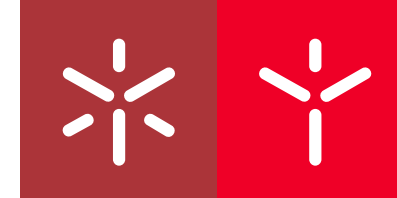


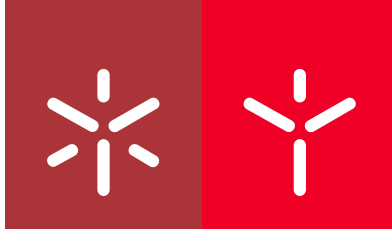


Carla Marina Mendes da Silva

A descoberta eletrónica da prova no âmbito do direito privado

Universidade do Minho
Escola de Direito





Universidade do Minho
Escola de Direito

Carla Marina Mendes da Silva

A descoberta eletrónica da prova no âmbito do direito privado

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

Trabalho efetuado sob a orientação do
Prof. Doutor Francisco António Carneiro Pacheco de Andrade
e do
Professor Doutor Henrique Manuel Dinis Santos

Direitos de autor e condições de utilização do trabalho por terceiros

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos. Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada. Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho



**Atribuição
CC BY**

<https://creativecommons.org/licenses/by/4.0/>

Agradecimentos

Aos meus Pais. Sem eles, nada do que sou seria.

À minha irmã, o meu apoio incondicional.

Ao Ricardo, o amigo e companheiro da minha vida.

À Benedita, o meu último verdadeiro amor.

A minha profunda gratidão aos meus orientadores, o Exmo. Senhor Professor Doutor Francisco António Carneiro Pacheco de Andrade e o Exmo. Senhor Professor Doutor Henrique Manuel Dinis Santos, pela orientação, apoio e paciência ao longo deste trabalho. A sua expertise e conselhos foram inestimáveis para a realização desta dissertação.

Agradeço também à Escola de Direito da Universidade do Minho por proporcionar um ambiente académico estimulante e pelos recursos disponibilizados que foram essenciais para a conclusão deste estudo.

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 descoberta eletrônica da prova no âmbito do Direito Privado.

Resumo

O objetivo deste trabalho é demonstrar a importância da descoberta eletrônica da prova, destacando sua atualidade, pertinência e relevância jurídica. O Direito, mais do que nunca, precisa de se adaptar às novas realidades, especialmente no que diz respeito às relações jurídicas estabelecidas por meio eletrônico. Portanto, é essencial que a tecnologia e a realidade jurídica estejam alinhadas, especialmente no que diz respeito ao uso de meios de prova decorrentes da nova tecnologia, que devem ser válidos e eficazes em processos judiciais.

Os diversos setores da vida social dependem cada vez mais dos meios eletrônicos. Assim, é necessário conjugar esforços para viabilizar que tais recursos possam ser obtidos, aceitos e utilizados com segurança e de acordo com os princípios fundamentais do Direito nos processos judiciais. Considerando a substituição da comunicação escrita tradicional pela comunicação através de meios eletrônicos, nas mais variadas formas, devido à globalização e aos avanços tecnológicos, e a necessidade de o Direito recorrer a todos os meios de prova essenciais para a descoberta da verdade material e a justa composição do litígio, é essencial discutir e implementar procedimentos uniformes para a obtenção da descoberta eletrônica da prova. Desta forma, torna-se importante a discussão sobre a obtenção, conservação e utilização dos meios eletrônicos de prova.

Palavras-chave: descoberta eletrônica da prova, processo civil, prova digital.

The Electronic Discovery of Evidence in the Context of Private Law

Abstract

The objective of this work is to demonstrate the importance of electronic discovery of evidence, highlighting its current relevance, pertinence, and legal significance. Law, now more than ever, needs to adapt to new realities, especially regarding legal relationships established through electronic means. Therefore, it is essential that technology and legal reality are aligned, particularly concerning the use of evidence derived from new technology, which must be valid and effective in judicial proceedings.

Various sectors of social life increasingly depend on electronic means. Thus, it is necessary to coordinate efforts to ensure that such resources can be obtained, accepted, and utilized securely and in accordance with fundamental legal principles in judicial processes. Given the replacement of traditional written communication by electronic communication in various forms due to globalization and technological advances, and the need for the Law to employ all essential means of evidence for discovering material truth and achieving a fair resolution of disputes, it is essential to discuss and implement uniform procedures for obtaining electronic discovery of evidence. In this way, the discussion on the acquisition, preservation, and use of electronic evidence becomes crucial.

Keywords: civil procedure, digital evidence, electronic discovery of evidence.

Índice

Direitos de autor e condições de utilização do trabalho por terceiros.....	ii
Agradecimentos	iii
Declaração de integridade.....	iv
Resumo	v
Abstract.....	vi
Índice	vii
Abreviaturas	x
A relevância do objeto	1
Objetivos	4
Capítulo I – O documento eletrónico	12
1. O documento eletrónico no direito europeu e no direito português	12
2. O formato e suporte	16
3. Escrito, assinatura, prova	20
4. Original versus cópia	23
Capítulo II – A descoberta eletrónica da prova	25
1. Regime geral da prova em Processo Civil.....	25
1.1. Provas atendíveis	25
1.1.1. Prova por documentos.....	27
1.1.2. Prova por confissão das partes	29
1.1.3. Prova por declarações de parte	29
1.1.4. Prova pericial.....	30
1.1.5. Prova por inspeção judicial	32
1.1.6. Prova testemunhal.....	33
1.2. Dever de cooperação	36
1.3. Princípio do inquisitório	39
1.4. Possibilidade de impugnação	42
1.5. Valor probatório	44
1.6. Produção antecipada de prova	48
1.7. Ónus da prova	50
1.8. Princípio da igualdade das partes, da proporcionalidade e da razoabilidade	53

2.	Prova digital	55
2.1.	Definição	55
2.2.	Neutralidade tecnológica	56
2.3.	A prova digital e a natureza documental	58
2.4.	Cópia de documentos eletrónicos	58
2.5.	Prova mediante comunicação eletrónica	59
2.6.	Valor probatório	59
2.7.	Ónus da prova	60
2.8.	Presunção de autoria, de vontade e de integridade	61
2.9.	Desafios da prova digital	62
3.	A descoberta eletrónica da prova	64
3.1.	Definição	64
3.2.	“Common Law” versus “Civil Law”	65
3.3.	Dificuldades da descoberta eletrónica da prova	66
3.4.	A descoberta eletrónica da prova – Breve análise comparativa	69
3.4.1.	EUA	69
3.4.2.	Canadá	71
3.4.3.	Reino Unido	73
3.4.4.	Austrália	73
3.4.5.	Brasil	74
3.4.6.	Portugal	75
3.5.	Direito Norte Americano (Federal Rules Civil Procedure)	76
3.6.	The Sedona Conference	90
3.7.	A descoberta eletrónica da prova – Princípio da igualdade das partes	94
3.7.	eDiscovery: O Direito português em comparação com os EUA	97
Capítulo III – A inteligência artificial, o machine learning e a descoberta eletrónica da prova		100
1.	Definição	100
2.	Algoritmos	101
3.	Integração da Inteligência Artificial e o Machine Learning na descoberta eletrónica da prova	103
4.	Benefícios da IA e do ML na descoberta eletrónica	104
5.	Implicações éticas e legais	106

6. Futuro da IA e do ML na Descoberta Eletrónica da Prova	106
7. A autenticidade e integridade	108
Capítulo IV - Exemplos práticos.....	110
Exemplo 1: Uso de IA no Caso Enron.....	110
Exemplo 2: Revisão de documentos no Caso de Antitruste da Microsoft	112
Conclusão	115
Bibliografia.....	119

Abreviaturas

CC – Código Civil

CE – Conselho Europeu

Cfr – Confrontar

CPC – Código de Processo Civil

CRP – Constituição da República Portuguesa

DEP – Descoberta eletrónica da prova

DL – Decreto-Lei

eDiscovery – Descoberta eletrónica da prova

ESI – Electronically Stored Information

EUA – Estados Unidos da América

FRCP – Federal Rules Civil Procedure

IA – Inteligência artificial

In fine – parte final

ML – Machine Learning

PE – Parlamento Europeu

RGPD – Regulamento Geral de Proteção de Dados

RJDEAD – Regime Jurídico do Documento eletrónico e assinatura eletrónica (DL 290-D/1999)

SS – Seguintes

UE – União Europeia

V.G. – Por exemplo

Vol. – Volume

A relevância do objeto

A prova serve para criar uma crença firme num determinado facto, e o estudo da prova no Direito é de crucial importância na resolução de conflitos, pois são as provas que oferecem os critérios necessários ao juiz para que possa dirimir uma situação. A sua importância é tanta que, em muitos casos, a produção de provas é imprescindível para chegar a conclusões sobre os factos em discussão. Somente através da apresentação das provas, o juiz pode desvendar a veracidade alegada no processo judicial pelas partes e, após a apreciação destas, fazer o seu julgamento com vista a apurar, com a maior certeza possível, a descoberta da verdade material.

Essa relevância é particularmente destacada no âmbito do Direito Processual, pois é através deste que o juiz forma sua convicção sobre a procedência ou não da pretensão deduzida, servindo de base para o desenrolar dos trâmites legais. A disseminação da tecnologia e seu impacto no meio jurídico trazem a necessidade de uma reflexão objetiva e pragmática sobre as mudanças que se apresentam cada vez mais na esfera do Direito, especialmente no Direito de Processo Civil.

