser exercido em juízo, sendo que o foco principal é o de saber a quem os factos aproveitam. Esta valorização da análise dos factos em concreto e em função da relação material em juízo denota uma tendência casuística do nosso Processo Civil, que impede que se considere a existência de factos cuja prova seja fixamente atribuída a dados sujeitos processuais, evidenciando ainda a ligação entre as normas de direito substantivo e o ónus da prova, na medida em que a distribuição do encargo probatório se deverá concretizar por meio da interpretação da lei (note-se, consoante a teoria das normas de ROSENBERG, que considerou o ónus da prova como sendo *"a espinha dorsal do processo"*[49]).

Na linha deste raciocínio, ELISABETH FERNANDES entende que em Portugal, o ónus da prova subjetivo (determinação da parte onerada com a prova) é irrelevante, uma vez que o princípio da aquisição processual determina a atendibilidade de todas as provas produzidas no processo[50]. Desenvolvendo esta questão, LEBRE DE FREITAS mostra-se favorável à designação de "ónus de iniciativa da prova", encarando a figura jurídica como uma conveniente iniciativa com o objetivo de evitar sair prejudicada perante a não consideração do facto não provado na decisão[51][52].

Devido à dificuldade de caracterização, na prática, dos factos como constitutivos, impeditivos, modificativos ou extintivos, a doutrina de ROSENBERG colhe adesão em Portugal, bem como o seu critério de auxílio de qualificação dos factos, segundo o qual as normas jurídicas são compostas por uma previsão e uma estatuição. A estatuição encontra-se dependente da prova dos factos que integram a previsão da norma[53], pelo que o não preenchimento desses pressupostos de previsão implica uma não aplicação da estatuição.

Revela-se aqui uma ligação estreita entre as normas de direito substantivo e o ónus da prova, sendo necessário atentar nestas normas para identificar quem delas beneficia, de acordo com a chamada Teoria das Normas[54]. Se for a quem pretende exercer um direito subjetivo (factos constitutivos), trata-se de norma de base, se for a outro quem obstar ao exercício desse

---

[48] ROSENBERG, "*Die Beweislast*", 1990, p. 14 e ss.; HELLWIG, "*System des Deutschen Zivilprozessrechts*", Lípsia, 1912, p.468.
[49] ROSENBERG, "*Lehrbuch des Deutschen Zivilprozessrechts*", 8ª edição, 1960, p. 559.
[50] FERNANDEZ, Elisabeth, *"A prova difícil ou impossível, Estudos em homenagem ao prof. doutor José Lebre de Freitas"*, 1.ª edição, 2013, pp. 817-823.
[51] LEBRE DE FREITAS, José, "*A ação declarativa comum, à luz do Código de Processo Civil de 2013*", 3ª edição, 2013, p. 211.
[52] LEBRE DE FREITAS, José, "*Introdução ao processo civil, conceitos e princípios gerais à luz do novo código*", 2013, p. 177, nota 60.
[53] (...) ao abordar o silogismo judiciário dizendo que *"[a] aplicação das consequências jurídicas previstas na norma (estatuição) está, pois, dependente da prévia demonstração da ocorrência dos factos descritos hipoteticamente na previsão da norma"* – MARQUES DA SILVA, Germano, "*Curso de Processo Penal: vol. II*". 3.ª edição, Lisboa: Verbo, 1993, pp. 110-135.
[54] LEITÃO, Hélder, "*Da instrução em processo civil das provas*", 3ª edição, 2016, p. 22.

direito, temos contra norma (factos impeditivos, modificativos ou extintivos)[55]. Esta orientação doutrinária encontra-se plasmada no CPC, nomeadamente no seu artigo 414º, que estabelece que *"a dúvida sobre a realidade de um facto e sobre a repartição do ónus da prova resolve-se contra a parte a quem o facto aproveita"*.

Assim, deve-se ter em conta a norma de direito substantivo que se pretende aplicar, bem como a posição das partes em juízo em relação a essa norma, de acordo com o efeito jurídico pretendido por cada parte. Convém ressalvar que nada disto impede que o legislador possa prever diferentes factos para uma estatuição.[56]

2.1 Inversão do Ónus da Prova

Motivado por uma necessidade de conferir equilíbrio ao processo em situações de proximidade probatória altamente desfavorável a uma das partes e de alcançar a verdade material e a celeridade processual, o conjunto de casos de inversão do ónus da prova é cada vez mais encarado como um grupo que visa alterar a distribuição do ónus probatório em casos cujo desfecho se aparenta predestinado, de acordo com a regra geral[57].

A inversão do ónus da prova encontra os seus fundamentos elencados no artigo 344º do Código Civil, verificando-se aquando de convenção celebrada entre as partes, por via de presunções criadas pela lei, pela libertação do demandado do ónus da prova relativamente a um facto ou quando a parte contrária tiver culposamente impossibilitado a prova a realizar pela parte onerada, relativamente a dado facto.

De forma sucinta, a *ratio legis* que justifica a inversão do ónus da prova diz respeito a questões de ordem particular (tutelando dadas situações subjetivas) e em razões de ordem pública. Conclui-se assim que se visa um processo equitativo em que as partes possam fazer valer os seus direitos em juízo (ordem pública) e onde a parte onerada não se veja impossibilitada de provar a sua pretensão por facto não imputável (ordem particular).

Esta tutela das "partes débeis" da relação jurídica ramifica-se num panorama tanto objetivo como subjetivo, podendo justificar o *favor laboratoris* (inversão do ónus da prova em

[55] ROSENBERG, "*Die beweislast"*, editada em 1990.
[56] DE CASTRO, Anselmo, *"Lições de processo civil, vol. IV",* Atlântida, Coimbra, 1969, pp. 127-128.
[57] CENDON, Paolo, ZIVIL, Patricia, *"L' inversione dell'onere della prova nel diritto civile, Rivista trimestrale di diritto e procedura civile"*, Milano, a.46n.3, 1992, pp. 757-796.

favor do trabalhador) tanto a nível de debilidade subjetiva (no que respeita à proteção do lesado numa ação de responsabilidade civil), como a nível de debilidade objetiva.

Há grande plausibilidade em acreditar no risco do incentivo configurado pela transferência para a parte contrária da prova e das consequências da falta da prova de um facto e as consequências jurídicas do artigo 414.º do CPC[58]. Surge o problema de a parte onerada focar a sua atenção em provar a sua dificuldade probatória ao invés de se esforçar para produzir prova, acabando por ter o efeito paradoxal de potenciar as suas debilidades probatórias[59].

3. Produção da Prova

No geral, a prova é produzida perante o tribunal, na fase de instrução do processo[60], nos trâmites previstos no artigo 410º do Código de Processo Civil, que identifica o objeto da instrução como sendo *"os temas da prova enunciados ou, quando não tenha de haver lugar a esta enunciação, os factos necessitados de prova"*.

Exceção surge nos termos do artigo 419º do Código de Processo Civil, que encontra a sua base em situações em que haja *um "justo receio de vir a tornar-se impossível ou muito difícil o depoimento de certas pessoas ou a verificação de certos factos por meio de perícia ou inspeção"*, e nas quais o depoimento, a perícia ou a inspeção se poderão realizar antecipadamente (inclusive antes de ser proposta a ação), tratando-se assim de uma produção antecipada da prova.

O racional por trás desta figura jurídica é explicitado em doutrina estrangeira, que estabelece que a produção antecipada de provas se prende sempre numa ótica de assegurar a viabilidade da produção da prova na ação futura[61].

---

[58] *"A dúvida sobre a realidade de um facto e sobre a repartição do ónus da prova resolve-se contra a parte a quem o facto aproveita"*.

[59] BEIRÃO, Joana Maria, "*Da Distribuição do Ónus da Prova no Direito Processual Civil Português – Contributo para o Estudo da Possibilidade de Flexibilização através de uma Distribuição Dinâmica"*, Dissertação de Mestrado Profissionalizante Mestrado em Ciências Jurídico-Forenses pela Faculdade de Direito da Universidade de Lisboa, 2017.

[60] MACHADO, Costa, "*Código de Processo Civil Interpretado"*, 6.ª edição, Editora Manole, Barueri -São Paulo, 2007, pp. 353-354

[61] MARINONI, Luiz Guilherme e ARENHART, Sérgio Cruz, "*Curso de Processo Civil, Processo Cautelar, vol. 4, 3.ª ed. revista e atualizada"*, Editora Revista dos Tribunais, São Paulo, 2011, pp. 92-93.

4. Classificações Metodológicas da prova

Para sermos capazes de compreender como funciona o entendimento da prova digital em Portugal e a forma como esta é tratada, torna-se necessário compreender como é que as provas, em geral, estão organizadas e classificadas em Portugal, de forma a conseguirmos tirar algumas conclusões.

Se as provas se dividem em classificações legais (previstas na letra da lei e, portanto, devidamente explicitadas), será talvez mais pertinente dar um enfoque doutrinário às classificações metodológicas da prova.

Com base nisto, neste ponto cabe-nos fazer uma brevíssima explicitação da classificação que as provas podem obter, de acordo com o ponto de vista em que são analisadas. Mais tarde, nomeadamente no que diz respeito ao entendimento do nosso sistema jurídico relativamente à prova digital e à ausência de regime que nela existe, alguns conceitos aqui explanados serão de grande relevância, em particular, a noção de provas atípicas e provas indiretas, nas quais a prova digital facilmente se integrará.

4.1. Prova pré-constituída e prova constituenda

A principal distinção entre estes dois tipos de prova diz respeito à sua relação com o processo e à tempestividade do seu surgimento, bem como ao momento da sua inclusão no processo.

A prova pré-constituída caracteriza-se por surgir de forma independente ao litígio, em procedimentos extra-processuais, uma vez que não se encontra ligada ao processo para o qual releva, sendo-lhe anterior. Apenas passa a fazer parte do processo quando trazida por alguma das partes. Exemplo claro de uma prova pré-constituída é um qualquer documento apresentado por uma das partes.

Por sua vez, a prova *constituenda* encontra-se dependente do processo e do litígio, sendo produzida no âmbito dos mesmos, em simultâneo com estes e recolhida no seu decurso. Por serem produzidas no decurso do próprio processo, implicam atividade processual das partes e do juiz; bem como um certo tempo para serem produzidas em contraditório. Exemplos claros

de prova *constituenda,* produzidos e formados no decurso do processo, são por exemplo a prova testemunhal, a pericial, entre outras.

4.2. Prova pessoal e prova real

Se a prova recai sobre um *"elemento utilizado para criar a convicção do julgador sobre determinado facto"*[62], então a distinção entre prova pessoal e prova real diz respeito à natureza (humana ou não humana) desse mesmo elemento, e à sua influência na tomada de decisão do juiz. De forma resumida, as provas pessoais são aquelas relativamente às quais o convencimento parte da atuação de um sujeito, como é o caso das provas testemunhais e das confissões; enquanto que as provas reais partem das coisas, como o são os documentos.

A prova pessoal é uma fonte de prova constituída pela parte e pela testemunha, enquanto detentores de conhecimentos de relevo para o desfecho do litígio. É necessário confrontar os factos articulados com o conhecimento das partes e testemunhas como forma de os verificar, sendo que não se pode descurar de que a parte ou o seu representante legal e a testemunha ocupam posições diferentes no processo e constituem fontes de prova pessoal igualmente distintas.

Já a prova real é constituída por coisas, portadoras de indícios naturais do facto relevante, conforme descreve LEBRE DE FREITAS[63] (impressões digitais, por exemplo), apurando-se a descoberta da verdade através delas.

4.3. Prova direta e prova indireta

No que concerne a relação entre o sujeito e o objeto, torna-se relevante analisar o nível de interferência entre o juiz e o facto a apurar, apesar de, conforme dito por CARNELUTTI[64], em qualquer caso é fulcral que o juiz recorra ao seu raciocínio, pois este tem de concluir pela existência ou não do facto a apurar.

Assim, a classificação da prova como sendo "direta" ou "indireta" diz respeito à capacidade do meio processual em introduzir os factos no processo e à relação entre o órgão

---

[62] ANTUNES VARELA, João, MIGUEL BEZERRA, José, SAMPAIO E NORA, *"Manual de Processo Civil: De Acordo com o Decreto-lei 242/85"*, 2ª edição, Coimbra Editora, Coimbra, 2006, p. 442.

[63] LEBRE DE FREITAS, José, *"A ação Declarativa Comum - À luz do Código de Processo Civil de 2013"*, 3.ª ed., Coimbra Editora, Coimbra, 2013, pp. 201-202

[64] CARNELUTTI, Francesco, *"Sistema di diritto processuale"*, vol. I, p. 719.

jurisdicional e a *thema probandi* (todo o facto que carece de demonstração para constituir pressuposto de decisão), o objeto da prova e os factos a serem provados. Nesse sentido, CARNELUTTI[65] afirma que a diferença entre os dois tipos de prova se encontra na coincidência ou na divergência do facto a provar (objeto da prova) e do facto apreendido pelo juiz (objeto da perceção), sendo que para este autor, na prova indireta existe uma separação entre o objeto da prova e o da perceção judicial.

Partindo do pressuposto de que os factos não podem ser conhecidos senão por meio do raciocínio e da aplicação da lógica por parte do órgão jurisdicional, BENTHAM concebeu a prova direta como sendo aquela que se relaciona imediatamente com o facto principal, sendo que a prova indireta diria respeito a um facto que, ainda que não o principal, conduziria à demonstração do mesmo[66]. CABANÃS GARCIA[67], por sua vez, entende prova direta como aquela mediante a qual o órgão jurisdicional apreende a realidade dos factos em que escolhe acreditar; e prova indireta quando se realiza por meio de um facto diverso do facto principal, sendo representado por meio de uma dedução.

Numa perspetiva nacional, na aceção de ALBERTO DOS REIS[68], por prova direta entende-se aquela na qual nada se interpõe entre juiz e o facto a apurar, havendo um contacto direto do julgador com o objeto da prova. Exemplo disto é o caso da inspeção judicial (artigos 490.º a 494.º), onde o juiz recorre à sua própria perceção.

Por outro lado, está-se perante uma prova indireta há intervenção de dada coisa ou pessoa entre o juiz, influenciando a perceção do julgador e tornando-a dependente de outros fatores. Isto implica uma utilização de outros instrumentos, desde o raciocínio e regras de experiência, até elementos documentos (artigos 423.º e ss.), prova pericial (artigos 467.º e ss.), e prova testemunhal (artigo 495.º e ss.).

Com todas estas considerações, parece ser relevante separar o facto a ser provado, o meio de prova que o elucida e a perceção judicial que os engloba; isto porque a prova nem sempre possibilita entender a natureza dos factos (se são diretos[69] ou indiretos[70]), uma vez que é perfeitamente possível o juiz apreender factos diretos por meio de provas indiretas.

---

[65] CARNELUTTI, Francesco, *"La prova civile"*, 1992, p.54 e ss.
[66] BENTHAM, J., *"Tratado de las pruebas Judiciales",* t. I, Buenos Aires 1959, p.31.
[67] CABAÑAS GARCIA, J.C., *"La valoración de las pruebas y su control en el processo civil"*, ed. Trivium, Madrid 1992, p.27.
[68] REIS, José Alberto dos, "Código de Processo, *Código de Processo Civil Anotado*, vol. III", 3.ª ed., Coimbra Editora, Coimbra, 2012, pp. 241-242.
[69] Aqueles que devem ser afirmados na petição inicial e na contestação, visando demonstrar a verdade.

4.3.1. Prova representativa e prova indiciária

Dentro do âmbito das provas indiretas, pode-se ainda apontar duas subcategorias[71] da mesma, as chamadas prova representativa e prova indiciária, distintas, contudo, conjugáveis nos seus elementos.

As fontes de prova representativa correspondem a uma dedução do juiz sobre a realidade do facto a que se reporta, estando tal facto registado, representado ou reproduzido por meio de uma representação da realidade (por exemplo, um registo cinematográfico ou fotográfico[72]), e que é passível de conhecimento através da análise do seu conteúdo, incidindo assim não sobre o facto a provar, mas sim sobre o facto que o representa

No âmbito do processo civil, a prova indiciária traduz-se numa uma probabilidade séria da existência do direito, relevando aqui indícios (que, por necessitarem de serem elucidados por meios de prova, devem ser considerados equiparáveis ao facto direto, servindo como elemento para formação de juízo) que permitem elaborar uma presunção relativa à ocorrência de um facto, por meio de presunções lógicas feitas pelo juiz[73].

4.4. Prova Atípica

Por prova atípica perspetivamos aquela prova cujos meios de obtenção não encontram expressa previsão legal na lei enquanto tal[74], sendo assim esta prova alcançada por recurso a procedimentos probatórios anómalos (o depoimento de parte não precedido de juramento ou das advertências respeitantes às consequências da falsidade) ou, na aceção de REMÉDIO MARQUES[75], num plano empírico, por meio de uma aquisição em modalidades lícitas, mas desprovida dos habituais pressupostos legais para obtenção de elementos probatórios (como é o caso dos escritos de terceiro que não se formam de acordo com os critérios legais formais de admissão e produção da prova testemunhal, tal como acontece com as perícias extrajudiciais).

Relativamente à admissibilidade das provas atípicas, não existe um claro entendimento doutrinal nos diversos ordenamentos jurídicos.

---

[70] Incapazes de demonstrar diretamente a verdade das afirmações de factos, embora auxiliem na convicção do julgador.
[71] MANNARINO, Nicola, *"La Prova Nel processo"*, CEDAM, Padova, 2007, pp. 93-97.x
[72] LEBRE DE FREITAS, José, *"A ação Declarativa (...)"*, 3.ª ed., Coimbra Editora, Coimbra, 2013, p. 202.
[73] Neste sentido, será pertinente analisar a letra do artigo 351° do Código Civil, referente às presunções judiciais, a serem admitidas apenas *"nos casos e termos em que é admitida a prova testemunhal"*.
[74] ALEXANDRE, Isabel, *"Provas Ilícitas em Processo Civil"*, Almedina, Coimbra, 1998, p. 34 e ss.
[75] REMÉDIO MARQUES, João Paulo Fernandes, *"A aquisição e a valoração probatória de factos (des)favoráveis ao depoente ou à parte chamada a prestar informações ou esclarecimentos"* in "*Revista Julgar n° 16"*, Coimbra Editora, Coimbra, 2012, p. 141.

Por exemplo, a doutrina espanhola[76], no que concerne à possibilidade de admissão de meios de prova não previstos expressamente para o processo, opta, na sua maioria, por seguir o princípio da legalidade, considerando que o artigo 299.1 da *Ley de Enjuciamento Civil* espanhola é taxativo e limitador relativamente aos meios de prova passíveis de serem apresentados em juízo.

Já a doutrina italiana apresenta-se geralmente a favor das provas atípicas e da sua admissão no âmbito do processo civil, sendo que CAVALLONE[77] rejeita a existência de um elenco taxativo de provas, fruto da ausência de uma homogeneidade lógica dos elementos dos meios de prova do código civil italiano. Nessa senda, TARUFFO[78] considera que a admissibilidade da prova atípica se encontra dependente da sua relevância processual, entendendo esta relevância como característica constitutiva da prova.

No que concerne ao ordenamento jurídico português, e não obstante a tendência de aproximação dos pressupostos da doutrina italiana (até porque o catálogo do artigo 349º e seguintes do Código Civil, referentes aos meios de prova, não estabelece uma homogeneidade lógica nos elementos que o compõem[79]) não há uma postura consensual, particularmente tomando em conta o texto do artigo 345º nº2 do Código Civil, que afirma que *"é nula (...) a convenção que excluir algum meio legal de prova ou admitir um meio de prova diverso dos legais"*.

Nessa senda, encontramos três posições doutrinárias em vigor em Portugal, no que respeita à prova atípica. Encontramos, assim, (i) uma corrente legalista, defendida por autores como LEBRE DE FREITAS[80], que defendem a inadmissibilidade da prova atípica devido a acreditarem no caráter taxativo da enumeração legal dos meios de prova; (ii) uma corrente analógica, defendida por autores como ANTUNES VARELA, J.M. BEZERRA e SAMPAIO E NORA[81], e que é flexível na sua aceitação de novos meios de prova, via analogia ao meio de prova enunciado pela lei; e, por fim (iii) uma corrente discricionária, partilhada por autores como ISABEL ALEXANDRE[82], que colocam os meios de prova à admissibilidade do juiz, o que implica

[76] AROCA, Juan Montero, *"La Prueba en el Proceso Civil"*, S.L. Civitas Ediciones, Madrid, 2005, p. 149.
[77] CAVALLONE, Bruno, *"Il giudice e la prova nel processo civile" in "Processo e Giudizio, Vol. III"*, CEDAM, Padova, 1991, pp. 692-693.
[78] TARUFFO, Michele, *"La prova dei fatti giuridici: nozioni generali"*, Giuffrè, Itália, 1992, p. 364.
[79] REMÉDIO MARQUES, João Paulo Fernandes, *"A aquisição e a valoração probatória (...)"* in "*Revista Julgar nº 16"*, Coimbra Editora, Coimbra, 2012, p. 142-143.
[80] LEBRE DE FREITAS, José, *"A confissão no direito probatório: um estudo de direito positivo"*, 2ª Edição, Coimbra Editora, Coimbra, 2013, p. 293.
[81] ANTUNES VARELA, João, MIGUEL BEZERRA, José, SAMPAIO E NORA, *"Manual de Processo Civil: De Acordo com o Decreto-lei 242/85"*, 2ª edição, Coimbra Editora, Coimbra, 2006, p. 469.
[82] ALEXANDRE, Isabel, *"Provas Ilícitas (...)"*, Almedina, Coimbra, 1998, p. 46.

uma admissão restritiva das provas análogas, na qual o elenco dos meios de prova do artigo 345º do Código Civil poderá ser reduzido ou complementado com outros meios de prova situados fora do CC.

Parece-nos razoável concordar que a prova atípica não deve ser considerada inadmissível meramente com base na ausência de uma expressa previsão legal, sendo que as orientações de TARUFFO, motivadas por uma ideia de economia processual, se alinham com a tese discricionária de ISABEL ALEXANDRE, que pela sua dimensão casuística, parece ser um bom meio termo entre o legalismo restritivo e a analogia desregrada.

4.4.1. Prova Atípica e Prova Ilícita

Uma pequena ressalva deve ser feita da distinção entre prova atípica e prova ilícita, cabendo-nos o dever de indicar que a prova atípica, ainda que não prevista na lei, não constitui uma violação dos seus limites. O mesmo não acontece na prova ilícita[83].

Assim, é preciso uma análise cuidada, visto que a impossibilidade de classificar uma prova como típica não a torna atípica *per si*. Pelo contrário, a falta de tipicidade de uma prova ilícita advém da sua violação do direito material, pelo que a rejeição destas provas como modalidade das provas atípicas é um evitar de um encobrimento da transgressão de regras materiais.

5. Prova e Certeza

A verdade é essencial para o processo e, mesmo não constituindo um fim em si mesmo, TARUFFO entende a sua procura como condição indispensável para a efetividade da justiça estatal[84]. Não obstante, deve-se frisar que o conceito de verdade não é sinónimo do conceito de certeza.

[83] Nesse sentido, deve ser feita uma leitura atenta do artigo 32º nº8 da Constituição da República Portuguesa, que menciona que *"são nulas todas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações"*, apesar de a ausência de uma norma que vede a utilização das provas ilícitas no processo civil provocar divergências no que concerne à sua admissão no Processo Civil, seja a nível doutrinal, seja a nível jurisprudencial.
[84] TARUFFO, Michele, *"A Prova"*, Revista de Processo nº 16: Revista dos Tribunais, São Paulo, p. 168.

Derivada do verbo *cernere*, que significa *"discernir"*, a certeza corresponde à adesão firme a algo que seja enunciado, definido, apontado, demonstrado. Ora, num sistema como o nosso, alicerçado no *judici fit probatio*, ou seja, no juiz enquanto destinatário da prova, a relação entre prova e certeza assume um destaque inegável, visto que é o juiz quem vai conhecer dos factos e das provas que definirão a sua convicção quanto à veracidade do caso e dos elementos que o compõem. Apenas com base neste exercício mental é que este irá pronunciar-se[85]. Com efeito, CARNELUTTI afirma que *"as provas são (...) um equivalente sensível do facto para uma avaliação, no sentido de que proporcionam ao avaliador uma perceção mediante a qual lhe é possível adquirir o conhecimento desse facto"*[86].

Assim se depreende que a investigação processual é fruto dos factos afirmados em juízo, visando reconstituir e demonstrar a realidade do que é alegado, sendo a aplicação das normas jurídicas a comprovação da verificação das hipóteses dos factos previstos. Isto explica o motivo pelo qual DESCARTES entendia a certeza como critério da verdade[87] e pelo que TEIXEIRA DE SOUSA define a prova como uma atividade tendente à formação da convicção dos tribunais sobre a realidade dos factos controvertidos[88].

De facto, como o plasma o artigo 341º do Código Civil, *"as provas têm por função a demonstração da realidade dos factos"*, pelo que demonstrar a realidade dos factos é exercer juízo de certeza sobre os mesmos, distanciando o conceito de prova daquilo que constitui a matéria de direito, e aproximando-se do que compõe a matéria de facto.

Ora, esta definição implica compreender o que se entende por "demonstrar", de forma a ser possível entender e interpretar o artigo e compreender o conceito de prova. Demonstrar corresponde a explicitar, via sinais exteriores, de um acontecimento ou de um facto passado, visto que as provas têm o intuito de reconstituir eventos pretéritos.

MANUEL DE ANDRADE entende a prova não como uma certeza lógica nem absoluta, mas sim como o grau de probabilidade dos factos apresentados com base posições assumidas pelos sujeitos processuais[89], implicando um âmbito intelectual em conjunto com o alcance processual do conceito, que humaniza o exercício do poder jurídico.

---

[85] CASTRO MENDES, João de, "*Do conceito de Prova"*, Lisboa: Ática, 1961, p. 178.
[86] CARNELUTTI, Francesco, *"Teoria Geral do Direito"*, tradução de A. Rodrigues Queiró e Artur Anselmo de Castro, Armênio Amado Editor, Coimbra, 1942, pp. 491-492.
[87] LALANDE, André, *"Vocabulário técnico e crítico da filosofia"*, 3ª edição, São Paulo: Martins Fontes, 1999, p. 149
[88] TEIXEIRA DE SOUSA, Miguel, *"As partes, o objecto e a Prova em processo declarativo"*, Lex-Edições Jurídicas, 1995, p.194
[89] ANDRADE, Manuel Domingues de, *"Noções elementares de Processo Civil"*, Coimbra Editora, Coimbra, 1993, p.191

Torna-se evidente a única meta possível é a da presunção da verdade relativa. Com efeito, cabe-nos destacar a prova *prima facie*, que não produz o mesmo grau de probabilidade para a convicção do juiz, mas que, em todo o caso, é bastante para inverter o ónus da prova, ou até implicar apresentação de uma contraprova pela contraparte.

Esta noção de que o julgador recorre ao facto conhecido pelas máximas de experiência como ponto de partida[90] repercute-se, desta forma na credibilização de uma afirmação fática, tendo a parte contrária de provar a sua veracidade[91], o que levou muitos autores a considerarem uma inversão do ónus da prova, com a exceção notória de VAZ SERRA[92].

Deve-se olhar para a obra de ALBERTO DOS REIS, que hierarquiza os tipos de prova de acordo com a sua eficácia, ou seja, o grau de certeza que estas conferem, nomeadamente, (i) a *"prova suficiente"*, cimeira, funcionando como presunção natural e responsável pela suscetibilidade de produzir a plena convicção do juiz, (ii) a *"prova prima facie"*, baseada em acontecimentos ditos "habituais" e que não produz o mesmo grau de probabilidade para a convicção do juiz, mas que, em todo o caso, é bastante para inverter o ónus da prova, ou até implicar apresentação de uma contraprova pela contraparte, e por último, (iii) encontramos a *"simples justificação"* que se destina a apenas produzir um *"mero juízo de verosimilhança"*[93].

6. Princípios do Processo Civil

Relativamente aos princípios jurídicos que gerem o Processo Civil, desde cedo se encontra uma forte disparidade entre as doutrinas processuais, no que diz respeito aos processos a serem considerados parte do ordenamento jurídico processual, fazendo-se, em primeira instância, uma divisão entre uma postura jusnaturalista[94] e juspositivista[95].

Tomando em conta o nosso ordenamento jurídico, e da mesma forma que ILLÁN FERNÁNDEZ[96] o fez relativamente ao ordenamento jurídico espanhol, cremos que não há lugar

[90] GASTAL, Alexandre Fernandes, *"A Suficiência do Juízo de verosimilhança para a decisão das questões fáticas"*, Universidade do Rio Grande do Sul, Porto Alegre, 2006, p. 109.
[91] RANGEL, Rui Manuel, *"O ónus da prova no Processo Civil"*, 3ª edição, Almedina, Coimbra 2006, pp. 255-256
[92] VAZ DA SERRA, Adriano, *"Provas: Direito Probatório Material"*, Lisboa, 1962, pp.98-99
[93] ALBERTO DOS REIS, José , *"Código de Processo Civil* Anotado, vol. III *"*, 3.ª ed., Coimbra Editora, Coimbra, 2012, p. 246.
[94] Esta doutrina considera que os princípios do Direito correspondem a normas do Direito Natural que não dispõem de uma formulação positiva, nem gozam do reconhecimento do Estado.
[95] Que entende que os princípios correspondem a normas derivadas de um processo de abstração normativa, em que este ato de indução permite uma integração destes princípios no Direito, via analogia.
[96] FERNANDÉZ, J. Mª Illán, *"La prueba eletrónica, eficácia y valoración en el processo civil"*, 1ª Edição, Thomson Reuters, 2009, pp.305-306.

para a doutrina jusnaturalista, face a um sistema normativo como o ordenamento jurídico português, claramente codificado, inclusive relativamente aos princípios.

Assim, parece razoável seguir a ótica da doutrina positivista, que pode ser decomposta em princípios gerais do Direito e em princípios processuais.

Os princípios gerais do Direito são, *prima facie*, os critérios ou valores que informam o Direito presente em leis e costumes, nos quais encontramos os valores e fundamentos das normas e do sistema jurídico, servindo, assim, como forma de colmatação de lacunas ou de casos não previstos normativamente.

Por sua vez, os princípios processuais correspondem a nada mais que normas práticas que dão resposta a diretrizes e orientações do legislador para, conforme EISNER[97] o observou, ordenar o processo e a alcançar os objetivos por si delineados.

Não podemos, contudo, cair no erro de acreditar que existe um *numerus clausus* de princípios de Direito, uma vez que, a partir do momento em que estes se encontram interligados ao sistema jurídico e à sua evolução, estes vivem num estado de constante mutação, surgindo constantemente novos princípios e havendo diferentes valorações aos olhos das várias doutrinas. A *analogia iuris*, baseada na interpretação e elaboração de juízos lógicos das normas, assim o implica.

Na perspetiva de CASTRO MENDES[98], seriam elencáveis cinco princípios estruturantes e incontornáveis ao processo civil português; nomeadamente, o dispositivo, o contraditório, a legalidade, a tutela provisória da aparência e a submissão aos limites substantivos.

Por sua vez, MANUEL DE ANDRADE[99] valoriza outro leque, marcadamente distinto, sob o elenco da autorresponsabilidade das partes, da igualdade das partes, da preclusão, da livre apreciação das provas, da aquisição processual, imediação, concentração, oralidade e identidade do juiz, economia processual, celeridade processual, salvaguarda dos interesses da parte perante a uma inevitável demora no processo.

---

[97] EISNER, Isidoro, *"La prueba en el proceso civil"*, Abeledo-Perrot, Buenos Aires, 1964.
[98] CASTRO MENDES, Luís Filipe, *"5 Direito Processual Civil"*, I Vol, AAFDL, pp. 181-228.
[99] ANDRADE, Manuel de, *"Noções elementares de Processo Civil"*, Coimbra Editora, 1979, pp. 373-393.

Assim, para efeitos deste estudo, e seguindo a estratégia de organização de RUI MOREIRA[100], procederemos a um desenvolvimento de um conjunto de princípios que considero pertinentes para a temática a ser abordada neste projeto.

6.1. Princípio da Legalidade

O princípio da legalidade, no âmbito do processo civil, manifesta-se sob a forma legalidade das formas processuais e da legalidade do conteúdo da decisão[101].

Exemplo deste princípio encontra-se no artigo 137º do CPC, relativamente à forma dos atos processuais, que devem ter a *"forma que, nos termos mais simples, melhor corresponda ao fim que visam atingir"*, podendo inclusive *"obedecer a modelos aprovados pela entidade competente, só podendo, no entanto, ser considerados obrigatórios, salvo disposição especial, os modelos relativos a atos da secretaria"*.

A dimensão deste princípio quanto ao conteúdo da decisão respeitava à obrigação de julgamento por aplicação da lei aos factos, princípio este com condicionantes, desde logo as resultantes do princípio do dispositivo (ver ponto 6.4).

6.2. Princípio da Livre Apreciação das Provas

O princípio da livre apreciação das provas é um princípio estruturante no tema da prova, ligando-se ao seu valor e à sua eficácia.

Por "*livre apreciação das provas"*, entende-se que a prova é apreciada livremente pelo julgador, em perfeita conformidade com as regras de experiência e as leis que regulam a atividade mental, sem obedecer a uma tabela ditada externamente[102]. Na perspetiva de WALTER, entende-se que o juiz pode valorar a prova de acordo com a sua experiência[103].

O CPC confirma esta posição no seu artigo 607º nº5, ao mencionar que *"o juiz aprecia livremente as provas segundo a sua prudente convicção acerca de cada facto"*.

---

[100] MOREIRA, Rui, *"Os princípios estruturantes do processo civil português e o projeto de uma nova Reforma do Processo Civil" in "O Novo Processo Civil: contributos da doutrina para a compreensão do novo Código de Processo Civil"*, 2ª Edição, Centro de Estudos Judiciários, 2013, pp. 59-85.

[101] MOREIRA, Rui, *"Os princípios estruturantes do processo civil português e o projeto de uma nova Reforma do Processo Civil", in O Novo Processo Civil: contributos da doutrina para a compreensão do novo Código de Processo Civil"*, 2ª Edição, Centro de Estudos Judiciários, 2013, p. 59.

[102] REIS, José Alberto dos, *"Código de Processo..."* op.cit, p. 245.

[103] WALTER, Gerhard, *"Freie Beweiswürdigung"*, 1979, p. 285.

6.3. Princípio da Aquisição Processual

Previsto no artigo 413º do CPC, o princípio da aquisição processual indica que, independentemente de emanarem (ou não) da parte sujeita ao ónus subjetivo da prova, o tribunal deve tomar em consideração todas as provas produzidas, tenham ou não emanado da parte que deva produzi-las.

O principal ónus a considerar neste princípio é o ónus objetivo, que aponta para quais os factos que devem ser provados para que a decisão apresente determinado conteúdo.

ALBERTO DOS REIS considera fulcral "que os factos relevantes estejam apurados", sendo que todas as provas produzidas, independentemente da sua origem (documentos, fotografias, etc.), servem de base para que o julgador possa proferir a decisão de mérito da causa.

6.4. Princípio do Dispositivo

O princípio do dispositivo é aquele que se afirma por oposição ao princípio do inquisitório, sendo as suas principais manifestações detetáveis no facto de que (i) são as partes quem determina o pedido de impulso inicial do processo, como nos indica o artigo 3º do CPC; (ii) as partes são quem detém a disponibilidade do objeto do processo e, também (iii) as partes são quem tem a disponibilidade do termo do processo, podendo prevenir a decisão por compromisso arbitral, desistência, confissão ou transação.

A causa de pedir invocada condiciona o desenvolvimento da instância, sendo limitadas as situações da sua alteração ou ampliação, seja por acordo (artigo 264º do CPC) ou mesmo com a ausência do mesmo (artigo 265º do CPC).

A ausência de uma causa de pedir determina a ineptidão da petição inicial, como nos indica o artigo 193º nº2 a) do CPC.

6.5. Princípio do Inquisitório

Há doutrinas que entendem o princípio do inquisitório como sendo um poder discricionário do juiz, atribuindo-lhe um critério de exercício ou não exercício, em contrapartida a uma noção de "poder absoluto".

Por sua vez, no direito anglo-saxónico, em particular nos Estados Unidos da América, marcado por um *adversary system*, a instrução probatória continua a depender em grande parte da iniciativa das partes (nomeadamente, dos advogados), anulando o princípio do inquisitório, visto que juiz é um mero árbitro passivo no processo. Tópico importante no ordenamento americano é o procedimento de *discovery*[104], com base no qual os advogados podem procurar fontes de prova fora do âmbito judicial (p.e, sujeitar a contraparte e eventuais testemunhas a interrogatório sob juramento, sem a presença do juiz).

O princípio do inquisitório visa saber se a imparcialidade do juiz é, ou não, colocada em causa com o seu exercício. Esta imparcialidade do juiz não deve ser considerada como sendo violada no momento em que este exerce o seu poder instrutório dentro do processo, pois tal exercício de poder não implica um conhecimento de qual das partes será beneficiada. Nesse sentido, neste estudo seguiremos as posições doutrinais que defendem que o juiz deve, nesta sede, atuar com iluminada e cautelar parcimónia.

O princípio do inquisitório tem grande relevo no processo civil português, visto que, em conjunto com o princípio do dispositivo[105], configura um sistema processual híbrido, que se coaduna em torno de ambos os princípios.

É necessária uma leitura do Código de Processo Civil, nomeadamente nos seus artigos 436.º, 452.º, 490.º n.º 1, 511.º, n.º 4, 526.º, n.º 1 e 601.º, n.º 1, já que estes, em bom rigor, concretizam a força do princípio.

A letra da lei clarifica que *"incumbe ao juiz realizar ou ordenar, mesmo oficiosamente, todas as diligências necessárias"*, podendo este ordenar diligências e devendo obter informações ou esclarecimento de factos e prover pela produção de provas necessárias ao apuramento da verdade *"quando aos factos de que lhe é lícito conhecer"*.