A descoberta eletrónica da prova (eDiscovery) refere-se a qualquer método de busca, pesquisa, localização e obtenção de dados e informações eletrónicas para serem utilizados como prova num processo judicial. A eDiscovery tem-se tornado uma parte crucial do processo jurídico moderno, especialmente à medida que o volume de dados digitais continua a crescer exponencialmente. A análise da relevância do objeto na eDiscovery é fundamental para entender como os dados eletrónicos podem influenciar a resolução de litígios e a administração da justiça.

O objeto na eDiscovery refere-se aos dados eletrónicos específicos que são identificados, recolhidos, preservados, revistos e produzidos durante o processo de descoberta. Esses dados podem incluir e-mails, documentos, mensagens de texto, registos de redes sociais, bases de dados, arquivos de áudio e vídeo, entre outros.

A importância deste objeto prende-se a três vertentes principais:

1. Relevância probatória: O objeto da eDiscovery deve ser relevante para as questões em disputa no litígio. Dados eletrônicos que podem provar ou refutar uma reivindicação ou defesa são cruciais para o processo judicial.
2. Proporcionalidade e igualdade: A seleção do objeto deve ser proporcional às necessidades do caso e permitindo a igualdade das partes, evitando a recolha de dados excessivos que possam aumentar desnecessariamente os custos e o tempo de revisão.
3. Integridade e autenticidade: Garantir que o objeto recolhido seja íntegro e autêntico é essencial para que as provas sejam admissíveis em tribunal.

A relevância do objeto na descoberta eletrônica de prova é fundamental para garantir que o processo de eDiscovery seja eficaz, eficiente e justo. A análise detalhada dos critérios e práticas para determinar a relevância dos dados eletrônicos pode proporcionar conhecimentos valiosos sobre como otimizar o processo de eDiscovery e melhorar a administração da justiça.

A implementação de boas práticas, o uso de tecnologias avançadas e a colaboração entre as partes são essenciais para superar os desafios associados à determinação da relevância do objeto. À medida que a tecnologia continua a evoluir e o volume de dados eletrônicos aumenta, a capacidade de identificar e utilizar dados relevantes de maneira eficaz será cada vez mais crucial para o sucesso do processo jurídico.

A informática deve ser um importante aliado do mundo judicial. Com o uso cada vez mais frequente da mesma, surgem novas ferramentas tecnológicas com relevância jurídica, que devem ser tratadas com naturalidade pelos operadores judiciários. Pensemos nos e-mails, nos chats de conversação (WhatsApp, Telegram ou Messenger), no Skype, no Zoom, no Teams, no Facebook, no Instagram, no Tik Tok, entre outros. A integração de Inteligência Artificial e Machine Learning na descoberta eletrônica de prova está a transformar significativamente a área jurídica. Estas tecnologias permitem a análise eficiente de grandes volumes de dados, aumentando a precisão e a velocidade na identificação de evidências relevantes.

O documento digital é uma realidade e faz parte da nossa vida de modo tão ou mais natural do que o documento físico. Considerando os avanços tecnológicos dos últimos anos, a utilização do documento eletrónico é uma realidade inevitável e, conseqüentemente, as barreiras à sua utilização são cada vez

mais reduzidas. A comparação do documento eletrónico com o documento tradicional, a sua utilização como meio de prova, bem como as reflexões sobre o tema, principalmente a defesa da validade dos meios eletrónicos de prova, desde que preenchidos requisitos imprescindíveis: a segurança, a confiança, a autenticidade, a integridade, a tempestividade e a conservação do conteúdo, revela a necessidade de uma regulamentação específica e uniforme. Tal regulamentação visa garantir que os documentos eletrónicos sejam aceites em processos judiciais com a mesma validade dos documentos tradicionais, proporcionando uma base sólida para a tomada de decisões justas e seguras.

É ainda importante destacar o papel do profissional do Direito como agente ativo na construção de uma estrutura funcional para a execução das atividades jurídicas, de modo a obter um melhor benefício dos recursos tecnológicos como ferramenta capaz na busca da verdade material e justa composição do litígio, para a aplicabilidade do Direito ao caso concreto de modo mais eficiente e justo. A interação do jurista com a máquina e do jurista com o especialista da área da tecnologia da informação é fundamental.

Objetivos

Com o presente trabalho, pretendemos desenvolver uma análise pormenorizada e crítica sobre a descoberta eletrónica da prova¹ no âmbito do direito civil^{2 3 4}. A transformação contemporânea, impulsionada pelo surgimento de novas tecnologias, está cada vez mais presente no nosso dia a dia. É indubitável que há uma explosão crescente no volume e diversidade de formas de informações armazenadas eletronicamente, bem como uma constante evolução da tecnologia aplicada à descoberta eletrónica da prova.

O avanço das comunicações instantâneas, estimuladas pelas inovações tecnológicas, desde o telégrafo até à internet, proporcionou ao ser humano vastas opções na transmissão de informações. O século XX foi considerado o século do papel, e talvez por essa razão seja tão difícil compreender uma transição tão rápida, no início do século XXI, para o século digital. A compreensão de novas tecnologias, cujas informações não são representadas na forma gráfica, é um dos obstáculos a serem superados pelos operadores do direito.

A recolha e o processamento de todos os meios de prova para um determinado caso em tribunal, quer por iniciativa das partes, quer por iniciativa dos tribunais, são essenciais, mas enfrentam várias questões devido às novas tecnologias⁵ e às diversas formas de comunicação atuais.

Nos EUA, foram alteradas as Federal Rules of Civil Procedure, em dezembro de 2006⁶, para contemplar a utilização de provas digitais. The Sedona Conference⁷ publicou a terceira edição, em 2018: The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, onde se analisam um conjunto de princípios fundamentais

¹ BALL, C. E. The eDiscovery Primer: The Essentials of eDiscovery Law.

² ORLANDO, de Carvalho. Teoria Geral do Direito Civil. 3ª Ed. Coimbra: Coimbra Editora, 2012.

³ PINTO, Carlos Alberto da Mota. Teoria Geral do Direito Civil. 4ª Ed., 2005.

⁴ ASCENSÃO, José Oliveira. O Direito: Introdução e Teoria Geral. 10ª edição. Coimbra: Almedina, 1997. ASCENSÃO, José Oliveira de. Direito Civil: Teoria Geral, Vol. III. Coimbra: Coimbra Editora, 2002.

⁵ ANDRADE, Francisco. Derecho, nuevas tecnologías e Inteligencia Artificial. Editorial DYKINSON, 2023.

⁶ [Federal Rules of Civil Procedure 2006 | United States Courts](https://www.frcp.org/)

⁷ The Sedona Conference (<https://thesedonaconference.org/>) é uma organização sem fins lucrativos dos EUA, que tem como objetivo abordar os grandes desafios do direito na atualidade. Possui um grupo de trabalho específico relativo às questões sobre os documentos eletrónicos e a descoberta eletrónica de prova.

e recomendações das melhores práticas para abordar a produção de informações eletrónicas em litígios. No entanto, mesmo nos EUA, esta questão ainda está longe de ser consolidada.

Em Portugal, as disposições relativas ao documento eletrónico estiveram presentes no Decreto-Lei n.º 290-D/99, nas normas do Regulamento Europeu n.º 910/2014 e que foi alterado pelo Regulamento (UE) n.º 2024/1183 de 11 de Abril (também conhecido como Regulamento eIDAS⁸ e no Decreto-Lei n.º 12/2021, de 09 de Fevereiro, que revogou na íntegra o DL n.º 290-D/99.

Dada a existência de um novo ambiente, em que o foco mudou do fornecimento e uso de identidades digitais rígidas para o fornecimento e a confiança em atributos específicos relacionados a essas identidades, surgiu a necessidade de revisão do Regulamento eIDAS. Existe uma procura crescente de soluções de identidade eletrónica que possam proporcionar estas capacidades, proporcionando ganhos de eficiência e um elevado nível de confiança em toda a UE, tanto no setor privado como no setor público, baseando-se na necessidade de identificar e autenticar os utilizadores com um elevado nível de garantia. E a avaliação da versão inicial do Regulamento eIDAS (Regulamento n.º 910/2014) revelou que o regulamento não conseguia dar resposta a estas novas exigências do mercado, principalmente devido às suas limitações inerentes ao setor público, às possibilidades limitadas e à complexidade para os prestadores privados em linha se ligarem ao sistema, à sua disponibilidade insuficiente de soluções de identificação eletrónica notificadas em todos os Estados-Membros e à sua falta de flexibilidade para apoiar uma variedade de casos de utilização. Além disso, soluções de identidade fora do escopo do eIDAS, como as oferecidas por provedores de plataformas digitais e instituições financeiras, levantavam preocupações de privacidade e proteção de dados. Não conseguiam responder eficazmente às novas exigências do mercado e careciam de alcance transfronteiriço para dar resposta a necessidades sectoriais específicas em que a identificação é sensível e exige um elevado grau de certeza.

⁸ O Regulamento (UE) n.º 910/2014, mais conhecido como Regulamento eIDAS, é uma legislação da União Europeia que estabelece um quadro jurídico para transações eletrónicas no mercado interno europeu. Foi adotado em 23 de julho de 2014 e entrou em vigor em 1 de julho de 2016, revogando e substituindo a Diretiva 1999/93/CE. Recentemente, este Regulamento foi alterado pelo Regulamento (UE) n.º 2024/1183 do Parlamento Europeu e do Conselho, datado de 11 de Abril de 2024, publicado a 30 de abril de 2024 e que entrou em vigor a 20 de maio de 2024. Este novo regulamento visa criar um Regime Europeu para a Identidade Digital, proporcionando maior segurança e interoperabilidade nos serviços digitais dentro da União Europeia, alinhando-se com os objetivos do Programa Estratégico da Década Digital para 2030 e a Declaração Europeia sobre os Direitos e Princípios Digitais para a Década Digital.

Assim, este novo Regulamento da UE⁹ criou a Carteira Europeia de Identidade Digital¹⁰, como meio de identificação eletrónica que permite aos utentes armazenar, gerir e validar dados de identificação pessoal e declarações eletrónicas de atributos de forma segura¹¹. Esta carteira permitirá que *“os cidadãos da União, os residentes na União, na aceção do direito nacional, e as empresas se identifiquem e autenticem a sua identidade em linha e fora de linha de forma segura, fiável, de fácil utilização, conveniente, acessível e harmonizada, em toda a União”*¹². Desta forma, procura a harmonização de identidade digital para *“contribuir para a criação de uma União mais integrada do ponto de vista digital, ao reduzir as barreiras digitais entre os Estados-Membros e capacitar os cidadãos da União e os residentes na União para usufruírem dos benefícios da digitalização e reforçar simultaneamente a transparência e a proteção dos seus direitos”*¹³.

O Regulamento altera vários artigos do Regulamento (UE) n° 910/2014, incluindo a introdução de novos artigos e a modificação de anexos existentes¹⁴, como os requisitos de certificados qualificados de

⁹ [Regulation - EU - 2024/1183 - EN - EUR-Lex \(europa.eu\)](#)

¹⁰ Meio de identificação eletrónica que permite ao utente armazenar, gerir e validar de forma segura dados de identificação pessoal e certificados eletrónicos de atributos, com o objetivo de os fornecer aos utilizadores e a outros utentes de carteiras europeias de identidade digital, e assinar com assinatura eletrónica qualificada e apor selos com selos eletrónicos qualificados – art° 3° n° 42 do Regulamento eIDAS.

¹¹ Cfr. Art° 3° n° 43 do Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho de 11 de abril de 2024: *“Atributo”: uma característica, qualidade, direito ou autorização de uma pessoa singular ou coletiva ou de um objeto.*

¹² Considerando 7 do Regulamento (UE) 2024/1183 de 11 de Abril.

¹³ Considerando 6 do Regulamento (UE) 2024/1183 de 11 de Abril.

¹⁴ Principais alterações introduzidas pelo Regulamento (UE) 2024/1183 de 11 de Abril:

a. Supressão de artigos e parágrafos:

- Artigo 24, parágrafo 2, alínea (j)
- Artigo 25, parágrafo 3
- Artigo 27, parágrafo 4
- Artigo 35, parágrafo 3
- Artigo 37, parágrafo 4
- Artigo 41, parágrafo 3
- Capítulo III, seção 2, artigo 17
- Capítulo III, seção 2, artigo 18

b. Inclusão de novos artigos e parágrafos:

- Artigo 3, novos pontos 5-A, 23-A, 23-B, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57
- Artigo 11-A
- Artigo 20, parágrafos 1-A e 1-B
- Artigo 24, parágrafo 2, com novos parágrafos e alíneas (fa) e (fb)
- Artigo 26, parágrafo 2
- Artigo 29, parágrafo 1-A
- Artigo 29-A
- Artigo 30, parágrafo 3-A
- Artigo 32, novo parágrafo 1
- Artigo 32-A

assinatura eletrónica e dispositivos qualificados de criação de assinatura eletrónica. O objetivo principal é proporcionar uma identidade digital acessível, segura e fiável para todos os cidadãos e residentes da UE, permitindo-lhes controlar seus dados e identidades nas interações digitais, facilitando o acesso a serviços públicos e privados de maneira segura e interoperável em toda a União Europeia.

Fazendo uma breve comparação entre o Regulamento (UE) n° 910/2014¹⁵ e o Regulamento (UE) 2024/1183¹⁶, verificamos que, no contexto geral, o Regulamento (UE) n° 910/2014 foi estabelecido para criar um quadro comum de identificação eletrónica e serviços de confiança para transacções eletrónicas na União Europeia e tem como objetivo principal aumentar a confiança e a segurança das transações eletrónicas transfronteiriças na EU; o Regulamento (UE) 2024/1183 introduz alterações ao Regulamento (UE) n° 910/2014 e foca-se na criação do Regime Europeu para a Identidade Digital, com vista ao cumprimento dos objetivos do Programa Estratégico da Década Digital para 2030.

Quanto às alterações e novidades, destacam-se quatro:

1. Identificação Eletrónica: o Regulamento (UE) n° 910/2014 define níveis de segurança para identificação eletrónica e cada Estado-Membro pode notificar seus sistemas de identificação eletrónica, que serão reconhecidos por outros Estados-Membros. Por sua vez, o Regulamento (UE) n° 2024/1183 introduz a carteira europeia de identidade digital como um meio de identificação eletrónica. A carteira permite aos utentes armazenar, gerir e validar dados de identificação e declarações eletrónicas de atributos de forma segura.

- Artigo 34, parágrafo 1-A

- Artigo 36, parágrafo 2

- Artigo 39-A

- Artigo 42, parágrafo 1-A

- Artigo 44, parágrafos 1-A, 2-A e 2-B

- Artigo 45-A

c. Anexos adicionados ou modificados:

- Anexo I: Requisitos de certificados qualificados de assinatura eletrónica (modificação da letra i)

- Anexo II: Requisitos de dispositivos qualificados de criação de assinatura eletrónica (supressão dos pontos 3 e 4)

- Anexo III: Requisitos de certificados qualificados de selo electrónico (modificação da letra i)

- Anexo IV: Requisitos de certificados qualificados de autenticação de sites web (modificação das letras c e j)

- Anexo V: Requisitos aplicáveis à declaração eletrónica qualificada de atributos (novo)

- Anexo VI: Lista mínima de atributos (novo)

- Anexo VII: Requisitos aplicáveis à declaração eletrónica de atributos emitida por um organismo público responsável de uma fonte autêntica ou em nome deste (novo)

¹⁵ eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0910

¹⁶ eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401183

2. Serviços de Confiança: o Regulamento (UE) n° 910/2014 estabelece requisitos para vários serviços de confiança, como assinaturas eletrónicas e selos eletrónicos. Por sua vez, o Regulamento (UE) n° 2024/1183 mantém os serviços de confiança existentes, mas introduz modificações específicas em vários anexos:
 - Anexo I: Requisitos dos certificados qualificados de assinatura eletrónica.
 - Anexo II: Requisitos dos dispositivos qualificados de criação de assinatura eletrónica.
 - Anexo III: Requisitos dos certificados qualificados de selo electrónico.
 - Anexo IV: Requisitos dos certificados qualificados de autenticação de sites web.
 - Novos anexos V, VI e VII relacionados a declarações eletrónicas de atributos e listas de atributos mínimos.
3. Interoperabilidade e reconhecimento mútuo: o Regulamento (UE) n.º 910/2014 promove o reconhecimento mútuo de sistemas de identificação eletrónica entre Estados-Membros. Cada Estado deve designar uma autoridade de supervisão para monitorar os prestadores de serviços de confiança. Por sua vez, o Regulamento (UE) n° 2024/1183 reforça o conceito de interoperabilidade com a introdução da carteira europeia de identidade digital, que é reconhecida em todos os Estados-Membros. A carteira facilita o acesso seguro e interoperável a serviços digitais públicos e privados.
4. Segurança e Proteção de Dados: o Regulamento (UE) n° 910/2014 exige que os prestadores de serviços de confiança implementem medidas adequadas para gerir riscos de segurança e notificar incidentes de segurança relevantes. Por sua vez, o Regulamento (UE) n° 2024/1183 continua a ênfase na segurança, mas com um foco maior na proteção contra riscos de cibersegurança e crimes cibernéticos. Visa proporcionar aos cidadãos maior controle sobre seus dados e identidades digitais.

Em suma, o Regulamento (UE) n° 2024/1183 complementa e expande o escopo do Regulamento (UE) n° 910/2014, introduzindo a carteira europeia de identidade digital, reforçando a interoperabilidade e a proteção de dados, e adaptando os requisitos para serviços de confiança para atender às necessidades digitais contemporâneas. Visa aumentar a eficiência e segurança das transações eletrónicas na União Europeia, facilitando o acesso a serviços digitais seguros para todos os cidadãos e residentes da UE.

Isto posto, prosseguindo, não temos uma previsão expressa no Código de Processo Civil¹⁷ relativa à produção de provas eletrónicas e ao enquadramento processual do documento eletrónico. O Código de Processo Civil¹⁸ foi construído para a utilização apenas de documentos em papel. No entanto, há uma necessidade crescente de conciliar os processos, considerando a interação homem-computador na descoberta da prova. O jurista tem de lidar com as tecnologias e saber utilizá-las. Deve existir colaboração entre o jurista e os especialistas em tecnologias da informação.

O art.º 362º do Código Civil português¹⁹ estipula que os documentos devem ser gerados pelo homem, ou seja, o documento é o resultado de uma atividade humana. E os documentos eletrónicos? Muitos são produto da atividade humana, mas muitos documentos eletrónicos já não são necessariamente produto de uma atividade humana. Esta disposição legal precisa ser revista. Até lá, uma interpretação extensiva pode ser a solução.

Além disso, no contexto de toda a transformação existente, os princípios da igualdade das partes, da proporcionalidade e da razoabilidade devem ser assegurados. Será também necessário repensar o ónus da prova, nos termos do art.º 342º, n.º 2 do Código Civil²⁰, face às necessidades e exigências da descoberta eletrónica da prova.