Assim, defendemos que o princípio do inquisitório atribui um verdadeiro poder-dever ao juiz de instrução, não como poder absoluto, mas sim como uma verdadeira prerrogativa

[104] O que levanta novas questões relativamente à descoberta eletrónica de prova e que suscitou as alterações de 2007 às *Federal Rules of Civil Procedure*.

[105] Apesar de serem mencionados aqui em conjunto, há que dar menção ao contributo de GÖNNER naquela que foi a distinção entre o princípio do dispositivo (*disposition máxime*) e o princípio do inquisitório (*offizielprincip*), e, consequentemente, a abertura da discussão de quais os princípios estruturantes do processo.

intransferível de indagação sobre o tema da prova, pois o princípio permite ao juiz procurar provas com o fito de esclarecer os factos contraditórios[106].

O princípio do inquisitório deve ser entendido como um poder-dever limitado, devendo restringir-se na busca pelas provas dentro dos factos alegados pelas partes (factos essenciais), com vista à justa composição do litígio e ao apuramento da verdade. É assim o entendimento defendido pela lei, pela doutrina e jurisprudência portuguesa, bem como pelo direito comparado[107].

6.6. Princípio do Contraditório

Este princípio indica que não se deve proferir qualquer decisão sobre um pedido ou um argumento de qualquer uma das partes sem se facultar à outra a oportunidade de se pronunciar sobre esse pedido ou sobre esse argumento[108].

Por conseguinte, se perante o julgador ambas as partes se encontrarem em igualdade, ambas devem ter a mesma chance de se justificarem, tudo em favor da procura da decisão mais justa, como o indica o artigo 3º do CPC, ao mencionar que *"o tribunal não O princício pode resolver o conflito de interesses que a ação pressupõe sem que a resolução lhe seja pedida por uma das partes e a outra seja devidamente chamada para deduzir oposição"*. Isto, por sua vez, torna claro que o princípio do contraditório é um corolário do princípio da igualdade das partes[109].

6.7. Princípio da Proporcionalidade

O princípio da proporcionalidade diz respeito à indagação da adequação de uma relação entre dois bens ou dois valores variáveis e comparáveis. Dentro do tema probatório, o princípio assume notável relevância, sendo a sua aplicação mais comum a de um instrumento de restrição de um direito fundamental, referindo-se a "*avaliação entre o bem que se pretende proteger ou prosseguir com a sua restrição"* e o bem jusfundamentalmente protegido que resulta, em consequência, desvantajosamente afetado[110].

---

[106] MACHADO, Costa, *"Código de Processo (...)"*, p.125.
[107] Numa perspectiva do direito comparado espanhol, aconselha-se AROCA, Juan Montero, *"Los principios políticos de la nueva Ley de Enjuiciamiento Civil - Los poderes del juez y la oralidade"*, Tirant Lo Blanch, Valencia, 2001, pp. 52-56.
[108] SILVA, Germano Marques, *"Do Processo Penal Preliminar"*, Editorial Minerva, 1990, p. 69.
[109] AMARAL, Maria Lúcia, *"A Forma da República: Uma introdução ao estudo do direito constitucional"*, Coimbra, Coimbra, Editora, 2005, p. 141.
[110] MOREIRA, Vital, *"A ordem jurídica do capitalismo"*, 1ª Edição, Caminho, Lisboa, 1973, p. 149.

6.8. Boa fé

As partes agem em defesa dos seus próprios interesses dentro do processo, e acreditar no contrário seria ignorar que ambas possuem posições opostas. No entanto, se por um lado elas devem agir na proteção dos seus direitos, por outro, não devem olvidar da lealdade processual e do dever de verdade[111], corroborado pelo dever de cooperação, que pauta o bom desenvolvimento e andamento da lide[112].

Entende-se a importância da lealdade processual das partes (inclusive do julgador) como crucial para a eficácia do andamento e funcionamento do processo, de maneira transparente e justa, sendo que a falta de lealdade e verdade das partes e de todos que de qualquer participam do processo é contrária ao exercício da jurisdição e incompatível com o objetivo do processo, ou seja, a justa composição do litígio e a descoberta da verdade[113].

Sob uma ótica moderna do direito comparado, a doutrina alemã, com base no artigo 138º do ZPO (*Erkalärungspflicht Tatsachen; Wahrheitspflicht*) considera que as partes têm um dever de verdade entendido por JAUERNIG como uma imposição legal, em que a parte não pode alegar um facto contra a parte contrária nem impugnar alegações da mesma caso esteja ciente ou convicta da inveracidade ou da veracidade, respetivamente, das alegações.

JAUERNIG salienta a natureza subjetiva deste dever de verdade, não sendo possível a escolha de não se ser verdadeiro no âmbito do processo.

Mesmo que não haja a produção de consequências específicas, uma vez que não está em causa um ónus, assim que é verificada a falta de verdade pelo juiz, o nº286 do ZPO (Freie Beweiswürdigung) aponta para o sentido de que o juiz, na formação da sua convicção deve tomar nota dessa falta e, na prática, penalizar a parte prevaricadora.

[111] SOUSA, Luís Pires de "Prova por Presunção no Direito Civil", 1ª Edição, Almedina, Coimbra, 2012, p. 33.
[112] MACHADO, Costa, *"Código de Processo (...)"*, p.21.
[113] LUSO SOARES, Fernando, "A Responsabilidade Processual Civil", 2ª Edição, Almedina, 1987, p. 164.

6.9. Princípio da Economia Processual

Este princípio traduz-se numa transmissão de eficiência ao processo, exigindo uma adoção dos meios necessários e suficientes à resolução de um dado processo, e não mais do que esses, como o indica LEBRE DE FREITAS[114]. Este princípio implica ainda a adequação da tramitação processual às especificidades da causa, a proibição da prática de atos inúteis e a simplificação dos atos úteis, o que o torna corolário do princípio da adequação formal[115].

Exemplos práticos da concretização deste princípio são a proibição de atos inúteis, constante do artigo 130º do CPC[116], e a redução das formalidades dos atos ao essencial, prescrita no artigo 131º nº1 do CPC.

6.10. Princípio da Celeridade Processual

O processo respeita a conjunto atos que visam ser conducentes a um resultado, pelo que, no âmbito do processo civil, que tem em vista alcançar a justa composição do litígio e a busca da verdade material, assinala-se também regras e prazos para a prática dos seus trâmites, como o indicam os artigos 137º e 138º do CPC.

Com esta informação, entende-se que o princípio da celeridade processual se encontra em consonância com o princípio da economia processual, visando um termo razoável e rápido do processo, e manifestando-se na fixação dos prazos para a prática de atos pelas partes ou pelo tribunal, na possibilidade de prorrogação dos atos[117], de suspensão da instância, nas regras de continuidade das diligências ou de marcação dos atos adiados, ou ainda na classificação com caráter de urgência de alguns atos ou tipos de processos[118].

A celeridade processual implica assim um romper com comportamentos processuais arcaicos, dando prioridade ao mérito e à substância, em detrimento da mera formalidade processual[119].

---

[114] FREITAS, José Lebre de *"Introdução ao processo civil: conceito e princípios gerais à luz do novo código"*, 3ª Edição, Coimbra, Coimbra Editora, 2013, pp. 203-204.
[115] FREITAS, José Lebre de *"Introdução ao processo civil: conceito e princípios gerais à luz do novo código"*, 3ª Edição, Coimbra, Coimbra Editora, 2013, pp. 222-223.
[116] *"Não é lícito realizar no processo atos inúteis."*
[117] Artigo 141º do CPC.
[118] Artigo 150º nº6 do CPC, por exemplo, no que respeita a recursos de decisões que retirem a palavra a mandatário judicial ou lhe ordene a saída do local onde o ato se realiza.
[119] GOMES CANOTILHO, J. J., "Direito Constitucional e Teoria da Constituição", Coimbra, Almedina, 2003, p. 499

No direito comparado, quanto aos aspetos formais, a doutrina brasileira[120], já influenciada pela doutrina estrangeira, defende mesmo a existência de uma Teoria Geral do processo, por meio da qual se definem os conceitos lógicos-jurídicos dos institutos fundamentais do processo, que são aplicados a qualquer dos ramos do direito processual.

6.11. Princípio da Oralidade

O princípio da oralidade encontra-se traduzido no contacto direto entre o juiz e as diversas fontes da prova, nomeadamente, na discussão das questões da causa. Assim, discussão da matéria de facto é oral, como o indica o artigo 604º do CPC, por exemplo.

Em Portugal, autores como PESSOA VAZ[121] desenvolveram grande parte da doutrina relativamente a este princípio.

6.12. Síntese

Feita esta exposição, talvez não seja de espantar que haja considerações relativamente a uma natureza "garantística" do processo. Neste sentido, LEBRE DE FREITAS[122] discorda, entendendo que os tribunais possuem poderes suficientes para suprimir os abusos das partes, e que a concessão desmedida de poderes discricionários não irá garantir mais sensatez no exercício da função judicial.

7. Boa Fé Processual

A palavra boa fé tem origem latina ("*fides*", que, na Roma Antiga, significava honestidade, confiança, lealdade e sinceridade), sendo que a sua existência decorre do primado da pessoa humana. De uma forma bastante geral, já nesses tempos se vislumbrava uma caracterização simultânea da "*bona fides*" e da "*fides bona*". Ora, se por um lado se analisava a crença de um sujeito para avaliar a sua conformidade os ditames legais, por outro, todas as relações se baseavam na confiança, pelo que o juiz, dentro do processo, era remetido a critérios de decisão éticos, sociais e de equidade.

---

[120] DIDIER JÚNIOR, Fredie, *"Curso de Direito Processual Civil: introdução ao direito processual civil, parte geral e processo de conhecimento"*, 18ª Edição, Salvador, Edições JusPodivm, 2016, pp. 101-102.
[121] PESSOA VAZ, Alexandre, *"Direito Processual Civil – Do antigo ao novo Código"*, 2ª Edição, Almedina, Coimbra.
[122] LEBRE DE FREITAS, José, *"Os princípios fundamentais na lei processual civil de hoje"*, VII Congresso dos Advogados Portugueses, 11, 12 e 13 de novembro (2011).

O conceito tende a dividir-se em boa fé objetiva (conjunto de deveres exigidos nos negócios jurídicos, mais explicitamente, nos contratos, destinado a pautar a conduta dos contratantes, num silogismo de honestidade e honra[123]) e boa fé subjetiva (referente ao estado psicológico da pessoa, consistente na justiça, ou, na licitude de seus atos, ou na ignorância da ilicitude dos seus atos). Uma corrente minoritária apoia a superação da distinção entre boa fé objetiva e subjetiva, optando por uma unidade de conceitos, como é o caso de HERNANDEZ GIL[124].

Usada para moralizar o funcionamento das sociedades e para fixar esferas de risco, a boa fé, enquanto regra de conduta, tem uma consagração generalizada nos códigos civis da atualidade. Não obstante, e conforme aponta MENEZES CORDEIRO, o conceito pauta-se pelo seu elevado grau de abstração, não sendo possível determiná-lo se não se for confrontado com a sua aplicação concreta.

Para efeitos deste trabalho, utilizaremos o exemplo alemão e o exemplo francês, sendo que são os ordenamentos jurídicos mais marcantes daquele que é o direito civil, para alcançar algumas noções relativas ao mesmo.

De facto, no paradigma alemão, encontramos um largo apelo à boa fé no que diz respeito à lei sobre cláusulas contratuais gerais, assim como uma aplicação mais tradicional, ainda que paralela a uma evolução pós-reunificação alemã, mantendo-se, muito estrito, o seu papel, nas invalidades formais. Assim, surgem ou negam-se a aplicação da *culpa in contrahendo* e da boa fé no domínio da receção de declarações negociais, das fianças, dos seguros, das relações familiares, desportivas e de trabalho, da locação financeira, da interpretação dos títulos executivos. Fala ainda de um dever de verdade subjetiva, que JUARNIG[125] considera constituir uma verdadeira imposição legal de sinceridade entre as partes num processo.

Já em França, as mais significativas aplicações da boa fé dizem respeito à resolução unilateral dos contratos, e, paralelamente, a cláusulas abusivas, sancionadas, nos termos da lei, assim como com a responsabilidade pré-contratual ou com a responsabilidade pela aparência[126].

---

[123] DIDIER JÚNIOR, Fredie, *"Fundamentos do princípio da cooperação no Direito Processual Civil Português"*, Coimbra editora, Coimbra, 2010, pp. 80-81.
[124] HERNANDEZ GIL, António, *"La función social de la posesíon"*, 1ª Edição, Madrid, Alianza, 1969, p.174.
[125] JAUERNIG, Othmar, *"Direito Processual Civil"*, 25.ª edição, tradução de Silveira Ramos, Almedina, Coimbra, 2002, p. 151.
[126] JAUERNIG, Othmar, *"Direito Processual Civil"*, 25.ª edição, tradução de Silveira Ramos, Almedina, Coimbra, 2002, p. 152.

Em Portugal, o instituto, assente na boa fé objetiva, que nos surge, com maior frequência, é o do abuso do direito e, dentro deste, o do *venire contra factum proprium*[127], como nos indica MOTA PINTO[128].

[127] *"Venire contra factum proprium postula dois comportamentos da mesma pessoa, lícitos em si e diferidos no tempo. O primeiro – factum proprium – é, porém, contrariado pelo segundo."* - MENEZES CORDEIRO, António Manuel, *"Da Boa Fé no Direito Civil"*, Almedina, Coimbra, 1997. p. 753.

[128] MOTA PINTO, Paulo, *"Boletim da Faculdade de Direito: Volume Comemorativo."*

Capítulo II – A Prova Digital

Um tipo de prova considerado fulcral em todos os ordenamentos jurídicos é o de prova documental, sendo que a nossa análise de documentos em formato eletrónico e a própria redação dos mesmos se baseia num precedente de recriação visual e funcional da forma "em papel" dos mesmos, como se de fotocópias e pastas se tratassem[129]. Da mesma forma, o próprio conceito de *e-mail*/correio eletrónico nada mais é que uma transposição do conceito de correspondência de cartas/correio para um meio tecnológico/eletrónico.

Se o documento eletrónico e digital é uma representação material idónea que visa reproduzir uma manifestação de vontade, palavras, dados (entre outros), materializados por meio; então é justo estabelecer que este constitui realidades pré e extra processuais, que se incorporam no processo sob a forma de meios de prova[130].

SENG e MASON chamam a atenção para esta aparente semelhança, passível de induzir muitos no erro de considerarem a prova digital como sendo análoga à prova documental convencional. De facto, esta generalização traduz-se numa sobrestimação das garantias de integridade e imutabilidade das provas digitais em si, o que nos leva à análise que se segue, pois torna-se premente elencar aquilo que se entende por prova digital e quais as suas características particulares[131].

1. Definição

Duas definições comuns de prova digital são "informações de valor probatório que são armazenadas ou transmitidas em formato binário" e "informações armazenadas ou transmitidas em formato binário que podem ser invocadas em juízo", ambas bastante simplificadas e redutoras.

De facto, não existe uma definição linear daquilo que se entende por prova digital, sendo que não há sequer um consenso na denominação a utilizar para o conceito, pois autores distintos referem-se à mesma como "prova eletrónica" ou "prova computacional". Da mesma forma,

[129] FERNANDÉZ, J. Mª Illán, *"La prueba eletrónica, eficácia y valoración en el processo civil"*, 1ª Edição, Thomson Reuters, 2009, p.241.
[130] FERNANDÉZ, J. Mª Illán, *"La prueba eletrónica(...)"*, 1ª Edição, Thomson Reuters, 2009, p.231.
[131] MASON, Stephen, SENG, Daniel, *"Electronic Evidence"*, 4ª edição, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017, p.21.

ainda que seja intuitivo que existem características que distinguem este tipo de prova dos restantes, torna-se difícil elencar tais elementos em jeito enumerativo.

A principal causa desta problemática prende-se com a velocidade evolutiva do paradigma tecnológico, que implica que diversas noções se tornem sucessivamente obsoletas num curto prazo, e que as que acabam por ser elencadas se pautam por uma extrema ambiguidade.

DIAS RAMOS fornece uma definição concisa relativamente ao que se poderá entender por prova digital, classificando-a como a *"informação passível de ser extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta"*[132].

SILVA RODRIGUES[133] entende *que "a prova eletrónico-digital pode definir-se como qualquer tipo de informação, com valor probatório, armazenada (em repositório eletrónico-digitais de armazenamento) ou transmitida (em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis), sob a forma binária ou digital"*.

Assumindo uma perspetiva orientada pela necessidade do sistema jurídico em converter elementos eletrónicos/digitais em provas, alcançamos a definição de EOGHAN CASEY, que entende prova digital como sendo *"quaisquer dados armazenados ou transmitidos usando um computador que suporte ou refute uma teoria de como uma ofensa ocorreu ou que aborda elementos críticos da ofensa, como intenção ou álibi"*[134].

Esta definição de pendor essencialmente criminológico deve ser encarada com várias ressalvas, sendo que por "dados" se devem entender ficheiros de texto, áudio e imagem; e que a palavra "computador" deve ser encarada na sua maior abrangência possível, designando qualquer sistema que seja capaz de armazenar, modificar e transmitir dados.

Para efeitos deste trabalho, tentaremos elencar o tipo de informações relevantes no âmbito da prova eletrónica-digital, os meios em que são transmitidos e o seu âmbito[135], tomaremos em conta a definição dada por SENG e MASON, que entendem prova digital como sendo *"dados (compreendendo tanto a saída de dispositivos analógicos como a de dados em formato digital) que são manipulados, armazenados ou comunicados por qualquer dispositivo fabricado,*

[132] RAMOS, Armando Dias, "*A Prova Digital em Processo Penal*, Chiado Editora", 1.º edição, 2014, pág. 86.
[133] RODRIGUES, Benjamim Silva, *"Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital"*, Rei dos Livros, Lisboa, 2011, p. 722
[134] CASEY, Eoghan, *Digital Evidence and Computer Crime"*, 3ª edição Academic Press, 2011, p.7.
[135] MASON, Stephen, SENG, Daniel, *"Electronic Evidence"*, 4ª edição, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017, pp.19-20.

computador ou sistema de computador ou transmitidos por meio de um sistema de comunicação; e que têm o potencial de tornar a matéria de facto de qualquer parte mais ou menos provável"[136].

1.1. Características da Prova Digital

Independentemente da jurisdição vigente, a recolha e a utilização de provas eletrónicas passa pelos processos (i) de obtenção de informação, da (ii) incorporação dos dados obtidos no processo, seguindo-se uma (iii) valoração destes mesmos dados.

KLUWER[137] clarifica que a valoração de um elemento de prova implica uma concessão de credibilidade, de acordo com o sistema de regras de avaliação estabelecido pela lei vigente. Assim, caso a prova digital cumprir com os requisitos de obtenção e de incorporação no processo, ser-lhe-á reconhecida eficácia probatória, sendo objeto de valoração por parte do Juiz ou do Tribunal, como o indica o disposto no artigo 46º do Regulamento 910/2014 (Regulamento EIDAS), ao indicar que *"não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a um documento eletrónico pelo simples facto de se apresentar em formato eletrónico"*.

A valoração da prova eletrónica passa pela análise da presença de duas características, nomeadamente, a autenticidade e a integridade.

Tradicionalmente, entende-se por autenticidade a coincidência do aparente autor do documento eletrónico com o real autor do mesmo. Numa perspetiva de prova eletrónica, define-se como sendo a propriedade que nos dê um garante da fonte da qual provêm os dados. Em caso de dúvidas relativamente à autenticidade, será negada força probatória ao elemento de prova a ser valorado.

Já por integridade da prova eletrónica, entende-se como sendo a consistência dos dados constantes da mesma, que não poderão ter sido alterados de maneira não autorizada, numa perspetiva de preservação dos mesmos. Indícios da manipulação desses mesmos dados comprometem a prova, sendo que, caso tal se verifique, o juiz deverá negar força probatória ao elemento de prova a ser valorado.

---

[136] MASON, Stephen, SENG, Daniel, *"Electronic Evidence"*, 4ª edição, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017, p.19.
[137] KLUWER, Wolters, *"Diario La Ley, Nº 6, Sección Ciberderecho"*, 2017.

Posto isto, e de forma a seguir os objetivos delineados na presente dissertação, farei uma análise aprofundada daqueles que são os requisitos de admissibilidade de provas digitais, bem como fases de obtenção das mesmas, conforme delineado numa perspetiva anglo-saxónica.

1.2. Obtenção de Prova Digital

Neste subtópico será pertinente abordar a forma como as novas tecnologias da informação permitem um acesso aos eventuais elementos de prova digital, pelo que o principal enfoque se verterá nos meios mais comuns para tal, que são os dispositivos digitais e as redes.

1.2.1. Dispositivos Digitais

Num mundo em que a computação digital e as bases de armazenamento de dados são a norma, acreditamos que por *"dispositivos digitais"* devemos entender não só computadores *lato sensu*, mas também rastreadores de condicionamento físico e elementos de domótica[138] (por exemplo, medidores de energia inteligentes, sistemas de aquecimento central automatizados[139]), visto que a grande maioria destes compartilha recursos importantes com dispositivos de computação mais reconhecidamente convencionais, como *desktops*, *laptops* e *tablets*, seguindo o tradicional modelo de *input-processing-output*, resumido aqui:

i. O dispositivo recebe uma ou mais informações via uma determinada entrada, por meio de um arquivo local, sensor, teclado ou através de um canal de comunicação (como uma conexão de rede).
ii. O dispositivo processa a informação recebida.
iii. O dispositivo produz uma saída (para um display, *arquivo local* ou impressora, por exemplo).
iv. O dispositivo passa a ser capaz de armazenar (e/ou retransmitir) informações.
v. O dispositivo passa a ser capaz de disponibilizar funcionalidades que permitem a consulta e/ou modificação da totalidade ou de parte da

[138] Termo resultante da fusão da palavra *"domus"*, que significa casa, com a palavra "robótica", ligada ao ato de automatizar. Assim, a domótica é responsável pela gestão dos recursos habitacionais, de forma a introduzir conforto e melhoria de vida nas residências dos seus utilizadores, aliada a uma noção de comunicação e segurança.
[139] ANDRADE, Francisco Pacheco, *"Comunicações eletrónicas e Direitos Humanos: O perigo do homo connectus"* in *"Direitos Humanos e sua efetivação na Era da Transnacionalidade"*, Juruá Editora, Curitiba, pp. 209-210.

informação armazenada, porventura mediante mecanismos de controlo de acesso[140].

Assim, dentro destes dispositivos, torna-se relevante filtrar os vários elementos dos quais é passível extrair uma prova:

a) Ficheiros

Os dispositivos digitais encontram-se munidos de um conjunto de aplicações que permitem ao utilizador a partilha arquivos, que armazenam mensagens, *spreadsheets*, bases de dados, textos, fotografias e apresentações multimédia, as quais se podem constituir como provas digitais.

b) Imagens

Em primeiro lugar, cabe-nos clarificar que por "imagens", neste contexto, entendemos reproduções digitais exatas do conteúdo de um dispositivo de armazenamento, as quais são frequentemente denominadas de *"clones"*, *"mirrors"* ou "imagens" desse armazenamento original.

O processo de criação de imagens é um processo não destrutivo que cria uma cópia digital externa exata de todos os dados no dispositivo, o que levanta a questão de uma análise de dados a ser realizada na cópia da imagem e não nos dados armazenados no dispositivo original.

Deve, contudo, ser feita a ressalva de que nem sempre é possível realizar uma cópia completa ou fidedigna de um dispositivo de armazenamento, uma vez que há situações em que o microcontrolador que gere o dispositivo não permite mais do que uma mera cópia parcial ou, caso esteja comprometido do ponto de vista de segurança, adultera a cópia produzida.

Nessa mesma linha de pensamento, não podemos descurar de que, por vezes, a cópia produzida, ainda que considerada completa e íntegra, não permite a

[140] Em jeito de clarificação, referimo-nos aqui a eventuais mecanismos de autenticação e de controlo de acesso a registos de bases de dados, pastas e arquivos de um sistema de ficheiros, ou ainda a mecanismos de DRM (um dispositivo com saída HDMI pode apresentar imagens ou vídeo apenas em monitores compatíveis DRM).

extração de informação devido ao dispositivo de armazenamento original estar total ou parcialmente cifrado (como é o caso de discos SATA, que podem estar sujeitos a cifragem/decifragem transparente por hardware). Nesses casos, apenas conhecendo a chave/segredo poder-se-á extrair informação da cópia/imagem obtida.

c) Históricos de Registo/*Logs*

Na maioria dos sistemas operativos, como é o caso do Windows, do Mac e do Linux, praticamente tudo o que é no sistema fica registado na forma de *logs*, disponibilizando informações relativas aos dados de visita de um utilizador a um determinado *site* da Internet (nome, endereço de IP[141][142][143], número de telefone, endereço de e-mail e senhas).

Nisto, em teoria, será passível de se incluírem informações, como o são o registo de acesso a aplicações e programas, o que pode ajudar a determinar, por exemplo, se um utilizador não autorizado obteve acesso a um sistema ou se fez *download* de um arquivo da Internet e a primeira página que visitou ao aceder.

Sucede que, na maioria dos sistemas, os *logs* apenas registam eventos considerados importantes pelo administrador do sistema (ou na configuração por omissão do sistema). Por outro lado, é realmente importante ponderar se podemos realmente confiar nestes *logs* para ter certeza de que o sistema não terá sido comprometido por um eventual atacante. Se um atacante conseguir, de algum modo, privilégios de administração do sistema, poderá, tendo literacia

---

[141] Protocolo de Internet (IP) é um protocolo de comunicação usado entre todas as máquinas em rede para se proceder à transmissão dados, e que pode ser fixo ou de atribuição dinâmica, o que quer dizer que muda em função do tempo. Traduz-se um standard de endereços, descrito no RFC 791 da Internet Engineering Task Force (IETF), sendo que os computadores recorrem ao serviço DNS (*Domain Name System*) para traduzir os nomes, acessíveis ao públic, em endereços TCP/IP.

[142] Existem serviços gratuitos na Internet, destinados a disponibilizar informações sobre os titulares de endereços IP e de páginas Internet, por recurso às bases de dados dos denominados RIR (*Regional Internet Registry*), organizações responsáveis pela gestão, alocação e registo dos recursos de endereços da Internet nas várias regiões do mundo. Exemplos destas páginas são o https//www.centralops.net (fornece endereços tanto na versão IPv6, como na versão IPv4) e o https://www.domaintools.com.

[143] Na senda da nota supra, será relevante estabelecer a distinção entre o IPv4 e o IPv6. O IPv4 disponibiliza aproximadamente 4.3 biliões (2^{32}) de endereços, pelo que a *Internet Engineering Task Force* (IETF) teve necessidade de estudar uma forma de expandir a capacidade de endereçamento na Internet, fruto da banalização da utilização de sistemas informáticos, introduzindo o protocolo IPv6, que disponibiliza 2^{128} endereços, ou seja, 340 triliões de triliões de triliões de endereços únicos e acessíveis à população mundial.

para isso, fabricar/adulterar os *logs* depositados no sistema[144], o que comprometeria qualquer confiança nas informações por estes transmitidas.

Em cenários de administração mais profissional, seja no sector público, seja no privado; muitos administradores optam por disponibilizar um equipamento cuja única função é a de colecionar cópias constantemente atualizadas dos *logs* dos restantes dispositivos da infraestrutura. Esses equipamentos, por vezes passivos, funcionam como autênticas *"caixas negras"* e aí sim, será mais justificável podermos depositar confiança na informação armazenada.

d) Ficheiros *cache*

Quando um dispositivo acede à Internet, registam-se uma série de informações sobre as suas atividades, incluindo os sites que foram visitados e os conteúdos que foram visualizados, sendo feitas cópias temporárias de sites que foram visitados.

Estas cópias são assim armazenadas em pastas *cache*, que contêm fragmentos do *site*, incluindo imagens e texto, e informações de localização, o que é útil para recolha de informações. Não obstante, e na senda do ponto anterior, cabe-nos apontar o risco de possível adulteração destas pastas e do seu conteúdo.

e) Ficheiros eliminados

Mesmo quando um ficheiro é eliminado, continua a ser possível recuperar dados que foram excluídos, dependendo da quantidade de atividade de gravação em disco que foi executada no período entre a eliminação do ficheiro e a recolha de dados.

Outra possibilidade de recolha de elementos de prova diz respeito às circunstâncias em que um dispositivo declarado não funcional seja restaurado ou desbloqueado. Nesses momentos pode ser possível descobrir ou inferir

[144] Um ponto importante a ter em conta é que é mais fácil poder afirmar que um elemento de prova foi adulterado do que afirmar que ele é autêntico, como ocorre, por exemplo, no caso eventos causalmente relacionados e registados em ordem inversa. Naturalmente que isto não descura do facto de que eventos registados na sua ordem correta não poderão ter sido "plantados" ou adulterados de alguma forma.

elementos de irregularidades no dispositivo, por comparação aos elementos contidos antes da respetiva restauração.

f) Dispositivos móveis

O uso de *tablets* e *smartphones*, que combinam as funcionalidades dos computadores pessoais[145] com as aplicações de telefone e câmara, é praticamente omnipresente, pelo que, juntamente com os *laptops*, estes poderão ser utilizados para obter provas digitais.

Assim, além da lista dos números de telefone contactados mais recentemente, um *smartphone* será capaz de produzir quantidades substanciais de dados, incluindo *e-mails* e outros dados de uma rede que, no caso do Processo Penal, poderão ajudar numa investigação de *e-mails.*

Da mesma forma, a localização através de antenas celulares e a informação de localização GPS e/ou WiFi, passível de ser registada pelas localmente pelas aplicações e/ou remotamente na *"cloud"*[146]; apresentam-se como potencialidades particularmente úteis no domínio da investigação. Exemplos claros desta aplicação serão, por exemplo, a deteção do IP do utilizador de um dispositivo aquando do seu acesso a um sinal de rede, permitindo (ainda que casuisticamente) estabelecer uma comprovação da presença de indivíduos suspeitos em locais nos quais possam ter ocorrido eventuais ilicitudes de natureza informática, como o será o acesso forçado a algum servidor ou rede interna.

[145] Estes dispositivos são autênticos computadores, uma vez que contêm CPU, memória, teclado, ecrã, sistemas de entrada (para USB) e saída (para *headphones*, por exemplo) e, tal como os computadores portáteis, sistemas de ROM e RAM. Em jeito de clarificação, a ROM armazena o sistema operacional e qualquer software essencial necessário para o dispositivo funcionar, sendo que, por sua vez, a RAM é usada para armazenar outros softwares e dados que o usuário deseje reter.

[146] De forma muito simples, a computação na *cloud* é um exemplo de computação distribuída (ver ponto 1.2.2 do presente capítulo) que se refere a um modelo de cliente/servidor (respetivamente, dispositivos móveis e um ou mais centros de dados) no qual o acesso a dados/serviços requer uma conexão transparente com um conjunto de servidores, aparentemente com recursos ilimitados.

g) Metadados[147]

Conforme o nome indicada, "metadados" traduz-se em "dados sobre dados", podendo esses dados apresentar-se de várias formas, tais como bancos de dados, arquivos, documentos, *spreadsheets*, e muitos outros além de arquivos temporários da Internet (dos navegadores). Estas informações podem referir-se a um determinado conjunto de dados, a um objeto ou até a uma fonte de prova, sendo necessária uma compreensão dos dados com que se trabalha e dos próprios standards[148] de metadados.

A partir daí, é intuitivo entender que passa a ser possível visualizar, documentar, e utilizar os metadados para obter conclusões ou organizar em relatórios, os quais, em conjunto com informações recolhidas em investigações, podem auxiliar na descoberta da verdade e na deteção de eventuais alterações de informações.

1.2.2. Redes

A maioria de computadores estão agora conectados a outros computadores por diferentes nós de computação que cooperam e competem através de troca de mensagens em ambiente de rede, naquilo que se entende como uma "computação distribuída"[149]. Tal modelo de computação que permite aos utilizadores acederem, partilharem, e armazenarem informação através da Internet, entre os quais se encontrarão elementos de prova.

Em muitos casos, pode ser que a única prova que estará disponível se encontre em dispositivos que compõem a infraestrutura de rede, fruto da eliminação dos elementos de prova nos computadores em si.

a) Internet

A grande quantidade *logs* e ficheiros contidos em computadores implicam vários elementos passíveis de constituírem elementos de prova *online*, incluindo o uso de *e-*

[147] MOSS, Bert, *"Metadata in Digital Forensics"*, eForensics Magazine, pp. 58-60.
[148] http://www.dcc.ac.uk/resources/metadata-standards/list (Consultado a 10 de outubro de 2019).
[149] ANDRADE, Francisco, *"Comunicações Eletrónicas e Direitos Humanos: O Perigo do Homo Conectus"* in "Direitos Humanos e sua Efetivação na Era da Transnacionalidade", Juruá Editora, Curitiba, 2012, p. 208.

mail[150], a visualização de *sites*, a transferência de ficheiros entre computadores, os registos de acesso ao servidor, o conteúdo dos dispositivos conectados à rede (ver o tópico anterior, referente aos dispositivos digitais), os registos da atividade de tráfego e a consulta do estado de páginas internet no passado[151].

Na senda desta linha de pensamento, será relevante mencionar os mecanismos de retenção dos operadores que fornecem serviços de Internet, pela enorme quantidade de informações passíveis de serem recolhidas.

b) Intranet

Encontra-se grande utilidade no que concerne à Intranet, a rede privada de determinadas instituições, acessível apenas aos seus funcionários, e que pode muito provavelmente conter informações relevantes para a constituição de elementos de prova; como o serão o registo de quadros de profissionais (quando se trate de identificar algum sujeito) ou documentos que em mais nenhum lugar se encontrem disponíveis.

c) Redes Sociais

No que concerne a uma realidade atual, as redes sociais (como é o caso do *Facebook*, do *Instagram* e do *LinkedIn*) são particularmente úteis para confirmação de informações relativamente a sujeitos de litígios, seja para se verificarem identidades, seja para se confirmarem residências ou currículos profissionais, o que se torna útil na identificação de testemunhas[152].

1.3. Requisitos de admissibilidade de provas digitais

Salvo as suas exceções, a legitimidade da avaliação de provas digitais está dependente de uma autorização legal, impondo-se o respeito pela proteção dos dados e privacidade dos

[150] Seja via programas como o Microsoft Outlook, seja via os vários serviços de e-mail, como o *Gmail*, o *Hotmail*, o *Yahoo* ou o *Sapo*, por exemplo.
[151] Para efetuar estas pesquisas existem duas possibilidades, nomeadamente (i) através do operador cache do Google, na qual o comando a introduzir na caixa de pesquisa do Google é *"[cache:www.pagina_a_procurar.dominio]"* ou (ii) o motor de busca *"WaybackMachine"*, um serviço acessível através da ligação www.archive.org. Devemos realçar que o *cache* do Google é de pouca duração, sendo constantemente atualizada, pelo que pode deixar de existir o conteúdo pretendido bastante rapidamente, tal como acontece caso a página seja apagada.
[152] Duas ferramentas adquirem particular utilidade neste domínio, nomeadamente (i) a Lococitato (contida no endereço http://www.lococitato.com), tendencialmente utilizada pelas autoridades, e que permite mapear os vários contactos de determinado perfil nas redes sociais; e (ii) o *site* http://namechk.com, que permite pesquisar e aceder a nomes de utilizadores em dezenas de redes sociais.

litigantes, de forma a evitar que os órgãos responsáveis pelo cumprimento da legalidade atropelem direitos, liberdades e garantias. Tomando em conta que mandatos de busca e outras formas de investigação tendem a implicar o acesso a dispositivos eletrónicos e provas digitais, a ausência de autorização legal pode minar a prova e colocar em risco a investigação do caso.

A relevância é um importante determinante da admissibilidade da prova digital. Segundo MASON e SENG, para que as provas sejam admissíveis, devem ser *"suficientemente relevantes"* para os fatos em questão[153], ou seja, devem deve ser propícia a provar ou refutar um facto no processo, alicerçando nisso o seu valor probatório.

A autenticidade é outro critério importante que afeta a confiabilidade das provas, pelo que, para um registo digital ser admissível, tem de ser possível para o tribunal verificar que o registo foi de fato gerado pelo indivíduo que supostamente o elaborou. O caso da *American Express Travel Related Services Inc. vs Vee Vinhnee*[154] destaca a importância do requisito de autenticidade, sendo que, nesse caso, o juiz se pronunciou contra a *American Express* com base na sua falha em autenticar os registos.

A integridade também é um requisito principal para a admissibilidade da prova digital e serve como base para determinar o seu peso na investigação. Ao avaliar a integridade da prova digital, os tribunais exigem que esta integridade seja estabelecida e garantida durante as investigações e que as provas sejam preservadas das modificações durante todo o seu ciclo de vida. Na República da África do Sul, a originalidade das provas digitais depende da sua integridade, conforme descrito no artigo 14º nº2 da *Electronic Communications and Transactions Act of 2002*[155].

De forma a garantir a confiabilidade da prova digital, quem apresenta a prova deve estabelecer que nenhum aspeto da mesma é suspeito. LEROUX[156] sublinha que que, para que as provas sejam consideradas confiáveis, *"não deve haver nada que lance dúvidas sobre como as provas foram coletadas e posteriormente tratadas"*. Olhando para um exemplo comparado, o

[153] MASON, Stephen, SENG, Daniel, *"Electronic Evidence"*, 4ª edição, University of London School of Advanced Study – Institute of Advanced Legal Studies, 2017.

[154] O tribunal recusou-se a admitir os registos de negócios do autor em formato digital por os considerar inadequadamente autenticado, mas deu ao autor a chance de retifocar os defeitos fundamentais numa apresentação pós-julgamento. As informações relativas a este caso encontram-se devidamente detalhadas e elencadas em https://casetext.com/case/in-re-vee-vinhnee (consultado a 05 de outubro de 2019).