Na Europa, o Regulamento Europeu 910/2014 revogou a Diretiva n.º 1999/93/CE para estabelecer um quadro jurídico comum, aplicado diretamente em todos os Estados-Membros. Foi estabelecido um quadro comum de documentos e assinaturas eletrónicas admissíveis pelo Tribunal, bem como um novo conjunto de instrumentos jurídicos, adaptados às possibilidades tecnológicas atuais, destinados a garantir a segurança e fiabilidade das comunicações e transações eletrónicas. Um aspeto importante do Regulamento Europeu é a opção do legislador europeu por uma abordagem tecnologicamente neutra. A neutralidade tecnológica²¹ e a equivalência funcional²² são dois fatores importantes na

¹⁷ Lei n.º 41/2013, de 26 de Junho

¹⁸ VARELA, Antunes - Manuel de Andrade e o ensino do processo Civil. Boletim da Faculdade de Direito. Coimbra. vol. 35, 2005. VARELA, Antunes; BEZERRA, J. Miguel; NORA, Sampaio E. - Manual de processo Civil. 2ª edição (reimpressão), Coimbra: Coimbra Editora, 2006. VASCONCELOS, Pedro Pais de. Teoria Geral do Direito Civil. 7ª Ed. Coimbra: Almedina, 2012. VAZ, Alexandre Pessoa- Direito Processual Civil – Do antigo ao novo Código. 2ª edição, Coimbra: Almedina, 2002.

¹⁹ Cfr artº 362º do CC: “Prova documental é a que resulta de documento; diz-se documento qualquer objecto elaborado pelo homem com o fim de reproduzir ou representar uma pessoa, coisa ou facto.”

²⁰ Cfr. artº 342º n.º 2 do CC: “A prova dos factos impeditivos, modificativos ou extintivos do direito invocado compete àquele contra quem a invocação é feita.”

²¹ A neutralidade tecnológica é um princípio que procura garantir a imparcialidade e igualdade de tratamento de diferentes tecnologias em determinado contexto, sem favorecer ou discriminar uma tecnologia em relação a outras.

construção de um mercado digital europeu inovador, confiável e seguro, do qual o Regulamento 910/2014 é um instrumento jurídico fundamental.

O art.º 46 do Regulamento Europeu 910/2014²³ estabelece a necessidade de cooperação entre os Estados-Membros para garantir que os sistemas de identificação eletrónica sejam compatíveis e interoperáveis em toda a União Europeia, promovendo assim a livre circulação de pessoas, bens e serviços dentro do mercado único digital europeu. Este artigo resolve a questão dos efeitos legais dos documentos eletrónicos, estabelecendo que não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a um documento eletrónico pelo simples fato de se apresentar em formato eletrónico.

Os termos de conteúdo e o suporte são diferentes e devem ser concretamente definidos. O suporte pode ser importante para efeito de prova, mas não para efeito de escrito ou não escrito²⁴. O papel deixou de ser o único suporte e até é o suporte menos usado. E no suporte temos de ter em conta o formato²⁵.

Mais importante do que o suporte, para efeito de prova, é a questão da inalterabilidade do documento. O documento em formato Word (o original) pode ser mais facilmente alterado do que o documento em PDF (a cópia). O suporte permite guardar/conservar/arquivar. O formato pode ser mais ou menos seguro. É necessário analisar a distinção entre cópia em suporte diferente (digital e papel) e a cópia em formato diferente (Word e PDF). Conceitualmente, nada impede que o original seja o PDF e a cópia seja um Word. Essa não é a situação mais comum, mas é possível.

²² No Regulamento (UE) n.º 910/2014, "equivalência funcional" refere-se ao princípio de que os documentos eletrónicos e as assinaturas eletrónicas devem ser tratados com a mesma validade e eficácia que os documentos e assinaturas em papel, desde que cumpram certos requisitos essenciais. Este regulamento estabelece um quadro comum para a identificação eletrónica e os serviços de confiança para transações eletrónicas no mercado interno da União Europeia, promovendo a confiança e a segurança nas transações eletrónicas. A equivalência funcional é fundamental para garantir que os meios eletrónicos de prova sejam aceites e utilizados de forma segura e eficaz nos processos judiciais e nas transações comerciais. O regulamento visa assegurar que as assinaturas eletrónicas qualificadas tenham o mesmo efeito legal que as assinaturas manuscritas e que os documentos eletrónicos possam ser utilizados como prova em tribunal, desde que cumpram os requisitos de segurança, autenticidade e integridade.

²³ O artigo 46 do Regulamento (UE) n.º 910/2014 não foi alterado pelo Regulamento (UE) 2024/1183. Contudo, foi adicionado o artº 46º-A que estabelece o regime de "*Supervisão do Regime para a carteira europeia de identidade digital*".

²⁴ Cfr. artº 3º n.º 1 do DL 12/2021: "1 - O documento eletrónico satisfaz o requisito legal de forma escrita quando o seu conteúdo seja suscetível de representação como declaração escrita."

²⁵ VENÂNCIO, Pedro. A Tutela Jurídica do Formato de Ficheiro Electrónico. Tese de doutoramento, Universidade do Minho, Braga, 2013.

É importante também analisar e discutir a questão da migração de um formato para outro. A migração de um formato de documento, especialmente quando se trata da transição para a assinatura digital, pode apresentar uma série de desafios, como a integridade do documento, compatibilidade e formatação, validade legal da assinatura digital, segurança da assinatura digital e o processo de verificação.

Capítulo I – O documento eletrónico ^{26 27}

1. O documento eletrónico no direito europeu e no direito português²⁸

O documento é, por definição, um qualquer registo de informação, independentemente do formato ou suporte utilizado para registá-la.

No Código Civil Português²⁹, no seu artigo 362º, o documento é definido como *“qualquer objeto elaborado pelo homem com o fim de reproduzir ou representar uma pessoa, coisa ou facto”*. Temos, assim, uma definição geral de documento enquanto meio de prova e a simultaneidade de dois requisitos: o funcional e o teleológico. Funcional, enquanto representação de uma pessoa, coisa ou facto; teleológico atenta a finalidade representativa do documento.

O documento encerra em si uma representação eterna de um facto, projetando-o no futuro, motivo pelo qual a prova documental é considerada mais objetiva e permanente. Contudo, o efeito representativo não se produz do mesmo modo em todos os documentos. Vejamos, por exemplo, uma fotografia e um vídeo: a fotografia tem a sua capacidade representativa imediata, ao passo que o vídeo precisa de um aparelho de reprodução para o efeito.

O documento assume diversas funções, designadamente, a eternização (da declaração num suporte idóneo), probatória (demonstra a existência da declaração), a autenticação (imputa a declaração a um autor) e a constitutiva ou de eficácia (quando tem dupla natureza de meio de prova e formalidade existencial do negócio).

O documento tem carácter material (corpus e a forma de representação) e imaterial (pensamento, conteúdo e autor). O *corpus* é o suporte (v.g. papel, fotografia, pen-drive, CD, etc.) e permite que a informação seja reproduzida ou copiada. A representação é o conteúdo, a manifestação de vontade expressa pelo seu autor. Maria Enza La Torre defende a teoria da complexidade documental, segundo a qual *“o documento é ao mesmo tempo representação e veículo: representação enquanto coisa artificial, feita pelo homem, à maneira de forma e invólucro material que encerra o conteúdo da realidade nele expressa; veículo enquanto fonte de conhecimento, por vezes única e insubstituível, do acto ou facto.”*³⁰

²⁶ ANDRADE, Francisco (2019). O documento eletrónico revisitado face ao Regulamento (EU) n° 910/2014 (Regulamento EIDAS). In Jornadas Comemorativas dos 25 anos EDUM, Direito e Pessoa no Mundo Digital.

²⁷ PIRES DE SOUSA, Luís Filipe. O valor probatório do documento eletrónico em processo civil. Almedina, 2017.

²⁸ Andrade, Francisco; Silva, Marina "O documento eletrónico: suporte e formato", publicado na Revista da Ordem dos Advogados (ROA | Ano 81 - Vol. III/IV - Jul./Dez. 2021).

²⁹ DL n.º 47344/66, de 25 de Novembro

³⁰ Maria Enza La Torre, "Contributo Alla Teoria Giuridica Del Documento", Giuffrè 2004, pág. 45 e 46.

À tradicional forma oral e escrita, junta-se agora uma nova forma eletrónica. A era da tecnologia confronta-nos com um novo tipo de documento: o documento eletrónico, cuja constituição abrange diferentes fases:

- Criação: uso do computador com recurso a um programa informático e que converte a linguagem humana em binária;
- Armazenamento: a informação é gravada num determinado formato de ficheiro eletrónico e num determinado suporte;
- Visualização: leitura do conteúdo.

Podemos, portanto, definir o documento eletrónico como um documento criado em linguagem binária³¹, armazenado em formato e suporte informático, convertível em linguagem compreensível ao homem e que pode ser modificado, copiado ou transmitido por meios informáticos³². O documento eletrónico completa-se quando ocorre a gravação dos bits num formato e suporte. São vários os elementos, relacionados entre si, que compõem o documento eletrónico: o software, o hardware, o suporte, o conteúdo e os metadados.

No direito europeu, a definição de documento eletrónico é dada pelo artº 3º, nº 35 do Regulamento (EU) nº 910/2014, como sendo “qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual;”³³

Esta definição vem não só alargar o conceito de documento eletrónico que constava do artigo 2º alínea a) do DL 290-D/99 (e que apenas referia o “*documento elaborado mediante processamento electrónico de dados*”), como veio colocar em causa a distinção estabelecida na doutrina³⁴ entre documento eletrónico em sentido estrito e documento eletrónico em sentido amplo: “*em sentido estrito, o documento eletrónico é aquele que se encontra gravado de forma digital num suporte*

³¹ Sistema de numeração posicional em que todas as quantidades se representam com base em dois números, ou seja, zero e um (0 e 1).

³² Luís Filipe Pires de Sousa, “O valor probatório do documento eletrónico em processo civil”, Almedina 2017, pág. 25.

³³ Regulamento (UE) nº 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 (Regulamento eIDAS), alterado pelo Regulamento (EU) nº 2024/1183, de 11 de abril de 2024, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.

³⁴ Miguel Teixeira de Sousa in “O valor probatório dos documentos eletrónicos”, in “Direito da Sociedade da Informação”, vol. II, Coimbra Editora, 2001, pág. 172. Mas já Miguel Pupo Correia, in “Assinatura eletrónica e certificação digital”, in “Direito da Sociedade da Informação”, vol. VI, Coimbra Editora, 2006, págs. 277 - 317, pág. 286, estabelecia a seguinte distinção: “documentos eletrónicos em sentido estrito, que são memorizados em forma digital em memórias magnéticas ou óticas e são destinados apenas a ser lidos pelo computador, pelo que não podem ser lidos ou apercebidos directamente pelo homem; e documentos eletrónicos em sentido amplo, ou simplesmente documentos informáticos, que são todos os gerados através dos equipamentos periféricos do computador – impressora, “plotter”, etc. – de modo a serem lidos ou interpretados pelo homem”. No entanto, parece-nos evidente que, no caso de documento gerado em papel através de impressora, estaremos perante uma cópia de documento eletrónico em diferente tipo de suporte e não perante um verdadeiro documento eletrónico.

magnético ou magnético-óptico; em sentido amplo, o documento eletrónico é aquele que é elaborado na sua forma definitiva, em suporte de papel ou equivalente, por um computador (como, por exemplo, o talão emitido pela caixa Multibanco)”. No entanto, apesar de ser discutível o modo como o ilustre processualista português, Miguel Teixeira de Sousa, inclui documentos em suporte papel no conceito de “documento eletrónico em sentido amplo”³⁵, e se verificar que o Regulamento eIDAS veio clarificar aquilo que é efetivamente um documento eletrónico, não se pode deixar de constatar que a distinção estabelecida por Pupo Correia³⁶ e Miguel Teixeira de Sousa deixou as suas marcas entre nós. Assim, poderíamos ser levados a entender o documento eletrónico em sentido estrito como uma fonte de prova; e o documento eletrónico em sentido amplo como um meio de prova, v.g., impressão de um documento eletrónico num papel é o meio de prova pelo qual o documento eletrónico (fonte de prova) se insere num processo judicial. Mas este entendimento está cada vez mais afastado da realidade. É que, cada vez mais, o documento eletrónico vem assumindo a dupla condição de fonte e de meio de prova³⁷.

Sendo incontestável que o documento eletrónico é uma nova realidade, são várias as opções com que legislador se confronta para dirimir a sua existência e utilização: Aplicação analógica, interpretação extensiva e princípios gerais? Nova regulamentação? Documento analógico em suporte papel conjugado com a doutrina e a jurisprudência para assegurar a coerência e a unidade do sistema jurídico? Em Portugal, a aplicação analógica e a interpretação extensiva, têm sido a opção dos operadores do direito. Mas tal, ainda que se afigure uma solução *ad hoc*, exigia uma nova regulamentação, o que seria a melhor opção do legislador. Não podemos ter a pretensão de usar mecanismo de regulamentação idênticos para realidades distintas.

Essa terá sido uma das razões, entre muitas outras, para a aprovação do Regulamento Europeu 910/2014, alterado recentemente pelo Regulamento (EU) 2024/1183, de 11 de abril, que revogou a Diretiva 1999/93/CE³⁸ e veio estabelecer um quadro jurídico comum, aplicado diretamente em todos os Estados-Membros. Foi estabelecido um quadro comum de documentos e assinaturas eletrónicas admissíveis pelo Tribunal, bem como um novo conjunto de instrumentos jurídicos, adaptados às

³⁵ entendendo que a impressão em papel de um documento eletrónico constituirá uma cópia em diferente tipo de suporte, sendo o documento eletrónico propriamente dito o original. Esta questão será abordada adiante a propósito da consideração das noções de suporte e formato.

³⁶ Miguel Pupo Correia, *in* “Assinatura eletrónica e certificação digital”, in “Direito da Sociedade da Informação”, vol. VI, Coimbra Editora, 2006.

³⁷ A este respeito, temos que constatar a total inexistência, no direito processual civil português, de normas que contemplem a produção de prova eletrónica.

³⁸ A Diretiva 1999 foi revogada com efeitos a 01/07/2016 pelo artigo 50º do Regulamento (EU) nº 910/2014, de 23 de julho (eIDAS), directamente aplicável aos Estados Membros (artº 288º do Tratado de Lisboa e artº 8º nº 4 da Constituição da República Portuguesa).

possibilidades tecnológicas atuais, destinado a garantir a segurança e fiabilidade das comunicações e transações eletrónicas.

Um aspeto importante do Regulamento Europeu é a opção assumida pelo legislador europeu por uma abordagem tecnologicamente neutra. Pode-se dizer que a neutralidade tecnológica e a equivalência funcional³⁹ são dois fatores importantes na construção de um mercado digital europeu inovador, confiável e seguro, do qual o Regulamento 910/2014 será, sem dúvida, o instrumento jurídico⁴⁰.

O Regulamento eIDAS veio reconhecer a importância dos documentos eletrónicos *“para o futuro desenvolvimento das transações electrónicas transfronteiriças no mercado interno”*, estabelecendo ainda o relevantíssimo princípio de que não podem ser recusados efeitos legais a um documento eletrónico, *“pelo simples facto de se apresentar em formato electrónico”*⁴¹. Este princípio ficou expressamente assumido no artigo 46º do Regulamento sobre os efeitos legais do documento eletrónico⁴². No entanto, o Regulamento não pretendeu regular a noção de documento estabelecida em cada direito nacional. Nessa esteira, deparamo-nos com o Decreto-Lei nº 12/2021, de 09 de fevereiro que veio assegurar a execução na ordem jurídica interna do Regulamento (EU) 910/2014. Ainda que o Regulamento seja obrigatório e diretamente aplicável na ordem jurídica portuguesa, incumbe aos Estados-Membros assegurar a sua execução nos respetivos ordenamentos.

O art.º 362º Código Civil português⁴³, estipula que os documentos têm de ser gerados pelo homem, ou seja, o documento é o resultado de uma atividade humana. Se assim é, questiona-se: e os documentos eletrónicos? Na verdade, nos tempos que correm, a grande parte dos documentos são produto da atividade humana, mas alguns documentos eletrónicos já não serão necessariamente um produto de uma atividade humana, v.g., produtos feitos por robôs. A função representativa destes documentos é indiscutível. Mas poderemos considerá-los ainda e sempre como uma mera reprodução mecânica? A introdução no circuito comercial de “documentos” elaborados por entes eletrónicos providos de capacidade de atuação autónoma, sem intervenção humana⁴⁴ vem tornar, cada vez mais premente, a adoção de um conceito amplo de documento eletrónico, seja este elaborado ou não pelo homem.

³⁹ Cfr. nota 22.

⁴⁰ Francisco C. P. Andrade, “Identificação eletrónica, assinatura e serviço de confiança”, UNIO - *EU Law Journal*. Vol. 4, No. 2, Julho 2018, pp 103-112.

⁴¹ Considerando 63 do Regulamento 910/2014, de 23 de julho.

⁴² Saliente-se que o Regulamento 910/2014, alterado pelo Regulamento (EU) 2024/1183, de 11 de abril de 2024, sendo um Regulamento Europeu, tem aplicação directa e imediata em todos os Estados-Membros. O que nos leva a constatar a existência de uma norma europeia, diretamente aplicável em Portugal, que impõe a consideração legal dos documentos electrónicos, mas sem que existam regras correspondentes em matéria de direito processual civil que regulem a produção deste novo meio de prova.

⁴³ Decreto-lei nº 47344/66, de 25 de novembro.

⁴⁴ O que já motivou uma importante inovação do legislador português na Lei do Comércio Electrónico (DL 7/2004) artº 33º que, expressamente, refere em epígrafe “contratação sem intervenção humana”.

2. O formato e suporte

O artº 3º do Decreto-lei nº 290-D/99, de 2 de Agosto (RJDEAD)⁴⁵ estipulava que “O documento eletrónico satisfaz o requisito legal de forma escrita quando o seu conteúdo seja susceptível de representação como declaração escrita.”

Este artigo fala-nos de “conteúdo”. Sucedem que, posteriormente, o legislador português criou uma evidente confusão com o Decreto-lei nº 7/2004, de 7 de janeiro⁴⁶ ao referir o termo “suporte”, no seu art.º 26º, nº 1: *“As declarações emitidas por via eletrónica satisfazem a exigência legal de forma escrita quando contidas em suporte que ofereça as mesmas garantias de fidedignidade, inteligibilidade e conservação.”* A referência ao “suporte”, considerando a referência prévia de “conteúdo”, denota uma confusão grosseira de conceitos por parte do legislador.