[155] *"(...)integrity must be assessed- (a) by considering whether the information has remained complete and unaltered. except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display: 35 (0) in the light of the purpose for which the information was generated; and (c) having regard to all other relevant circumstances".*

[156] LEROUX, Olivier, *"Legal admissibility of electronic evidence"* in *"International Review of Law, Computers & Technology, 18:2"*, 2004, pp. 193-220.

caso Daubert[157] fornece a base e os critérios para avaliar a confiabilidade das provas científicas nos Estados Unidos, nomeadamente, saber (i) se a técnica foi testada e (ii) submetida a revisão, (iii) se existe uma taxa de erro conhecida associada à técnica, (iv) se os padrões que controlam suas operações existem e foram mantidos, e (v) se a técnica é geralmente aceite pela comunidade científica.

Não obstante deixarmos a ressalva de que estas questões apresentam as suas particularidades nos vários ordenamentos jurídicos, especialmente se as transpusermos para um contexto de sistemas europeus continentais, achamos o regime detalhado norte-americano meritório pelas exigências de segurança que impõe e pelo impacto que adquire no bom funcionamento de valoração da prova digital dentro do seu contexto.

A integração dos requisitos técnicos e legais discutidos acima fornece a base de uma estrutura harmonizada para avaliar a admissibilidade de provas digitais. Deve ser enfatizado que o exame cruzado em procedimentos legais é um elemento importante que impacta a avaliação dos requisitos técnicos e legais.

Na União Europeia, estas questões de regulamentação da autenticidade e integridade foram inicialmente previstas e tratados com a Diretiva 1999/93, o Parlamento Europeu e do Conselho, de 13 de dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas eletrónicas; que entretanto foi revogado pelo Regulamento 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 , relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.

Em Portugal, a integridade e autenticidade dos documentos eletrónicos é feita por meio de uma articulação entre a lei geral (Código Civil) e o Decreto-Lei 290-D/1999, de 2 de agosto (elaborado na transposição da diretiva 1999/93 do Parlamento Europeu e do Conselho), em conjunto com o Regulamento 910/2014, de aplicação direta e imediata em todo o território da União (que revogou grande parte do Decreto-Lei 290-D/1999) sendo que estas questões serão aprofundadas posteriormente (Capítulo III).

[157] *Daubert vs. Merrell Dow Pharmaceuticals, Inc.*, de 1993. Nesse processo americano, discutia-se um fármaco denominado Bendectin, passível de ter provocado lesões num recém-nascido. O juiz Blackmun ditou um tratado epistemologia, visando elencar os critérios com base o juiz se deve pautar para admitir ou excluir os meios de prova científicos apresentados pelas partes. As informações relativas a este caso encontram-se devidamente detalhadas e elencadas em https://caselaw.findlaw.com/us-supreme-court/509/579.html (consultado a 05 de outubro de 2019).

1.4. Prova per si ou meio de prova?

1.4.1. Recapitulação e Distinção

"Prova" diz respeito a um dado facto que é reconhecido pelo juiz como sendo verdadeiro, sendo, por isso, a demonstração da existência, ou não, de um determinado facto necessário para convencer o julgador a decidir a causa do litígio num dado sentido.

Já por *"meio de prova"* se entende tudo o que se destina a formar a convicção do juiz, ou seja, *"qualquer elemento que possa ser utilizado para estabelecer a verdade dos factos da causa"*[158].

Assim, torna-se possível que, na produção de um meio de prova, a parte poderá recorrer a técnicas ilegais, comprometendo o meio de prova e a sua admissibilidade[159]. Seguindo esta linha de pensamento, considera-se o meio de prova como sendo ilícito quando obtido por meios vedados pelo ordenamento jurídico, durante a produção do meio de prova, sendo que o que se considera ilícito não é a prova nem o meio de prova, mas sim o modo pelo qual o meio de prova foi alcançado.

Para fazer ponte com esta explanação, o CPC, no seu artigo 369º, clarifica que *"as partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz"*.

Por "meios legais", e tomando como base o artigo citado, devem-se entender como sendo *"meios de provas produzidos licitamente ou legitimamente"*.

Feitas estas considerações, parece-nos razoável considerar a prova digital como sendo um meio de prova, especialmente tomando em conta a decisão tomada em seguir a definição de SENG e MASON, que, conforme dito anteriormente, definem prova digital como sendo *"dados (compreendendo tanto a saída de dispositivos analógicos como a de dados em formato digital) que são manipulados, armazenados ou comunicados por qualquer dispositivo fabricado, computador ou sistema de computador ou transmitidos por meio de um sistema de*

[158] MICHELLE TARUFFO, "*A prova"*, São Paulo: Marcial Pons, 2014.
[159] Nesse sentido, ver o Capítulo I, no que se refere à prova ilícita.

comunicação; e que têm o potencial de tornar a matéria de facto de qualquer parte mais ou menos provável"[160].

Na verdade, e numa perspetiva de Direito Penal, os meios de obtenção da *prova digital*, não obstante com as adaptações necessárias, em muito se aproximam dos meios ditos "tradicionais" de obtenção da prova (exames, revistas, buscas, apreensões ou interceções de comunicações)[161].

1.4.2. Documentos Eletrónicos e Documentos Digitais

Por *"meios eletrónicos"*, entendem-se todos os instrumentos criados para obter uma troca de informações de forma automatizada, passando pela utilização de equipamentos eletrónicos de tratamento e armazenamento de dados para concretizar esta difusão, envio e receção de forma audiovisual.

Cabe-nos aqui fazer uma breve distinção entre documento eletrónico e documento digital, pelas suas características próprias.

Por *"documento eletrónico",* e seguindo o Regulamento 910/2014, do Parlamento Europeu e do Conselho, de 24 de julho de 2014, entendemos *"qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual"*. Assim, englobam-se todos os objetos materiais em que é possível (ou não) identificar-se uma manifestação de vontade ou que sejam representativos de um ato de interesse para o processo, com a particularidade de que estes estejam armazenados e sejam acessíveis por recurso às novas tecnologias da informação ou meios modernos de reprodução audiovisual (fotografia, fonografia, cinematografia, CDs, disquetes, pen-drives, etc). A transformação de documentos em suporte de papel para documentos em suporte eletrónico implica a sua digitalização por meio de um processo de captura digital e a formatação desses dados para tratamento com determinado software.

Um *"documento digital"* é um conjunto selecionado e organizado de objetos materiais digitais (documentos eletrónicos) em conjunto com os meta dados que os descrevem e com a interface ou conjunto de interfaces que facilitam o seu acesso, acessíveis por meio de

[160] MASON, Stephen, SENG, Daniel, *"Electronic Evidence"*, 4ª edição, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017, p.19.
[161] MILITÃO, Renato Lopes, *"A propósito da prova digital no processo penal"*, p. 266.

equipamentos computacionais adequados, por estarem codificados em forma analógica ou dígitos binários.

Em suma, todos os documentos digitais são documentos eletrónicos, mas nem todos os documentos eletrónicos são documentos digitais.

Analisando a questão de forma prática, o documento eletrónico mais utilizado e melhor regulado acaba por ser o contrato eletrónico[162], pela presença de assinaturas eletrónicas uma vez que um documento eletrónico em si mesmo não é capaz de atestar nem creditar a vontade dos contraentes. Conforme mencionado anteriormente, a prova é o resultado de todo um processo de elaboração mental, sendo que, neste caso concreto o órgão jurisdicional obtém a sua convicção mediante o esclarecimento do seu entendimento quanto ao conteúdo do contrato eletrónico.

1.5. Limitações da prova digital

Por se tratar de uma prova tecnicamente complexa e de carente de interpretação especializada, tornam-se claras várias limitações inerentes a este meio de prova, as quais trazem diversas implicações que não podem ser ignoradas.

1.5.1 Efemeridade, Volatilidade e instabilidade

A prova eletrónica é altamente volátil. Ao contrário dos tipos tradicionais de prova, a prova eletrónica é alterável com o recurso à computação, sendo a alteração os meta-dados (elemento chave da admissibilidade das provas) possível com simples alterações de arquivos. Deve-se assim tomar em conta que, quando um utilizador clica num arquivo, independentemente daquela que seja a sua intenção, incorre na possibilidade de alterar os meta-dados registados (por exemplo, relativos a última hora de acesso ao sistema), o que pode tornar o arquivo em questão inadmissível enquanto prova.

A instabilidade demonstrada por este tipo prova verifica-se em situações em que o investigador se depara inicialmente com uma prova com certas características, e mais tarde,

[162] De facto, constam de regulamentação na Diretiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de junho de 2000 (elativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno) e o Decreto-Lei 7/2004, de 7 de janeiro; que transpõe essa diretiva em Portugal.

esta se modifica, total ou parcialmente, colocando em causa a sua apreensão, interpretação e aceitação.

A natureza mutável da tecnologia, a fragilidade do meio na qual os dados eletrónicos são armazenados e a natureza intangível dos mesmos tornam todas as provas digitais potencialmente vulneráveis a alegações de erros, alterações acidentais, interferência prejudicial e falsificação. Essas questões técnicas, quando combinadas com erros legais ou dificuldades, podem afetar a admissibilidade da prova digital, bem como o grau da sua valoração nos casos em que esta é admitida.

VLADIMIR ARAS manifesta-se neste sentido[163], concluindo que "salvo quando o usuário do computador faça uso de uma assinatura digital, dificilmente se poderá determinar quem praticou determinada conduta"[164].

Esta fragilidade e mutabilidade implicam um cuidado redobrado da parte do investigador forense na sua recolha, cabendo-lhe a tarefa de identificar, de forma muito rigorosa, qual o tipo de prova digital em causa, de forma a garantir a força probatória da prova digital, sem perigo de esta ser alterada ou desaparecer.

Implicam-se também cuidados acrescidos a nível da fiabilidade dos dados, visto que numa comunicação, por exemplo existem diversos fornecedores de serviços, o que implica que estes deverão revelar expeditamente à autoridade judiciária competente quais os envolvidos na comunicação em causa, identificando e garantindo preservação dos dados de tráfego respeitantes à comunicação.

---

[163] *"No ciberespaço. o exame da identidade e a autenticação dessa identidade não podem ser feitos visualmente, ou pela verificação de documentos ou de elementos identificadores (...). Quando um indivíduo está plugado na rede, são-lhe necessários apenas (...) o endereço da máquina que envia as informações à Internet e o endereço da máquina que recebe tais dados. Esses endereços (...) não revelam nada sobre o usuário da Internet e muito pouco sobre os dados que estão sendo transmitidos"* – ARAS, Vladimir, "*Crimes de informática. Uma nova criminalidade"*, Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em https://jus.com.br/artigos/2250 (consultado a 05 de outubro de 2019).

[164] Cabe-nos mencionar que esta afirmação por si só não está completa. Deverá ser uma assinatura digital qualificada (por uma terceira parte de confiança), conforme explicitaremos no Capítulo III.

1.5.2. Implicações a nível da privacidade

Da mesma forma, a prova eletrónica apresenta-se como altamente intrusiva no que diz respeito a direitos fundamentais, como é o caso do direito à privacidade. Estas questões implicam que a lei processual vise regular a forma em que se deva percecionar e gerir os novos meios de prova, o acesso aos mesmos, e a ressalva da intimidade.

Assim, ILLÁN FERNANDEZ sugere não só a adoção de medidas *ante legem*, que salvaguardem estes direitos fundamentais e assegurem a não adulteração das provas (mencionada no ponto anterior); mas também o recurso a notários que registem conteúdos que vão sendo obtidos, bem como a data da entrada das informações, de forma a salvaguardar possíveis volatilidades e alterações das provas[165].

1.5.3. Caráter Incorpóreo

Não podemos descurar do caráter incorpóreo/imaterial das provas em formato eletrónico, o que se traduz num conjunto de implicações que nem sempre são favoráveis à aplicação e aceitação da prova eletrónica-digital.

Por um lado, esta imaterialidade traduz-se numa necessidade de *know-*how altamente específico da parte dos investigadores ou responsáveis pela recolha da mesma, que deverão estar dotados das técnicas e conhecimentos científicos específicos para dar uso a palavras-chave ou servir-se de técnicas de cifração de informações, implicadas pela Criptografia, por exemplo.

Numa análise pragmática, torna-se claro que fica aqui implícito um gasto em formação dos investigadores no âmbito do Processo Penal, e um maior esforço de atualização naquela que é a compreensão do funcionamento destas novas técnicas, em geral.

Aliada a esta imaterialidade acresce ainda a noção da dispersão/distribuição da prova por vários terminais, computadores e redes que, no advento da Era Digital, não conhecem qualquer tipo de fronteira. Isto implica uma adaptação com o caráter difuso e disperso da informação, que deverá implicar uma análise estruturada e atempada, comparando vários períodos temporais, permitindo aceder à prova digital de maior utilidade para a investigação.

[165] FERNANDÉZ, J. Mª Illán, "La prueba eletrónica...", 1ª Edição, Thomson Reuters, 2009, p.287.

A disposição incorpórea dos dados implica a necessidade de reprodução para estes serem apreendidos, o que se traduz na extensão das durações dos atos processuais em que são expostos, pelo que isso implica alguma resistência por parte de juízes na sua utilização.

1.5.4. Dificuldade de atribuição de Pertinência

A falta de previsão legal que se verifica na maioria dos países implica uma grande dificuldade na delineação da pertinência, utilidade ou licitude das provas eletrónicas, especialmente no que respeita à fase de audiência prévia.

Segundo ILLÁN FERNANDÈZ, no que concerne ao espaço europeu, pode-se considerar que a prova eletrónica se encontra limitada de uma forma restringida e estrita[166].

Por "limitação restringida", entendemos o conjunto de países que estabelece amplos critérios de admissibilidade da prova e, consequentement, restringe ou limita a possibilidade de o órgão jurisdicional travar a admissão da prova eletrónica[167].

Já por limitação estrita, é-nos possível delinear os países em que a legislação processual regula de forma concreta a admissão dos meios probatórios eletrónicos e digitais, as suas particularidades procedimentais, a sua eficácia e a sua valoração[168].

1.5.5. Perspetiva Geral

A fim de assegurar que as provas são admissíveis, o tribunal deve considerar-se satisfeito caso as provas sejam cientificamente relevantes, autênticas, fiáveis e obtidas dentro dos trâmites da legalidade, em consonância com os princípios orientadores da prova em processo civil no nosso ordenamento.

Assim, têm-se verificado esforços para harmonizar processos e atividades forenses digitais, abordando as questões técnicas e jurídicas relativas à admissibilidade de provas digitais. Contudo, torna-se claro que continua a não existir uma estrutura facilmente replicável e estandardizada que facilite a admissão da prova digital em procedimentos e processos legais

[166] FERNANDÉZ, J. Mª Illán, "La prueba eletrónica...", 1ª Edição, Thomson Reuters, 2009, p.281.
[167] Exemplos concretos são os da Áustria e os países escandinavos (Dinamarca, Finlândia e Suécia), confome nos indicam em FERNANDÉZ, J. Mª Illán, "La prueba eletrónica...", 1ª Edição, Thomson Reuters, 2009, p.281.
[168] Exemplos concretos são a Espanha, a Itália, a França e a Alemanha, conforme nos indicam em FERNANDÉZ, J. Mª Illán, *"La prueba eletrónica..."*, 1ª Edição, Thomson Reuters, 2009, p.281.

continua a não ser abordada numa perspetiva holística a nível de investigação[169] e a nível jurisprudencial.

1.6. Dificuldades da prova digital

Se no ponto anterior se fez um elencar de problemas inerentes a questões técnicas e jurídicas que são problemáticas na utilização da prova digital no Direito Processual, neste ponto dar-se-á uma pequena perspetiva mais prática, na qual se analisam défices do atual sistema e problemas de interpretação deste tipo de prova.

1.6.1. Infoexclusão/Sistemas Obsoletos

Verifica-se uma falta de conhecimento generalizada dos juízes no que concerne à prova digital, notória por ser comum pedirem todas as informações contidas nos dispositivos, sem tomarem em conta o desafio imposto pelos grandes volumes de dados armazenados nos mesmos. A isto acresce o facto de que o sistema judicial não se encontra munido dos meios técnicos capazes de levar a cabo a análise de alguns tipos de sistemas e dispositivos eletrónicos.

As autoridades competentes não estão, por norma, habilitadas a proteger ou usar provas digitais para preservar a *chain of custody* e, posteriormente, a admissibilidade dessas provas em tribunal, o que coloca em causa quer os métodos, quer a admissibilidade de novas técnicas de recolha de provas.

A isto acresce a problemática de a maioria dos departamentos judiciais, policiais e jurisdicionais não estarem munidos de número suficiente de trabalhadores para processar e controlar o volume de provas digitais, independentemente das ferramentas utilizadas. Isto traduz-se em grandes atrasos e em processos morosos, fruto da inexistência de ferramentas adequadas para representar conjuntos de dados complexos de maneira compreensível para efeitos de investigação e de apresentação dos mesmos. Da mesma forma, as mudanças constantes do paradigma tecnológico tornam muito difícil uma adaptação destes departamentos a estes novos meios, pelo que o conceito de *"inovação técnica*" é altamente relativo, e ainda mais complicado de se atingir.

[169]ANTWI-BOASIAKO, Albert e VENTER, Hein, *"A model for digital evidence admissibility assessment"*, p.1.

A admissibilidade dos resultados da análise de provas digitais pode ser facilmente posta em causa no tribunal nos casos em que a extração e a análise em si não são sejam efetuadas com recursos às ferramentas mais recentes e adequados. Isto acontece em casos de dados provenientes de dispositivos eletrónicos como telemóveis, em que a captura ampla de um conjunto de elementos pode levar à acumulação de dados inúteis que confundam e atrasem a investigação. Da mesma forma, as imagens gravadas por câmaras de circuito fechado de televisão (CCTV) são altamente falíveis, visto que existem ferramentas limitadas para avaliar e processar evidência[170]s. A situação agrava-se quando se torna necessário gerir vários fluxos de informação deste tipo ao mesmo tempo durante investigações de grande porte, pois a gestão desta quantidade astronómica de dados pode ser morosa e infrutífera.

Outro problema manifesta-se com alguns dispositivos GPS, disponíveis no mercado, que usam tecnologias proprietárias de software e acesso que dificultam a extração de dados durante as investigações, particularmente devido às restrições levantadas pelo RGPD.

Casos em que seja necessário o acesso a Históricos de dados públicos (por exemplo, publicações do *Craigslist*[171] ou de alguma página de troca de mensagens) representam um desafio de custos para os departamentos e investigações.

1.6.2. Dificuldades de análise

Em contraste com documentos tradicionais, que possibilitam que quem os analise tenha acesso à informação a qualquer altura sem quaisquer custos adicionais (apenas se requer acesso ao documento, capacidade de leitura e de compreensão do idioma em que o texto se encontra escrito), os dados em formato eletrónico estão dependentes de questões de hardware e software, precisando de ser transpostos em formatos passíveis de serem lidos por humanos para poderem ser considerados úteis[172].

Da mesma forma, não é possível de criar, alterar ou atualizar documentos eletrónicos sem o hardware adequado, o que se pode tornar problemático se tomarmos em conta as dificuldades de atualização tecnológica de vários departamentos elencados no ponto anterior,

[170] ASHBY, Matthew P.J., *"The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis",* European Journal on Criminal Policy and Research, abril de 2017, pp. 4-12.
[171] Rede comunitária *online* americana que disponibiliza anúncios e fóruns de conteúdos variados.
[172] MASON, Stephen e SENG, Daniel, in *"Electronic Evidence"*, 4ª Edição, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017, p.21.

especialmente no paradigma de evolução tecnológica rápida e constante em que vivemos, que rapidamente torna sistemas operativos obsoletos e dificulta o exercício destas análises.

Isto pode implicar um resvalar numa impossibilidade de verificação absoluta dos meios eletrónicos de prova, bem como de um exercício válido do contraditório, o que traz ao de cima a possibilidade de que o órgão jurisdicional incorra num erro de valoração de uma prova, no caso de lhe dar maior fiabilidade ou credibilidade do que deve, implicando (i) uma consideração de factos falsos como sendo verdadeiros, mesmo perante outras provas mais fiáveis (que são desconsideradas perante esta má análise) ou (ii) que o órgão jurisdicional prive de valor a prova eletrónica, não a admitindo, por a considerar falsa no seu conteúdo e por não existir outro meio que se oponha a esta certeza dos factos, que poderão ser verdadeiros[173].

2. Prova Digital à Luz da Principiologia

A aplicação das novas tecnologias trouxe consigo um alargar do leque de matérias e de foros jurídicos a serem tomados em conta no âmbito dos processos, pelo que o esbater de fronteiras implica um progressivo recurso às normas e previsões do Direito Internacional.

No que concerne às novas tecnologias, o legislador está destinado a orientar-se consoante os avanços tecnológicos que, pela velocidade a que funcionam, implicam sempre um certo grau de desfasamento da lei com a realidade que se pretende regulamentar e com o processo que visa concretizar essa regulamentação.

Numa matéria tão mutável como são os princípios, conforme foi indicado no capítulo anterior, esta realidade torna-se ainda mais intensa. Não se pode negar, igualmente, que a prova eletrónica apresenta uma natureza distinta do resto das provas, entendidas no seu sentido mais convencional.

Não será de espantar, portanto, quando cada vez mais se discute o hipotético surgimento de novos princípios processuais, tais como o princípio da fiabilidade da prova

[173] FERNANDÉZ, J. Mª Illán, "La prueba eletrónica...", 1ª Edição, Thomson Reuters, 2009, pp.275-276.

eletrónica, o princípio do respeito pelos direitos fundamentais[174], o princípio da legalidade da prova eletrónica[175] ou o princípio da proporcionalidade dos meios eletrónicos ou digitais.

Para efeitos deste estudo, será pertinente fazer uma análise análoga, como exige a *analogia iuris*, daqueles que são os princípios processuais mais discutidos, e a forma como estes se interrelacionam com a prova eletrónica.

2.1. Princípio da Oralidade

Os sistemas de registo eletrónicos apresentam um conjunto de vantagens, uma vez que não implicam uma modificação da forma de realização dos atos orais, podendo, inclusive, implicar uma valoração e aproveitamento dos benefícios destes atos[176].

Por meio da gravação em formato eletrónico, torna-se possível retransmitir "em diferido" ou fazer publicidade *ex post facto*, implicando um reforço do princípio da oralidade e, na ótica de GOMEZ MARTINEZ[177], a conversão de um juiz leitor para um juiz espectador.

2.2. Princípio da Celeridade Processual

Este princípio é potenciado pelas novas tecnologias, a começar, por exemplo, com as declarações testemunhais que não se possam fazer representar em sede de tribunal. A possibilidade de uma representação em formato digital permite acautelar este leque de limitações, como é possível de inferir com a potencial utilização de gravações, que possibilita uma chance de visualizar elementos de prova as vezes que forem necessárias para o julgador.

Neste sentido, a videoconferência pode igualmente contribuir para a agilização da tramitação do processo, ao eliminar as dilações implicadas pelos auxílios judiciais em caso de residência fora do território nacional. O principal problema que esta prática implica é a necessidade de consenso relativa à sua equiparação a uma presença física de quem vá prestar declarações.

---

[174] *"Os direitos fundamentais económicos (...) têm por objecto impedir o estado de restringir ou eliminar o domínio de liberdade circunscrito por cada direito. (...) essa restrição está limitada, quer pela necessidade da sua adequação e proporção ao fim que a motivou (princípio da proporcionalidade), quer pela intocabilidade do mínimo de esfera de liberdade (princípio da intocabilidade do núcleo essencial do direito fundamental)."* - MOREIRA, Vital, *"A ordem jurídica do capitalismo"*, 1ª Edição, Caminho, Lisboa, 1973, pp. 149-150

[175] Nomeadamente, a sua consagração em texto da lei.

[176] VALENTÍN, Gabriel, *"Las nuevas tecnologías en la actividad procesal de registro"*, Revista Trilogía, Número 5, ed. Alex, 2008, pp.45-56.

[177] GOMEZ MARTINEZ, Carlos, *"La grabación del sonida y de la imagen en los juicios civiles"*, Revista Jueces para la democracia, Número 48, Madrid, 2003, p.11.

Tomando em conta a importância de testemunhos presenciais e de análises periciais no processo, a utilização das novas tecnologias apresenta-se como uma mais valia, no sentido acima explicitado, contribuindo para uma maior eficiência do exercício das funções dos peritos a quem se recorre.

No que concerne a testemunhas, há inclusive uma proteção da livre e espontânea da declaração, fruto da falta de pressões potenciadas por um ambiente eletrónico remoto, o que desde já permite clarificar e agilizar mais o processo, estando assim, o princípio da celeridade salvaguardado.

2.3. Princípio da Economia Processual

Não é difícil de inferir que o impacto das novas tecnologias implica um acesso mais fácil às informações dos expedientes, bem como uma maior facilidade no envio das informações, o que por si só, reduz os tempos de tramitação processual.

A simplicidade técnica apela ao cumprimento de um processo sem quaisquer dilações indevidas, fruto da ausência de lapsos ou incumprimentos de prazos, pela maior agilização processual e pela facilidade de acesso aos dados relevantes para avançar as fases processuais.

Para verificar impactos concretos, basta tomar em conta que, em Espanha, a utilização de suportes de gravação digital de imagem e som se repercutiu numa concentração da audiência prévia e da audiência pública num único dia[178], o que por si só corresponde a uma grande poupança de tempo e de diligências processuais.

2.4. Princípio da Boa Fé

Se o princípio de boa fé por si só implica conferir um certo grau de confiança naquela que será a boa atuação do julgador e das partes, com o progressivo recurso aos meios de prova eletrónicos, passamos a ter uma maior garantia concreta relativamente a tais comportamentos.

Colocado de uma forma muito simples, o acesso a gravações e a outros suportes digitalizados implica um registo imparcial e claro de atos e factos, insuscetíveis de relativização circunstancial, por estarem gravados da exata forma em que aconteceram.

[178] FERNANDÉZ, J. Mª Illán, "La prueba eletrónica...", 1ª Edição, Thomson Reuters, 2009, p.310.

Torna-se assim, por um lado, muito mais difícil haver arbitrariedade do juiz naquela que será a sua decisão, bem como das partes, no apresentar das suas declarações, dificultando a mentira.

2.5. Princípio do Contraditório

O princípio do contraditório, conforme mencionado no ponto 6.6 do capítulo I, consiste no direito das partes em se oporem a um ato realizado pela contraparte, pressupondo-se um patamar de igualdade entre ambas, de forma a que nenhuma se encontre indefesa perante a outra.

A partir do momento em que o legislador autorize a utilização de quaisquer outros meios para comprovar a exatidão e autenticidade dos documentos eletrónicos, este princípio, no que respeita à prova eletrónica, estará salvaguardado.

2.6. Princípio da Publicidade

Este princípio pode-se considerar cumprido na sua génese, uma vez que a facilidade de envio de ficheiros, especialmente tomando em conta os sistemas de *cloud computing* e o acesso que as plataformas dos vários órgãos estatais permitem ao geral da população.

É razoável considerar que é muito mais simples para as partes conhecer os atos levados a cabo dentro do processo (publicidade interna) e que terceiros ou interessados lhe tenham acesso pelos meios adequados (publicidade externas)[179]; uma vez que estes são disponibilizados em plataformas adequadas para o efeito (em Portugal, o Portal CITIUS, por exemplo), acessíveis às entidades relevantes (mandatários judiciais, na sua maioria).

3. Direito Probatório Digital Comparado

Os vários ordenamentos jurídicos reagiram de forma distinta ao desafio colocado pela prova digital e o processo civil eletrónico. Enquanto que alguns sistemas introduziram nova legislação para tratar especificamente desta temática, outros sistemas procuraram ligar a prova

[179] DIAS, Wladimir Rodrigues, *"Princípio da publicidade e comunicação estatal"*, ALMG, pp. 1-15.

digital aos meios de prova pré-existentes, e aplicando as regras pré-existentes da prova de forma análoga. A maioria dos sistemas adota uma combinação de ambas as estratégias, sendo que a ênfase se encontra nas diferenças entre formas de prova digitais e tradicionais.

Assim, cabe-nos fazer uma análise comparativa não só entre a abordagem adotada pelos ordenamentos jurídicos, mas também entre as principais diferenças entre os sistemas de *"Civil Law"* e os de *"Common Law"* no que diz respeito a estes fenómenos jurídicos.

3.1. Sistema de "Civil Law" v. Sistema de "Common Law"

"Common Law" diz respeito aos países baseados no Direito anglo-saxónico ou provenientes da sua corrente, sendo que exemplos preponderantes são os Estados Unidos da América, o Reino Unido, a Irlanda, a Austrália, a Nova Zelândia, o Canadá, a Índia, Singapura, Israel, entre outros.

"Civil Law", também conhecida por "direito continental", diz respeito aos países cujos ordenamentos jurídicos se basearam no Código Civil Francês ou Alemão.

No sistema de "Common Law, as novas tecnologias da informação aplicadas no processo civil já o estão a transformar, conforme é possível de observar na realização e registo dos atos de iniciação, de comunicação, de prova ou de decisão[180]. Assim, a atividade de informação efetuada pelos tribunais por meio de páginas *web*, relativamente ao seu funcionamento, a normas aplicáveis e decisões judiciais de relevo, evitará consultas de rotina e alcançará uma maior compreensão e aceitação por parte dos utilizadores do serviço de justiça na busca de uma justiça "mais humana".

A incorporação das tecnologias nos países e *"Civil Law"* foi levada a cabo de forma normativa, por meio de leis devidamente consagradas, enquanto que a nível de *"Common Law"* se incorporou as tecnologias com maior velocidade e intensidade, fruto de um processo mais pragmático e progressivo, o que explica a distinção entre os dois sistemas.

[180] FERNANDÉZ, J. Mª Illán, "La prueba eletrónica...", 1ª Edição, Thomson Reuters, 2009.

3.2. Ordenamentos Jurídicos

3.2.1. Europa

Portugal

A discussão do valor probatório dos documentos eletrónicos, no que diz respeito ao paradigma nacional, encontra a sua génese com a doutrina de RIBEIRO MENDES (1991), sendo seguida de análise por parte de autores como TEIXEIRA DE SOUSA[181] (1999), que cedo reconheceram a atribuição de valor probatório aos documentos eletrónicos como uma inevitabilidade, procurando defini-los num sentido amplo (aquele que é elaborado na sua forma definitiva em suporte de papel, ou equivalente, por um computador) e estrito (aquele que se encontra gravado de forma digital num suporte magnético ou magneto-ótico).

No que dizia respeito ao tratamento da privacidade de dados, Portugal foi altamente progressista na redação do artigo 35º da CRP, no que se trata de atos processuais, fazendo uma quebra paradigmática com as normas em vigor durante grande parte da vigência do CPC de 1961 (nomeadamente o seu artigo 138º nº5[182]), que confundiam a execução de atos ou peças processuais com o tratamento informático de dados sem nunca abordarem o valor probatório (ou não) dos meios utilizados.

Não obstante, tornou-se inegável aos órgãos governamentais portugueses o impacto da informática e do comércio eletrónico na atuação das pequenas, médias e grandes empresas[183].

Um ponto de viragem sério na interação de Portugal com as novas tecnologias da informação e, consequentemente, a regulamentação dos documentos eletrónicos, foi precisamente a Resolução do Conselho de Ministros 115/1998, responsável pela criação da *"Iniciativa Nacional para o Comércio Eletrónico"*.

Visando criar um quadro normativo que disciplinasse a legislação aplicável aos documentos eletrónicos, foi publicado o Decreto-Lei 290-D/1999, responsável por regulamentar a validade e eficácia e o valor probatório dos documentos eletrónicos e das assinaturas digitais e

[181] TEIXEIRA DE SOUSA, Miguel, *"O Valor Probatório dos Documentos Eletrónicos" in "Direito da Sociedade da Informação – Volume II"*, Coimbra Editora, 2001, pp.171-201.
[182] Permite-se *"o uso de meios informáticos no tratamento e execução de quaisquer atos ou peças processuais, desde que se mostrem respeitadas as regras referentes à proteção de dados pessoais e se faça a menção desse uso."*.
[183] AMARAL, Paulo Osternack, *"Provas: atipicidade, liberdade e instrumentalidade"*, 2ª edição, Thomson Reuters, 2017, pp.192-193.

eletrónicas. Alterado ao longo dos anos para estar em conformidade com as diretivas europeias, o seu impacto foi marcadamente significativo.

De forma muito sucinta, com o Decreto-Lei 290-D/1999, tornou-se possível estabelecer as diretrizes relativamente à força probatória dos documentos eletrónicos em Portugal, estabelecendo-se como requisitos de força probatória de documento particular assinado[184] (i) a presença de uma assinatura eletrónica qualificada certificada por uma entidade de credenciação autenticada (hoje, haverá que fazer referencia aos critérios estabelecidos no Regulamento 910/2014, ou seja terá de ser uma assinatura eletrónica avançada criada por um dispositivo qualificado de criação de assinaturas eletrónicas e que se baseie num certificado qualificado de assinatura eletrónica) e (ii) a possibilidade de representação como declaração escrita do documento eletrónico. Daqui se retira uma tripla presunção[185] de identificação (quem assina é titular da assinatura), confirmação (quem assina manifesta a sua vontade de assinar) e de autenticidade (o documento não foi alterado).

A legislação acautelou a eventualidade de o documento eletrónico não ser suscetível de representação escrita, atribuindo-lhes prova plena dos factos (caso não sejam impugnados na sua exatidão), nos termos do artigo 368º do Código Civil[186] e do artigo 167º do Código de Processo Penal[187].

Caso haja ausência de uma assinatura eletrónica qualificada, o documento será apreciado nos termos gerais de direito.

Perante a ausência de uma assinatura eletrónica qualificada, caso seja convencionado pelas partes ou haja aceitação pelo sujeito a quem o documento vá ser oposto, a autoria e integridade do documento serão objeto de prova.

[184] O artigo 7º do Decreto-Lei 290-D/1999, na redação atribuída pelo Decreto-Lei 62-D/1999, equipara a "assinatura eletrónica qualificada aposta a um documento eletrónico" com a "assinatura dos documentos com forma escrita sobre suporte de papel".

[185] SAMPAIO, José Mª Gonçalves, *"A prova por documentos particulares: na doutrina, na lei e na jurisprudência"*, 3ª edição, Coimbra: Almedina, 2010, pp. 113-114 e 159-160.

[186] As reproduções fotográficas ou cinematográficas, os registos fonográficos e, de um modo geral, quaisquer outras reproduções mecânicas de factos ou de coisas fazem prova plena dos factos e das coisas que representam, se a parte contra quem os documentos são apresentados não impugnar a sua exatidão.

[187] As reproduções fotográficas, cinematográficas, fonográficas ou por meio de processo eletrónico e, de um modo geral, quaisquer reproduções mecânicas só valem como prova dos factos ou coisas reproduzidas se não forem ilícitas, nos termos da lei penal.

Alemanha

A Alemanha é um caso de análise pertinente, uma vez que, ainda que tenha sido o primeiro país a levar a cabo a regulamentação dos aspetos jurídicos da assinatura eletrónica enquanto instrumento probatório, se encontre, nas palavras de GOTTWALD[188], numa fase de "hiperinformalização", fruto de elevados custos de automatização e de uma ausência de consciencialização dos juízes e advogados alemães relativamente à necessidade de implantar o processo civil eletrónico na Alemanha.

Não obstante, esta consideração da lei alemã deve ser feita em consonância com o Regulamento 910/2014, que se aplica em toda a União Europeia.

França

A França foi um dos países pioneiros na inclusão do documento eletrónico no seu ordenamento jurídico, sendo certo que, já na década de oitenta, com a Lei 80/525 de 12 de julho de 1980, estabeleceu que o documento eletrónico, caso cumpra os requisitos de inalterabilidade e durabilidade, possui o mesmo valor probatório que o documento em suporte escrito e assinado.

No início do milénio, por meio da Lei 230/2000 de 13 de março de 2000, assiste-se a uma forte clarificação relativamente à adaptação do direito probatório às novas tecnologias da informação e à assinatura eletrónica, como o indica o artigo 1316.1 do Código Civil francês, que estabelece que:

"O [documento] escrito em formato eletrónico é admitido como prova, da mesma forma que o [documento] escrito em papel, desde que a pessoa de quem emana possa ser devidamente identificada, e que [o documento] esteja estabelecido e preservado em condições que permitam garantir a sua integridade"[189].

Por consequência disto, no ordenamento jurídico francês e na jurisprudência francesa, os documentos, independentemente do formato ou suporte em que sejam emitidos (mesmo em caso de cópias de originais), gozam de validade e eficácia, sempre que se garanta a sua autenticidade, integridade e conservação.

---

[188] GOTTWALD, P., *"Congresso Mundial de Direito Processual"* (Brasil), 16-20 de setembro de 2007.

[189] *"L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité"*

Não obstante, esta consideração da lei francesa deve ser feita em consonância com o Regulamento 910/2014, que se aplica em toda a União Europeia.

Espanha

É com a *"Ley Orgânica"* 16/1994, durante a reformação da Lei Orgânica do Poder Judicial espanhol de 1994 que se começa a assistir às primeiras previsões de adaptação do processo civil aos desafios tecnológicos e informáticos. Esta lei, no seu artigo 230º reconheceu que os tribunais poderiam recorrer a meios técnicos, eletrónicos, informáticos e telemáticos, os termos da Lei Orgânica de Proteção de Dados.

No seu seguimento, o Regulamento 5/1995, de 7 de junho, procedeu à regulamentação da aplicação dos sistemas informáticos da Administração e da Justiça espanhóis, frisando a necessidade de compatibilizar os programas informáticos, de forma a que os dados eletrónicos se arquivassem, processassem e movimentassem de acordo com as normas de seguranças definidas pela legislação espanhola.

Todo este processo de regulação culminou com a promulgação do Real Decreto 84/2007, de 26 de janeiro, relativamente à implementação de um sistema informático de telecomunicações na administração da justiça, denominado de LEXNET.