O suporte, por definição, é o que serve de sustentáculo a alguma coisa. O conteúdo, por definição, é o escrito, o assunto, a ideia ou o recheio de algo. Logo, o suporte pode ser importante para efeito de prova, mas não para efeito de consideração de existência ou não de escrito. Um escrito é, por definição, algo que pode ser lido e, neste sentido, está mais correta a expressão da antiga norma do DL 290-D/99, agora confirmada no Decreto-Lei nº 12/2021. De facto, quanto ao requisito de forma escrita, o Decreto-Lei nº 12/2021, de 09 de fevereiro acabou com as dúvidas que existiam ao estipular, no seu artº 3º nº 1, o que já constava no Decreto-Lei nº 290-D/99, de 2 de agosto: *“O documento eletrónico satisfaz o requisito legal de forma escrita quando o seu conteúdo seja suscetível de representação como declaração escrita.”* Porém, a questão relativa ao suporte mantém-se.

No documento eletrónico temos uma desvinculação entre o conteúdo e o suporte: o conteúdo pode mudar de suporte sem que seja alterado ou perdido. Sem suporte, a sequência de bits é efémera e não constitui um documento. O documento eletrónico precisa de suporte para conservar a sequência de bits. Mas o documento eletrónico não está adstrito a um corpo físico, pode ser transferido entre vários tipos de suporte sem perder a sua capacidade representativa.

Acresce que, até podemos ir mais longe ao afirmar que o aludido artº 26º nº 1 quando se refere ao suporte como garantia de fidedignidade e inteligibilidade das declarações emitidas por via eletrónica, deveria falar em formato de ficheiros. É diferente falar em suporte e em formato. O suporte permite o guardar, conservar ou arquivar. O formato é a forma de organização de dados e de representação da

⁴⁵ O Decreto-lei nº 290-D, de 2 de agosto foi revogado pelo Decreto-Lei nº 12/2021, de 09 de fevereiro.

⁴⁶ Transposição da Directiva nº 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000 sobre comércio eletrónico.

informação, v.g., Word, Excel, PDF, PowerPoint, JPEG, etc. E o conteúdo de um documento pode, na verdade, ser expresso em diferentes formatos⁴⁷.

Mais importante do que o suporte, para efeito de prova, é a questão da inalterabilidade do documento. E aqui devemos analisar o formato. Contudo, entramos noutra contrassenso: o documento em formato Word (o original?) pode ser mais facilmente alterado do que o documento em formato PDF (a cópia?). Conclui-se, portanto que o formato é que pode ser mais ou menos seguro. E isto poderia (e deveria) ser tido em consideração pelo legislador. No art. 26º do DL 7/2004 em vez de se confundir escrito com suporte, poderia ter havido um privilegiar de formatos que permitissem a inalterabilidade ou a rastreabilidade das alterações dos documentos. Tais formatos, sim, dariam garantias de fidedignidade e conservação.

Posto isto, os termos de conteúdo, de suporte e de formato, são diferentes e devem ser concretamente definidos pelo legislador sob pena de entrarmos em contrassensos jurídicos.

A conservação de longo prazo de documentos eletrónicos é importante e está intrinsecamente ligada ao suporte e ao formato. Os ritmos da evolução levam a que os documentos, com as rápidas e constantes atualizações, deixem de ser legíveis. Temos de considerar esta questão como importante para o direito. Qual a solução? Preservação de longa duração de documentos eletrónicos, diremos. Mas como? *A priori* temos duas opções:

1) Emulação: pressupõe que tudo seja conservado no formato original, onde os formatos são importantes. Para tal tem de se assegurar que o hardware e software sejam mantidos, o que implica manter equipamentos e programas durante um longo tempo. Vantagem? Garante, em qualquer momento, a leitura do documento eletrónico. Desvantagem? Pesados custos. Logo não é eficiente. Se não é eficiente temos de ir para outra solução, ou seja, a migração;

2) Migração: quando aparece um novo formato, existe a possibilidade de migração dos documentos para o novo formato. Só que também este método encontra grandes dificuldades na sua aplicação, e uma das principais prende-se com a utilização das chamadas assinaturas digitais⁴⁸. É que um dos

⁴⁷ sobre os formato de ficheiro electrónico cfr. Pedro Dias Venâncio "A tutela jurídica dos formatos de ficheiro electrónico", Edições Almedina 2016, pág. 46: "embora todos os computadores trabalhem em sistema de numeração binário, os diferentes programas de computador utilizam inúmeros FFE distintos em função do tipo de dado que pretendem representar digitalmente, da maior ou menor precisão com que o pretendem fazer e das opções técnicas que façam quanto à forma de digitalização ou representação digital."

⁴⁸ questão que se poderá colocar também é a da própria capacidade de conservação da assinatura digital propriamente dita. Cfr. Sofie Van den Eynde, "Digitale Archivering: een juridische stand van zaken vanuit Belgisch perspectief. Deel 1", in Digitale Archivering in Vlaamse Instellingen en Diensten – DAVID, Faculteit Rechtsgeleerheid, Interdisciplinair Centrum voor Recht en Informatica, Leuven 2001, pág. 83: "De"houdbaarheid" van een digitale

pressupostos essenciais da utilização deste tipo de assinatura passa precisamente pelo controlo de integridade dos documentos. E a aplicação deste tipo de assinatura leva a que o próprio documento, ou pelo menos a assinatura, só sejam legíveis desde que não haja qualquer alteração do seu conteúdo. O que levanta evidentes dificuldades nos casos em que se pretenda migrar os dados eletrónicos para novos formatos ou novas plataformas de software. É que, por um lado, a simples modificação de um bit que seja pode tornar um texto (ou uma assinatura) simplesmente ilegível.⁴⁹ Mas por outro lado, também é necessário garantir que a própria assinatura digital pode ser devidamente aplicada, de modo que o documento seja lido e a origem e integridade do documento verificadas, muitos anos depois da criação e assinatura do documento eletrónico em causa.⁵⁰

Aqui temos um problema sério com as assinaturas digitais. O documento passa a ser diferente e, sendo modificado, a integridade do documento está afetado e o hash⁵¹, resultante da sua leitura, passa a ser diferente e, portanto, deixa de ser possível comprovar a autenticidade do documento. O que fazer? A solução, a nosso ver, passa pela utilização de um novo tipo de serviço da sociedade da

handtekening is ook niet onbeperkt. Net zoals de software waarmee een document werd aangemaakt, zullen ook de cryptografische technologieën verouderen waardoor de digitale handtekening niet meer leesbaar is. Bijgevolg zal ere en bepaald procédé moeten toegepast worden op de digitale handtekening, zoals migratie of emulatie, om ze leesbaar te houden" (A "capacidade de conservação" de uma assinatura digital também não é ilimitada. As tecnologias criptográficas também se tornarão antiquadas, tal como o software usado na elaboração de um documento, pelo que a assinatura digital deixará de ser legível. Consequentemente, deverá ser aplicado um determinado procedimento à assinatura digital, como a migração e a emulação, para que esta se mantenha legível). – Cfr. Francisco Andrade in "Da Contratação Electrónica - Em Particular da Contratação Electrónica Inter-Sistémica Inteligente", pag. 142.

⁴⁹ - questão esta que vem colocando algum ceticismo em torno da própria utilização das assinaturas digitais: "Skepticism appeared as soon as it became clear that, when using digital signatures, control of the integrity is only possible if the electronic data remain completely unchanged at the bit-level. This raises a problem when archivists want to migrate electronic data to new formats or software platforms in order to keep them accessible and legible. Some people have immediately concluded that digital signatures are therefore not useful and hence not relevant for archival purposes. ", cfr. Jos Dumortier, "E-Government and Digital Preservation", in "E-Government: legal, technical and pedagogical aspects", Universidad de Zaragoza, 2003, págs. 93-104; Cfr. DUMORTIER, Jos e Vandezande, Niels. "Critical observations on the proposed Regulation for electronic identification and trust services for electronic transactions in the internal market", 2013.

⁵⁰ - parece evidente que, após uma migração, se revestirá da maior importância a realização de cópias de segurança. Cfr. Sofie Van den Eynde, "Wat archiveren en hoe? Op zoek naar de rol van PKI voor digitale archieven" (O que arquivar e como? À procura da função da Infraestrutura de Chaves Públicas para arquivos digitais), in <http://www.expertisecentrumdavid.be/davidproject/teksten/Rapporten/Rapport6.pdf> ponto B.2.3: "Maken van veiligheidskopieën van gearcheveerd informatiekpakket" (A elaboração de cópias de segurança dos pacotes de informação arquivados). Mas, na verdade, o que a Autora na realidade propõe é a elaboração de um segundo exemplar do documento: "Het maken van deze kopie mag in geen geval uitgesteld worden. Beide exemplaren moeten idealiter tegelijkertijd gearcheveerd worden. Bovendien moet erover gewaakt worden dat de veiligheidskopie eveneens het origineel bevat. Het word "veiligheidskopie" is hier dus eigenlijk niet op zijn plaats. Beter is te spreken over "het tweede exemplar". (A elaboração dessa cópia não pode, em caso algum, ser adiada. O ideal é que ambos os exemplares sejam arquivados ao mesmo tempo. Além disso, deve ter-se em atenção que a cópia de segurança deve conter também o original. Portanto, o termo "cópia de segurança" não está aqui, de facto, no sítio correcto. Será melhor falar de um "segundo exemplar". Cfr. Francisco Andrade in "Da Contratação Electrónica - Em Particular Da Contratação Electrónica Inter-Sistémica Inteligente", pag. 142.

⁵¹ A função de hash é uma função matemática que transforma uma entrada de dados de comprimento arbitrário em uma saída de comprimento fixo. Esta saída é frequentemente chamada de "valor de hash" ou "resumo de hash". As funções de hash são amplamente utilizadas em diversas áreas da computação, incluindo segurança da informação, armazenamento de dados e verificação de integridade.

informação qual seja o serviço de migração certificada, v.g., serviço de notariado eletrónico⁵². No momento da migração, teríamos um terceiro de confiança que asseguraria que o conteúdo de um documento migrado é idêntico ao do documento original e que o documento original estava devidamente assinado, com assinatura aposta em determinada data, tudo conforme verificado pelo terceiro de confiança (notário eletrónico).

Por fim, o sistema de assinatura eletrónica digital contém três algoritmos: o algoritmo de hash, o algoritmo para a elaboração da assinatura digital no final do documento, e o algoritmo de verificação da assinatura. Contudo, este paradigma poderá estar em risco de ser comprometido devido a desenvolvimentos no campo da criptografia quântica. É certo que é pouco provável que esta tecnologia esteja disponível para uma utilização generalizada num futuro próximo, mas têm vindo a ser desenvolvidos projectos nesta área. E esta situação pode criar desigualdades entre pessoas singulares e colectivas ou entre estados. Como tal, é relevante interrogar a necessidade de regulamentação na utilização destas tecnologias. É importante encetar sinergias entre os intervenientes do Direito e da Informática⁵³ para obter soluções alternativas que permitam enfrentar os riscos associados à mudança de paradigma da criptografia tradicional para um novo paradigma de criptografia quântica. A convivência entre os dois modelos poderá colocar em risco o atual sistema técnico e legal que sustenta a utilização dos serviços de identificação eletrónica, tal como enunciados no Regulamento eIDAS.^{54 55} Ora, tudo isto também terá impacto relevante no âmbito do processo civil.

⁵²No novo Regulamento eIDAS, os serviços certificados de arquivo eletrónico são abordados especificamente no artigo 45º-J. Este artigo estabelece que os documentos eletrónicos conservados através de um serviço qualificado de arquivo eletrónico gozam da presunção de integridade e origem durante o período de conservação pelo Prestador Qualificado de Serviços de Confiança.

A nova versão do Regulamento eIDAS, introduz vários serviços de certificado e arquivo eletrónico. Aqui estão alguns dos principais:

1. Certificado Eletrónico de Atributos: Este serviço permite a autenticação de características específicas do titular do certificado, como diplomas, licenças e mandatos para representar ou agir em nome de outras pessoas.
2. Serviço Qualificado de Arquivo Eletrónico: Este serviço garante que os documentos eletrónicos mantidos por um Prestador Qualificado de Serviços de Confiança têm presunção de integridade e origem durante o período de conservação.
3. Livro-Razão Eletrónico Qualificado: Este serviço assegura a presunção de uma ordem cronológica única e exata e a integridade dos registos contidos no livro-razão.

Estes serviços visam aumentar a segurança e a confiança nas transações eletrónicas, promovendo a interoperabilidade e o reconhecimento mútuo entre os Estados-Membros da União Europeia.

⁵³ Cfr. 1) CANOTILHO, J. J. Gomes. Direito Constitucional e Teoria da Constituição. 7ª Edição. Coimbra: Almedina, 2018. 2) CASTRO, Anselmo de. Lições de processo civil, vol. IV. 1ª Edição. Coimbra: Atlântida, 1969. 3) CASTRO, Catarina Semedo de. Direito da Informática, Privacidade e Dados Pessoais. Almedina, 2005. 4) CASTRO, Catarina Sarmiento e. 40 anos de 'Utilização da Informática' - o artigo 35.º da Constituição da República Portuguesa. ePública: Revista Eletrónica de Direito Público. Lisboa. ISSN 2183-184X. vol. 3. nº 3, 2016.

⁵⁴Francisco Andrade e José Carlos Bacelar Almeida: "Digital Signatures and Quantum Computing", in "Legal Developments in Cybersecurity and Related Fields", Springer, 2024

3. Escrito, assinatura, prova

Outra questão é a de saber se um documento eletrónico pode ou não valer como documento escrito? A este propósito temos de esclarecer que um documento, seja ou não eletrónico, pode também ser ou não um escrito. A este respeito, o DL 290-D/99 era claro, no seu artigo 3º, ao estabelecer a distinção entre as situações previstas no seu nº 1 “quando o seu conteúdo seja suscetível de representação como declaração escrita” e no seu nº 3 “documento eletrónico cujo conteúdo não seja suscetível de representação como declaração escrita”. Porque um documento eletrónico pode ter representação textual (podendo ser lido) ou representação áudio ou vídeo e esses documentos não podem ser lidos. O Decreto-Lei 12/2021, no seu artº 3º nº 1, veio clarificar este aspeto.

O artº 46 do Regulamento Europeu 910/2014 veio resolver a questão dos efeitos legais dos documentos eletrónicos, ao estabelecer 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.

No entanto, o Regulamento Europeu não determina o que deve ou não ser entendido por escrito, deixando essa tarefa a cada legislador nacional. Em Portugal, apesar de termos de entender que o DL 290-D/99 foi em boa medida revogado pela aprovação do Regulamento eIDAS, temos por claro que o nº 1 do artigo 3º do DL 290-D/99 manteve-se plenamente em vigor⁵⁶ até à sua revogação pelo Decreto-Lei nº 12/2021⁵⁷.

Outra questão de fundamental importância prende-se, já não com a admissibilidade do documento eletrónico enquanto meio de prova, mas com a consideração do valor probatório de documento eletrónico assinado. O direito português estabelece a distinção entre documentos autênticos e documentos particulares, dizendo o nº 2 do artigo 363º do Código Civil: “Autênticos são os documentos exarados, com as formalidades legais, pelas autoridades públicas nos limites da sua competência ou, dentro do círculo de atividade que lhe é atribuído, pelo notário ou outro oficial público

⁵⁶ Francisco C.P. Andrade, “Assinatura digital: conceito e risco futuro”, in Joana Covelo de Abreu et al (Coords.), “O Contencioso da União Europeia e a cobrança transfronteiriça de créditos: compreendendo as soluções digitais à luz do paradigma da Justiça eletrónica europeia (e-Justice)”, Volume III, Coleção UNIO E-book), Escola de Direito, 2022, pp. 122-128.

⁵⁷ Nem sequer consideramos a hipótese, que conduziria a resultados absurdos, de o nº 1 do artigo 3º do DL 290-D/99 poder ter sido revogado pelo art. 26º do DL 7/2004, o qual seria de muito difícil compreensão e, sobretudo, de muito difícil compatibilização com a noção de escrito do DL 290-D/99. Mas há que referir, a este respeito, que a re-publicação do DL 290-D/99 após a sua última alteração, operada pelo DL 88/2009, manteve a referida norma em vigor.

⁵⁸ Cfr. Artigo 3º nº 1: “O documento eletrónico satisfaz o requisito legal de forma escrita quando o seu conteúdo seja suscetível de representação como declaração escrita.”

provido de fé pública; todos os outros documentos são particulares”. E os documentos particulares, como vimos, podem ser documentos escritos ou não escritos, assinados ou não assinados. Questão é saber em que situações o direito português considerará um documento eletrónico escrito como sendo um documento particular assinado. E a este respeito atendíamos ao disposto no artigo 3º nº 2 do DL 290-D/99: “Quando lhe seja aposta uma assinatura eletrónica qualificada certificada por uma entidade certificadora credenciada, o documento eletrónico com o conteúdo referido no número anterior⁵⁸ tem a força probatória de documento particular assinado, nos termos do artigo 376º do Código Civil”. O que o mesmo é dizer que “faz prova plena quanto às declarações atribuídas ao seu autor, sem prejuízo da arguição e prova de falsidade do documento”. Estes são aspetos regulados pelo direito civil português e que o Regulamento eIDAS não aborda de todo. No entanto, a aprovação do novo Regulamento Europeu, em 2014, veio trazer uma importante clarificação quanto aos efeitos jurídicos e valor de prova das assinaturas eletrónicas e dos documentos por elas assinados. Começa por dizer o artigo 25º do Regulamento eIDAS que “não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a uma assinatura eletrónica pelo simples facto de se apresentar em formato eletrónico ou de não cumprir os requisitos legais para as assinaturas eletrónicas qualificadas”. Ou seja, o Regulamento vem reconhecer que tanto as assinaturas eletrónicas avançadas⁵⁹ como as assinaturas eletrónicas qualificadas⁶⁰ são admissíveis como prova em Tribunal e não lhes podem ser negados efeitos legais. No entanto, o legislador europeu também veio reconhecer que às assinaturas eletrónicas avançadas e qualificadas corresponderão diferentes níveis de segurança e essa diferença traz consigo consequências jurídicas, o que o legislador europeu expressamente reconheceu e consagrou no nº 2 do artigo 25º: “A assinatura eletrónica qualificada tem um efeito legal equivalente ao de uma assinatura manuscrita”. Esta norma europeia veio, assim, pôr termo à estranha distinção então estabelecida pelo DL 290-D/99 entre assinaturas eletrónicas qualificadas e assinaturas eletrónicas qualificadas certificadas por entidades certificadoras credenciadas⁶¹. Agora, o conceito de “assinatura eletrónica qualificada” é igualmente estabelecido em todos os Estados-Membros e torna-se claro que todas as assinaturas eletrónicas qualificadas têm valor de assinatura manuscrita. Pelo que um

⁵⁸ - “...suscetível de representação como declaração escrita”.

⁵⁹ - “uma assinatura que obedeça aos requisitos estabelecidos no artigo 26º” (artigo 3º nº 11 do Regulamento).