A *"Ley de Enjuiciamento Civil"* espanhola, no seu artigo 299º, clarifica os diversos meios de prova passíveis de admissão no contexto jurídico, entre os quais consta o suporte eletrónico, ao mencionar que *"também se admitirão, nos trâmites da lei, os meios de reprodução de palavras, sons e imagens, bem como os instrumentos que permitem arquivar e conhecer ou reproduzir palavras, dados, cifras e operações matemáticas levadas a cabo com fins claros, relevantes para o processo"*[190].

Assim, os documentos eletrónicos são passíveis de serem apresentados enquanto provas no âmbito do processo civil. Ressalva-se, contudo, que o valor de tal prova, independentemente de conter conteúdo público ou privado, dependerá da não adulteração dos mesmos. A parte contrária pode contestar os documentos eletrónicos apresentados, o que exigirá um teste de especialistas, de forma a determinar a sua autenticidade.

[190] *"También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso."*

Ocasionalmente, é possível que o teste eletrónico não seja diretamente concretizado, devido a problemas organizacionais e instrumentais, sendo, portanto, aconselhável imprimir este teste para apresentá-lo como um documento de referência, indicando o arquivo autêntico e original (artigo 265.2º da *Ley de Enjuiciamento Civil*) e, assim, facilitar a acessibilidade ao Juiz.

Assim, ainda que avançando de forma lenta, pode-se comprovar uma atualização do ordenamento jurídico espanhol, bem como uma implementação das novas tecnologias no domínio probatório, ainda que este padeça de um conjunto de problemas, como é a sua dificuldade em distinguir entre fontes e meios de prova eletrónicos[191].

Não obstante, esta consideração da lei espanhola deve ser feita em consonância com o Regulamento 910/2014, que se aplica em toda a União Europeia.

Itália

Na doutrina italiana, fica estabelecido que qualquer meio probatório não tipificado na lei se denomina de *"prova atípica"*. Neste leque incluem-se os vários meios de prova em suporte digital, o que não implica uma menor eficácia probatória em relação às provas documentais tipificadas na lei.

De facto, no ordenamento jurídico italiano, a eficácia probatória passa pela satisfação dos requisitos de existência, validade e eficácia das mesmas, sendo a valoração dos meios de prova tida em conta de acordo com o contexto de cada processo em causa. Assim, é dada uma maior valorização ao impacto do meio de prova na resolução do litígio e à sua respetiva transposição para trâmites processuais.

Inicialmente concebido no âmbito penal, o documento eletrónico (ou "documento informático") do ordenamento jurídico italiano encontra-se definido[192], regulamentado e previsto no *"Codice dell' Amministrazione Digitale"* (doravante CAD), instituído pelo Decreto-Lei 82, de 7 de março de 2005[193].

[191] FERNANDÉZ, J. Mª Illán, "La prueba eletrónica...", 1ª Edição, Thomson Reuters, 2009, p.243.

[192] O artigo nº1 p) do CAD define-o como sendo a representação informática de atos, factos ou dados juridicamente relevantes (*"la rappresentazione informatica di atti, fatti o dati giuridicamente rilevant"*).

[193] Nesse ponto, devemos ter em atenção que, na Itália, a primeira lei que admitiu documentos informáticos e telemáticos ("*sono validi a tutti gli efetti di legge"*) foi a Legge nr. 59 de 15/3/1997, consultável em http://www.ordineingegneri.bergamo.it/Novita/cciaa/leggi.htm e https://www.privacy.it/archivio/dpr1997-513.html.

O CAD transpôs diversas indicações contidas na Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, respeitantes aos certificados qualificados e ao certificador[194], bem como ao valor jurídico da assinatura qualificada e da assinatura digital[195] e as regras de segurança das mesmas[196].

Dentro do CAD, prevê-se as assinaturas eletrónicas e assinaturas digitais (reconhecidas como elementos satisfatórios do requisito da forma escrita[197]) sendo estas últimas baseadas num sistema de chaves assimétricas (chave pública e chave privada) e empregues pelo sistema italiano como garante da procedência e autenticidade do documento[198].

Num sistema no qual a eficácia probatória do documento eletrónico se encontra proporcionalmente relacionada com o grau de segurança a que está submetido, é fácil de escalonar a forma como os documentos eletrónicos vão sendo organizados.

Assim, (i) assinaturas digitais ou assinaturas eletrónicas equiparadas assumem eficácia probatória de prova legal, presumindo-se a titularidade de quem a assina[199]; (ii) assinaturas eletrónicas simples implicam uma valoração objetiva pelo juiz, que irá considerar as características objetivas de qualidade e segurança[200] e (iii) a ausência de assinatura implica uma livre valoração judicial, nos termos do artigo 2.712 do Código Civil italiano, podendo, ou não, ser impugnado.

O ordenamento jurídico italiano também se pauta por conferir eficácia probatória ao envio telemático do documento eletrónico, sendo esta equivalente a uma notificação por meio postal cujas datas serão oponíveis a terceiros, caso preencha requisitos de segurança.

Reino Unido

Desde o "*Civil Evidence Act"* de 1968 que o documento eletrónico foi introduzido no processo britânico, apesar de, até meio da década de 90, se ter verificado uma grande resistência do ordenamento jurídico britânico no que dizia respeito à admissibilidade de documentos eletrónicos como elementos de prova em tribunal, em grande parte devido à

[194] Artigo 1°, I, f) do CAD.
[195] Artigo 21°, IV, a) e artigo 26° do CAD.
[196] Artigo 35° do CAD.
[197] INFANTINO, Daniela, *"Le prove civili",* Torino: G. Giappichello, 2012, pp.176-177.
[198] Artigo n°1 Decreto Presidencial 445/2000
[199] GRAZIOSI, Andrea, *"Premese ad una teoria probatória del documento informatico"* in *Rivista trimestrale di diritto e procedura civile n°2 (anno LII)*, 1998, pp.514-515.
[200] NOVARIO, Filippo*, "Le prove informatiche nel processo Civile"*, Torino: G. Giappichelli, 2014, p.79.

"Hearsay Rule". Este princípio, altamente característico do sistema de "*Common Law"*, proíbe a admissão de depoimentos ou documentos probatórios atinentes a confirmação da veracidade dos factos quando as declarações nestes contidas provêm de um interlocutor terceiro que não pode testemunhar relativamente a tais declarações em tribunal.

Apenas com o "*Civil Evidence Act"* de 1995 é que o processo civil britânico deixou de ficar sujeito a tal proibição, sendo que o processo penal continua sujeito à "*Hearsay Rule"*. De acordo com a *"Best Evidence Rule"*, um documento poder-se-á fazer valer em juízo apenas na ausência do original[201].

União Europeia

A atuação das instituições europeias em matérias de assinaturas eletrónicas e digitais e do seu reconhecimento legal enquanto certificadoras do valor probatório de documentos eletrónicos data de dezembro de 1999, com a aprovação da Diretiva 1999/93/CE do Parlamento Europeu e do Conselho da União Europeia[202], que instituiu aquele que seria o quadro legal comunitário da certificação eletrónica e das respetivas assinaturas eletrónicas.

Clarificando o que entende como sendo assinaturas eletrónicas e certificados, desenvolvendo cada uma destas noções com requisitos adicionais, de forma a alcançar versões "qualificadas" dos mesmos e que se repercutam em maiores garantias de segurança (visível nos seus anexos I e II, referentes aos certificados eletrónicos qualificados). Consequências retiráveis destas regulamentações encontram-se plasmadas no artigo 5º da Diretiva, que estabelecem que uma assinatura eletrónica avançada baseada em certificado qualificado é (i) equiparável a uma assinatura manuscrita, (ii) admissível como meio de prova para fins processuais e (iii) funciona como impedimento à negação da eficácia probatória das assinaturas eletrónicas sem certificado qualificado ou não concebidas com base num dispositivo seguro de criação.

Com a entrada em vigor do Regulamento 910/2014, a Diretiva é revogada, instituindo-se um novo regime de assinaturas eletrónicas, no qual se destaca a assinatura eletrónica qualificada, cujo regime de validade se encontra consagrado nos artigos 32º e 26º do Regulamento em causa.

[201] Apesar de já existir jurisprudência na qual se rejeitou o princípio de "Best Evidence" em favor de provas secundárias, caso se prove uma explicação razoável para o não recurso aos documentos originais. Exemplo jurisprudencial foi o caso *Masquerade Music Ltd & ors v Springsteen* (Court of Appeal, 10 de abril de 2001;).

[202] Consultável em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31999L0093&from=PT

3.2.2. América

Estados Unidos

Ainda que os Estados Unidos sigam o sistema de *"Common Law"*, comum nos países anglófonos, estes divergem do Reino Unido no que concerne à *"Hearsay Rule*", uma vez que admitem os documentos eletrónicos no processo civil, inclusive não carecendo de prova testemunhal do autor dos mesmos, fruto do transposto na Lei Federal com a exceção *"Business Records"*. Casos particulares de destaque a mencionar são os dos estados de Nova Iorque e da Califórnia, que exigem que o juiz se pronuncie relativamente à pertinência da prova documental eletrónica.

O ordenamento jurídico norte-americano prevê igualmente que, em caso de destruição do documento original, se confira valor probatório a cópias de documentos que tenham sido produzidas dentro do escopo de negócios por meio de um processo de reprodução fiável e durável; fruto do disposto no *Uniform Photographic Copies of Business and Public Records as Evidence Act*.

Numa perspetiva mais técnica, é de realçar que os EUA conseguem assegurar um elevado grau de proteção da privacidade no processo civil eletrónico[203], uma vez que limitam o acesso aos expedientes judiciais eletrónicos por meio de um complexo sistema de cartões e chaves eletrónicos, recorrendo a técnicas de criptografia para proteger os mais de trinta milhões de expedientes informatizados.

Da mesma forma, será relevante analisar as *"Federal Rules of Civil Procedure"*[204], que regem o funcionamento do Processo Civil nos tribunais distritais dos EUA[205]. Pautando-se por princípios de celeridade, imparcialidade e economia processual, mostraram-se adaptadas às novas necessidades impostas pelas tecnologias da informação com a sua revisão em 2007[206], na qual desenvolveram regras relativamente à descoberta eletrónica da prova. Destas regras destacamos as *Rules 34* e *35*, referentes à produção de documentos (e outras informações eletrónicas) e ao seu armazenamento para inspeção.

---

[203] TARUFFO, Michelle, *"O sistema jurídico dos Estados Unidos: Aspetos Fundmentais"*, Revista Ius et Praxis, 12 (1), versão on-line, 2006, pp.69-94.

[204] Adotadas a 20 de dezembro de 1937 por ordem do Supremo Tribunal Americano, tendo sido transmitidas ao Congresso a 3 de janeiro de 1938 e entrando em vigor a 16 de setembro desse ano (informação consultada em https://www.uscourts.gov/rules-policies/current-rules-practice-procedure/federal-rules-civil-procedure a 6 de outubro de 2019)

[205] O documento legal pode ser consultado em detalhe em https://www.law.cornell.edu/rules/frcp (consultado a 6 de outubro de 2019).

[206] Esta revisão pode ser encontrada em https://www.uscourts.gov/sites/default/files/federal_rules/FRCP12.1.2007.pdf (consultado a 6 de outubro de 2019).

Brasil

Com a Lei 11.280, de fevereiro de 2006, o legislador processual brasileiro deu os primeiros passos em munir o Código de Processo Civil Brasileiro de dispositivos orientados à compatibilização das novas tecnologias da informação com o processo tradicional, resvalando na Lei 11.419, de dezembro de 2016, na qual se informatiza o processo judicial, permitindo a tramitação eletrónica de processos e peças judiciais[207].

Seguindo a tendência global (bebendo, em particular, dos modelos europeus e do modelo argentino) em termos da segurança da informação e dos documentos, o Brasil opta pela implementação do método de criptografia assimétrica de chave pública e privada, estabelecendo o Instituto Nacional de Tecnologia de Informação como a Autoridade Certificadora principal do país[208].

Assim, o Estado Brasileiro adquiriu funções de coordenação, supervisão, auditoria e credenciamento de autoridades certificadoras[209].

Uma análise da Lei 11.419/2006, no seu artigo 11º, permite concluir que o legislador optou por não considerar o documento eletrónico como equivalente ao original, apenas lhe atribuindo o mesmo valor probatório, o que colheu a desaprovação de pate da doutrina, como é o caso de CALMON[210].

Argentina

A doutrina argentina sustenta que é possível considerar-se que o documento eletrónico é passível de constituir um objeto material, enquadrando-se na definição dada pelo Código Civil argentino, no seu artigo 2311[211], uma vez que a conversão de um documento para formato eletrónico a partir de um formato escrito não o desnaturaliza ou caracteriza enquanto coisa.

O sistema jurídico argentino considera documento eletrónico como sendo a representação digital de atos ou eventos, sendo equiparado ao documento escrito e passível de

[207] AMARAL, Paulo Osternack, *"Provas..."*, 2ª edição, Thomson Reuters, 2017, pp.196-198.
[208] Artigo 12º da MP 2.200-2/2001 do Brasil.
[209] CALMON, Petrônio, *"Comentários à lei de informatização do processo judicial"*, Rio de Janeiro: Forense, 2007, p.59.
[210] CALMON, Petrônio, *"Comentário..."*, Rio de Janeiro: Forense, 2007, p.148.
[211] *"Se llaman cosas en este Código, los objetos materiales susceptibles de tener un valor. Las disposiciones referentes a las cosas son aplicables a la energía y a las fuerzas naturales susceptibles de apropiación."*

ser assinado eletronicamente (via assinatura eletrónica simples, ou assinatura digital, de acordo com o grau de confiabilidade que se pretender)[212].

Há um elevado grau de confiabilidade atribuído à assinatura digital (como o sistema a denomina), que estabelece uma dupla presunção[213] de autoria e de integridade, tanto que a Ley 25.506 da Argentina, no seu artigo 3º, estipulou que a exigência de uma assinatura manuscrita também poderá ser satisfeita por uma assinatura digital[214].

Chile

O ordenamento jurídico chileno caracteriza-se por uma organização taxativa das leis reguladoras da prova, sendo que, segundo ILLÁN FERNANDEZ[215], o Código de Procedimento Civil chileno veio a considerar que o documento eletrónico poderá ser considerado um meio de prova caso seja analogamente enquadrável nas previsões do artigo 341º do Código de Procedimento civil chileno, atinente aos meios de prova (documentos, testemunhos, confissões, presunções legais, prova pericial, entre outras).

Peru

O Código Civil peruano, ainda que adote um conceito amplo de documento, definindo-o como *"todo o escrito ou objeto que sirva para creditar um acontecimento"*[216] (artigo 233º), faz a diferenciação entre meios de prova tradicionais e meios de prova atípicos, como o indica o seu artigo 194º, que estabelece que esses meios de prova serão apreciados de forma análoga aos meios tradicionais conforme entendimento casuístico do juiz.

Ao longo dos anos, a jurisprudência peruana, no âmbito deste artigo, tem vindo a considerar um conjunto de elementos eletrónicos (impressões, fax, suportes eletrónicos e digitais, meios audiovisuais, fotografias e radiografias, entre outras) como pertencentes a estes meios de prova atípicos

[212] AMARAL, Paulo Osternack, *"Provas..."*, 2ª edição, Thomson Reuters, 2017, p.195.
[213] QUADI, Gabriel H., *"La prueba en el processo civil y comercial"*, Buenos Aires: Abeledo-Perrot, 2011, p.873.
[214] *"Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia."*
[215] FERNANDÉZ, J. Mª Illán, "La prueba eletrónica...", 1ª Edição, Thomson Reuters, 2009, pp.386-387.
[216] *"Documento es todo escrito u objeto que sirve para acreditar un hecho".*

Uruguay

A Lei 16736, de 5 de janeiro de 1996, no seu artigo 697[217], consagra que no ordenamento jurídico uruguaio, haja uma equiparação dos meios informáticos aos meios tradicionais de prova, reconhecendo-lhes validade jurídica e valor probatório.

Assim, não restam dúvidas de que os documentos eletrónicos são admitidos enquanto meios de prova, sendo considerados e sentido amplo, de acordo com os meios de prova admitidos pelo artigo 349 (testemunhas, perícias, inspeções, documentos, entre outros) do *"Código de Procedimiento Civil"* uruguaio[218].

3.2.3. Israel

Desde 2007 que Israel adotou o sistema *"Next Generation Court System"*, no qual se procede a uma apresentação, arquivamento e seguimento dos documentos judiciais num formato eletrónico. Assim, toda a tramitação do processo é eletrónica, com exceção do que diz respeito a audiências e vistorias[219].

3.3. Análise Comparativa

Do que é passível de inferir, partindo de uma leitura deste subcapítulo, é que de forma geral, os vários ordenamentos jurídicos não se alhearam relativamente às novas tecnologias da informação e à forma como estas se têm vindo a inserir na realidade social e jurídica. Desde já, com isto, é mais do que comprovada a pertinência e relevância do tema, tomando em conta a primazia que assume na generalidade dos ordenamentos.

De facto, o ponto comum na maioria dos países que aplicam o sistema de *Civil Law* (o qual, por ser aquele em que Portugal se insere, nos mereceu um particular interesse) parece ser uma regulamentação do funcionamento das assinaturas eletrónicas e digitais na autenticação dos documentos em formato eletrónico, como forma de atestar a sua confiabilidade e de mitigar ceticismos que possam advir das fragilidades já elencadas das provas digitais.

---

[217] *"La documentación emergente de la transmisión por médios informáticos o telemáticos constituirá de por sí documentació auténtica y hará plena fé, a todos sus efectos, en cuanto a la existência del origen transmitido".*

[218] OLIVEROS, Raúl Tavolari, *"La videoconferência como mecanismo de comparência y la garantia del debido processo"* in *"Revista Uruguaya de Derecho Procesal Número 1/2006"*, Fundación de Cultura Universitaria, Montevideo, Uruguay, pp.113-130.

[219] RABINOVICH-EINY, Orna, *"Beyond Efficiency: The Transformation of Courts Through Technology"*, UCLA Journal of Law and Technology, Volume 12, Issue I, 2008. (Consultado a 05 de outubro de 2019 em https://uclajolt.com/wp-content/uploads/2018/11/01_080424_rabinovich_einy.pdf).

Concluímos então, que, independentemente da velocidade de implementação, parece haver uma preocupação do legislador em considerar estes novos meios de prova. Cabe-nos chamar particular atenção ao exemplo do Uruguay, em particular[220], que enquadra os meios informáticos num patamar de igualdade com os meios de prova ditos tradicionais e, indo mais além, consagra-os na sua lei processual geral.

Esta ambição de inclusão da prova digital na lei processual será um dos enfoques do próximo capítulo, seja via análise do Processo Civil, seja via análise do Processo Penal, pelo que devemos retirar daqui o exemplo uruguaio para indicar que esta ideia não é sem precedentes, e que foi já posta em prática.

[220] Não devemos, contudo, descurar da menção ao ordenamento jurídico chileno que, conforme mencionado supra, apesar de não ir tão longe como o modelo uruguaio, prima por considerar que o documento eletrónico poderá ser considerado um meio de prova caso seja analogamente enquadrável nas previsões do seu código civil.

Capítulo III – A Prova Digital no Processo Civil Português

Naquele que é o Código de Processo Civil português, cuja versão mais recente foi aprovada com a Lei 41/2013, de 26 de junho, encontramos um conjunto de diferentes tipos de prova, elencados devidamente como sendo prova por apresentação de coisas imóveis ou móveis[221], prova documental[222], prova por confissão[223] das partes, prova por declaração das partes[224], prova pericial[225], prova por inspeção, prova por verificações não judiciais qualificadas e prova testemunhal[226].

Com o advento das novas tecnologias e de diferentes meios de apreensão de informação, torna-se relevante questionar até que ponto não será fulcral os tomar em conta de forma a levar a cabo um funcionamento diligente do nosso Processo Civil.

Procurando inserir a necessidade de se prever uma prova digital neste elenco de tipos de prova, devemos confrontar-nos com duas realidades: em primeiro lugar, apenas no âmbito do processo penal e do combate ao cibercrime é que se realizaram esforços por consagrar uma funcionalidade e regulamentação das provas digitais; e, em segundo lugar, que há sérias ineficiências na forma como esses esforços se materializaram.

Assim, caber-nos-á não só analisar a forma como o Processo Civil e o Processo Penal português se organizam relativamente à previsão da prova eletrónica-digital, mas também propor meios de melhoria do sistema processual por recurso às novas tecnologias, de forma a potenciar uma eventual consagração legislativa e uma mitigação de outros problemas que marcam um marasmo do nosso ordenamento.

[221] Artigo 416º e seguintes do Código de Processo Civil.
[222] Artigo 423º e seguintes do Código de Processo Civil.
[223] Prevista no artigo 352º e seguintes do Código Civil.
[224] Artigos 452º a 465º do Código de Processo Civil.
[225] Artigo 467º do Código de Processo Civil.
[226] Artigo 496º do Código de Processo Civil.

1. Status Quo do Processo Civil Português

No âmbito do terceiro capítulo deste projeto, cabe-nos começar por fazer uma breve análise da regulamentação processual e da atenção dadas à temática da prova digital no nosso ordenamento. Semelhante ao que foi desenvolvido no Ponto 3 do capítulo anterior, elencaremos o panorama atual, em comparação com os novos desafios que surgem para o Processo e para o Direito em geral, nesta nova Era Digital.

1.1. Matérias Reguladas

Naquele que é um regime geral, não é difícil concluir que a prova digital adquire uma natureza documental, pelo seu objetivo de fazer prova dos fundamentos de ação ou defesa, conforme o sugere o artigo 423º do Código de Processo Civil, referente à prova documental. Isto implica que, semelhante à prova documental, esta prova também é passível de impugnação, seja por questões de genuinidade[227] ou de ilisão da autenticidade ou força probatória[228], tal como ocorre com os restantes documentos escritos, nos termos do artigo 374º nº1 do Código Civil.

Isto levanta a questão pertinente de que um documento eletrónico poderá (ou não) ser considerado equivalente a um documento escrito. De facto, o artigo 26º do Decreto-Lei 7/2004, de 7 de janeiro, estabelece que os documentos eletrónicos valem como documentos escritos assinados caso ofereçam as mesmas garantas de fidedignidade, inteligibilidade e conservação[229] e satisfaçam os requisitos da legislação sobre assinatura eletrónica e certificação[230]. Estes requisitos encontram-se plasmados em detalhe no Decreto-Lei 290-D/99, de 2 de agosto, implicando assim uma análise articulada entre ambos estes diplomas legais, o que nem sempre é simples.

Não obstante, é notório observar que a nossa legislação, nomeadamente o artigo 34º do Decreto-Lei 7/2004 menciona que *"é permitido o funcionamento em rede de formas de solução*

---

[227] *"A impugnação da letra ou assinatura do documento particular ou da exatidão da reprodução mecânica, a negação das instruções a que se refere o n.º 1 do artigo 381.º do Código Civil e a declaração de que não se sabe se a letra ou a assinatura do documento particular é verdadeira devem ser feitas no prazo de 10 dias contados da apresentação do documento, se a parte a ela estiver presente, ou da notificação da junção, no caso contrário."* – Artigo 444º nº1 do Código de Processo Civil.

[228] *"No prazo estabelecido no artigo 444.º, devem também ser arguidas a falta de autenticidade de documento presumido por lei como autêntico, a falsidade do documento, a subscrição de documento particular por pessoa que não sabia ou não podia ler sem a intervenção notarial a que se refere o artigo 373.º do Código Civil, a subtração de documento particular assinado em branco e a inserção nele de declarações divergentes do ajustado com o signatário."* – Artigo 446º nº1 do Código de Processo Civil.

[229] Artigo 26º nº1 do Decreto-Lei 7/2004, de 7 de janeiro.

[230] Artigo 26º nº2 do Decreto-Lei 7/2004, de 7 de janeiro.

extrajudicial de litígios entre prestadores e destinatários de serviços da sociedade da informação, com observância das disposições concernentes à validade e eficácia dos documentos (...)".

Feita esta consideração, procederemos a um elencar das particularidades destes regimes e da regulamentação da prova eletrónica e do seu alcance no nosso ordenamento.

1.1.1. Valor probatório dos documentos eletrónicos

No que respeita aos formulários e outras comunicações eletrónicas (como é o caso do e-mail), ou seja, aos documentos eletrónicos, o seu valor probatório encontra-se discriminado no artigo 3º do Decreto-Lei 290-D/99, de 2 de agosto, bem como no artigo 25º do Regulamento 910/2014.

Caso se verifique a aposição de uma assinatura eletrónica qualificada (artigo 3º nº2 do Decreto-Lei 290-D/99 e artigo 25º nº2 do Regulamento 910/2014, que afirma que a assinatura eletrónica qualificada tem um efeito legal equivalente ao de assinatura manuscrita), o documento eletrónico terá valor probatório equivalente ao do documento particular assinado, nos termos do artigo 376º do Código Civil, fazendo *"prova plena quanto às declarações atribuídas ao seu autor, sem prejuízo da arguição e prova da falsidade do documento"*, sendo que os "*factos compreendidos na declaração consideram-se provados na medida em que forem contrários aos interesses do declarante; mas a declaração é indivisível, nos termos prescritos para a prova por confissão"*.

Por sua vez, a ausência desta assinatura qualificada implicará uma apreciação nos termos gerais de direito (artigo 3º nº5 do Decreto-Lei 290-D/99), o que não implica que não existam outros meios de comprovação da autoria e da integridade dos documentos eletrónicos, como o é o caso da a assinatura eletrónica não qualificada adotada pelas partes ao abrigo de válida convenção sobre prova ou aceite pela pessoa a quem for oposto o documento (artigo 3º nº4 do Decreto-Lei 290-D/99).

Esta questão da assinatura eletrónica qualificada repercute-se igualmente no valor formal conferido à comunicação de documentos eletrónicos, sendo que o artigo 6º nº3 do Decreto-Lei 290-D/99, clarifica que documentos dotados de assinatura digital, e comunicados

por meio de telecomunicação (protocolos *"standard da Internet"*) que assegurem a sua efetiva receção[231], equivalem a remessa por via postal registada**.**

Será de relevo mencionar que o artigo 6° n°2 do Decreto-Lei 290-D/99 clarifica que *"são oponíveis entre as partes e a terceiros a data e a hora da criação, da expedição ou da receção de um documento eletrónico que contenha uma validação cronológica emitida por uma entidade certificadora"*, o que ganha valor no domínio probatório, visto que permite que as partes possam opor entre si ou perante terceiros a data e hora da prática do que se encontra contido no documento eletrónico.

1.2.À Luz da Era Digital – Novos Desafios

Todo o sistema jurisdicional existe com o intuito básico de resolver da forma mais eficiente possíveis conflitos (na sua índole subjetiva e objetiva[232]) que possam surgir entre entes coletivos e/ou singulares no desenvolvimento das suas atividades pessoais ou profissionais.

De forma a levarmos a cabo uma análise organizada e coerente, precisamos de tomar em conta o contexto em que vivemos, ou seja, o da Era Digital[233], em que o conceito tradicional de indústria que a Revolução Industrial trouxe por meio da industrialização acaba por dar lugar a um novo padrão político e económico, baseado na tecnologia da informação. Fala-se inclusive de uma Quarta Revolução Industrial, que vai muito além da mecanização e da automatização.

Em tal mundo, a indústria da informação está incumbida de não apenas permitir que os indivíduos satisfaçam as suas necessidades personalizadas, mas também de simplificar os procedimentos de tomada de decisão para transações e administração, assim como de reduzir os custos, tanto para produtores quanto para compradores.

ALVIN TOFFLER, futurista e escritor norte-americano, perspetivou a História da Humanidade como dividida em "três vagas"[234], sendo cada uma referente ao principal método de subsistência das comunidades. Passando da "primeira vaga", alicerçada na agricultura; à

---

[231] Nos termos do artigo 6° n°1 do Decreto-Lei 290-D/99, o documento eletrónico comunicado por um meio de telecomunicações considera-se enviado e recebido for transmitido para o endereço eletrónico definido pelas partes (convenção expressa), sendo nele recebido. Por norma, contudo, a convenção será tácita, sendo o documento enviado para o endereço do destinatário, sendo que a resposta do destinatário indica a receção da comunicação, muito nos termos do artigo 224° do Código Civil, referente a teoria da receção na perfeição negocial; da mesma forma que o próprio n°4 do artigo 6° do Decreto-Lei 290-D/99 regula a situação dos documentos transmitidos, clarificando que os dados e documentos comunicados por meio de telecomunicações consideram-se em poder do remetente até à receção pelo destinatário.

[232] *"Subjectively, approaches to define conflict involve attempts to explain it analyzing the ways in which parties understand and behave towards each other. On the other hand, the objective aspects used to define are, roughly, those that are widely independent of the parties' perceptions (...)."* – NOVAIS, Paulo, GOMES, M., "*Conflict and its Different Dimensions"*, p.1.

[233] CASTELLS, Manuel, *A Sociedade em Rede: Do Conhecimento à Acção Política*, 2005; p.17.

[234] TOFFLER, Alvin (1980) A Terceira Onda.

segunda vaga, correspondente ao mundo da Revolução Industrial (no qual o auge setor da indústria e o apogeu do fenómeno do êxodo rural atingiram o seu expoente máximo); a "terceira vaga", correspondente à Sociedade da Informação (na qual se alicerçam as bases económicas e sociais de todo o sistema), será aquela em que nos situamos e aquela a partir da qual teremos de organizar o nosso raciocínio.

Fazendo uma análise histórica daquela que é a realidade jurisdicional e do mundo globalizado em que vivemos, não será difícil constatar que já não se vive num mundo em que os processos judiciais possam ser perspetivados como restritos a um único território nacional[235] ou até mesmo passíveis de uma representação unicamente em papel.

Quando as noções de *e-commerce*[236], *e-business*[237] e *e-procurement*[238] são uma realidade quotidiana, torna-se facilmente compreensível que a possibilidade de se efetuarem negócios e transações entre partes situadas em diferentes pontos do globo se acabou por tornar uma banalidade.

Toda e qualquer relação jurídica de natureza civil ou comercial é suscetível de originar litígios[239], pelo que não se poderá continuar a afirmar que o anterior modelo jurisdicional é capaz de acompanhar os desafios do novo milénio[240].

É nesta ótica, e por uma necessidade de afirmar de novo a confiança dos cidadãos[241] naquela que é a capacidade das entidades Estatais de assegurarem a sua segurança, bem como a melhor resolução dos litígios que entre estes possam surgir; que se torna importante perspetivar uma "aliança" as novas tecnologias e o próprio funcionamento do sistema

---

[235] *"Na verdade, o direito de acesso aos tribunais, bem como o direito de obtenção de uma decisão em prazo razoável no âmbito de um litígio transfronteiriço, impõe a adoção de regras que permitam determinar facilmente qual o tribunal competente para a resolução de um litígio, assim como o rápido e efetivo reconhecimento e execução das decisões proferidas por qualquer tribunal de um Estado Membro da União Europeia."* – GONÇALVES, Marco Carvalho, *"Integração judiciária e tutela jurisdicional dos interesses económicos e sociais",* 2016, p.3.

[236] Qualquer tipo de negócio ou transação comercial que implique a transferência de dados e informação por meio da Internet.

[237] Realização de setores chave da área empresarial por meio das novas tecnologias da informação.

[238] Em suma, a compra de bens e serviços, por meio da Internet.

[239] *"Evidently, as the number of transactions increases, the number of transactions that go wrong also increases: buyers that do not pay, objects that arrive to its destination damaged or that do not arrive at all, missing parties, among others. The current way of solving these issues is, most of the times, impracticable."* – CARNEIRO, Davide, NOVAIS, Paulo, ANDRADE, Francisco, *"On-Line Dispute Resolution"*, p.9.

[240] *"Neste enquadramento, não se compreende que, no âmbito de uma relação jurídica plurilocalizada, em que uma empresa fornece mercadorias ou presta serviços a outra e pretende obter o pagamento correlativo, seja confrontada, na falta de convenção em sentido contrário, com a obrigação de litigar junto dos tribunais do Estado-Membro onde os bens foram entregues ou os serviços prestados, e não dos tribunais do Estado-Membro do seu domicílio."* - GONÇALVES, Marco Carvalho, *"Integração judiciária e tutela jurisdicional dos interesses económicos e sociais",* 2016, p.4.

[241] *"Coincidentes com os dados referidos são os de uma outra sondagem, realizada, em abril de 2014, pelo CESOP – Universidade Católica Portuguesa e publicada no Jornal de Notícias no dia 22 de abril de 2014 (páginas 4 e 5). Neste caso, 62% dos portugueses avaliam "muito negativamente" ou "negativamente" o papel dos Tribunais nos últimos 40 anos (apenas 31% fazem uma avaliação "positiva" ou "muito positiva")."* – ABRUNHOSA, Ângelo , disponível na seguinte hiperligação (consultado a 22.07.2019).

processual. Nesta ótica, faremos nossas as palavras de TERESA COELHO MOREIRA[242] e diremos que, *"conforme a história tem vindo a demonstrar ao longo do tempo, tão curto e tão longo, as inovações tecnológicas só dependem da utilização que lhes é dada pelo homem"*.

Em suma, a Era Digital anda de mãos dadas com as mais variadas ciências, sendo que as ciências jurídicas não são nem podem querer ser uma exceção.

Com o advento das novas tecnologias e de diferentes meios de apreensão de informação, torna-se relevante questionar até que ponto não será fulcral os tomar em conta de forma a levar a cabo um funcionamento diligente do nosso Processo Civil.

2. Ausência de Regime Processual e a sua necessidade

O legislador português, na ótica de CONDE CORREIA[243], apresenta uma tendência em optar por um sistema marcado por uma complexa rede legislativa, na qual as leis gerais e as leis secundárias parecem convergir, divergir e ganhar autonomia de forma quase anárquica, pelo que, parafraseando DOHNA[244], afirma que *"a jurisprudência dificilmente conseguirá resolver a quadratura do círculo ou desatar os apertados nós que o legislador foi atando"*.

Ainda que as considerações do autor fossem dirigidas para o âmbito de Processo Penal, não é de todo descabido fazer uma ponte para o Processo Civil, até porque o que ocorre relativamente à prova digital no seu âmbito é bastante análogo, uma vez que todas as disposições relativas à mesma se encontram dispostas de forma bastante dispersa, conforme explorado no Ponto 1.2 do presente capítulo.

O que encontramos é uma ausência de menção no Código Civil e no Código de Processo Civil, sendo que apenas o Decreto-Lei 290-D/99 faz considerações de equiparação do valor probatório dos documentos eletrónicos a documentos escritos, bem como da perfeição das comunicações eletrónicas, em pontes estabelecidas com o Código Civil, de forma a que se tenha uma base de referência.

---

[242] MOREIRA, Teresa Coelho, *"Novas Tecnologias: Um admirável mundo novo do Trabalho?"*, Revista de Direitos e Garantias Fundamentais, Vitória, n. 11, p. 15-52, jan./jun. 2012, p. 17.

[243] CONDE CORREIA, João, *"Prova digital: enquadramento legal"* in *"Cibercriminalidade e prova digital: Jurisdição Penal e Processual Penal"*, Centro de Estudos Judiciários, 2018, p. 15.

[244] DOHNA, Alexander Graf zu, "Kernprobleme der Rechtsphilosophie", Gentner, 1966.

Um Processo descentralizado traduz-se numa jurisprudência altamente fragmentada, uma vez que a ambiguidade legal e as diversas fontes de leis implicarão uma maior probabilidade de diferentes leituras e diferentes perceções da parte dos juízes, o que, por si só, contribuirá para dificultar futuros processos, já que não só existirá uma divergência e ambiguidade legislativa e doutrinal, mas também jurisprudencial.

Torna-se igualmente necessário adequar o Código de Processo Civil às necessidades e aos desafios lançados pelas novas realidades tecnológicas e pelas potencialidades que são providenciadas pelas novas tecnologias da informação, especialmente tomando em conta a sua velocidade de evolução[245]. Se o leigo recorre às mesmas para celebrar os seus negócios, o sistema jurídico tem de se encontrar preparado a acompanhar litígios que delas possam surgir.

O facto de mantermos as menções aos meios de prova oriundos das novas tecnologias de informação fora daquela que é a lei processual geral, implica um menor contacto com estas, seja por parte dos aplicadores de direito, seja por parte de quem aceda à lei processual geral. Esta ausência de contacto, aliada ao tradicional ceticismo doutrinário para com novas metodologias que irrompam com as noções pré-estabelecidas, apenas se traduzirá numa maior resistência à inovação do processo e, consequentemente, no agravar de um atraso que se começa a tornar notório relativamente ao nosso ordenamento jurídico, especialmente numa ótica comparativa com outros países, como o são a Itália, a França, ou os Estados Unidos.

O ordenamento jurídico, mais do que um aglomerar de normas e decisões, reflete a mentalidade do Estado que representa, sendo que esta relação não é unilateral, conforme o dita a influência que a lei tem em mudar costumes sociais ou ideias pré-concebidas. Assim, devemos não só anuir às exigências da Era Digital e atualizar o nosso processo (seja civil, seja penal), mas também contribuir nestes avanços, por meio da influência exercida para com as futuras gerações de juristas.

[245] Exemplo disto encontra-se a nível da tecnologia de reconhecimento facial, que passou de categorizar imagens com 98% de fiabilidade, ultrapassando o padrão humano de 95%. Isto torna-se prodigioso se pensar que, a nível da criação de imagens, sistemas de Inteligência Artificial se tornaram capazes de produzir imagens sintéticas praticamente indistinguíveis em comparação com fotografias, quando há uns anos essas mesmas imagens eram profundamente irrealistas. Mais informações encontram-se disponíveis em *"The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation"*, Oxford University, 2018, p. 13.

3. Prova Digital no Processo Penal

ROGÉRIO BRAVO, no que diz respeito à eficácia da norma penal, enquanto dissuasora e preventiva do ato ilícito, identifica quatro ideias que devem ser colocadas à ponderação do legislador no advento do Direito da Informática, nomeadamente (i) o avanço tecnológico, (ii) o tempo, (iii) a "natureza" do espaço virtual e (iv) as relações deste com outros espaços de existência humana[246].

Conforme se pôde observar ao longo do projeto, e muito de acordo com a ótica de MILITÃO[247], torna-se claro que as normas referentes à obtenção da prova eletrónica-digital devem ser delineadas à luz e no quadro do regime geral de obtenção da prova, devendo gozar de uma integração no Processo Penal, sem nunca descurar das necessárias adaptações às especificidades da prova digital.

De facto, os meios de obtenção da prova eletrónica-digital, não obstante as suas particularidades, acabam por ser englobados nos tradicionais meios de obtenção de provas, seja via exames, revistas, buscas, apreensões ou interceções de comunicações.

Numa ótica de agilização processual e de investigação, é inegável que há um caráter mais simples e menos moroso para com os agentes das entidades policiais e judiciárias no que diz respeito à recolha deste tipo específico de provas; em grande parte devido à perda do caráter volátil das telecomunicações e da sua tendência em registar históricos e sinais[248].

Contudo, e tomando em conta que, segundo LOPES E CABREIRO[249], *"20% dos inquéritos em investigação ou investigados na área da criminalidade informática são concluídos com proposta de arquivamento por inexistência de elementos que permitam prosseguir a investigação"* (apesar de Relatório Anual da Procuradoria Geral da República de 2014, na ótica de MILITÃO[250], desmistificar este cenário aparentemente tenebroso), não admira que se tenha vindo a exigir que a lei processual penal deve promover o desenvolvimento de todas as ações consideradas necessárias e adequadas à obtenção de prova eletrónica-digital de forma célere e

---

[246] BRAVO, Rogério, *"As Tecnologias de Informação e a Compressão dos Direitos, Liberdades e Garantias – os efeitos das regras 10/10 e 1/1"*, Lisboa, 2012, p. 1.

[247] MILITÃO, Renato, *"A propósito da prova digital no Processo Penal"*, p. 266.

[248] COSTA ANDRADE, Manuel, *"Bruscamente no Verão Passado: A Reforma do Código de Processo Penal — Observações críticas sobre uma Lei que podia e devia ter sido diferente"*, Coimbra, Coimbra Editora, 2009, p. 156.

[249] LOPES, José Mouraz, e CABREIRO, Carlos Antão, *"A Emergência da Prova Digital na Investigação da Criminalidade Informática" in* "Sub Judice — Justiça e Sociedade, n.º 35", Almedina, Coimbra, 2006, pp. 72 e ss.

[250] "[o] número de inquéritos arquivados foi de 366.579, o que representa aproximadamente 51% do valor dos movimentados. Percentagem que atingiu 52,4% em 2007, 55% em 2008 e 53,9% em 2009" - MILITÃO, Renato, *"A propósito da prova (...)"*, p. 263.

eficaz, numa ótica de cooperação das operadoras de comunicação com investigações nos equipamentos dos arguidos; por forma a evitar as dificuldades de obtenção de provas eletrónicas-digitais que se constatam m boa parte dos crimes[251].

Da mesma forma, não têm faltado exigências de um aprimorar das entidades e técnicas de investigação criminal e da recolha deste tipo de provas, bem como da formação dos agentes nesta especialização. Clama-se, assim, por uma ciência de *"digital forensic"*, que possa orientar a investigação criminal na a preservação, recolha, gravação, validação, identificação, análise, interpretação, documentação e apresentação deste específico tipo de prova[252].

Assim, para efeitos deste subcapítulo, faremos uma brevíssima análise dos nossos instrumentos de regulação de provas digitais, no âmbito do Processo Penal, seja na forma como foram implementados, seja na sua interação com o Processo Penal.

Procuramos assim, ver que lições podemos retirar para o Processo Civil, a nível do que se deve pretender e do que se deve evitar.

3.1. Lei 109/2019

A realidade da cibercriminalidade não era um conceito alheio ao legislador português quando este elaborou a Lei 109/91 (a então Lei da Criminalidade Informática), de 17 de agosto, ainda que, não obstante, esse mesmo legislador não incluiu no texto legal um regime jurídico de recolha da prova digital, não prevendo a sua recolha durante a investigação.

Já numa perspetiva internacional se foram fazendo esforços para a consagração de um regime relativo à criminalidade informática e à prova digital, como o comprovou (i) a aprovação da Convenção sobre o Cibercrime do Conselho da Europa, que procedeu à consagração de medidas processuais de obtenção de prova digital; e (ii) a Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24/02, relativa a ataques contra sistemas de informação, e que, não obstante não compreender normas processuais, procedeu à implementação de medidas de cooperação internacional com vista à obtenção de prova digital e, genericamente, ao combate à criminalidade informática.

---

[251] SANTOS, Rita Coelho dos, *"O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos"*, Boletim da Faculdade de Direito, Coimbra, Coimbra Editora, 2005, pp. 55-56.

[252] RODRIGUES, Benjamin, *"Da Prova Penal, IV, Da Prova-Eletrónico-Digital e da Criminalidade Informático-Digital"*, Lisboa, Rei dos Livros, 2011, p. 31 e ss.

No que concerne à atuação nacional, a Convenção sobre o Cibercrime foi ratificada em Portugal com a Resolução da Assembleia da República 88/2009 e pelo Decreto do Presidente da República 92/2009, ambos publicados a 15/09.

A Lei n.º 109/2009, de 15/09, transpôs para o ordenamento jurídico português a Decisão-Quadro n.º 2005/222/JAI, do Conselho da UE., adaptando igualmente ao direito português a Convenção sobre o Cibercrime, do Conselho da Europa.

De uma forma generalista, a Lei n.º 109/2009 introduziu e ampliou diversos conceitos jurídico-informáticos, bem como os tipos incriminadores dos *cibercrimes* anteriormente previstos na Lei n.º 109/91, de 17/08 (sendo que revogou esta mesma lei) e estabeleceu o princípio da competência universal quanto à sua aplicação no espaço

Relativamente ao tema do presente projeto de tese, nomeadamente à prova eletrónico-digital, deve-se destacar que esta Lei (i) fixou diversas obrigações para terceiros, em particular às operadoras de comunicação, no que diz respeito à preservação e apresentação de prova digital, (ii) definiu várias medidas de cooperação internacional relativamente obtenção de prova digital e, acima de tudo, (iii) consagrou um regime processual penal geral de obtenção de prova digital, potencialmente dirigido a todos os crimes.

Dentro desse regime processual penal, a Lei fez questão de consagrar vários meios processuais, deveres para terceiros e mecanismos de cooperação internacional, desde a preservação expedita de dados (artigo 12.º), a revelação expedita de dados de tráfego (artigo 13.º), a pesquisa de dados informáticos (artigo 15.º), a apreensão de dados informáticos e de correio eletrónico (artigos 16º e 17º).

Conforme reiterado anteriormente, e nos termos do artigo 11º, todas estas especificidades de medidas processuais aplicam-se a todos os processos crimes (i) tipificados na lei, (ii) cometidos por meio de um sistema informático e (iii) em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico[253].

Releva apontar que as medidas, gerais ou excecionais, e obrigações previstas na Lei n.º 109/2009, cumular-se-ão ainda, salvo exceções que as contrariem, com as estabelecidas no CPP. De facto, tudo parece apontar para que esta Lei consagre um regime processual penal

[253] *"(...) as regras de direito probatório previstas no diploma não são assim meras normas processuais sobre cibercrimes ou sequer apenas relativas a crimes praticados em sistemas informáticos, mas correspondem a um regime consideravelmente mais abrangente sobre prova eletrónica em processo penal, aplicável a qualquer crime"*- DÁ MESQUITA, Paulo, "Processo Penal, prova e sistema judiciário", 1ª Edição, Coimbra Editora, Coimbra, 2010, p.98.

geral de obtenção de prova digital, o que pareceria apontar para a sua integração no Título III do Livro II CPP[254], referente aos meios de obtenção de prova, ao invés de mais um diploma especial.

Ainda que a área penal nacional se caracterize pela emanação de matérias especiais, como é o caso da criminalidade fiscal ou económica, as dificuldades de interpretação e aplicação legislativas revelam, para alguns autores[255], falta de racionalidade lógica da parte do legislador.

3.2. Interceção das Comunicações e registo de voz e imagem

Um dos tópicos que mais discussão tem implicado é, precisamente, o respeitante à interceção das comunicações, também conhecido como "regime das escutas telefónicas", relevante para efeitos deste estudo por se tratar de uma recolha de prova em suporte eletrónico, e também como forma de analisar a harmonização (ou ausência dela) feita pelo Processo Penal Português relativamente a este regime.

Antes de expormos a problemática que se segue, cremos que a génese deste problema tem natureza constitucional, visto que se encontra previsto no artigo 17.º da Constituição da República Portuguesa, o princípio da proibição do excesso, que estabelece que qualquer limitação aos direitos, liberdades e garantias (como o serão, para efeitos destas leis, o direito à reserva da intimidade da vida privada) deverá cumprir critérios de adequação, necessidade e proporcionalidade (artigo 18º nº 3 da Constituição da República Portuguesa). Neste sentido, é sempre pertinente tomar em conta a doutrina de GOMES CANOTILHO e VITAL MOREIRA[256], ao afirmarem que os *"direitos fundamentais só podem ser restringidos quando tal se torne indispensável, e no mínimo necessário, para salvaguardar outros direitos ou interesses constitucionalmente protegidos. (...) Por conseguinte, a restrição de direitos fundamentais implica necessariamente uma relação de conciliação com outros direitos ou interesses constitucionais e exige necessariamente uma tarefa de ponderação ou de concordância prática dos direitos ou interesses em conflito".*

---

[254] DÁ MESQUITA apoia a integração destas normas no Código de Processo Penal, muito na índole do ordenamento jurídico italiano, que passou por uma adaptação dos meios de obtenção de prova para prever as especificidades das disposições processuais que advêm da criminalidade informática, conforme indicado em *"Processo Penal, prova e sistema judiciário"*, 1ª Edição, Coimbra Editora, Coimbra, 2010, p.126.

[255] BARROS, Juliana Isabel Freitas, *"O Novo Processo Penal: Os Meios de Obtenção de Prova Digital consagrados na Lei 109/2009, de 15 de setembro"*, Tese de Mestrado pela Universidade de Coimbra, 2012, p. 46.

[256] CANOTILHO, J. J. Gomes, e MOREIRA, Vital, *"Fundamentos da Constituição"*, 2ª edição., Coimbra, Coimbra Editora, 1991, pp. 133-134.

Talvez com base nesta ideia de acautelar liberdades, o legislador tenha agido no sentido em que agiu, procurando fazer a maior harmonização possível entre o interesse objetivo de eficácia da investigação criminal e o interesse de proteção dos direitos fundamentais afetados, tomando em conta as particularidades da prova digital, que foram elencadas no capítulo anterior.

Consagrada no artigo 18º da Lei 109/2019, a interceção das comunicações em processos crimes encontra-se dependente de autorização por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, num leque específico crimes devidamente elencados no artigo 187º nº1 do Código de Processo Penal (estando a base genérica deste requisito transposta no artigo 18º nº2[257] da Lei 109/2019), sempre com elevados requisitos de fundamentação do âmbito da recolha no contexto da investigação concreta em causa.

Na mesma senda, o artigo 6º da Lei 5/2002, de 11 de janeiro, relativa ao combate à criminalidade organizada e económico-financeira, estabelece a admissibilidade do *"registo de voz e de imagem, por qualquer meio, sem consentimento do visado"*, mediante prévia autorização do juiz em casos específicos de crimes particularmente graves (elencados no artigo 1º dessa mesma lei). Da mesma forma que o artigo 18º da Lei 109/2019 se encontra fortemente vinculado e disciplinado pelo artigo 187º do Código de Processo Penal, também este artigo 6º da Lei 5/2002 se encontra dependente dos ditames do artigo 188º do Código de Processo Penal (relativos às formalidades das operações a serem levadas a cabo), pelo que o não cumprimento destas disposições implica uma nulidade destes elementos de prova[258].

Assim, o artigo 188º nº9 do Código de Processo Penal torna claro que apenas têm valor probatório as comunicações que (i) o Ministério Público mande transcrever ao órgão de polícia criminal responsável pela interceção e a gravação, devendo o Ministério Público também as indicar como meio de prova na acusação; (ii) que o arguido transcrever a partir de cópias de comunicações intercetadas e juntar ao requerimento de abertura da instrução ou à contestação; (iii) ou as que o assistente transcrever a partir das cópias e juntar ao processo no prazo previsto

[257] "A interceção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público."

[258] Neste sentido, ler o Acórdão do Tribunal da Relação de Lisboa de 28/05/2013, que menciona que a *"inobservância dos requisitos e condições impostos pelos artigos 187º, 188º e 189º do CPP constitui nulidade relativa de prova proibida (...)"*, bem como o Acórdão do Tribunal da Relação do Porto de 13/05/2015, referente ao processo 1/13.9PEVNG.P1, que clarifica que a *"(...) inobservância das regras do art. 188.º, do CPP, constitui nulidade que impede toda e qualquer utilização do material probatório assim obtido ? esta invalidade atinge apenas essas concretas comunicações"*.

para requerer a abertura da instrução, ainda que não a requeira ou não tenha legitimidade para o efeito.

Deve-se ressalvar que estas recolhas de informações apenas poderão ser utilizadas contra suspeitos, intermediários (relativamente aos quais haja fundadas razões para crer que recebem ou transmite mensagens destinadas ou provenientes de suspeito ou arguido) e vítimas de crime (em caso de consentimento efetivo ou presumido destas)[259], ficando proibida a interceção e a gravação de conversações ou comunicações entre o arguido e o seu defensor (exceto perante razões fundadas que façam o juiz crer que tais comunicações constituem objeto ou elemento de crime)[260].

O que fica claro é uma total ideia de "último recurso" na utilização da interpretação de comunicações, seja pelo texto do artigo 187° n°1 do Código de Processo Penal[261], seja por declarações jurisprudenciais, como é o caso do Tribunal da Relação de Évora, em 2015[262], ao clarificar ser *"possível lançar-se mão das escutas telefónicas logo como o primeiro meio de obtenção da prova utilizado, quando - e apenas nesta hipótese - o juiz de instrução se convença, em face dos concretos dados factuais trazidos pelo Ministério Público, que ela é a única diligência capaz de fazer carrear para os autos os elementos probatórios aptos à descoberta da verdade"*.

Mais do que esta noção de "último recurso", transparece-se uma postura completamente limitadora da investigação de crimes informáticos ou inclusive de crimes que impliquem uma recolha de elementos de prova digitais, inclusive porque o artigo 189° do Código de Processo Penal, após a sua reforma de 2007, faz questão de frisar que *"o disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceção das comunicações entre presentes"*.

Equiparam-se assim as escutas telefónicas às comunicações eletrónicas em gerais, ou seja, e conforme entendido por DIAS VENÂNCIO, *"falamos da interceção de mensagens de correio eletrónico em tempo real, ou seja, no seu trajeto do computador do emissor para o*

[259] Artigo 187° n°4 do Código de Processo Penal.
[260] Artigo 187° n°5 do Código de Processo Penal.
[261] *"(...)se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter (...)".*
[262] Processo 55/11.2GDSTC.E1, de 17/03/2015 (consultado a 01.08.2019).

computador do recetor através da rede de servidores. Ou ainda a interceção de mensagens trocadas através de processos de comunicação instantânea (usualmente designados por serviços de "chat", como são os casos do "IRC", do "MSN Messenger", ou do "ICQ".[263]

Esta equiparação generalizada torna-se particularmente gravosa, visto que tudo aponta para que se equipare outros suportes de informação digital, como é o correio eletrónico, ao regime das escutas telefónicas, regime esse que, pelas suas especificidades altamente restritivas, impedirá o recurso a estas fontes de informação, visto que muitos crimes não irão implicar penas superiores a três anos de prisão[264].

A doutrina e a jurisprudência[265] já manifestaram o seu profundo desagrado e sentimento de discórdia para com a forma como este artigo (e todo o regime das escutas telefónicas e interceções de comunicações está planificado) se mostra completamente desadequado ao nível de exigência conceptual no pensamento sobre a teleologia e a semântica da prova face aos novos paradigmas tecnológicos e à relevância do registo de dados[266], implicando grande incerteza e insegurança jurídicas, por englobar várias realidades distintas num ponto de três linhas[267].

3.3. Investigação - Chain of Custody (paradigma anglo-saxónico)

Fazendo uma ótica comparativa, referente a meios de aperfeiçoamento da recolha de provas digitais, torna-se interessante abordar o tópico do *chain of custody*, comum no contexto anglo-saxónico, e de grande utilidade na determinação da autenticidade documental, e, por conseguinte, relevante num conjunto de áreas, das quais se destaca a investigação, especialmente se houver possibilidade de os litigantes usarem dados analíticos ou conclusões que usem os dados mencionados supra em litígios[268].

Isto sucede devido ao facto de o processo de aquisição de dados ser eletrónico, pelo que, tanto os elementos de prova, como o processo em si poderão estar sujeitos a diversos desafios no panorama jurídico, implicando novos meios de autenticação, ferramentas forenses, entre outros.

---

[263] VENÂNCIO, Pedro Dias, *"Lei do Cibercrime: Anotada e Comentada"*, 1ª edição., Coimbra, Coimbra Editora, 2011, p. 119

[264] Requisito do artigo 187º nº1 do Código de Processo Penal.

[265] Neste sentido, ver os acórdãos 08.1PBGMR – A.G1, do Tribunal da Relação de Guimarães, de 12/10/2012 e 896/07.5JAPRT.P1, do Tribunal da Relação do Porto, de 27/1/2012; que recorrem a aplicações *contra legem* destas disposições legais.

[266] MESQUITA, Paulo Dá, *"Processo Penal, Prova e Sistema Judiciário"*, 2010, Coimbra, Coimbra Editora, p. 89.

[267] ANDRADE, Manuel da Costa, *"Bruscamente no verão passado - a Reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente"*, Coimbra Editora, Coimbra, 2009, pp. 185-186.

[268] *2017 QAQ Quality Assurance Manual*, Chapter 10 Revision No. 8 December 31, 2017, p.1.

Uma vez que estamos a abordar questões de integridade de meios de prova e dos seus meios de obtenção, e que uma parte essencial de qualquer processo de análise de dados é a de garantir a integridade da amostra recolhida, não nos podemos esquecer que a garantia de integridade dos meios de prova digital ao longo do processo apresenta problemas diferentes daqueles encontrados ao lidar com provas físicas ou documentais ditas "tradicionais", sendo que alguns problemas mais simples que neste segundo grupo se encontrariam são exacerbados pela complexidade dos computadores em rede[269].

Encaramos a *chain of custody* como sendo um procedimento no tratamento das provas ao longo de uma série de investigações, encarregue de garantir a admissibilidade das provas pelo sistema judicial, dando resposta às questões de *"onde, quando, por que, quem, como?"* em qualquer etapa do processo de investigação[270].

A *chain of custody* exige que, a partir do momento em que todos os elementos de prova são recolhidos, qualquer transferência desses dados para terceiros seja documentada e que haja um elevado grau de probabilidade que mais ninguém lhes tenha acedido, o que restringe e controla o número de transferências a partir desse ponto, evitando e desencorajando manipulações no material obtido.

Assim, caso se coloque em causa a autenticidade da prova, poder-se-á provar um nexo de causalidade da mesma com a investigação e o litígio em questão. Perante esta análise, caso se verifiquem discrepâncias e se tornar impossível associar os elementos de prova ao caso em concreto, a *chain of custody* será quebrada e a prova resultante será muito provavelmente não admitida.

[269] GIOVA, Giuliano, *"Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems*", IJCSNS International Journal of Computer Science and Network Security, VOL. 11 nº 1, Janeiro de 2011, pp. 1-5.
[270] YUDI PRAYUDI, SN, Azhari, "*Digital Chain of Custody: State of the Art"*, International Journal of Computer Applications (0975 – 8887), Volume 114 – No. 5, 2015.

3.3.1. Processo de *"chain of custody"*

Fase 1 - Avaliação

A fase de avaliação de provas digitais estabelece a base legal da prova digital a ser analisada em si, abordando as questões preliminares relacionadas com a sua admissibilidade legal e fornecendo os fundamentos para uma análise mais aprofundada das provas digitais em questão. Geralmente, as provas digitais são consideradas inadmissíveis se não cumprirem os requisitos impostos nesta fase importante.

Em jeito de exemplificação, quando a prova respeitante ao conteúdo contido num disco rígido, pertencente a um sujeito alvo de investigação, é apresentada em tribunal, a primeira preocupação do tribunal será a de determinar a base legal para a apreensão do disco rígido. Na maioria das jurisdições, uma ordem judicial pode satisfazer esse requisito, sendo que algumas políticas e protocolos organizacionais também podem fornecer a base para a autoridade legal em causa[271].

Fase 2 – Análise dos Requisitos Técnicos[272].

Esta fase diz respeito aos padrões e requisitos técnicos que sustentam a admissibilidade de provas digitais com base no manuseio e processamento de provas digitais, sendo este procedimento levado a cabo em três fases após a base legal da prova ter sido estabelecida.

(i) **Pré-requisito**: A serem considerados antes que qualquer atividade técnica principal seja conduzida, os requisitos desta fase incluem o modelo forense digital, a ferramenta, o analista / especialista e os requisitos e avaliações do laboratório.

(ii) **Requisitos Básicos**: Afetando significativamente a determinação da admissibilidade da prova digital, dizem respeito a requisitos e avaliações de verificação de cadeia de custódia e da integridade técnica[273].

[271] PRAYUDI, Yudi, SN, Azhari, "Digital Chain of Custody: State of the Art", International Journal of Computer Applications (0975 – 8887) , Volume 114 – Nº. 5, março de 2015, pp. 1-2.
[272] https://thecybersecurityplace.com/digital-forensics-the-essential-chain-of-custody (Consultado a 13 de outubro de 2019).

(iii) **Requisitos Pós-requisitos**: Esses requisitos aprimoram ou clarificam os requisitos nas duas categorias anteriores, dizendo respeito testemunhas especialistas em relatórios periciais digital e relatórios de requisitos e avaliações.

Este foco nos requisitos técnicos e nas considerações da prova digitais tem grande relevância no processo penal anglo-saxónico, uma vez as conclusões judiciais se baseiam maioritariamente nos resultados desta avaliação.

Fase 3 – Conclusões Judiciais

A fase final serve como forma de sustentar decisões judiciais no que concerne à determinação da admissibilidade e do peso da prova digital, com base nos resultados da avaliação dos requisitos técnicos mencionados supra, sendo que cada critério técnico tem um impacto específico na prova.

Considerando um exemplo prático, basta pensar que, embora a falta de um laboratório forense digital possa impactar um caso envolvendo provas digitais, no que diz respeito à obtenção quantitativa destas, a falha de documentação e rastreio da *chain of custody* de uma prova digital poderá ter um impacto mais amplo sobre a prova do que a falta de um laboratório[274], visto que é esta que determina a admissibilidade de toda e qualquer prova obtida[275].

[273] https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/legal-and-ethical-principles/chain-of-custody-in-computer-forensics/ (Consultado a 13 de outubro de 2019).

[274] YUSOFF, Yunus, ISMAIL, Roslan, HASSAN, Zainuddin, *"Common Phases of Computer Forensics Investigation Models"*, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, N° 3, junho de 2011, pp. 1-15.

[275] ANTWI-BOASIAKO, Albert, V ENTER, Hein, *"A Model for Digital Evidence Admissibility Assessment" in "Peterson G., Shenoi S. (eds) Advances in Digital Forensics XIII. DigitalForensics 2017. IFIP Advances in Information and Communication Technology, Volume 511"*, Springer, Cham, 2017, pp. 23-24.

3.3.2. Conclusões

Podemos concluir que este modelo fornece uma base tecnológica e holística para avaliar a admissibilidade de provas digitais em processos judiciais, integrando os principais requisitos técnicos associados à análise forense digital e os princípios legais que sustentam a admissibilidade de provas em diferentes jurisdições (como o são os vários Estados Americanos), contribuindo para os esforços de padronização forense digital[276].

3.4. Ponte com o Processo Civil

Se por um lado se nota um desnível entre o Processo Civil e o Processo Penal no que concerne à preparação deste tipo de registo de prova, por outro lado, podemos tirar ilações relativamente ao modo como este se deve processar, e à sua eventual adequação às necessidades do sistema jurídico para com as Novas Tecnologias da Informação.

Nota-se um elencar dos vários meios de prova eletrónica, seja via exames, revistas, buscas, apreensões, cópias e certidões e escutas telefónicas na Lei 109/2009, o que torna claro que surge a necessidade de fazer o mesmo para efeitos do Processo Civil, e não a confiarmos na rotulação de "prova atípica".

A doutrina respeitante ao Processo Penal, nomeadamente, a ótica de MILITÃO[277], entende que a harmonização das normas referentes à obtenção da prova digital com o regime geral de obtenção das provas apenas poderá acontecer com a integração deste primeiro grupo normativo no Código de Processo Penal, *"delineadas à luz e no quadro do regime geral de obtenção da prova",* sem prejuízo, claro *"de algumas adaptações, face a certas particularidades daquele tipo específico de prova".*

Numa ótica do garante da autenticidade e fiabilidade das provas digitais, basta pensar no Decreto-Lei 290-D/99 e no Regulamento 910/2014 (Regulamento EIDAS), referentes às assinaturas digitais e eletrónicas, naquele que é o impacto da Criptografia na análise de documentos em Portugal. Até que ponto não será pertinente conter no Código de Processo Civil disposições que colmatem as dificuldades e limitações implicadas pelas provas digitais, fazendo uma real ponte com os nossos diplomas legais?

---

[276] GOODISON, Sean, DAVIS, Robert, JACKSON, Brian, "Digital Evidence and the US Criminal Justice System: Identifying technology and other needs to more effectively acquire and utilize digital evidence", 2015, pp. 3-32.
[277] MILITÃO, Renato, *"A propósito da prova digital no Processo Penal"*, p. 266.

Se o que nos propomos é a uma maior celeridade do Processo, em nada nos parece produtivo fazer cláusulas gerais que generalizem a aplicação dos vários meios de obtenção de prova eletrónica (como acontece com o artigo 189º do Código de Processo Penal), pelo que fica já essa ótica de aviso a ser considerado. Assim, advertências como as de CONDE CORREIA[278], que apela a uma recuperação da *"centralidade normativa do CPP, enquanto instrumento nevrálgico da perseguição criminal, reservando para a legislação especial aquilo que é acessório, técnico, excecional"* (referindo-se a uma centralidade da regulamentação da prova digital, pelo seu uso cada vez mais frequente) devem ser transpostas para a ordem do processo civil, evitando *"a desordem e a insegurança jurídicas, coincidentes com uma profunda crise dos nossos valores comunitários e expressão de reflorescentes conceções do mundo, turvas e regressivas"*.

Fica aqui a ressalva de que o apontado até agora parecer tornar claro que, a serem consideradas para um panorama de Processo Civil, devemos cuidar de não criar regimes avulsos e especiais de aplicação das provas eletrónicas-digitais, pelas dificuldades de interpretação que implicam, e pela problemática de equiparação com outros diplomas que delas advém.

Da mesma forma, e seguindo as orientações apresentadas no ponto anterior, torna-se relevante considerar análises de *"chain of custody"* dos elementos de prova que se vão recolhendo, por forma de facilitar a sua autenticidade e admissibilidade, enquanto suporte aos métodos criptográficos em vigor (como os que constam no Decreto-Lei 290-D/99 e no Regulamento 910/2014).

4. Meios de Aperfeiçoamento do Sistema

Conforme apontado no capítulo anterior, num panorama nacional e internacional, temos assistido a uma utilização das tecnologias da informação e da comunicação naquela que é a administração da justiça, não só no que diz respeito a questões como a prova eletrónica e o processo eletrónico, mas também o funcionamento do próprio processo em geral.

[278] CONDE CORREIA, João, *"Prova digital: enquadramento legal"* in *"Cibercriminalidade e prova digital: Jurisdição Penal e Processual Penal"*, Centro de Estudos Judiciários, 2018, p. 26.

Como entendido por DIAS PEREIRA, *"em causa está o choque tecnológico no corpus iuris, em especial no aparelho judiciário"*[279], sendo que este processo de informatização da justiça não passa apenas pela utilização dos sistemas informáticos enquanto mera ferramenta de processamento e transmissão de dados, mas também pela sua ponderação enquanto dispositivo de solução de casos, como se de agentes se tratassem.

Ao longo deste subcapítulo, será do nosso interesse perspetivar várias ferramentas do domínio das novas tecnologias, numa lógica de interação entre o domínio das ciências exatas e das ciências humanas e jurídicas, que procura potenciar a função de validação que as primeiras nos potenciam[280] com as ponderações normativas que as segundas levantam, em toda a sua complexidade[281]. Visamos, assim, tornar clara a necessidade de um Processo cada vez mais ligado às novas tecnologias da informação, especialmente tomando em conta o impacto desta conexão.

Além desta dicotomia de colaboração e confronto no condicionamento (ou não) das regras de convivência humana às novas tecnologias, daremos igualmente enfoque à forma como estas questões interagem diretamente com o tema da presente dissertação, nomeadamente o da prova eletrónica/digital.

Se temos em falta todo um regime de lei processual para este tipo de prova no que respeita ao Processo Civil e Penal, e se a prova digital padece das limitações elencadas anteriormente, respeitantes às suas questões de confidencialidade e autenticidade, torna-se relevante ponderar até que ponto estamos a utilizar os sistemas informáticos que estão em vigor de forma correta[282].

Da mesma forma, cabe-nos elencar considerações relativamente às suas potencialidades de interdisciplinaridade e à forma como se poderão ligar os campos da Criptografia e da Lógica Formal, no que diz respeito ao aperfeiçoamento das provas digitais e da

---

[279] DIAS PEREIRA, Alexandre Libório, "*Lex informatica, ius ex machina e justiça artificial"* in *"Boletim da Faculdade de Direito – Studia Iuridica 9 Ad Honorem 3"*, Coimbra Editora, p. 817.

[280] *"(...) comment peut-on rendre plausible aux yeux des masses ells-mêmes leur proper dépolitisation? Marcuse pourrait répondre à cela: par le fait que science et technique assument aussi le rôle d'une iéologie"* - HABERMAS, Jürgen, *"La technique et la science comme idéologie – La fin de la métaphysique",* Denöel Gonthier, Paris, 1973, pp. 42-43, (tradução de Jean-René Ladmiral do *original "Technick und Wissenschaft als Ideologie"*, 1968).

[281] Por exemplo, no que respeita à interpretação de lacunas, leia-se OLIVEIRA ASCENSÃO, José, *"O Direito: Introdução e Teoria Geral"*, 10ª edição, Coimbra, 1997, p. 446, que diz que "determinar, porém, onde há verdadeiramente e onde não há analogia é extremamente difícil, e por isso exige toda a finura por parte do intérprete" -

[282] *"E a questão que, desde logo, se coloca é a de saber se o tratamento de dados pessoais associado à enorme facilidade da sua recolha, tratamento e circulação através das inovações tecnológicas se poderá circunscrever aos parâmetros tradicionais ou se será necessária uma regulamentação nova, num mundo novo3 que atenda às características extremamente intrusivas das NTIC (...)"* - MOREIRA, Teresa Coelho, *"Novas Tecnologias: Um admirável mundo novo do Trabalho?"*, Revista de Direitos e Garantias Fundamentais, Vitória, n. 11, p. 15-52, jan./jun. 2012, p. 17.

sua apreciação no próprio processo, do colmatar das suas limitações e no repensar do funcionamento do sistema processual.

4.1. Portal CITIUS

4.1.1. Contextualização

O portal CITIUS, lançado em Lisboa em julho de 2005, no CEJ (Centro de Estudos Judiciários), insere-se no âmbito do programa governamental PIIP (Programa de Investimentos em Infraestruturas Prioritárias), tendo sido pensado e desenvolvido pelo Ministério da Justiça com o intuito de desmaterializar e simplificar processos na área da justiça. Neste domínio meramente introdutório e concetual é já possível de inferir a forma como as plataformas informáticas se motivam e alinham em torno da celeridade e economia processuais, visando uma desburocratização do sistema jurídico.

Cabe-nos evidenciar que o disposto no artigo 5º nº1 da Portaria 280/2013, de 26 de agosto, respeitante à regulação da tramitação eletrónica dos processos judiciais (e que revogou a anterior Portaria 114/2008, de 6 de fevereiro), clarifica que a apresentação de peças processuais e de documentos por transmissão eletrónica de dados por mandatários judiciais (o que engloba advogados e solicitadores[283]) é efetuada através do sistema informático de suporte à atividade dos tribunais, ou seja, o portal CITIUS. Com a instalação do *software* "JAVA" e de um *software* que possibilite a leitura de ficheiros "PDF", qualquer mandatário habilitado terá capacidade de levar a cabo o tratamento eletrónico das suas peças processuais, sendo possível obter-se comprovativos da data de entrega das mesmas peças.

Já na sua altura, a Portaria 114/2008, no seu artigo 17º, determinava que *"os atos processuais dos magistrados judiciais são sempre praticados em suporte informático através do sistema informático CITIUS – Magistrados Judiciais, com aposição de assinatura eletrónica qualificada ou avançada"*, e que *"os atos processuais dos magistrados do Ministério Público são sempre praticados em suporte informático, através do sistema informático CITIUS – Ministério público, com aposição de assinatura eletrónica qualificada ou avançada"*, sendo que *"a*

[283] MADEIRA, Luís Cláudio Magalhães, *"Peças e atos processuais judiciais por transmissão eletrónica via internet"in "Direito da Sociedade da Informação – Separata do Volume IX"*, Associação Portuguesa do Direito Intelectual, Coimbra Editora, pp.70-74.

assinatura eletrónica substitui e dispensa para todos os efeitos a assinatura autógrafa em suporte de papel dos atos processuais".

A Portaria 280/2013 consagra ainda, no seu artigo 4º, que a apresentação de peças processuais e documentos por transmissão eletrónica de dados dispensa a remessa dos respetivos originais, duplicados e cópias, nos termos da lei; salvo em casos particulares, em o juiz determine necessário (dúvidas quanto à autenticidade ou genuinidade das peças e documentos)[284], ou que, nos processos penais e tutelares educativos, sejam integrados no suporte físico do processo os originais das peças e documentos apresentados nessa forma pelo Ministério Público[285].

As implicações destes novos meios tecnológicos são facilmente discerníveis, desde uma forte diminuição do tempo e dos gastos implicados aos mandatários judiciais, mas também aos órgãos estatais, como o indicou, aliás, o Decreto-Lei 34/2008, de 26 de fevereiro, que aprovou o primeiro Regulamento das Custas Processuais, que demonstrou de imediato uma diminuição clara dos gastos implicados pela tramitação processual.

4.1.2. Preocupações e ceticismo

As principais preocupações prendem-se maioritariamente com um receio de que os grandes progressos oferecidos no que diz respeito à celeridade processual possa colocar em causa princípios processuais como é o caso do princípio da legalidade ou o princípio do contraditório, para não falar da questão que tem estado em voga nas discussões de foro europeu dos últimos anos, ou seja, a privacidade e a segurança dos dados que vão circulando em formato eletrónico.

Não obstante estas preocupações, há desde já garantias de segurança que permitem um apaziguar dos receios plasmados, uma vez que qualquer mandatário judicial apenas será capaz de manusear o portal mediante apresentação de certificado de assinatura eletrónico disponibilizado pela própria Ordem dos Advogados Portugueses (no caso de advogados) ou pela Câmara dos Solicitadores (no caso dos solicitadores).

[284] Artigo 4º nº2 a) da Portaria 280/2013, de 26 de agosto.
[285] Artigo 4º nº2 b) da Portaria 280/2013, de 26 de agosto.

No que diz respeito aos magistrados, o processo é ainda mais seguro, visto que a assinatura digital é incorporada num cartão de identificação pessoal dotado de um chip, sendo este chip lido via leitores tipo *smartcard* que implicam códigos PIN[286].

Grande parte do ceticismo e das críticas apresentadas, na sua maioria, não são válidos nem fundamentados, mostrando não só uma resistência à mudança de paradigma, mas também um desfasamento relativamente àquelas que são as especificidades da utilização de uma assinatura digital ou eletrónica e aos requisitos de segurança que esta implica, visto que se torna claro que é impossível a qualquer funcionário ou técnico do DGAJ ou do Ministério da Justiça conseguir manipular decisões de magistrados.

Mais do que ser cético, torna-se necessário conferir a segurança e a confiança aos operadores a quem a mudança é exigida, incluindo-os no processo como de mudança paradigmática, de forma a que os efeitos de surpresa, de novidade e de alienação sejam atenuados ao máximo.

4.1.3. Pontos de melhoria

Não obstante esta defesa do sistema, não será aconselhável adotar uma postura conformista, pelo que devemos reconhecer pontos que o CITIUS necessita de melhorar alguns dos seus aspetos.

Relativamente ao seu funcionamento interno, no que diz respeito a questões de logística interna do mesmo, o sistema encontra-se dependente de um número reduzido de oficiais de justiça e engenheiros informáticos, por não existirem os devidos manuais de procedimentos e transcrições da programação, o que torna procedimentos de atualizações do mesmo e de resolução de problemas altamente morosos. Da mesma forma, este número reduzido de responsáveis implica uma má formação dos utilizadores do portal, que, por serem quem aplica e manobra o Direito, não se devem sentir alienados relativamente ao sistema em que desenvolvem a sua atividade.

Esta ausência de formação e a dificuldade de resposta aos problemas tecnológicos[287] levou a que utilizadores favoráveis apontassem um uso de tecnologia ultrapassada e incapaz de

[286] MAURÍCIO, Rui, *"O paradigma do processo eletrónico no Direito Processual Civil português" in "Direito da Sociedade da Informação: Volume IX"*, Coimbra Editora, 1ª Edição, 2011, pp. 106-107.

dar resposta às suas necessidades; e que utilizadores céticos clamassem por uma substituição completa do sistema até 2023[288]. Assim, aponta-se desde já necessidades de revisão da política interna do sistema e da forma como é articulada a utilização e a formação em relação ao *software*.

A perceção pública do Portal CITIUS acaba por ter impacto no tema do presente trabalho, visto que o aumento das reservas em relação a sistemas eletrónicos processuais está diretamente ligado à confiança que lhe é dada, bem como à permeabilidade em aceitar a utilização das novas tecnologias na recolha e composição dos meios de prova.

Outro problema que se coloca é a utilização da plataforma de execução e *software* JAVA, na qual a aplicação do Portal CITIUS se baseia, e que está associada a alguns erros arquiteturais na conceção do Portal, bem como problemas de programação, operacionalização e escalabilidade. Os impactos do mau funcionamento da aplicação (particularmente se tomarmos em conta a dependência que os tribunais passaram a ter em relação a esta) são aterrorizantes, apesar de se começarem a abrir discussões relativas à sua substituição[289].

Assim, a utilização de meios de segurança e sistemas mais avançados, capazes de aferirem e darem resposta a necessidades processuais passa a ser uma exigência relevante, como o demonstrará o resto do presente capítulo.

4.2. Recurso à Criptografia

A privacidade cada vez mais se afigura relevante, fruto dos problemas suscetíveis de ocorrer caso um terceiro tenha acesso a dados pessoais (saldo bancário, faturas do cartão de crédito, senhas bancárias ou de crédito automático), sendo que, no caso de empresas, os danos podem ser de elevado nível para a organização e para os próprios funcionários. Aqui, entra a importância da criptografia[290].

---

[287] Exemplo claro desta dificuldade diz respeito à falha do Portal CITIUS em setembro de 2014, que implicou uma quase paralisação dos tribunais durante 44 dias, no arranque do calendário judicial de 2014. Nesse ponto, ler os seguintes artigos, datados de 2014 (https://www.publico.pt/2014/09/01/sociedade/noticia/site-citius-continua-indisponivel-no-arranque-do-mapa-judiciario-1668298) e de 2018 (https://www.publico.pt/2018/03/30/sociedade/noticia/tres-anos-e-meio-apos-colapso-do-citius-nao-se-sabe-o-que-parou-os-tribunais-1808572), consultados a 6 de agosto de 2019.

[288] Neste sentido, ler o seguinte artigo, datado de 2018 (https://www.publico.pt/2018/03/30/sociedade/noticia/tres-anos-e-meio-apos-colapso-do-citius-nao-se-sabe-o-que-parou-os-tribunais-1808572), e consultado a 6 de agosto de 2019.

[289] http://www.bluechip-india.com/no-brainer-alternative-to-oracle-java-runtime-jre/ (consultado a 6 de outubro de 2019).

[290] MORENO, Edward David, PEREIRA, Fábio Dacêncio, CHIARAMONTE, Rodolfo Barros, *"Criptografia em Software e Hardware"*, Novatec Editora, p. 24.

De forma genérica, "criptografia" diz respeito a um conjunto de princípios e de técnicas que visam garantir uma comunicação segura[291] na presença de terceiros, passando por uma construção e análise de protocolos que impedem esses terceiros, ou inclusive a generalidade do público, de lerem mensagens privadas e informações privadas.

Em Criptografia é costume discutir-se a questão clássica de "Bob e Alice"[292], dois estranhos que comunicam online, sem nunca saberem realmente se a pessoa do outro lado é quem diz ser, precisando de garantias de que realmente estão a comunicar um com o outro e que não há intenções de nenhum roubar *"os segredos"* ou" informações*"* do outro. É em torno de situações como esta que versará o seguinte subtópico.

Conforme mencionado no capítulo anterior, a segurança dos documentos eletrónicos e, consequentemente, das provas eletrónicas, prendem-se acima de tudo com o triplo vetor da autenticidade, da integridade e da confidencialidade do documento.

Na terminologia criptográfica, usa-se o termo *"trusted agent"*, ou seja," agente em que se confia", sendo que em qualquer documento que se analisar e se procurar valorar ter-se-á sempre um ou mais *"trusted agents"*. O processo de confiança que se visa estabelecer em determinado agente diz respeito a uma crença que necessita de fundamentação, sendo que o que fundamenta tal crença é a noção de prova, a qual (i) se baseia em documento credível que justifica a validade de uma crença ou (ii) em processo cognitivo, que estabelece uma relação de confiança com uma crença (por exemplo, provas matemáticas, como é o caso do teorema de Fermat-Wiles).

No que diz respeito aos documentos eletrónicos, torna-se essencial cruzar a identidade social e a identidade digital dos indivíduos, em todas as suas manifestações públicas[293] e privadas[294], de forma a conseguir acreditar em algo e satisfazer os três vetores mencionados supra de forma satisfatória.

---

[291] Para a criptografia, a segurança exprime-se em propriedades específicas, como a integridade, a confidencialidade e não-repúdio (entre outras).

[292] CALEIRO, Carlos, VIGANÒ, Luca, BASIN, David, *"Deconstructing Alice and Bob"* in *"Electronic Notes in Theoretical Computer Science 135 (2005) 3–22"*, ELSEVIER, 2005, p. 4.

[293] A nível de identidade social serão questões de pertença social (ingresso na Ordem dos Advogados, por exemplo) e a nível da identidade digital tratar-se-á de uma "chave pública" (termo a ser elaborado em breve).

[294] A nível de identidade social serão questões específicas dentro de um determinado grupo (curso de estágio na Ordem dos Advogados, por exemplo) e a nível da identidade digital tratar-se-á de de uma "chave privada" (termo a ser elaborado em breve, mas que diz respeito ao permite provar quem se é no contexto digital, sendo esta manifestação "os segredos que se conhecem" como se de uma "personalidade digital" se tratasse).

Nesse sentido, são atualmente desenvolvidas, de forma a salvaguardar este vetor, as técnicas de criptografia, consistindo na criação de condições de ininteligibilidade dos dados para quem não detenha as chaves de cifrar e decifrar os documentos[295].

Assim, neste ponto iremos desenvolver o âmbito da utilização da criptografia na segurança e autenticação de documentos eletrónicos e a ponte que esta faz com a prova eletrónica, de forma a garantir a sua viabilidade. Pelo impacto e desenvolvimento que obteve, versaremos em grande parte sobre as assinaturas eletrónicas e respetivas autoridades de certificação.

Dentro desse subtópico, não obstante se conhecerem dois sistemas de criptografia baseada em assinaturas, nomeadamente, o de chave única[296] e o de chave assimétrica[297], o nosso enfoque prender-se-á com o sistema de chave assimétrica, por ser aquele que é consagrado na legislação europeia e portuguesa.

4.2.1. Assinaturas Digitais e Eletrónicas

Conforme apontado por PUPO CORREIA[298], o valor probatório dos documentos eletrónicos depende, entre outros requisitos, da assinatura do seu autor[299], sendo que o artigo 376º do Código Civil clarifica que um documento não assinado não tem legalmente valor superior a qualquer outro meio de prova comum.

Neste sentido, e perante uma ausência de definição legal daquilo que se entende por "assinatura" da parte do ordenamento jurídico português, optaremos por seguir a visão funcional (ou seja, que tenha em conta as funções essenciais desempenhadas pela assinatura dos documentos[300]) do conceito, apresentada por PUPO CORREIA[301], que entende que, em geral, *"a assinatura constitui um sinal ou meio, suscetível de ser usado com exclusividade por uma dada pessoa através da sua aposição num documento, sinal esse através do qual o autor deste revela a sua identidade pessoal de forma inequívoca, manifesta as suas declarações de vontade ou*

---

[295] Numa perspetiva de antecedentes europeus, será pertinente ler a *"Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões, tendo em vista a segurança e a confiança na comunicação eletrónica"*, COM(97)503, de outubro de 1997.

[296] Baseado numa única chave, possuída pelo emissor e pelo recetor da mensagem e que serve para a codificar e descodificar.

[297] Utiliza uma "chave pública" e uma "chave privada", sendo que a primeira descodifica mensagens codificadas pela segunda.

[298] PUPO CORREIA, Miguel, *"Assinatura eletrónica e certificação digital"* in *"Direito da Sociedade da Informação: Volume VI"*, Coimbra Editora, 1ª edição, 2006, pp. 292-293.

[299] Neste tópico, aliás, o artigo 373º nº1 do Código Civil indica que os documentos particulares devem ser assinados pelo seu autor.

[300] POULLET, Yves, *"Probate Law: From Liberty to Responsibility"* in *"The EDI Law Review"*, 1994, pp. 85 e ss.

[301] PUPO CORREIA, Miguel, *"Assinatura eletrónica..."*, Coimbra Editora, 1ª edição, 2006, p. 293.

conhecimento dele constantes e, na medida do possível, procura preservar a integridade do documento, quando é transmitido a outra pessoa".

Sob esta definição estão englobados vários processos de autenticação com recurso às novas tecnologias de informação (códigos secretos[302], assinaturas digitalizadas[303], chaves biométricas[304], entre outros), sendo que, para efeitos do presente estudo, e tomando em conta as suas particularidades, apenas iremos desenvolver as nuances das assinaturas eletrónicas e digitais.

4.2.1.1. Definição e Caracterização

Há uma tendência em conferir maior confiabilidade à prova documental, havendo um permanente receio de adulteração das informações contidas num documento eletrónico, caso um terceiro que detenha conhecimentos informáticos assim o deseje[305], sendo a confiabilidade da autoria e a integridade das informações desse documento a base da sua eficácia probatória.

O sistema universalmente utilizado, e considerado o mecanismo mais seguro é o da assinatura eletrónica, conseguida através do recurso a algoritmos criptográficos. Os métodos criptográficos mais conhecidos e comummente utilizados são o DES[306] (*Data Encryption Standard*[307]) e o RSA (de nome atribuído em honra de Rivest, Shamir e Adleman e ligado aos algoritmos de chaves assimétricas e públicas), sendo este último particularmente seguro e eficiente e o primeiro a possibilitar criptografia e assinatura eletrónica[308].

Tendo em conta que o mundo Digital, tal como se veio a provar, representa uma fatia gigantesca do mercado global, cada vez mais entidades supranacionais, como é o caso da União Europeia, consagraram a importância da utilização e aplicação das assinaturas digitais,

---

[302] Combinação de algarismos ou letras que condiciona o acesso à utilização de sistemas informáticos, seja sob forma alfanumérica, seja sob a forma de PIN, e geralmente combinadas com a utilização de um cartão magnético ou de um microprocessador (chip).

[303] Reprodução da assinatura do autor, via *scanner*, sendo depois aposta como cópia nos documentos que se pretenda assinar. De todos os meios de assinatura elencados aqui, é uniformemente considerada a menos segura, pela facilidade de réplica e recolocação semelhante ao que se faria num caso manuscrito.

[304] Alicerçada no reconhecimento de características físicas do indivíduo (impressões digitais, íris, sangue, face). Principais falhas recaem na dificuldade em comprovar a vontade do autor.

[305] ARENHART, Sérgio e MARINONI, Luiz, *"Prova e Convicção"*, Thomson Reuters, 2015, p. 621.

[306] [O] "DES, não obstante a sua fiabilidade, comporta a enorme desvantagem de não comprovar a exata origem da mensagem" – ANDRADE, Francisco, *"Assinatura eletrónica para «agentes de software»?",* p. *7*.

[307] Artigo 2º do Dec. Lei nº 290-D/99 de 2 de agosto com a redação que lhe foi introduzida pelo Dec. Lei 62/2003 de 3 de abril (e após as alterações introduzidas pelos DL nº 165/2004 de 6 de julho e DL nº 88/2009 de 9 de abril).

[308] REED, Chris**,** *"Computer Law",* Blackstone Press Limited, 1990, p. 268.

conforme se verifica na Diretiva 1999/93/CE[309] do Parlamento Europeu e do Conselho Europeu (entretanto revogado pelo Regulamento da UE 910/2014[310]), mais tarde transposta para os ordenamentos dos Estados Membros.

A transposição da Diretiva 1999/93/CE, apresentada e definida (na legislação portuguesa) por meio do Decreto-Lei 290-D/99, de 2 de agosto, entendeu que, por assinatura eletrónica, se entenderia o *"resultado de um processamento eletrónico de dados suscetível de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico ao qual seja aposta"* (artigo 2º b)), de modo a que identificasse o titular como autor do documento, bem como a confirmação da vontade do mesmo; enquanto assegurava a autenticidade do documento (e a sua não adulteração).

Este diploma[311] permite-nos desde já distinguir "assinatura eletrónica" de "assinatura digital", sendo que esta última se traduz como:

> *[O] "processo de assinatura eletrónica baseado em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo, e ao declaratário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura"*
>
> - Artigo 2º c) do DL-299-D/1999, de 2 de agosto

A esta definição deve-se aliar o conceito explanado pelo Regulamento 910/2014, que clarifica, no seu artigo 3º nº10, que *"os dados em formato electrónico que se ligam ou estão*

---

[309] *"As comunicações e o comércio eletrónicos necessitam de assinaturas eletrónicas e de serviços a elas associados, que permitam a autenticação dos dados (...) reforça a confiança e a aceitação geral das novas tecnologias; a existência de legislações divergentes nos Estados-Membros cria obstáculos à livre circulação de bens e serviços no mercado interno"* – considerando 4 da Diretiva 1999/93/CE.

[310] *"A Diretiva 1999/93/CE do Parlamento Europeu e do Conselho trata das assinaturas eletrónicas sem oferecer um quadro transfronteiriço e transetorial geral que garantisse a segurança, a fiabilidade e a facilidade de realizações das transações eletrónicas. O presente regulamento melhora e desenvolve as disposições daquela diretiva"* – considerando 3 do Regulamento 910/2014 da EU.

[311] Não obstante, devemos esclarecer que, na sua versão original. o Decreto-Lei 290-D/99 apenas referia a assinatura digital. Só com o Decreto-Lei 62/2003 (que veio compatibilizar a lei portuguesa com a Diretiva Europeia) é que se passou a uma abordagem tecnologicamente neutra, passando-se a falar de assinaturas eletrónicas (conceito amplo) e assinaturas digitais (conceito específico, relativa a uma tecnologia concreta e determinada). Dentro deste escopo, as assinaturas digitais são as mais comummente utilizadas, embora seja possível equacionar outras tecnologias de assinatura eletrónica, como as assinaturas dinâmicas.

logicamente associados a outros dados em formato electrónico e sejam usados pelo signatário para assinar".

Feita esta exposição, passa a ser possível explicar o funcionamento e as mais valias do sistema de chaves assimétricas mencionadas na definição acima explanada.

O sistema de dupla chave do emitente (uma privada[312] e outra pública[313]) possibilita a chamada assinatura digital e a transmissão de uma mensagem com a devida garantia da autenticidade do emitente e da integridade da informação recebida, independentemente do meio de expressão dessa mensagem.

Elencamos de seguida uma visão simplificada das operações implicadas neste sistema:

- A cada utilizador são atribuídas duas chaves que se complementam, nomeadamente, uma chave privada (de assinatura) e uma chave pública (de verificação);

- O emitente produz um resumo derivado do texto original[314], que pretende enviar com o uso de um algoritmo "*hash*"[315], obtendo um valor denominado de "*valor hash*". A este processo também se chama de *"message digest"*, por se tratar de uma sequência de dados com uma determinada extensão, que constitui uma espécie de *"impressão digital eletrónica"* dos dados cifrados, claramente mais extensos;

- O emitente cifra o resumo dos dados com a sua chave privada, sendo que o resultado desta cifra é a assinatura digital;

- Após aposição da assinatura eletrónica ao texto original, ambos são enviados, eletronicamente, ao seu destinatário; que aplicará a chave pública do emitente à assinatura eletrónica deste, de forma a obter um "*valor hash"*;

- Posto isto, o destinatário comprime o texto enviado com o mesmo algoritmo *"hash"* usado pelo emitente, apurando um novo "*valor hash"*;

---

[312] *"Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública"* – Artigo 2° d) do DL-299-D/99, de 2 de agosto.

[313] *"Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves"* – Artigo 2° e) do DL-299-D/99, de 2 de agosto.

[314] Em teoria, duas mensagens distintas podem ter o mesmo "*hash"* (calculado) mas, estatisticamente, será virtualmente impossível encontrar duas mensagens com o mesmo *"hash"*.

[315] Existem três tipos de algoritmos de *"hash"* que visam garantir a confiança e autenticidade, nomeadamente *o "Cyclic Redundancy Check" (CRC), o "Message Digest "5* ***(MD5)*** e o *"Secure Hash Algorithm"* (SHA).

- Finalmente, por meio da comparação entre os dois *"valores hash"* obtidos, é possível de apurar que a assinatura eletrónica do emitente é autêntica e de que o texto recebido coincide com o enviado caso o *"valor hash"* proveniente da assinatura eletrónica coincida com aquele que é apurado a partir do texto original.

- Caso pretenda manter a confidencialidade, o emitente poderá utilizar a chave pública do destinatário para cifrar a mensagem de dados, sendo que o destinatário a decifrará com a sua própria chave privada, e vice-versa.

Conforme visto, o *hashing* pode ser uma ferramenta muito útil na a quem tem de efetuar uma triagem num sistema informático, garantindo (i) a certeza de que determinado objeto (ficheiro, por exemplo) não foi alterado; (ii) a chance de filtrar a pesquisa num sistema, via método conhecido na comunidade forense como "*Negative Hashing*"; (iii) a identificação de ficheiros via lista de valores *hash* de determinados, via método conhecido na comunidade forense como "*Positive Hashing*"; e, ainda (iv) verificar a integridade do documento[316].

Torna-se claro que a assinatura eletrónica pode ser utilizada para garantir que apenas um destinatário tenha acesso à mensagem enviada, mas também para questões e autenticação documental (o que se torna particularmente relevante para oficiais públicos autenticarem documentos, especialmente se estes puderem adquirir valor probatório, sendo que qualquer sujeito poderá posteriormente comprovar a autenticidade do documento por meio do recurso à chave pública desse agente, para comprovar a não alteração do conteúdo documental).

Basicamente, as assinaturas eletrónicas ajudam a garantir que o signatário é quem ele afirma ser (autenticidade), a garantir que o conteúdo não foi alterado nem violado desde que foi assinado digitalmente (integridade), ajudando também a provar a todas as partes a origem do conteúdo assinado (não-repúdio). O termo *"repúdio"* serve para designar as situações em que o signatário nega qualquer associação com o conteúdo assinado. Como se pode inferir, com as assinaturas digitais, é impossível um signatário alegar não ter assinado dado conteúdo.

Fazendo aqui uma breve análise doutrinária, nota-se um contraste entre as posições assumidas por autores como SILVA RODRIGUES, que defende que integridade da prova depende do *"seguimento das corretas etapas do método de obtenção de prova eletrónico-digital,*

[316] COSTA MARQUES, Pedro Penha Leitão da, *"Informática Forense: Recolha e preservação da prova digital"*, Tese de Mestrado pela Universidade Católica Portuguesa, 2013, p. 40.

consagradas para manter a sua capacidade probatória"[317], em contraste com a posição de autores DIAS VENÂNCIO (na qual nos basearemos para efeitos desta tese), que interpreta a assinatura digital como uma medida de preservação e garante da integridade dos dados apreendidos relativamente a alterações posteriores à apreensão[318].

As autoridades de certificação poderão também contribuir na atribuição e confirmação da propriedade das características da chave pública do emitente, assegurando uma confirmação de identidade que cada vez mais se torna fulcral, com a progressiva aplicação dos novos meios tecnológicos no domínio processual. Este tema será aprofundado de seguida.

4.2.1.2. Entendimento Legal e Força Probatória

Sob dadas circunstâncias, o ordenamento português confere especial força aos documentos, pelo que a apresentação de documentos eletrónicos ao juiz como meio de prova se afigura como uma possibilidade, até porque nos termos do artigo 380°n°1 do Código Civil se clarifica a admissibilidade dos "registos e outros escritos onde habitualmente alguém tome nota dos pagamentos" poderem ser apresentados como prova contra o seu autor, caso indiquem inequivocamente a receção de algum pagamento, sendo que o autor do escrito terá a chance de provar, por qualquer meio, que tal documento não corresponde à realidade. Não obstante, os ficheiros informáticos não estão excluídos do seu âmbito.

O artigo 25° do Regulamento 910/2014 do Parlamento Europeu e do Conselho, no que diz respeito a esta questão, torna perfeitamente claro que a assinatura eletrónica qualificada por serviços de confiança tem o mesmo valor que uma manuscrita. Da mesma forma, e analisando o Decreto-Lei n° 7/2004 (respeitante ao comércio eletrónico), no seu artigo 26° n°1, parece vir consubstanciar (ainda que se suscitem dúvidas a este respeito) uma ideia de valorização de documentos consubstanciados em suportes eletrónicos fiáveis, ao realçar uma necessidade de garantias de conservação, fidedignidade e inteligibilidade do que é declarado eletronicamente.

Este recurso a prestador de serviços de confiança, relevantes no domínio da criptografia de chave assimétrica, afigura-se também como uma possível solução a um dos principais

[317] RODRIGUES, Benjamin Silva, *"Da Prova Penal, Tomo II, Bruscamente, A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal"*, 2010, pp. 530-531.
[318] CANCELA, Alberto Gil Lima, *"A prova digital: os meios de obtenção de prova no cibercrime"*, Tese de Mestrado pela Universidade de Coimbra, 2016, p. 46.

problemas daquela que é a prova digital, que concerne com a facilidade de adulteração de documentos que se encontrem nesta modalidade de suporte.

Naturalmente que isto levanta a questão de se colocar os prestadores de serviços de confiança numa posição cimeira e de excessiva vantagem relativamente a provas, o que não se afigura como algo particularmente nocivo se tomarmos em conta a diferença e o peso que estas assumem relativamente a documentos eletrónicos pensados unicamente para um âmbito contratual. É relevante, por tanto, fazer uma análise de custo e benefício que ponha em causa os impactos positivos e negativos do recurso à certificação eletrónica de forma a se obter uma devida conclusão.

Será igualmente relevante analisar o papel de novos meios de garantia de segurança plasmados no Regulamento 910/2014, nomeadamente selos eletrónicos, selos temporais, serviços de envio registado eletrónico e certificados de autenticação de sítios web; plasmados no artigo 3º do dito diploma e com um peso significativo para a temática da presente dissertação.

Para que todas as garantias supramencionadas sejam fornecidas, é necessário que o conteúdo seja assinado digitalmente pelo seu criador, que deverá utilizar uma assinatura que verifique um conjunto de critérios, devidamente elencados no artigo 32º do Regulamento 910/2014, a ser analisado em conjunto com o artigo 28º nº1 do mesmo regulamento, referente aos serviços qualificados de certificação.

Assim, a assinatura eletrónica/digital deve ser válida, o certificado associado à mesma não deverá ter expirado, sendo que a autoridade de certificação que emitiu o certificado associado à assinatura digital deverá ser respeitável. Por sua vez, a organização signatária/o signatário deverão ser confiáveis. Todos estes critérios se encontram dependentes de vários fatores que irão ser esclarecidos de seguida.

4.2.2. Selos Eletrónicos e Selos Temporais

Da mesma forma que as autoridades competentes dos Estados-Membros utilizam atualmente diferentes formatos de assinatura eletrónica avançada de documentos, também

utilizam selos eletrónicos avançados, pelo será necessário garantir a sua compatibilidade técnica com, pelo menos, alguns formatos de selo eletrónico avançado[319].

Aqui, importa analisar o artigo 36º do Regulamento 910/2014, que enuncia os requisitos do selo eletrónico avançado, nomeadamente: (i) estar associado de modo único ao seu criador, (ii) permitir identificar o seu criador, (iii) ser criado através dos dados de criação de selos eletrónicos cujo criador pode, com um elevado nível de confiança e sob o seu controlo, utilizar para a criação de um selo eletrónico e (iv) estar ligado aos dados a que diz respeito de tal modo que seja detetável qualquer alteração posterior dos dado.

Além de autenticarem o documento produzido pela pessoa coletiva, os selos eletrónicos podem ser utilizados para autenticar qualquer bem digital da pessoa coletiva, como um código de software ou um servidor.

A especificidade desta figura prende-se com a sua exclusividade para com as pessoas coletivas, em contraste com o caráter predominantemente "individual" da assinatura eletrónica e das suas variantes.

4.2.2.1. Selos Eletrónicos

Os selos eletrónicos deverão servir de prova da emissão de um documento eletrónico por determinada pessoa coletiva, certificando a origem e a integridade do documento, usando a Decisão 2011/130/UE da Comissão como base[320].

Ressalva-se que o selo eletrónico não é idóneo para vincular contratualmente a pessoa coletiva, da mesma forma que um selo carimbado de uma organização não é suficiente para vincular a mesma.

O certificado de selo eletrónico é uma nova figura, introduzida pelo Regulamento eIDAS (Regulamento 910/2014), sendo que, do ponto de vista técnico, se apresenta bastante semelhante a um certificado de assinatura eletrónica. Segundo o artigo 38º do Regulamento 910/2014, os certificados qualificados de selos eletrónicos devem cumprir os requisitos estabelecidos no anexo III do Regulamento[321], não estando sujeitos a requisitos obrigatórios que

[319] Considerando 50 do Regulamento 910/2014.
[320] Considerandos 59 e 64 do Regulamento 910/2014.
[321] (i) Indicação de que o certificado foi emitido como certificado qualificado de selo eletrónico, (ii) dados que representem o prestador qualificado emissor do certificado, o seu Estado-Membro e a designação de pessoa singular ou pessoa coletiva, (iii) o nome do criador do selo e,

excedam os requisitos estabelecidos nesse anexo, sendo que certificados qualificados de selos eletrónicos poderão incluir características específicas adicionais não obrigatórias (de ressalvar que estas não prejudicam a interoperabilidade e o reconhecimento dos selos eletrónicos qualificados).

No que concerne aos efeitos legais conferidos pelo selo eletrónico aos documentos aos quais é aposto, destacam-se (i) o não repúdio dos seus efeitos legais nem da sua admissibilidade enquanto prova em processo judicial pelo simples facto de se apresentar em formato eletrónico ou de não cumprir os requisitos dos selos eletrónicos qualificados; e, caso se tratem de selos eletrónicos qualificados, (ii) a presunção legal de integridade e autenticidade da origem dos dados, (iii) o reconhecimento destes efeitos em todos os Estados-Membros da União Europeia[322].

Conforme indicado pelo artigo 36º do Regulamento 910/2014, um selo eletrónico avançado deve permitir (i) a identificação ao seu criador, (ii) a associação única a este, (iii) a elaboração de selos eletrónicos pelo seu criador e (iv) a sua conexão aos dados que contém, de forma a poder ser alterado em conformidade com alterações destes mesmos dados.

4.2.2.2. Selos Temporais

Com os requisitos plasmados no artigo 41º do Regulamento 910/2014, os selos temporais devem (i) vincular a data e a hora aos dados (de forma a tornar razoavelmente impossível a alteração dos dados de forma não detetável), (ii) ter por base uma fonte horária precisa ligada à Hora Universal Coordenada e (iii) serem assinados via uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, ou por outro método equivalente.

Beneficiando da presunção da exatidão da data e da hora que indica e da integridade dos dados aos quais a data e a hora estão associadas, o selo temporal qualificado emitido num Estado-Membro é reconhecido como tal em todos os Estados-Membros, não podendo ser

---

eventualmente, o número de registo, conforme constam dos registos oficiais, (iv) os dados necessários para a validação do selo eletrónico que correspondam aos dados necessários para a criação do selo eletrónico, (v) a indicação do início e do termo da validade do certificado, (vi) o código de identidade do certificado (deve estar associado de modo único ao prestador qualificado de serviços de confiança), (vii) a assinatura eletrónica avançada ou o selo eletrónico avançado do prestador qualificado de serviços de confiança emitente, (viii) o local em que está disponível, a título gratuito, o certificado que sustenta a assinatura eletrónica avançada ou o selo eletrónico avançado, (ix) a localização dos serviços aos quais se pode recorrer para inquirir da validade do certificado qualificado e (x) uma indicação da localização dos dados para criação do selo relacionados com os dados para a validação do selo eletrónico (caso estes se encontrem num dispositivo qualificado de criação de selo eletrónico).

[322] Artigo 36º do Regulamento 910/2014.

negados efeitos legais nem admissibilidade enquanto prova em processo judicial a um selo temporal pelo simples facto de se apresentar em formato eletrónico ou de não cumprir os requisitos do selo temporal qualificado[323].

4.2.3. Certificado Eletrónico

Neste ponto, cabe-nos esclarecer como é que os certificados eletrónicos possibilitam que o *browser* de um computador seja capaz de saber identificar chaves públicas e de as atribuir às chaves privadas para nos transmitir as informações que visamos obter, garantindo ainda a prevenção da intervenção de terceiros indesejados.

Convém esclarecer que um certificado eletrónico é um arquivo de computador, usado para a identificação e autenticação de indivíduos em sítios da internet e noutros sistemas eletrónicos. Com isto, fica implícito que este certificado contenha um conjunto de informações referentes à entidade para a qual o certificado foi emitido, mais a chave pública que corresponde à chave privada que se pretende acreditar, estando esta última na posse da entidade especificada no certificado.

Conforme indicado anteriormente, com estes certificados, torna-se possível que cada indivíduo possa assinar eletronicamente qualquer arquivo de computador (seja um documento, um e-mail ou até mesmo um programa), adquirindo a mesma validade jurídica de um documento com assinatura manuscrita. Neste sentido, um certificado eletrónico é passível de ser revogado[324] caso a sua chave privada relacionada seja comprometida, ou se a relação entre a entidade e a chave pública presente no certificado estiver incorreta ou for alterada (como é o caso das circunstâncias de mudança oficial de nome).

Convém realçar que os certificados eletrónicos são emitidos apenas para um determinado Nome de Domínio (*"Domain Name"*). Se o nome do certificado não corresponder ao domínio visitado, o motor de buscar irá exibir um erro[325].

Além destes dados, e no que diz respeito âmbito da segurança das comunicações quando um utilizador se liga a um sítio Web por meio dos servidores *"HTTPS"* (a serem abordados mais tarde), estes certificados permitem a autenticação de cliente nesses mesmos

[323] Artigo 41° do Regulameto 910/2014.
[324] A suspensão e revogação dos certificados estão devidamente elencados nos termos do artigo 31° do Decreto-Lei 290-D/99.
[325] KUROSE, Jim, ROSS, Keith, "Redes de computadores e a internet: uma abordagem top-down", 6ª edição, Pearson, São Paulo, 2015, pp. 95-106.

servidores (Apache, IIS)[326]. Referimo-nos aqui à chamada "autenticação inversa", em que os utilizadores apresentação os seus certificados a aos servidores. Na realidade, a situação mais comum de se verificar é aquela em que os utilizadores (clientes) conseguem confirmar a autenticidade dos servidores através de certificados por estes apresentados.

Quem nos disponibiliza esses Certificados são, efetivamente, as chamadas Autoridades de Certificação, as quais, para efeitos da Criptografia e do presente trabalho, serão entendidas como os terceiros confiáveis responsáveis pela emissão de um Certificado Digital.

Os certificados podem ser analisados com base na noção de certificado de raiz, instalado no dispositivo, e que é o momento decisivo para a criptografia determinar a autenticidade e respeitabilidade da autoridade de certificação, e, por conseguinte, a validade do certificado.

4.2.3.1. Autoridades de Certificação

Não basta a verificação da autenticidade e integridade dos dados para confirmar a identidade do signatário. O verdadeiro garante da não divulgação de chaves públicas sob identidades falsas passa por uma identificação dos utilizadores perante "terceiros de confiança", que assumam o papel de criarem e atribuírem pares de chaves e relacionarem esses pares de chaves com uma pessoa singular que com elas irá assinar, bem como a lista de chaves públicas. Estes terceiros são nada mais nada menos, que os prestadores de *"serviços de certificação"*, as chamadas autoridades de certificação.

De uma forma muito simples e sucinta, estas entidades estarão encarregues de autenticar a titularidade, prazo de validade e outras especificações das chaves públicas, mediante emissão de certificados que ligam uma chave pública a um determinado indivíduo, de forma a confirmar a sua identidade. O próprio certificado trata-se de um documento eletrónico, ele próprio dotado de uma assinatura digital, proveniente do prestador de serviços de certificação, podendo também estar sujeito a uma certificação por outro prestador de serviços, como forma de garante de confiabilidade e de segurança.

Existem Autoridades de Certificação de dois tipos, nomeadamente, (i) as Autoridades de Certificação de Raiz, as quais se encarregam de emitir diretamente os certificados, e (ii) as

[326] KUROSE, Jim, ROSS, Keith, "Redes de computadores e a internet: uma abordagem top-down", 6ª edição, Pearson, São Paulo, 2015, pp. 72-83.

Autoridades de Certificação Intermediárias, cujos certificados são emitidos indiretamente pelas Autoridades de Certificação de Raiz.

A relação entre as Autoridades de Certificação de Raiz e o Cliente pode ser perspetivada como uma estrutura hierarquizada, uma vez que as Autoridades de Certificação de Raiz emitem os certificados para as Autoridades de Certificação Intermediárias as transmitir ao Cliente/utilizador final, de forma a este poder usufruir e aplicar o conteúdo do certificado em questão.

O Regulamento 910/2014 contribuiu bastante para estas figuras, ao elencar a categoria de prestador de serviços de confiança, que entende como sendo *"a pessoa singular ou coletiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado de serviços de confiança"*[327], introduzindo ainda a categoria de prestador qualificado de serviços de confiança, referindo-se ao *"prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora"*[328].

Da mesma forma, o Regulamento em questão estabelece Entidades Supervisoras Nacionais (designadas pelos Estados-Membros), responsáveis por supervisionarem os prestadores qualificados de serviços de confiança estabelecidos no território do Estado-Membros, tomando ainda medidas relativamente aos prestadores de serviços de confiança[329].

Os prestadores de serviços de confiança encontram-se assim fortemente regulamentados em termos da regulamentação europeia, estando ainda sujeitos a vários requisitos de segurança, seja a nível dos certificados que emitem, seja à sua listagem e ao início do seu exercício de funções[330].

Efetivamente, as autoridades de certificação podem ser altamente funcionais numa perspetiva técnica, mas a obtenção de tal estatuto (entidade certificadora) é algo altamente complexo e trabalhoso, o que implica que muitas vezes fiquem as entidades governamentais habilitadas a desempenhar tais funções. De facto, há um pagamento de cauções elevadíssimas para se obter o reconhecimento enquanto autoridade de certificação, pelo que muitas entidades não têm interesse em serem reconhecidas como tal juridicamente.

[327] Artigo 3° n° 19 do Regulamento 910/2014.
[328] Artigo 3° n° 20 do Regulamento 910/2014.
[329] Artigo 17° do Regulamento 910/2014.
[330] Artigos 19 a 24° do Regulamento 910/2014.

4.2.3.2. Análise Custo-Benefício

Levanta-se a questão de se esta perspetiva de recurso à Criptografia não estará a colocar os prestadores de serviços de confiança numa posição cimeira e de excessiva vantagem relativamente a provas.

Aqui convém ressalvar que, ainda que a sujeição dos serviços de certificação a um regime de autorização prévia esteja expressamente excluída, como forma de respeito ao livre funcionamento de mercado, isto não exclui a elaboração e planeamento de um sistema de fiscalização[331] das autoridades de certificação[332], como até o indicou o Regulamento 910/2014, ao longo dos seus considerandos[333].

Aliás, olhando para o Considerando 11 do Regulamento 910/2014, fica plasmado que

> *"Nesta matéria (privacidade e proteção de dados pessoais), tendo em conta o princípio de reconhecimento mútuo estabelecido pelo presente regulamento, a autenticação para acesso a um serviço em linha deverá dizer respeito ao tratamento apenas dos dados de identificação que sejam adequados, pertinentes e não excessivos para conceder acesso ao serviço em linha em causa. Além disso, os requisitos previstos na Diretiva 95/46/CE em matéria de confidencialidade e segurança do tratamento dos dados deverão ser respeitados pelos prestadores de serviços de confiança e pelas entidades supervisoras."*

O próprio artigo 13º nº1 do Regulamento em causa clarifica que *"os prestadores de serviços de confiança respondem pelos danos causados deliberadamente ou por negligência a todas as pessoas singulares ou coletivas por incumprimento das obrigações"*, sendo que *"o ónus da prova da intenção ou negligência de um prestador não qualificado de serviços de confiança recai sobre a pessoa singular ou coletiva que intente a ação de indemnização pelos danos"*,

---

[331] *"Para facilitar a fiscalização dos prestadores qualificados de serviços de confiança, por exemplo no caso de prestação de serviços no território de outro Estado-Membro, onde o prestador não está sujeito a supervisão, ou no caso de os computadores do prestador estarem localizados no território de um Estado-Membro diferente daquele em que se encontra estabelecido, deverá ser criado um sistema de assistência mútua entre as entidades supervisoras dos Estados-Membros"* – Considerando 42 do Regulamento 910/2014.

[332] *"A criação de um regime de supervisão para todos os prestadores de serviços de confiança deverá garantir condições de igualdade no que respeita à segurança e à responsabilização no quadro das suas operações e serviços, contribuindo desta forma para a proteção dos utilizadores e para o funcionamento do mercado interno. Os prestadores não qualificados de serviços de confiança deverão ser sujeitos a uma supervisão ligeira e reativa realizada, a posteriori e justificada pela natureza dos seus serviços e operações. Por esse motivo, a entidade supervisora não deverá ter a obrigação geral de supervisionar prestadores de serviços não qualificados. A entidade supervisora só deverá tomar medidas quando for informada (por exemplo, pelo próprio prestador não qualificado de serviços de confiança, por outra entidade supervisora, por notificação de um utilizador ou parceiro comercial, ou com base na sua própria investigação) de que determinado prestador de serviços não qualificado não preenche os requisitos do presente regulamento."* – Considerando 36 do Regulamento 910/2014.

[333] *"Todos os prestadores de serviços de confiança deverão ficar sujeitos aos requisitos do presente regulamento, nomeadamente aos que dizem respeito à segurança e à responsabilidade para garantir a devida diligência, a transparência e a responsabilização das suas operações e serviços. Contudo, tendo em conta o tipo de serviços por eles prestados, é necessário distinguir entre prestadores qualificados e não qualificados de serviços de confiança relativamente a esses requisitos."* – Considerando 35 do Regulamento 910/2014

presumindo-se *"a intenção ou negligência de um prestador qualificado de serviços de confiança, exceto se este provar que os danos (...) não foram causados por sua intenção ou negligência"*.

4.3. O Papel da Lógica

Conforme dito por FULLER[334], uma das mais antigas e insatisfeitas aspirações da Humanidade diz precisamente respeito à busca pela perfeição da legalidade, pelo que no desenrolar da Era Digital nos cabe ponderar se a utilização das novas tecnologias da informação será efetivamente capaz de colmatar as falhas dos sistemas jurídicos e avançar para uma verdadeira "ciência legislativa"[335].

Segundo HARARI[336], para as capacidades passíveis de competição entre Homem e Máquina prendem-se com o domínio físico e com a cognição, sendo que, até ao século XX, a competitividade se prendia primordialmente no que dizia respeito ao nível físico, como se verificou ao longo da Revolução Industrial, com a automação de trabalhos manuais na agricultura e na indústria. Já o domínio cognitivo, concernente à capacidade de aprendizagem, análise, comunicação e compreensão de emoções humanas, tem sido tradicionalmente dominado pela espécie Humana, apesar de o paradigma se encontrar em mutação.

Todas e quaisquer tentativas de transposição da realidade jurídica nos meios informáticos implicam um conjunto de mecanismos intelectuais complexos, entre os quais a lógica ocupa um lugar de destaque, pelo que autores como LACAMBRA[337] afirmam que "desde cedo que a lógica tem sido uma atividade da qual os juristas têm feito uso consciente para alcançar um conhecimento científico do Direito".

Os sistemas informáticos constituem um instrumento para a elaboração de informações, tendo como base a conversão de uma série de dados ou informações (que entram via *"input"*) para outra série de dados e informações (*"output"*), que pressupõem nova informação. Este processo designa-se de "programação", visando obter uma linguagem capaz de ser assimilado pelas máquinas, daí se falar de uma *"machine language"*.

---

[334] FULLER, Lon L., *"The Morality of Law: Revised Edition"*, Yale University Press, 1969, p.49.
[335] LACAMBRA, Legaz, *"Filosofia Del Derecho"*, Bosch, Barcelona, 1961, pp. 91 e ss.
[336] HARARI, Yuval Noah, "21 Lessons for the 21st Century", Jonathan Cape, London, 1ª edição, 2018, pp. 19-20.
[337] LACAMBRA, Legaz, *"La lógica como posibilidad del pensamento jurídico"* in *"Anuario de Filosofia del Derecho"*, 1957, p.52.

Com base neste pressuposto, já muito se discutiu relativamente à transposição de problemas jurídicos para uma dimensão lógica, a fim de os submeter a uma posterior transformação, suscetível de os incorporar num processo cibernético[338].

Autores como PHILLIPS[339], por exemplo, demonstraram-se favoráveis à aplicação da informática no Direito, partindo de uma aplicação base em questões de acidentes rodoviários, e com uma aplicação a lógica formal na automatização de decisões concernentes a domínios como a fiscalidade e os seguros.

A lógica jurídica está associada à ideia de que fazemos do Direito e que se lhe adapta. Neste sentido, seja qual for a técnica de raciocínio utilizada em direito, este não pode desinteressar-se da reação das consciências diante da iniquidade do resultado ao qual o raciocínio conduziria. O esforço dos juristas é, e sempre foi, no sentido de procurar conciliar técnicas de raciocínio jurídico com a justiça ou, pelo menos, com a aceitabilidade social da decisão. Concluímos assim que, um raciocínio puramente formal, que se limita a controlar a correção das inferências, sem fazer um juízo sobre o valor da conclusão é, no direito, insuficiente[340].

Ora, mesmo com esta consideração, é inegável que a investigação jurídica está, em grande parte, integrada por uma série de processos estandardizados de caráter subalterno, destinados na acumulação e na ordenação de dados. Parece-nos razoável considerar estes como passíveis de automatização[341] sem nunca esquecer, claro, que de momento não se poderá tratar de uma automatização plena, mas sim de uma de colaboração com o investigador humano, pela natureza finalística da investigação que, de momento, se encontra vedada as máquinas, incapazes de decidirem e pensarem por si de forma criativa[342].

Este pensamento parece uma ótica razoável a adotar-se, visto que de nenhuma maneira visa suplantar ou substituir o juiz-humano por um juiz-robot, nem alcançar a chamada *"machine*

---

[338] PÉREZ LUÑO, Antonio-Enrique, *"Cibernética, Informática y Derecho (un análisis metodológico)"*, Publicaciones de Real Colegio de España Bolonia, 1976, p. 45.

[339] PHILLIPS, Lothar, *"Von nervösen und phlegmatischen Rechsbegriffen – Ein Beitrag zur Rechtstatsachenforschung"* in *"Informationsgetsellschaft und Rechtskultur in Europa"*, Nomos, Baden-Baden, 1995, p. 192.

[340] *"(...)a pretensão de computorizar o raciocínio e a decisão analógicos só é suscetível de resultados muito limitados (...) – possibilidades, pois, só de programação ou de controle, e nada mais (...). A razão decisiva está – digamo-lo em termos gerais – em que os computadores têm possibilidades sintátcas, mas não capacidade semântica"* - CASTANHEIRA NEVES, António, *"Metodologia Jurídica (Problemas fundamentais)"*, Coimbra Editora, Coimbra, 1993, pp. 251-252.

[341] *"(...) quando se trate de fenómenos massivos, que se apresentam sempre de maneira idêntica e onde as circunstâncias particulares do caso (...) não desempenhem qualquer papel, o juiz que decide o caso concreto pode ser substituído pelo computador, previamente instruído para todos os casos."* - LARENZ, Karl, *"Metodologia da Ciência do Direito"*, 2ª edição, Fundação Calouste Gulbenkian, Lisboa, p. 283.

[342] *"Machines can process data for and products of such procedures; but they cannot perform them"* - STONE, Julius, *"Computers, Behavioural Science and the Human Judge"*, p. 695.

made justice", mas antes adota uma solução pragmática e que visa aliar a facilidade de assimilação de informações mecânicas à facilitação e agilização dos vários processos que cada vez mais inundam o sistema judicial[343].

Aqui, entra a Lógica, cujo papel e relevância iremos agora explanar e ligar ao tema do presente trabalho.

4.3.1. Noções básicas de lógica

A Lógica tem como objeto de estudo as leis gerais do pensamento (raciocínio) e o modo como as irá aplicar corretamente na procura da verdade (mecanização do raciocínio), por meio da formulação de leis gerais de encadeamento que permitem a descoberta de novas verdades, tendo como base observações avaliadas como verdadeiras.

Assim, com base nas observações da realidade, o raciocínio[344] possibilita a análise de proposições[345] (afirmações passíveis de avaliação lógica, ou seja, de serem classificadas como verdadeiras ou falsas) e de silogismos (mecanismo de interpretação que obtém uma conclusão a partir de duas afirmações).

Ora, a lógica matemática adota dois princípios fundamentais de pensamento, nomeadamente o princípio da não negação (uma proposição não pode ser verdadeira e falsa ao mesmo tempo) e o princípio do terceiro excluído (uma proposição é apenas verdadeira ou falsa, nunca se verificando um terceiro caso que não um destes).

Por assunção do Princípio do terceiro excluído, qualquer proposição tem o valor lógico de verdade (V) ou de falsidade (F), sendo que no caso das proposições compostas, o seu valor lógico depende unicamente dos valores lógicos das proposições simples que a compõem. Para determinar o valor lógico de proposições compostas utiliza-se a construção de tabelas de verdade.

Representaremos de seguida exemplos de operações lógicas e as tabelas de verdade que lhes dizem respeito, para clarificar em termos práticos o que estamos a apresentar.

---

[343] Esta ideia aproxima-se bastante das teorias de Viktor KNAPP, o qual, não obstante considerar absurda qualquer criação automatizada de material legislativo, perspetivou a aplicação da cibernética e da lógica a certas fases do processo legislativo, para o agilizar e o tornar mais preciso, especialmente numa ótica de evitar repetições e contradições em projetos de lei.

[344] Entendido como sendo o modo como o encadeamento de observações permite obter novo conhecimento.

[345] Dentro das proposições podemos encontrar proposições simples (que não se decompõem noutras proposições, como é o caso de "Todos os Homens são mortais") ou proposições compostas (que se decompõem em proposições simples, como é o caso de "Todos os Homens são mortais e todos os Deuses são imortais")

4.3.2. Operações Lógicas e respetivas tabelas de verdade

Negação (¬): proposição representada por ***"¬p"***, cujo valor lógico é verdade quando p é falsa e falsidade quando p é verdadeira.

- ***p*** - Direito é uma ciência.
- ***¬p*** – Direito não é uma ciência.

p	***¬p***
V	F
F	V

Conjunção (**^**): proposição representada por ***"p ^ q"***, cujo valor lógico é verdade quando ambas as proposições ***"p"*** e ***"q"*** são verdadeiras e falsidade nos restantes casos.

- ***p*** – Direito é uma ciência jurídica.
- ***q*** – Direito é uma ciência social.
- ***p ^ q*** – Direito é uma ciência jurídica e uma ciência social.

p	***p***	***p^q***
V	V	V
V	F	F
F	V	V
F	F	F

Disjunção (**v**): proposição representada por ***"p v q"***, cujo valor lógico é verdade quando pelo menos uma das proposições é verdadeira e falsidade quando ambas as proposições são falsas.

- ***p*** – Direito é uma ciência jurídica
- ***q*** – Direito é uma ciência social.
- ***p v q*** – Direito é uma ciência jurídica ou uma ciência social.

p	***p***	***p v q***
V	V	V
V	F	V
F	V	V
F	F	F

Disjunção exclusiva (**v´**): proposição representada por "***p v´ q***", cujo valor lógico é verdade quando somente uma das proposições é verdadeira e falsidade quando ambas as proposições são falsas ou ambas são verdadeiras.

- **p** – Direito é uma ciência jurídica.
- **q** – Direito é uma ciência social.
- ***p v´ q*** – Ou Direito é uma ciência jurídica ou é uma ciência social.

p	***p***	***p v´ q***
V	V	F
V	F	V
F	V	V
F	F	F

Implicação (→): proposição representada por ***"p → q"***, em que o valor lógico é falsidade quando "p" é verdadeira e "q" é falsa e verdade nos restantes casos.

- p – Direito é uma ciência jurídica.
- q – Direito é uma ciência social.
- ***p → q*** – Se Direito é uma ciência jurídica, então é uma ciência social.

p	***p***	***p → q***
V	V	V
V	F	F
F	V	V
F	F	V

Equivalência (↔): proposição representada por ***"p ↔ q"***, cujo valor lógico é verdade quando ambas as proposições são verdadeiras ou são falsas e falsidade nos restantes casos.

- ***p*** – Direito é uma ciência jurídica.
- ***q*** – Direito é uma ciência social.
- ***p ↔ q*** – Direito é uma ciência jurídica somente se for uma ciência social.

p	***p***	***p ↔ q***
V	V	V
V	F	F
F	V	F
F	F	V

4.3.3. Caso Concreto: Viktor Knapp

De forma a conseguir compreender uma aplicabilidade prática destes pressupostos, particularmente no funcionamento e na automatização do processo, usaremos como exemplo os estudos desenvolvidos por KNAPP, nas suas tentativas de converter uma realidade social complexa para uma representação analógica e simplificada da mesma, suscetível de ser apreendida por máquinas.

Assim, pegando em diversos elementos e pressupostos das sentenças de divórcio do ordenamento jurídico checo, KNAPP representou em linguagem binária os seus diversos elementos e pressupostos. Com base nesta codificação, elencou as relações passíveis de se formalizarem e, por conseguinte, serem entendidas e processadas pelas máquinas designadas para o efeito.

Desta forma, por meio da expressão binária dos elementos tipicamente contidos em sentenças de divórcio, estes elementos jurídicos estariam disponíveis e acessíveis à compreensão mecânica, sugerindo uma possível automatização do processo.

Sucede que, dentro da terminologia legal, muitos conceitos adquirem valor altamente abstrato, devendo cada situação implicar uma noção altamente casuística e de definição bastante fluida, o que coloca sérios entraves na automatização e tradução destas nuances num número finito de fórmula lógico-matemáticas.

Em resposta a esta limitação, KNAPP procedeu a um levantamento estatístico das causas mais comuns de divórcio, dentro daquilo que era reconhecido pelos tribunais checos, conseguindo apontar alguma estabilidade comprovado no número de causas do divórcio, o que abonou a seu favor para possibilitar a expressão das causas de divórcio sob a forma de um número finito de fórmulas lógico-matemáticas, aproximando-se com alguma exatidão daquela que era a realidade.

Assim, não obstante não ser possível uma representação matemática das causas de separação em função das presunções legais de divórcio que seja uma representação exata da realidade, esta análise prova que é possível abrir novas perspetivas relativamente à aplicação da lógica matemática e cibernética no domínio jurídico, visto que o pensamento dialético humano,

no entendimento de KNAPP, se aproxima do autómato, no sentido em que opera com um número finito de matrizes[346].

4.3.4. Aplicação à prova eletrónica-digital

De forma geral, até mesmo leiga, por prova entende-se os enunciados sobre factos, pelo que dizer que um facto está provado significa comprovar a confirmação do seu referente empírico, ou seja, da sua verdade.

De uma forma mais simples, o procedimento probatório visa uma conexão de sentido, um processo de inferência mediante o qual, a partir dos meios de provas, se conhecem factos relevantes para a tomada de decisão, e onde se formulam ou verificam enunciados assertivos sobre os factos enunciados, possibilitando a sua descoberta pelo juiz, no fundo.

A nível do que foi exposto até ao momento, e sempre na lógica de tornar o processo mais célere e pragmático, parece clara a forma como se poderá aplicar a lógica matemático-formal em termos jurídicos, especialmente quando dirigida ao domínio da prova eletrónica, também ela fortemente ligada às novas tecnologias da informação. Neste sentido, é relevante analisar a postura de GARCIA MARQUES[347], certo do potencial da utilização da automação para *"testar a aplicação da lógica silogística"*, bem como para *"ajudar a detetar quais as regras de raciocínio seguidas em acervos cada vez mais abundantes de casos decididos"*.

Olhando para o subtópico anterior, referente às técnicas criptográficas, e com principal enfoque nos certificados eletrónicos das assinaturas digitais; parece bastante útil e razoável considerar a verificação e a autenticidade destes por via automática, e a sua consequente inclusão e análise processual, visto que o número de factos e situações passíveis de serem considerados na sua admissão ou rejeição são relativamente finitos, como o constatou KNAPP nas especificidades próprias do seu estudo.

Esta aplicação da lógica, ainda que perspetivada num sentido de sistema de apoio à decisão, afigura-se em muito útil na consagração de um sistema jurídico cujas infraestruturas se encontram capazes de facilitar a valoração e a agilização da apreciação da prova em si.

---

[346] KNAPP, Viktor, *"De l'application de la cybernétique au demaine du droite"*, pp. 15-18.
[347] GARCIA MARQUES, Gabriel, MARTINS, Lourenço, *"Direito da Informática"*, IJC, Almedina, Coimbra, 2000, pp. 39-40.

Conforme mencionado anteriormente (nomeadamente, no Ponto 2 do presente capítulo), a adesão doutrinária e consuetudinária a uma dada modalidade jurídica encontra-se ligada à facilidade com que esta nos chega ou é manobrada. Um forte sistema eletrónico de apoio à decisão do juiz pode-se afigurar como uma mais valia à normalização do uso processual da prova digital-eletrónica por via jurisprudencial e, por inerência, via doutrinal.

Ainda que não linear, e com a grande variedade de normas que encontramos no nosso ordenamento, há sugestões de autores sobre como colmatar insuficiências da automatização, como é o caso de DIAS PEREIRA[348]. Para este autor, mesmo no caso de lacunas não previstas nas hipóteses normativas, uma programação mais complexa poderá prever (ou sujeitar a consideração) casos formalmente distintos, porém, materialmente semelhantes, abrindo o regime de uma norma com base no argumento *a fortiori*, por maioria de razão ou *ad maius ad minus*, baseando-se na casuística jurisprudencial e em propostas doutrinais.

Abrimos aqui um grande leque de potencialidades para uma aplicação mais rápida e eficiente de Regulamentos (como é o caso do Regulamento 910/2014) e de Diretivas, facilitando e agilizando o processo e a valoração e consideração de provas que poderiam causar dificuldades na análise por parte de juízes, evitando assim um forte acumular processual e solucionando um dos grandes desafios daquela que é a modernidade jurídica.

Estes estudos alinham-se com as análises de FIEDLER[349], que considerou que a possibilidade da informatização e automação do Direito se manifestaria apenas em setores dependentes de regras elaboradas formalmente e que sejam dependentes de conceitos precisos, realidade à qual se adequa verdadeiramente o estudo elaborado até ao momento.

Conforme dito anteriormente, fica a ressalva de que, naturalmente, estas ideias só poderão vingar em setores caracterizados por uma dada "rotina lógica"[350], com um número restrito de processos exatos e regras precisas, o que exclui vários setores da índole jurídica[351] pautados por grande ambiguidade e discricionariedade nos seus conceitos.

Assim, não estaríamos naturalmente a confiar a máquinas as tarefas de apreciação das provas em si, nem muito menos da análise da matéria de facto ou de Direito, nunca lhes conferindo efetivamente a capacidade de julgarem ou tomarem qualquer decisão vinculativa no

[348] DIAS PEREIRA, Alexandre Libório, "*Lex informática...*" in *"Boletim da Faculdade de Direito – Studia Iuridica 9 Ad Honorem 3"*, Coimbra Editora, pp. 825-831
[349] FIEDLER, H., *"Rechenautomaten als Hilfsmittel der Gesetzesanwendung"*, pp. 152 ss.
[350] KLUG, Ulrich, "Máquinas electrónicas para la elaboración de dato sen el Derecho", pp. 55 ss.
[351] ZIPPELIUS, Reinhold, *"Einführung in die juristische Methodenlehre"*, C. H. Beck, München, 1971, pp. 126 ss.

âmbito do processo, afastando-se desde já a ideia do "juiz-máquina", mencionada anteriormente[352].

Agora, dentro do leque particular de especificidade e com um número finito de situações a serem abordadas, consideramos mais que pertinente o uso da lógica formal em conjunto com a lógica jurídica, não só como complementaridade à Criptografia no âmbito do apoio que representam para a prova eletrónica, mas também como ferramentas auxiliares ao longo de todo o processo.

Se pensarmos, o Portal CITIUS, conforme dito anteriormente, é o meio primordial no qual os mandatários judiciais exercem as suas funções, pelo que tarefas mais simples, tais como a determinação da competência territorial (ou inclusive o cumprimento ou não cumprimento de prazos), poderiam ser facilmente agilizados e alvo de resposta da parte das entidades estatais competentes, caso um processo automatizado e capaz de conferir respostas lógicas e rápidas estivesse implementado.

As possibilidades são inúmeras, e o receio de que diversos cargos possam estar comprometidos são colmatáveis via a evolução natural do mercado de trabalho, particularmente se o mundo jurídico adotar uma postura de colaboração homem-máquina, conforme o prevê HARARI[353] relativamente ao mundo do trabalho em geral.

De facto, desde o início da Revolução Industrial que os receios de uma onda massiva de desemprego no advento da tecnologia não se materializaram. Pelo contrário, cada emprego substituído por uma máquina originou, no mínimo, mais um novo emprego, num constante aprimorar do nível médio de vida[354]. Apesar de o paradigma que aqui está em causa ser diferente (por se tratar de trabalho mais qualificado), não devemos ser cínicos nem excessivamente pessimistas, visto que, no que concerne ao mundo jurídico e às suas especificidades, estamos dotados de uma zona de conforto da qual muitos outros setores de atividade não beneficiam.

---

[352] Mesmo que assim fosse, é relevante considerar o artigo 13° n°1 da Lei 67/98, de 26 de outubro (correspondente ao artigo 15° da Diretiva 95/46/CE), e que menciona que *"qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento".*

[353] *"AI might help create new human jobs in another way. Instead of humans competing with AI, they could focus on servicing and leveraging AI. For example, the replacement of human pilots by drones has eliminated some jobs but created many opportunities in maintenance, remote control data analysis and cyber security. (...) If so, the job market of 2050 might well be characterized by human-AI cooperation rather than competition."* – HARARI, Yuval Noah, "21 Lessons...", Jonathan Cape, London, 1ª edição, 2018, p. 29.

[354] WOIROL, Gregory R., *"The Technological Unemployment and Structural Unemployment Debates"*, Greenwood Press, Wesport, 1996, pp. 18-20.

Por fim, ressalvamos, novamente, que neste ponto nos limitamos a tecer meramente considerações hipotéticas de uma possível aplicação das tecnologias da informação ao serviço do Processo; sendo todos estes pensamentos meramente especulativos e alicerçados no campo da eventual possibilidade.

4.4. Privacidade e Proteção de Dados

Além do volume crescente de informação que circula e da velocidade com que esta se transmite em rede, particularmente se tomarmos em conta o fenómeno de *"cloud computing"*[355], torna-se impossível de negar que cada vez mais agentes (sejam públicos ou privados, humanos ou não humanos[356]) têm um acesso globalizado e facilitado aos dados pessoais dos cidadãos que os tenham colocado num qualquer *website*.

Se isto funciona como garante de uma prova forense eletrónica (e da sua eventual necessidade processual), torna-se inegável de que a publicação de informações em meios digitais se tornaram definitivas e irreversíveis, sendo cada vez mais difícil apagar os dados e exercer o direito ao esquecimento e de gerir as relações entre as autoridades estaduais e os parceiros civis e comerciais na defesa destes direitos.

Perante este risco de fragilização do direito fundamental à privacidade dos titulares de dados[357], muitos países e entidades visam dar resposta às ameaças do setor público e privado, no que diz respeito ao tratamento de dados[358] pessoais por meio da utilização das tecnologias de informação, sendo que por "dados pessoais" entendemos *"a informação relativa a uma pessoa singular ou identificável"*, definição dada pelo artigo 4º nº1 do Regulamento 679/2016 UE.

Assim, numa grande generalidade dos ordenamentos jurídicos se foram desenvolvendo alguns princípios fundamentais que, com nuances próprias em cada caso, apontam um conjunto

---

[355] *"A computação distribuída (ou em nuvem) é um novo modo de fornecer tecnologia, serviços e produtos informáticos, dando a possibilidade aos utilizadores de aceder, partilhar, e armazenar informação através da internet. A nuvem é uma rede de centros de dados – cada um composto por milhares de computadores trabalhando em rede – que conseguem executar programas de software em computadores pessoais ou comerciais, usando um fornecimento de acesso a sofisticadas aplicações, plataformas e serviços oferecidos através da internet."* – ANDRADE, Francisco, *"Comunicações Eletrónicas e Direitos Humanos: O Perigo do Homo Conectus"* in "Direitos Humanos e sua Efetivação na Era da Transnacionalidade", Juruá Editora, Curitiba, 2012, p. 208.

[356] Cada vez mais se recorre aos chamados "agentes de software" para a recolha de dados e sua transmissão a terceiros (humanos ou eletrónicos), como nos indica BETTELI, Alessandra Villeco, *"Agent Technology and On-line Data Protection"*, 2002.

[357] Neste sentido, ver o artigo 16º do Tratado sobre o Funcionamento da União Europeia (TFUE), na sua alteração fruto do Tratado de Lisboa, em 2009.

[358] Seguiremos a definição presente no artigo 4º nº3 do Regulamento Geral de Proteção de Dados (RGPD), também conhecido por Regulamento 679/2016 UE, que entende tratamento de dados como sendo a *"operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estrutura, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição"*.

de deveres base por parte das organizações públicas e privadas, seja ao nível de (i) indicação dos objetivos por trás da recolha de dados, (ii) limitação da recolha de informações com base no consentimento expresso dos indivíduos e no caráter de necessidade imposto pelos objetivos da recolha, (iii) garantias da conformidade, totalidade, proteção e atualização da informação e (iv) ao acesso dos indivíduos às suas informações pessoais, que apenas devem ser retidas quando necessárias e nunca utilizadas nem não divulgadas para fins que não os identificados, salvo com o consentimento do indivíduo (princípio da finalidade)[359].

No que diz respeito ao tema da presente tese, e tomando em conta o caráter de interdisciplinaridade que marca as várias áreas em análise neste capítulo, temos de verificar até que ponto a regulamentação atual garante a defesa dos direitos de privacidade dos cidadãos, a partir do momento em que estes começam a circular em plataformas judiciais digitais.

Não obstante termos clarificado que o Portal CITIUS beneficia de garantias de segurança que dificultam o acesso da generalidade da população aos dados das partes contidas em processos que circulam na plataforma; cabe-nos ainda plasmar de que forma conseguimos garantias da segurança e confidencialidade desses mesmos dados relativamente a quem os pode manobrar e relativamente aos Estados em si.

4.4.1. Proteção de Dados em Portugal

No paradigma português verifica-se que, já desde a sua redação original de 1976 que a Constituição da República Portuguesa prevê a epígrafe "Utilização da informática", consagrando direitos que especificamente protegem os dados pessoais dos cidadãos em relação às novas tecnologias, o que, na prática, instituiu um direito fundamental à autodeterminação informativa.

Conforme apontado por SARMENTO E CASTRO[360], esta autodeterminação informativa traduz-se num conjunto de direitos que visam proteger os dados pessoais dos cidadãos de ameaças de recolha e de divulgação (entre outras) pelas novas tecnologias; e, também, assegurar aos respetivos titulares um conjunto de poderes de escolha (ou seja, de autodeterminação) relativamente à forma como deverão ser tratados os seus dados, nesse âmbito.

---

[359] RAAB, Charles D., *"Vigilância e privacidade: as opções de regulação"* in *"A sociedade vigilante: Ensaios sobre identificação, vigilância e privacidade"*, ICS: Imprensa de Ciências Sociais, Lisboa, 2008, pp. 258-259.

[360] SARMENTO E CASTRO, Catarina, *"40 anos de 'Utilização da Informática' - o artigo 35.º da Constituição da República Portuguesa"*, ePública: Revista Eletrónica de Direito Público, vol. 3 nº 3, dezembro de 2016, p. 44.

No que diz respeito à jurisprudência do Tribunal Constitucional em questões de privacidade de dados pessoais, tem-se começado a assistir a uma abordagem progressiva, que recorre à invocação do artigo 35º para proteger o cidadão de um uso indevido e/ou abusivo das suas informações pessoais, como o indicam os acórdãos 355/97[361] e 368/2002[362]. Torna-se claro que o direito à reserva da intimidade da vida privada (previsto no artigo 26.º da Constituição) e o direito de inviolabilidade/sigilo das telecomunicações (artigo 34.º da Constituição) ganharam complementaridade na defesa dos interesses da privacidade dos dados dos cidadãos.

O âmbito da proteção conferida pelo artigo 35º extravasa o objeto do direito à reserva da intimidade da vida privada e do direito à inviolabilidade do segredo das telecomunicações, visando sempre garantir ao respetivo titular os direitos aí consignados, como inclusive o indica o Acórdão 213/2008[363].

Recentemente, releva chamar à atenção para a publicação da Lei 58/2019, de 8 de agosto, e que que assegura a execução do RGPD na ordem jurídica interna, revogando a Lei 67/98, de 26 de outubro (Lei de Proteção de Dados Pessoais) e fazendo alterações à Lei 43/2004, de 18 de agosto, que regula a organização e o funcionamento da Comissão Nacional de Proteção de Dados. O funcionamento do RGPD está uma realidade cada vez mais presente, e os vários órgãos, públicos e privados, necessitam de adequada preparação.

4.4.2. Na Europa – Regulamento Geral de Proteção de Dados

A competência da UE para regular a matéria relativa à proteção de dados de carácter pessoal está prevista no artigo 16º do Tratado sobre o Funcionamento da União Europeia (TFUE), que clarifica que *"todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito"*[364], devendo o Parlamento Europeu e o Conselho estabelecer normas relativas à proteção das pessoas singulares no que diz respeito (i) ao tratamento de

[361] Neste Acórdão, o Tribunal considerou que os dados de saúde eram dados sobre a reserva da intimidade da vida privada, recorrendo ao artigo 35º da CRP por se tratar de um tratamento de dados automatizados, previstos na letra desse mesmo artigo.

[362] Respeitante às normas que versam sobre dados de saúde, ao instituírem as fichas clínicas e de aptidão, no âmbito da segurança, higiene e medicina do trabalho.

[363] "Note-se, contudo, que esta proibição (do 35.º, n.º 4) não impede o acesso apenas aos dados íntimos duma pessoa, mas a todos os dados a ela relativos, mesmo que em nada afetem a sua privacidade. O que se pretende preservar é a informação individual de uma pessoa, independentemente desta respeitar ou não à sua intimidade, prevenindo-se um potencial risco de violação de direitos fundamentais do cidadão, nomeadamente o direito à reserva da intimidade da vida (...). Protege-se o chamado direito à autodeterminação informacional, o qual tem um círculo de aplicação, apenas parcialmente coincidente com o círculo de aplicação do direito à reserva da intimidade da vida privada, e que funciona como direito de garantia deste"

[364] Artigo 16º nº1 do Tratado sobre o Funcionamento da União Europeia (TFUE).

dados pessoais pelas instituições, órgãos e organismos da UE, bem como pelos Estados-Membros em aplicação do direito da União e (ii) à livre circulação desses dados entre os Estados-Membros e à garantia de um nível de proteção adequado para a transferência de dados pessoais para países terceiros[365]. ´

Assistimos a cerca de quarenta anos de desenvolvimento de leis gerais e específicas, destacando-se a Diretiva Europeia de Proteção de Dados 95/46/CE (também refletida na Diretiva das Telecomunicações de 97/66/CE), visando (i) obrigar os Estados-Membros à adoção de garantias semelhantes em todo o espaço da UE no domínio da proteção de dados pessoais e (ii) estipular procedimentos-regra quanto ao fluxo de dados pessoais para países terceiros. Em Portugal, a Lei 67/98, de 26 de outubro (também conhecida por "Lei da Proteção de Dados Pessoais"), transpôs esta diretiva

Pela sua natureza de Diretiva, o diploma legal nunca foi capaz de criar a harmonização pretendida[366] entre os vários Estados Membros, tendo cada qual levado a cabo uma transposição própria do diploma legal, o que resultou em abordagens distintas à questão da proteção de dados pessoais entre estes e numa incapacidade de atualização perante a evolução das tecnologias de informação[367]. Isto, por sua vez, resvalou numa profunda reforma legislativa europeia, que culminou com a elaboração do Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Com este novo diploma legal, conhecido também por Regulamento Geral de Proteção de Dados (RGDP), estabelece-se um quadro geral da EU em matéria de proteção de dados pessoais, tendo como principais objetivos reforçar a proteção dos titulares de dados pessoais alvo de tratamento, aumentar as oportunidades de negócio no mercado único digital, e contribuir para um aumento da competitividade económica europeia.

Uma modificação de relevo passa pelo alargar do âmbito de competência territorial do Regulamento, que passa a abranger também entidades responsáveis pelo tratamento de dados situados em países terceiros á EU quando os tratamentos de dados que efetuem se liguem à oferta de bens ou serviços dirigidos a residentes no território da União, ou com o controlo do seu

[365] Artigo 16° n°2 do Tratado sobre o Funcionamento da União Europeia (TFUE).

[366] Nos resultados do Eurobarómetro Especial 431 (2015), referente à proteção de dados, e disponível em https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf; 90% dos europeus consideraram relevante usufruir dos mesmos direitos e proteção numa lógica de uniformidade na Europa.

[367] SILVEIRA, Alessandra, MARQUES, João, "Do direito a estar a só ao direito ao esquecimento. Considerações sobre a proteção de dados pessoais informatizados no Direito da União Europeia: Sentido, Evolução e Reforma Legislativa", Revista da Faculdade de Direito – UFPR, Curitiba, vol. 61, n. 3, set./dez. 2016, p. 96.

comportamento (via *cookies*, por exemplo). No que diz respeito à prova eletrónica, isto passa a ser do máximo relevo, particularmente se tomarmos em conta o crescente número de processos que envolvem cidadãos europeus fora do território europeu.

O instituir de um princípio de responsabilidade também ganha relevo, ainda que não seja particularmente inovador da parte do RGPD.

4.4.3. Impacto na Prova Digital

O RGPD, no alcance que comporta, afeta a prova digital no que diz respeito aos riscos de privacidade que esta implica, fruto do grande influxo de informações que circulam nos meios tecnológicos, passíveis de utilização e acesso, que muito facilmente poderão violar o consentimento de tratamento por parte das partes.

Fica claro que poderosas ferramentas ficaram à disposição da investigação, cabendo ao legislador e ao julgador encontrarem um ponto comum entre estas ferramentas e a salvaguarda dos direitos, liberdades e garantias e a proteção dos dados pessoais e da privacidade.

Assim, mais do que advertência numa ótica de melhoria, é necessária uma análise e aplicação cuidadas na eventual codificação desta modalidade, de forma a se encontrar de acordo com os trâmites da legalidade de proteção de dados e da manutenção das suas garantias no seu tratamento para fins de arquivo de interesse público[368].

Dizemos isto porque em sede processual, seja civil, seja penal, o modo de recolha e utilização de dados poderá ser completamente comprometido se tomarmos em conta o potencial impacto na apreciação, admissibilidade e valoração das provas.

[368] O artigo 89º nº1 do RGPD clarifica que *"o tratamento para fins de arquivo de interesse público (...) está sujeito a garantias adequadas (...) para os direitos e liberdades do titular dos dados. Essas garantias asseguram a adoção de medidas técnicas e organizativas a fim de assegurar, nomeadamente, o respeito do princípio da minimização dos dados [nos termos do artigo 5º do RGPD, os dados devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados]. Essas medidas podem incluir a pseudonimização [tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares], desde que os fins visados possam ser atingidos desse modo. Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo."*.

4.4.3.1. Processo Penal

Olhando para o artigo 6º nº1 do RGPD, e no que interessa ao âmbito do Processo Penal e da investigação criminal, há um elencar da licitude do tratamento de dados perante a sua necessidade no "*cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito"*[369] ou na *"defesa de interesses vitais do titular dos dados ou de outra pessoa singular"*[370], o que parece apontar para uma previsão de um regime a ser seguido pelas autoridades competentes.

De facto, o próprio RGPD remete-nos[371] para um diploma em específico, nomeadamente, a Diretiva 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril. No artigo 15º desta Diretiva, é-nos clarificado que *"os Estados-Membros podem adotar medidas legislativas para limitar, total ou parcialmente, o direito de acesso do titular dos dados, se e enquanto tal limitação, total ou parcial, constituir uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de (...) evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais"* ou *"evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais"*[372].

Estas disposições parecem adequar-se a preocupações no âmbito penal, nomeadamente, a da inadmissibilidade de provas eletrónicas-digitais coletadas no âmbito da investigação, as quais, em grande parte não terão uma recolha consentida pelos seus titulares. A preocupação para com o sucesso da investigação criminal é clara da parte do legislador, o que, não obstante, não mitiga totalmente os receios de que o modo de recolha dos dados possa comprometer a sua apreciação em Tribunal, caso viole as garantias estipuladas pelo RGPD.

A própria jurisprudência europeia chama a atenção para esta sensibilidade, em acórdãos como o C-293/12 e o C-594/12 de 8 de abril de 2014 (*Digital Rights Ireland*[373] e *Seitlinger*[374], respetivamente), nos quais clarificam que os dados eletrónicos são *"suscetíveis de permitir tirar conclusões muito precisas relativamente à vida privada das pessoas cujos dados foram conservados"*, sendo essencial *"analisar a proporcionalidade da ingerência observada", no que respeita à conservação e tratamento de dados*.

[369] Artigo 6º nº1 alínea c) do RGPD.
[370] Artigo 6º nº1 alínea d) do RGPD.
[371] Considerando 19º do RGPD.
[372] Artigo 15º nº1 alíneas a) e b) da Diretiva 2016/680 do Parlamento Europeu e do Conselho.
[373] http://curia.europa.eu/juris/documents.jsf?num=c-293/12 (consultado a 11 de outubro de 2019).
[374] http://curia.europa.eu/juris/liste.jsf?language=pt&num=C-293/12 (consultado a 11 de outubro de 2019).

Conclui-se assim que o acesso a dados pessoais apenas é legítimo se não cumprir desproporcionalmente os direitos das pessoas seus titulares, mesmo estando em causa do combate ao crime, pelo que se deve sempre guiar pelos princípios de subsidiariedade e de proporcionalidade[375], particularmente no domínio processual e de tratamento e apresentação de dados suscetíveis de constituírem provas.

4.4.3.2. Processo Civil

Em sede de processo civil, cremos que faria sentido ponderar a consideração da admissibilidade de provas recolhidas em violação dos princípios de proteção de dados, especialmente se tomarmos em conta que a prova digital se trata de uma ferramenta poderosa na descoberta material da verdade, claramente fundamental noutros tribunais que não apenas os criminais[376].

Tal torna-se mais transparente se nos inteirarmos de que a própria natureza da prova eletrónica digital é agressiva em relação a vários direitos constitucionalmente consagrados, desde o direito à imagem[377], o direito à autodeterminação informacional e da comunicação e o direito à inviolabilidade do domicílio informático[378], o direito à reserva da intimidade da vida privada e familiar, entre outros, que se tornam vulneráveis pelo recurso à prova eletrónica-digital[379].

Assim, analogamente ao que se considera em sede criminal, as questões da análise da proporcionalidade da recolha de provas eletrónicas-digitais devem ser tomadas em conta, sendo confrontadas com os princípios e garantias do RGPD, de forma a garantir a licitude e admissibilidade clara desta nova figura probatória, que tantas vezes manobra com informações sensíveis e de natureza particularmente pessoal.

---

[375] MASSENO, Manuel David, *"A Prova Digital perante a Proteção de Dados Pessoais - uma perspetiva Portuguesa e Europeia"*, apresentação no âmbito da conferência *"Cibercriminalidade e Prova Digital – Jurisdição Penal e Processual Penal"*, promovida pelo Centro de Estudos Judiciários em julho de 2018.

[376] GONÇALVES, João Gama, *"A prova digital em 2017 – Reflexões sobre algumas insuficiências processuais e dificuldades da investigação"*, CEDIS Working Papers, Universidade Nova de Lisboa, 2017, p.35.

[377] Artigo 26° da Constituição da República Portuguesa.

[378] Artigo 34° da Constituição da República Portuguesa.

[379] RODRIGUES, Benjamin, *"Da Prova Penal, IV, Da Prova-Eletrónico-Digital e da Criminalidade Informático-Digital"*, Rei dos Livros, Lisboa, 2011.

4.5. Blockchain

A *Blockchain*, conforme o entendimento de alguns autores[380], diz respeito a uma *Distributed Ledger Technology*[381], altamente descentralizada, imutável e impossível e apagar ou modificar e que, por isso, tem vindo a ser denominada como uma *"máquina de produção de confiança"*[382], na qual a transmissão de informação consegue ser feita de forma muito mais célere e segura, garantindo a legitimidade de atuação e o anonimato de quem a ela recorre[383], uma vez que qualquer informação, para ser registada na *Blockchain* necessita que o bloco que a contém seja previamente validado.

Assim, *Blockchain* não constituí uma nova rede informática[384], mas sim uma forma de construir ou organizar uma rede[385], capaz de produzir e garantir confiança numa transação monetária ou transmissão de dados, pelo que a sua análise concretamente direcionada ao Processo, ainda que breve, se afigura altamente relevante.

4.5.1. Blockchain e o Processo

Dentro das suas especificidades, a tecnologia *Blockchain* ganha relevo no âmbito do atual projeto a partir do momento em que engloba a criptografia por meio do *hashing*[386] e o *proof of existence*[387] (prova da existência).

A primeira especificidade já tem a sua relevância mencionada no que diz respeito às técnicas criptográficas elencadas anteriormente, e à forma como estas garantem a autenticidade, confidencialidade e não repúdio das informações contidas em documentos, o que viabiliza a utilização da prova eletrónica.

O nosso foco aqui deve recair na segunda característica elencada, ou seja, a prova da existência, pelo caráter de complementaridade que possibilita às técnicas criptográficas pré-existentes e, consequentemente, pelas possibilidades que abre para a prova eletrónica. Este

---

[380] BALLANDIES, Mark, DAPP, Marcus, POURNARAS, Evangelos, "*Decrypting Distributed Ledger Design -Taxonomy, Classification and Blockchain Community Evaluation"*, Zurique, 2018, pp. 6-8.

[381] Conjunto de dados digitais replicados, compartilhados e sincronizados espalhados geograficamente em vários sites, países ou instituições

[382] MAHDI, Miraz, *"Blockchain: Technology Fundamentals of the Trust Machine"*, Hong-Kong, de 2017.

[383] Existem vários tipos de rede Blockchain, quanto ao nível de privacidade e de participação.

[384] Na realidade, ideia de uma DHT/Blockchain é mais o de oferecer um serviço de registo (BD) distribuído que oferece propriedades específicas como imutabilidade e integridade. Essa DHT é que é suportada sobre uma rede informática (Internet ou não).

[385] BARAN, Paul, *"On distributed communications: I. Introduction to distributed communications networks",* United States Air Force Project Rand, Califórnia, 1964, pp. 1-3.

[386] BRUYN, A. Shanti, *"Blockchain – An Introduction"*, *paper* de investigação para a Universidade de Amesterdão, agosto de 2017, p. 15.

[387] A *"proof of existenc*e" diz respeito a um serviço online que verifica a existência de ficheiros de computador a partir de uma altura específica, via transações de Blockchain marcadas por selos temporais. De forma muito simplista, poder-se-á dizer que a *"proof of existence"* corresponde a armazenar o *"hash"* em Blockchain, permitindo armazenar com segurança provas da existência de um dado documento.

processo implica um o registo de algo (seja fungível ou não fungível), sendo que os terceiros não autorizados se encontrarão impossibilitados de interpretar e aceder ao conteúdo *hash,* estando tal poder apenas acessível aos titulares do documento original, que podem provar a existência do documento ao repetirem o processo de *hashing* com uma cópia idêntica ao documento original.

Demonstrar a titularidade dos dados, inserir selos temporais, dar provas de propriedade e de integridade documental são algumas das várias potencialidades da prova de existência; visto que a mínima alteração a qualquer documento será apontada pela *Blockchain*.

Tomando em conta as insuficiências de portais como Portal CITIUS, ou inclusive os receios do comprometimento das provas eletrónicas pelo seu caráter de volatilidade, torna-se claro que com a *Blockchain* passamos a ter a possibilidade de registar publicamente um documento sem revelar nenhum dos seus conteúdos, o que aplicado na prática poderia simplificar a proteção dos documentos passíveis de constituírem elementos de prova, e, consequentemente, tornar muito mais simples a sua aceitação e confiança por parte do sistema jurídico.

O exposto supra, aliado às técnicas criptográficas, traduz-se num forte garante de autenticidade, não repúdio e integridade dos documentos passíveis de serem apresentados, o que em tudo aprece abonar em favor da prova eletrónico-digital e da confiança relativamente à mesma.

4.5.2. Perspetiva Comparada e integração da Blockchain

Levanta-se também a questão de uma eventual integração desta tecnologia enquanto meio de prova aceitável pelo nosso ordenamento jurídico, sendo que, a nível internacional, tanto a jurisprudência como a letra da lei se têm afigurado favoráveis, o que poderá servir como incentivo para a sua eventual implementação.

Numa perspetiva legal, observa-se o exemplo pioneiro americano que, em 2016, no Estado de Vermont, definiu quais os requisitos legais necessários a adotar para os tribunais considerarem informações contidas em redes *Blockchain* em termos de prova[388].

[388] "*(2) A digital record electronically registered in a blockchain, if accompanied by a declaration that meets the requirements of subdivision (1) of this subsection, shall be considered a record of regularly conducted business activity pursuant to Vermont Rule of Evidence 803(6) unless the source of information or the method or circumstance of preparation indicate lack of trustworthiness.*"- https://law.justia.com/codes/vermont/2016/title-12/chapter-81/section-1913 (consultado a 01 de agosto de 2019).

Numa perspetiva jurisprudencial, basta analisar a Pronúncia do Tribunal de Justiça de São Paulo, no que diz respeito ao Processo nº 2018.0001015661[389], tendo-se pronunciado favorável à aceitação de dados contidos numa rede *Blockchain* como meio de prova admissível em tribunal. Esta postura não é de todo inesperada, particularmente se tomarmos em conta que no artigo 369º do seu Código de Processo Civil especifica que, caso não os proíba expressamente, serão admissíveis *"todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz"*, tal como o é, neste caso, a *Blockchain*, enquanto elemento de prova atípico.

Da mesma forma, em 2018, o Supremo Tribunal Chinês, na sua interpretação da Lei 16/2018[390], pronunciou-se no sentido em que os tribunais da internet chineses deverão reconhecer dados digitais que sejam submetidos enquanto provas, caso as partes relevantes os tenham recolhido e armazenado por meio de tecnologia *Blockchain* e assinaturas digitais, selos temporais confiáveis e valores *hash* verificados; ou ainda via uma plataforma de depósito digital passível de provar a autenticidade da tecnologia utilizada.[391]

[389] Disponível em https://www.migalhas.com.br/arquivos/2019/3/art20190325-11.pdf (consultado a 01 de agosto de 2019).
[390] Disponível na língua original em http://www.court.gov.cn/zixun-xiangqing-116981.html (consultado a 01 de agosto de 2019).
[391] PEREIRA, José Carlos, Tese de Mestrado em Direito dos Contratos pela Universidade do Minho, 2019, pp.20-25.

Conclusão

Ao longo deste trabalho, foi-nos possível retirar várias conclusões a nível da forma como novos meios de prova devem ser perspetivados pelo julgador e pela doutrina, em termos das potencialidades da prova eletrónica-digital e no que concerne às exigências que devem ser feitas ao Processo Civil relativamente à sua integração deste tipo de prova nas suas disposições gerais.

Em primeiro lugar, é mais que claro que a tecnologia se imiscuiu nos negócios jurídicos, sendo que grande parte da prova documental que se poderá tentar apresentar em processo se encontra, na maioria dos casos, armazenada apenas e formato eletrónico. Com isto, conseguimos entender a pertinência de uma figura jurídica que permita o aproveitamento desta realidade para o Processo Civil.

Ainda que cientes das limitações e dificuldades deste tipo particular de prova, consideramos que o advento de tecnologias, como o são o fenómeno do *cloud computing*, da *Blockchain* e os novos meios de certificação eletrónica permitirão mitigar muitas das desconfianças que o sistema e o público possam sentir relativamente ao seu valor probatório e admissibilidade. Da mesma forma, acreditamos que a falta de preparação para esta mudança é um problema passível de ser relativizado com as devidas atividades de formação, não constituindo um argumento muito válido na resistência a este tipo de prova.

Se a prova eletrónica-digital pode ser perspetivada como sendo atípica, tomando em conta os trâmites escritos do Código de Processo Civil e do Código Civil, o certo é que a devemos analisar numa perspetiva de admissibilidade condicionada, mais atinente ao caso concreto e orientada em torno de um Processo Civil mais diligente e célere. O Processo Civil moderno enfrenta sérios desafios, não só na perspetiva de atualização face às novas tecnologias, mas também na busca da verdade material numa realidade em que cada vez mais se pedem soluções rápidas e eficientes. Não podemos, assim, rejeitar novas figuras e realidades, mas sim, atender ao caso concreto e verificar a sua pertinência, sempre em nome da correta resolução dos litígios.

As decisões jurisprudenciais, os entendimentos doutrinais e as escolhas legislativas dos vários ordenamentos nacionais estrangeiros deixam claro que a atualização dos vários sistemas

processuais civis é inevitável, recolhendo-se inclusive exemplos (como é o caso do Uruguai[392]) em que conferiram regimes próprios á prova eletrónica-digital, bem como o seu reconhecimento incondicional enquanto tipo de prova, ficando desde já estabelecida uma ponte comparativa relativamente à praticabilidade desta realidade.

De facto, os estudos realizados em relação à prova eletrónico-digital no âmbito do Direito Penal permitiram comprovar a necessidade de se preverem disposições deste âmbito nos códigos processuais, fruto da instabilidade de interpretação e conciliação de documentos legais que o acumular de leis e decretos-leis avulsos implicam. Um Processo Civil forte e centralizado, que preveja os vários tipos de prova, enquanto reflexo dos tempos, é algo a desejar-se em nome dos objetivos de celeridade e clareza processual.

Mais do que uma inserção de um regime específico de prova eletrónico-digital no Código de Processo Civil, concluímos também que existe uma grande margem de desenvolvimento do próprio sistema processual em direção a um processo eletrónico, que alia as novas tecnologias da informação aos seus objetivos.

Os receios de suplantação de funções e perda de estabilidade profissional são dissipados se adotarmos uma perspetiva de colaboração homem-máquina. Em suma, não estará aqui em causa um desejo de substituição do julgador por um agente de *software* ou por uma Inteligência Artificial, mas sim um facilitar do seu trabalho por meio da delegação de tarefas mais procedimentais e com pouca margem de criatividade a um agente que consegue filtrar e dar respostas rápidas e eficientes ao influxo de materiais probatórios que lhe são disponibilizados, podendo aferir as suas características para efeitos de valoração. Da mesma forma, conforme a História sempre o tem provado, já desde a Primeira Revolução Industrial que o Ser Humano e o Mercado sempre se conseguiram adaptar e renovar o universo do trabalho de acordo com as evoluções tecnológicas, pelo que, na pior das hipóteses, surgirão novos cargos dentro do mundo jurídico, que continuará a existir como um ramo predominantemente humano, pelas suas características únicas.

Naturalmente que não nos iludimos, uma vez que existem vários problemas fundamentados relativamente à falta de privacidade implicada pela aldeia global que se foi criando com a tecnologia, e a importância dos dados a serem tratados em sede de Processo não deve ser ignorada, especialmente se os formos colocar num meio em que muito dificilmente

[392] *Ley nº 17.016 – Capitulo XIII*

poderão ser apagados. Ainda assim, somos da opinião que as mesmas tecnologias que ameaçam a privacidade também podem funcionar para a tornar uma garantia, seja por recurso a mecanismos de autenticação rigorosos (no âmbito da Criptografia ou até mesmo da *Blockchain*).

Terminamos com uma visão otimista relativamente ao futuro que aguarda o nosso ordenamento jurídico naquela que é a Terceira Onda do desenvolvimento da Humanidade, sendo que as tecnologias, que evoluem a cada dia que passa a um ritmo vertiginoso, cada vez mais se orientam em direção à concretização do objetivo máximo do processo: a verdade.

Bibliografia

"The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation", Oxford University, 2018.

ALEXANDRE, Isabel, *"Provas Ilícitas em Processo Civil"*, Almedina, Coimbra, 1998.

AMARAL, Maria Lúcia, *"A Forma da República: Uma introdução ao estudo do direito constitucional"*, Coimbra, Coimbra, Editora, 2005.

AMARAL, Paulo Osternack, *"Provas: atipicidade, liberdade e instrumentalidade"*, 2ª edição, Thomson Reuters, 2017.

ANDRADE, Francisco Pacheco, *"Comunicações eletrónicas e Direitos Humanos: O perigo do homo connectus"* in *"Direitos Humanos e sua efetivação na Era da Transnacionalidade"*, Juruá Editora, Curitiba, 2012.

ANDRADE, Manuel A. Domingues de, *"Noções elementares de processo Civil"*, Coimbra Editora, Coimbra, 1993.

ANTWI-BOASIAKO, Albert, **VENTER**, Hein, *"A Model for Digital Evidence Admissibility Assessment" in "Peterson G., Shenoi S. (eds) Advances in Digital Forensics XIII. DigitalForensics 2017. IFIP Advances in Information and Communication Technology, Volume 511"*, Springer, Cham, 2017.

ARENHART, Sérgio e **MARINONI**, Luiz, *"Prova e Convicção"*, Thomson Reuters, 2015.

AROCA, Juan Montero, *"La Prueba en el Proceso Civil"*, S.L. Civitas Ediciones, Madrid, 2005.

AROCA, Juan Montero, *"Los principios políticos de la nueva Ley de Enjuiciamiento Civil - Los poderes del juez y la oralidade"*, Tirant Lo Blanch, Valencia, 2001.

ASHBY, Matthew P.J., *"The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis",* European Journal on Criminal Policy and Research, abril de 2017, pp. 4-12.

BALLANDIES, Mark, **DAPP**, Marcus, **POURNARAS**, Evangelos, "*Decrypting Distributed Ledger Design -Taxonomy, Classification and Blockchain Community Evaluation"*, Zurique, 2018.

BARAN, Paul, *"On distributed communications: I. Introduction to distributed communications networks",* United States Air Force Project Rand, Califórnia, 1964.

BARROS, Juliana Isabel Freitas, *"O Novo Processo Penal: Os Meios de Obtenção de Prova Digital consagrados na Lei 109/2009, de 15 de setembro"*, Tese de Mestrado pela Universidade de Coimbra, 2012.

BEIRÃO, Joana Maria, *"Da Distribuição do Ónus da Prova no Direito Processual Civil Português – Contributo para o Estudo da Possibilidade de Flexibilização através de uma Distribuição Dinâmica"*, Dissertação de Mestrado Profissionalizante Mestrado em Ciências Jurídico-Forenses pela Faculdade de Direito da Universidade de Lisboa, 2017.

BENTHAM, J., *"Tratado de las pruebas Judiciales"*, t.1, Buenos Aires 1959.

BETTELI, Alessandra Villeco, *"Agent Technology and On-line Data Protection",* 2002.

BRAVO, Rogério, *"As Tecnologias de Informação e a Compressão dos Direitos, Liberdades e Garantias – os efeitos das regras 10/10 e 1/1"*, Lisboa, 2012.

BRUYN, A. Shanti, *"Blockchain – An Introduction"*, *paper* de investigação para a Universidade de Amesterdão, agosto de 2017.

CABAÑAS GARCIA, J.C., *"La valoración de las pruebas y su control en el processo civil"*, Trivium, Madrid 1992.

CALEIRO, Carlos, **VIGANÒ**, Luca, **BASIN**, David, *"Deconstructing Alice and Bob"* in *"Electronic Notes in Theoretical Computer Science 135 (2005) 3–22"*, ELSEVIER, 2005.

CALMON, Petrônio, *"Comentários à lei de informatização do processo judicial"*, Rio de Janeiro: Forense, 2007.

CANCELA, Alberto Gil Lima, *"A prova digital: os meios de obtenção de prova no cibercrime"*, Tese de Mestrado pela Universidade de Coimbra, 2016.

CANOTILHO, J. J. Gomes, "Direito Constitucional e Teoria da Constituição", Coimbra, Almedina, 2003.

CANOTILHO, J. J. Gomes, e **MOREIRA**, Vital, *"Fundamentos da Constituição"*, 2ª edição., Coimbra Editora, Coimbra, 1991.

CARNEIRO, Davide, **NOVAIS**, Paulo, **ANDRADE**, Francisco, *"On-Line Dispute Resolution"*, 2011.

CARNELUTTI, Francesco, *"La prova civile"*, 1992.

CARNELUTTI, Francesco, *"Sistema di diritto processuale* vol. I.".

CARNELUTTI, Francesco, *"Teoria Geral do Direito"*, tradução de A. Rodrigues Queiró e Artur Anselmo de Castro, Armênio Amado Editor, Coimbra, 1942.

CARNELUTTI, Francesco, *"Teoria Geral do Direito"*. tradução de A. Rodrigues Queiró e Artur Anselmo de Castro, Armênio Amado Editor, Coimbra, 1942.

CASEY, Eoghan, *Digital Evidence and Computer Crime"*, 3ª edição Academic Press, 2011.

CASTANHEIRA NEVES, António, *"Metodologia Jurídica (Problemas fundamentais)"*, Coimbra Editora, Coimbra, 1993.

CASTELLS, Manuel, *"A Sociedade em Rede: Do Conhecimento à Acção Política"*, 2005.

CASTRO MENDES, João de, "*Do conceito de Prova"*, Lisboa: Ática, 1961.

CASTRO MENDES, Luís Filipe, *"5 Direito Processual Civil"*, I Vol, AAFDL.

CAVALLONE, Bruno, *"Il giudice e la prova nel processo civile" in "Processo e Giudizio, Vol. III"*, CEDAM, Padova, 1991.

CENDON, Paolo, **ZIVIL**, Patricia, *"L' inversione dell'onere della prova nel diritto civile, Rivista trimestrale di diritto e procedura civile"*, Milano, a.46n.3, 1992.

CONDE CORREIA, João, *"Prova digital: enquadramento legal"* in *"Cibercriminalidade e prova digital: Jurisdição Penal e Processual Penal"*, Centro de Estudos Judiciários, 2018.

COSTA ANDRADE, Manuel, *"Bruscamente no Verão Passado: A Reforma do Código de Processo Penal — Observações críticas sobre uma Lei que podia e devia ter sido diferente"*, Coimbra Editora. Coimbra, 2009.

COSTA MARQUES, Pedro Penha Leitão da, "*Informática Forense: Recolha e preservação da prova digital"*, Tese de Mestrado pela Universidade Católica Portuguesa, 2013.

DE CASTRO, Anselmo, *"Lições de processo civil, vol. IV"*, Atlântida, Coimbra, 1969.

DIAS PEREIRA, Alexandre Libório, "*Lex informatica, ius ex machina e justiça artificial"* in *"Boletim da Faculdade de Direito – Studia Iuridica 9 Ad Honorem 3"*, Coimbra Editora.

DIAS, Wladimir Rodrigues, *"Princípio da publicidade e comunicação estatal",* ALMG, pp. 1-15.

DIDIER JÚNIOR, Fredie, *"Fundamentos do princípio da cooperação no Direito Processual Civil Português"*, Coimbra Editora, Coimbra, 2010.

DIDIER JÚNIOR., Fredie*, "Curso de Direito Processual Civil: introdução ao direito processual civil, parte geral e processo de conhecimento"*, 18ª Edição, Salvador, Edições JusPodivm, 2016.

DOHNA, Alexander Graf zu, *"Kernprobleme der Rechtsphilosophie"*, Gentner, 1966.

EISNER, Isidoro, *"La prueba en el proceso civil"*, Abeledo-Perrot, Buenos Aires, 1964.

ESTEVES, José, *"Um novo Mundo, uma nova Racionalidade, um novo processo Civil"*, in *"I Jornadas de processo civil - Olhares transmontanos"*, Valpaços, 2012.

FERNANDEZ, Elisabeth, *"A prova difícil ou impossível, Estudos em homenagem ao prof. doutor José Lebre de Freitas"*, 1.ª edição, 2013.

FERNANDÉZ, J. Mª Illán, *"La prueba eletrónica, eficácia y valoración en el processo civil"*, 1ª Edição, Thomson Reuters, 2009.

FIEDLER, H., *"Rechenautomaten als Hilfsmittel der Gesetzesanwendung".*

FOUCAULT, Michel, *"Vigiar e punir: história da violência nas prisões"*, 32ª Edição, Tradução de Raquel Ramalhete, Petrópolis: Vozes, 1987.

FULLER, Lon L., *"The Morality of Law: Revised Edition"*, Yale University Press, 1969.

GARCIA MARQUES, Gabriel, **MARTINS**, Lourenço, *"Direito da Informática"*, IJC, Almedina, Coimbra, 2000.

GASTAL, Alexandre Fernandes, *"A Suficiência do Juízo de verosimilhança para a decisão das questões fáticas"*, Universidade do Rio Grande do Sul, Porto Alegre, 2006.

GIOVA, Giuliano, *"Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems*", IJCSNS International Journal of Computer Science and Network Security, VOL. 11 nº 1, janeiro de 2011.

GOMEZ MARTINEZ, Carlos, *"La grabación del sonida y de la imagen en los juicios civiles"*, Revista Jueces para la democracia, Número 48, Madrid, 2003.

GONÇALVES, João Gama, *"A prova digital em 2017 – Reflexões sobre algumas insuficiências processuais e dificuldades da investigação"*, CEDIS Working Papers Universidade Nova de Lisboa, 2017.

GONÇALVES, Marco Carvalho, *"Integração judiciária e tutela jurisdicional dos interesses económicos e sociais",* 2016.

GOODISON, Sean, **DAVIS**, Robert, **JACKSON**, Brian, *"Digital Evidence and the US Criminal Justice System: Identifying technology and other needs to more effectively acquire and utilize digital evidence"*, 2015.

GOTTWALD, P., *"Congresso Mundial de Direito Processual"* (Brasil), 16-20 de setembro de 2007.

GRAZIOSI, Andrea, *"Premese ad una teoria probatória del documento informatico"* in *Rivista trimestrale di diritto e procedura civile nº2 (anno LII)*, 1998.

HABERMAS, Jürgen, *"La technique et la science comme idéologie – La fin de la métaphysique"*, Denöel Gonthier, Paris, 1973, tradução de Jean-René Ladmiral do *original "Technick und Wissenschaft als Ideologie"*, 1968.

HARARI, Yuval Noah, "21 Lessons for the 21st Century", Jonathan Cape, London, 1ª edição, 2018.

HELLWIG, *"System des Deutschen Zivilprozessrechts"*, Lípsia, 1912.

HERNANDEZ GIL, António, *"La función social de la posesíon"*, 1ª Edição, Madrid, Alianza, 1969.

JAUERNIG, Othmar, *"Direito Processual Civil"*, 25.ª edição, tradução de Silveira Ramos, Almedina, Coimbra, 2002.

KLUG, Ulrich, *"Máquinas electrónicas para la elaboración de dato sen el Derecho"*.

KLUWER, Wolters, *"Diario La Ley, Nº 6, Sección Ciberderecho"*, 2017.

KNAPP, Viktor, *"De l'application de la cybernétique au demaine du droite"*.

KUROSE, Jim, **ROSS**, Keith, *"Redes de computadores e a internet: uma abordagem top-down"*, 6ª edição, Pearson, São Paulo, 2015.

LACAMBRA, Legaz, *"Filosofia Del Derecho"*, Bosch, Barcelona, 1961.

LACAMBRA, Legaz, *"La lógica como posibilidad del pensamento jurídico"* in *"Anuario de Filosofia del Derecho"*, 1957.

LARENZ, Karl, *"Metodologia da Ciência do Direito"*, 2ª edição, Fundação Calouste Gulbenkian, Lisboa.

LEBRE DE FREITAS, José, *"A ação declarativa comum, à luz do Código de Processo Civil de 2013"*, 3ª edição.

LEBRE DE FREITAS, José, *"A confissão no direito probatório: um estudo de direito positivo"*, 2ª Edição, Coimbra Editora, Coimbra, 2013.

LEBRE DE FREITAS, José, *"Introdução ao processo civil, conceitos e princípios gerais à luz do novo código"*, Coimbra Editora, Coimbra, 2013.

LEITÃO, Hélder, *"Da instrução em processo civil das provas"*, 3ª edição, 2016.

LEROUX, Olivier, *"Legal admissibility of electronic evidence"* in *"International Review of Law, Computers & Technology, 18:2"*, 2004.

LESSONA, Carlos, *"Teoria general de la prueba en derecho civil"*, Madrid: Reus, 1928.

LIEBMAN, Enrico Tullio, *"Manuale di diritto processuale civile – Principi, vol. 1"*, 5ª edição, Milano: Giuffré, 1992.

LOPES, José Mouraz, **CABREIRO**, Carlos Antão, *"A Emergência da Prova Digital na Investigação da Criminalidade Informática" in* "Sub Judice — Justiça e Sociedade, n.º 35", Almedina, Coimbra, 2006.

LUSO SOARES, Fernando, "A Responsabilidade Processual Civil", 2ª Edição, Almedina, 1987.

MACHADO, Costa, "*Código de Processo Civil Interpretado*", 6.ª edição, Editora Manole, Barueri -São Paulo, 2007.

MADEIRA, Luís Cláudio Magalhães, *"Peças e atos processuais judiciais por transmissão eletrónica via internet"in "Direito da Sociedade da Informação – Separata do Volume IX"*, Associação Portuguesa do Direito Intelectual, Coimbra Editora.

MAHDI, Miraz, *"Blockchain: Technology Fundamentals of the Trust Machine"*, Hong-Kong, de 2017.

MANNARINO, Nicola, *"La Prova Nel processo"*, CEDAM, Padova, 2007.

MARINONI, Luiz Guilherme e **ARENHART,** Sérgio Cruz, "*Curso de Processo Civil, Processo Cautelar, vol. 4, 3.ª ed. revista e atualizada"*, Editora Revista dos Tribunais, São Paulo, 2011.

MARINONI, Luiz Guilherme e **ARENHART**, Sérgio Cruz, *"Prova e Convicção"*, 4ª Edição, Thomson Reuters.

MARQUES DA SILVA, Germano, *"Curso de Processo Penal: vol. II"*. 3.ª edição, Lisboa: Verbo, 1993.

MASON, Stephen, **SENG**, Daniel, *"Electronic Evidence"*, 4ª edição, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017.

MAURÍCIO, Rui, *"O paradigma do processo eletrónico no Direito Processual Civil português"* in *"Direito da Sociedade da Informação: Volume IX"*, Coimbra Editora, 1ª Edição, 2011.

MENEZES CORDEIRO, António Manuel, *"Tratado de direito civil português, tomo I"*, 3.ª edição, 2005.

MENEZES CORDEIRO, António Manuel, *"Da Boa Fé no Direito Civil"*, Almedina, Coimbra, 1997.

MESQUITA, Paulo Dá, *"Processo Penal, Prova e Sistema Judiciário"*, 2010, Coimbra, Coimbra Editora.

MILITÃO, Renato Lopes, *"A propósito da prova digital no processo penal"*.

MOREIRA, Rui, *"Os princípios estruturantes do processo civil português e o projeto de uma nova Reforma do Processo Civil" in "O Novo Processo Civil: contributos da doutrina para a compreensão do novo Código de Processo Civil"*, 2ª Edição, Centro de Estudos Judiciários, 2013.

MOREIRA, Teresa Coelho, *"Novas Tecnologias: Um admirável mundo novo do Trabalho?"*, Revista de Direitos e Garantias Fundamentais, Vitória, n. 11, p. 15-52, jan./jun. 2012.

MOREIRA, Vital, *"A ordem jurídica do capitalismo"*, 1ª Edição, Caminho, Lisboa, 1973.

MORENO, Edward David, **PEREIRA**, Fábio Dacêncio, **CHIARAMONTE**, Rodolfo Barros, *"Criptografia em Software e Hardware"*, Novatec Editora.

MOSS, Bert, *"Metadata in Digital Forensics"*, eForensics Magazine,

MOTA PINTO, Paulo, *"Boletim da Faculdade de Direito: Volume Comemorativo"*, Universidade de Coimbra, 2002.

NGONGO BARNABÉ, Augusto, *"Direito Probatório"*, Tese de Mestrado pela Universidade de Coimbra, 2014.

NOVAIS, P., **GOMES**, M., *"Conflict and its Different Dimensions"*, 2011.

NOVARIO, Filippo, *"Le prove informatiche nel processo Civile"*, Torino: G. Giappichelli, 2014.

NUNO PINTO DE OLIVEIRA, *"Estudos sobre o não cumprimento das obrigações"*, 2ª edição, Coimbra, Almedina, 2009.

OLIVEIRA ASCENSÃO, José, *"O Direito: Introdução e Teoria Geral"*, 10ª edição, Coimbra, 1997.

OLIVEROS, Raúl Tavolari, *"La videoconferência como mecanismo de comparência y la garantia del debido processo"* in *"Revista Uruguaya de Derecho Procesal Número 1/2006"*, Fundación de Cultura Universitaria, Montevideo, Uruguay.

PEREIRA, José Carlos, Tese de Mestrado em Direito dos Contratos pela Universidade do Minho.

PERELMAN, Chaïm, *"Retóricas",* tradução de Maria Ermantina Galvão G. Pereira, São Paulo: Martins Fontes, 1997.

PÉREZ LUÑO, Antonio-Enrique, *"Cibernética, Informática y Derecho (un análisis metodológico)"*, Publicaciones de Real Colegio de España Bolonia, 1976.

PESSOA VAZ, Alexandre, *"Direito Processual Civil – Do antigo ao novo Código"*, 2ª Edição, Almedina, Coimbra.

PHILLIPS, Lothar, *"Von nervösen und phlegmatischen Rechsbegriffen – Ein Beitrag zur Rechtstatsachenforschung"* in *"Informationsgetsellschaft und Rechtskultur in Europa"*, Nomos, Baden-Baden, 1995.

PIMENTA, Paulo, *"Processo Civil Declaratório"*, Almedina, 2015.

PISANI, Andrea Proto, *"Lezioni di diritto processuale civile"*, Napoli: Jovene, 1994.

POULLET, Yves, *"Probate Law: From Liberty to Responsibility"* in *"The EDI Law Review"*, 1994.

PUPO CORREIA, Miguel, *"Assinatura eletrónica e certificação digital"* in *"Direito da Sociedade da Informação: Volume VI"*, Coimbra Editora, 1ª edição, 2006.

QUADI, Gabriel H., *"La prueba en el processo civil y comercial",* Buenos Aires: Abeledo-Perrot, 2011.

RAAB, Charles D., *"Vigilância e privacidade: as opções de regulação" in "A sociedade vigilante: Ensaios sobre identificação, vigilância e privacidade",* ICS: Imprensa de Ciências Sociais, Lisboa, 2008.

RABINOVICH-EINY, Orna, *"Beyond Efficiency: The Transformation of Courts Through Technology",* UCLA Journal of Law and Technology, Volume 12, Issue I, 2008

RAMOS, Armando Dias, "*A Prova Digital em Processo Penal*, Chiado Editora", 1.º edição, 2014.

RANGEL, Rui Manuel de Freitas, "*O Ónus da Prova no Processo Civil"*, 3.ª edição, Almedina, Coimbra, 2006.

REED, Chris**,** *"Computer Law",* Blackstone Press Limited, 1990.

REIS, José Alberto dos, *"Código de Processo Civil Anotado, vol. III"*, 3º ed., Coimbra Editora, Coimbra, 2012.

REIS, José Alberto dos, Código de Processo, *Código de Processo Civil Anotado*, vol. III, 3.ª ed., Coimbra Editora, Coimbra, 2012.

REMÉDIO MARQUES, João Paulo Fernandes, *"A aquisição e a valoração probatória de factos (des)favoráveis ao depoente ou à parte chamada a prestar informações ou esclarecimentos"* in "*Revista Julgar nº 16"*, Coimbra Editora, Coimbra, 2012.

RODRIGUES, Benjamin Silva, *"Da Prova Penal, Tomo II, Bruscamente, A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal"*, 2010.

RODRIGUES, Benjamin, *"Da Prova Penal, IV, Da Prova-Eletrónico-Digital e da Criminalidade Informático-Digital"*, Rei dos Livros, Lisboa, 2011.

ROSENBERG, *"Die Beweislast"*, 1990.

SAMPAIO, José Mª Gonçalves, *"A prova por documentos particulares: na doutrina, na lei e na jurisprudência"*, 3ª edição, Coimbra: Almedina, 2010.

SANTOS, Rita Coelho dos, *"O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos"*, Boletim da Faculdade de Direito, Coimbra, Coimbra Editora, 2005.

SARMENTO E CASTRO, Catarina, *"40 anos de 'Utilização da Informática' - o artigo 35.º da Constituição da República Portuguesa"*, ePública: Revista Eletrónica de Direito Público, vol. 3 nº 3, dezembro de 2016.

SILVA, Germano Marques, *"Do Processo Penal Preliminar"*, Editorial Minerva, 1990.

SILVEIRA, Alessandra, **MARQUES**, João, *"Do direito a estar a só ao direito ao esquecimento. Considerações sobre a proteção de dados pessoais informatizados no Direito da União Europeia: Sentido, Evolução e Reforma Legislativa"*, Revista da Faculdade de Direito – UFPR, Curitiba, vol. 61, n. 3, set./dez. 2016.

SOUSA, Luís Pires de "Prova por Presunção no Direito Civil", 1ª Edição, Almedina, Coimbra, 2012.

STONE, Julius, *"Computers, Behavioural Science and the Human Judge"*.

TARUFFO, Michele, *"Funzione della prova: la funzione dimostrativa" in "Rivista Trimestrale di Diritto e Procedura Civile, Anno. 51, n.º 3"*, Giuffrè Editore, Milão, 1997.

TARUFFO, Michele, *"La prova dei fatti giuridici: nozioni generali"*, Giuffrè, Itália, 1992.

TARUFFO, Michelle, "*A prova"*, São Paulo: Marcial Pons, 2014.

TARUFFO, Michelle, *"O sistema jurídico dos Estados Unidos: Aspetos Fundmentais"*, Revista Ius et Praxis, 12 (1), versão on-line, 2006.

TEIXEIRA DE SOUSA, Miguel, *"As partes, o objecto e a Prova em processo declarativo"*, Lex-Edições Jurídicas, 1995.

TEIXEIRA DE SOUSA, Miguel, *"O Valor Probatório dos Documentos Eletrónicos" in "Direito da Sociedade da Informação – Volume II"*, Coimbra Editora, Coimbra, 2001.

TOFFLER, Alvin (1980) A Terceira Onda.

VALENTÍN, Gabriel, *"Las nuevas tecnologias en la actividad procesal de registro"*, Revista Trilogía, Número 5, ed. Alex, 2008.

VARELA, Antunes, *"Manuel de Andrade e o ensino do processo Civil"*, in Boletim da Faculdade de Direito de Coimbra, Vol.35, Coimbra.

VARELA, Antunes, **BEZERRA**, J. Miguel e **NORA**, Sampaio E., *"Manual de processo Civil"*, 2.ª edição, (Reimpressão), Coimbra Editora, Coimbra, 2004.

VAZ DA SERRA, Adriano, *"Provas: Direito Probatório Material"*, Lisboa, 1962.

VAZ SERRA, *"Provas: direito probatório material"*, Lisboa, 1962.

VENÂNCIO, Pedro Dias*, "Lei do Cibercrime: Anotada e Comentada"*, 1ª edição., Coimbra, Coimbra Editora, 2011.

WALTER, Gerhard, *"Freie Beweiswürdigung"*, 1979.

WAMBIER, Luiz Rodrigues, **TALAMINI**, Eduardo, *"Curso Avançado de Processo Civil, Teoria Geral do Processo e Processo de Conhecimento, Vol. 1",* 12.ª ed., Editora Revistas dos Tribunais - RT, São Paulo, 2012.

WOIROL, Gregory R., *"The Technological Unemployment and Structural Unemployment Debates"*, Greenwood Press, Wesport, 1996.

YUDI PRAYUDI, Azhari, "*Digital Chain of Custody: State of the Art"*, International Journal of Computer Applications (0975 – 8887), Volume 114 – No. 5, 2015.

YUSOFF, Yunus, **ISMAIL**, Roslan, **HASSAN**, Zainuddin, *"Common Phases of Computer Forensics Investigation Models"*, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, Nº 3, junho de 2011.

ZIPPELIUS, Reinhold, *"Einführung in die juristische Methodenlehre"*, C. H. Beck, München, 1971.