⁶⁰ - “uma assinatura eletrónica qualificada criada por um dispositivo qualificado de criação de assinaturas eletrónicas e que se baseie num certificado qualificado de assinatura eletrónica” (artigo 3º nº 12 do Regulamento).

⁶¹ - deve assim entender-se que o Regulamento 910/2014 veio alterar o nº 2 do artigo 3º do DL 290-D/99. Assim, onde se lia: “...aposta uma assinatura eletrónica qualificada certificada por entidade certificadora credenciada...”, deveria passar a ler-se “aposta uma assinatura eletrónica qualificada...”, eliminando-se a referência à entidade certificadora credenciada e passando o foco para o cumprimento dos requisitos estabelecidos no Anexo I do Regulamento 910/2014 e aplicáveis aos certificados qualificados de assinatura eletrónica”. Entretanto, a questão ficou ultrapassada com o DL 12/2021 e a revogação integral do DL 290-D/99.

documento eletrónico escrito ao qual seja aposta uma assinatura eletrónica qualificada deverá ser considerado, de acordo com a lei civil portuguesa, como documento particular assinado e gozar da força probatória estabelecida pelo artigo 376º do Código Civil.

Por sua vez, o Decreto-Lei 12/2021, no seu artº 3º nº 2, veio clarificar o que já resultava do Regulamento eIDAS de que a aposição de uma assinatura eletrónica qualificada a um documento eletrónico equivale à assinatura autógrafa dos documentos com forma escrita sobre suporte papel⁶². E, no seu artº 3º nº 3, em consonância com o disposto no Regulamento eIDAS, o DL nº 12/2021 diz-nos que “a assinatura eletrónica qualificada deve referir-se inequivocamente a uma só pessoa singular ou representante da pessoa coletiva e ao documento ao qual ela é aposta”. Estranha-se a referência “a assinatura eletrónica qualificada” quando, em bom rigor, o Regulamento eIDAS, no seu artigo 3º nº 9 diz que signatário é “a pessoa singular que cria uma assinatura eletrónica”, sem fazer distinção entre assinaturas eletrónicas simples, avançadas ou qualificadas; e, no artº 25º nº 1, diz-nos que “não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a uma assinatura eletrónica pelo simples facto de se apresentar em formato eletrónico ou de não cumprir os requisitos exigidos para as assinaturas eletrónicas qualificadas”. Afigura-se, portanto, evidente que qualquer assinatura eletrónica (seja ou não qualificada) deve referir-se inequivocamente a uma só pessoa singular ou representante da pessoa coletiva e ao documento ao qual ela é aposta. Assim, a palavra “qualificada” do artº 3º nº 3 do DL 12/2021 peca por excesso e deveria ser considerada resultado de um lapso de escrita, sob pena de podermos vir a ter uma confusão quando forem utilizadas assinaturas eletrónicas avançadas (v.g., assinaturas dos Advogados via Signius). A verdadeira importância da utilização de assinaturas eletrónicas qualificadas está no nível probatório e esse está previsto no artº 3º nº 5 do DL nº 12/2021.

Confusão escusada é a vertida no artº 3º nº 6 do DL 12/2021 ao estipular que: “Quando lhe seja aposta uma assinatura eletrónica qualificada, o documento eletrónico cujo conteúdo não seja suscetível de representação como declaração escrita tem a força probatória prevista no artigo 368.º do Código Civil e no artigo 167º do Código de Processo Penal, aprovado pelo Decreto-Lei nº 78/87, de 17 de fevereiro, na sua redação atual”. Significa isto que, a partir de agora, as reproduções mecânicas, para valerem como tal, têm de ter assinatura eletrónica qualificada?... Este preceito faz uma evidente confusão entre assinatura e reprodução mecânica, parece-nos claramente despropositado e poderá criar enormes incertezas quanto à aplicação dos artigos 368º do Código Civil e 167º do Código de Processo Penal.

⁶² Tais documentos eletrónicos, consequentemente, são considerados documentos particulares assinados.

Por fim, uma nota de preocupação para a revogação integral do DL nº 290-D/99 nos termos do artº 36º do DL 12/2021, uma vez que tal foi feito sem regular as matérias relativas à suspensão e revogação dos certificados qualificados e aos deveres e obrigações das entidades que emitem os certificados e dos titulares dos certificados (arts. 24º, 26º, 30º e 31º do DL nº 290-D/99), criando-se, assim, um verdadeiro vazio legal e que certamente criará situações de incerteza jurídica em matéria de fundamental relevo para a própria segurança da utilização de assinaturas eletrónicas.

4. Original versus cópia ⁶³

O artº 4º do RJDEAD dizia-nos que “As cópias de documentos eletrónicos, sobre idêntico ou diferente tipo de suporte, são válidas e eficazes nos termos gerais de direito e têm a força probatória atribuída às cópias fotográficas pelo nº 2 do artigo 387º do Código Civil e pelo artigo 168º do Código de Processo Penal, se forem observados os requisitos aí previstos.”

Esta era a tese de que a impressão de um documento eletrónico constitui cópia analógica de um documento eletrónico. Estranhamente, o DL 12/2021 procedeu à revogação integral do DL 290-D/99 sem se debruçar sobre este ponto. Mas vejamos os diferentes tipos de cópias existentes:

Cópias analógicas de documentos informáticos, ex: Impressão;

Cópia informática de documento analógico, ex: Scanner;

Cópia informática de documento informático: sequência diferente de valores binários do documento original;

Duplicado informático: sequência igual de valores binários do documento original⁶⁴.

Em todos o elo comum é o documento original ser eletrónico.

E o que é cópia e original de um documento eletrónico? O original é o documento em bits⁶⁵. O documento em formato Word, estando na base criativa, é o documento original. Transformar o documento do formato Word em formato PDF, é fazer uma cópia em diferente formato. Se, eventualmente, enviarmos o documento, em formato Word, para um terceiro, pese embora menos seguro quanto à possibilidade de alteração, estaríamos a enviar o documento original.

⁶³documento de um documento

⁶⁴ Código da Administração Digital Italiano (CAD), decreto legislativo 7 marzo 2005, n. 82, sucessivamente modificado e integrado pelos decretos legislativos 22 agosto 2016 n. 179 e 13 dicembre 2017 n. 217.

⁶⁵Unidade elementar de medida de informação que apenas pode tomar dois valores distintos (geralmente notados 1 e 0), *in* Dicionário Priberam da Língua Portuguesa.

O que é um documento gerado em papel através da impressora? É um documento ou é uma cópia de um documento eletrônico? Considerando que o documento original eletrônico é elaborado em bits (não em papel), logo, o documento em papel é uma cópia em diferente suporte, *maxime* uma reprodução mecânica.

Capítulo II – A descoberta eletrónica da prova

1. Regime geral da prova em Processo Civil^{66 67 68 69 70 71 72 73}

1.1. Provas atendíveis^{74 75 76}

Indica-nos o art. 341º do Código Civil que “as provas têm por função a demonstração da realidade dos factos”.

Podemos afirmar que a prova é o oxigénio do processo.

Nos termos do art. 413º do CPC “O tribunal deve tomar em consideração todas as provas produzidas, tenham ou não emanado da parte que devia produzi-las, sem prejuízo das disposições que declarem irrelevante a alegação de um facto, quando não seja feita por certo interessado”.

Ou seja, isto significa que, havendo provas que tenham sido produzidas relativamente aos factos em juízo, o tribunal deve tomá-las em consideração.

É mediante a prova produzida em julgamento que o juiz vai formar a sua convicção em relação aos factos e dita sentença.

A prova é essencial no direito processual civil. Seirmos, “o direito à prova significa que as partes conflitantes, por via de ação e da defesa, têm o direito a utilizarem a prova em seu benefício e como sustentação dos interesses e das pretensões que apresentarem em tribunal”⁷⁷. Para além disso, há sempre o direito de exercer o princípio do contraditório, isto é, “as partes têm ainda o direito a

⁶⁶ Código de Processo Civil, Lei nº 41/2013 de 26 de Junho.

⁶⁷ RANGEL, Rui Manuel de Freitas. O Ónus da Prova no Processo Civil. 3ª Edição. Almedina, 2006.

⁶⁸ RODRIGUES, Fernando Pereira. Os meios da prova em processo civil. 3ª edição. Almedina, 2017.

⁶⁹ SOUSA, Miguel Teixeira de. As partes, o objecto e a Prova em processo declarativo. 1ª edição. Lisboa: Lex-Edições Jurídicas, 1995.

⁷⁰ ALEXANDRE, Isabel. Provas Ilícitas em Processo Civil. 1ª edição. Coimbra: Almedina, 1998.

⁷¹ 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 (e-book). 2ª Edição. Lisboa: Centro de Estudos Judiciários (CEJ), 2013.

⁷² O Novo Processo Civil - Contributos da doutrina para a compreensão do novo código de processo civil. Centro de Estudos Judiciários, Caderno I, 2ª Ed., 2013.

⁷³ GONÇALVES, Marco Carvalho. Notas sobre o regime transitório de aplicação do novo Código de Processo Civil, in Cadernos de Direito Privado, n.º 44, Outubro-Dezembro de 2013;

⁷⁴ LEITÃO, Hélder Martins. A prova no código de processo civil – Como a requerer (anotado e comentado). Librum Editora, 2017. LEITÃO, Hélder - Da instrução em processo civil das provas. 3ª edição. Coimbra: Librum Editora/Almedina, 2016.

⁷⁵ MENDES, João de Castro. Do conceito de Prova. 1ª edição. Lisboa: Ática, 1961.

⁷⁶ TRINDADE, Cláudia Sofia Alves. A prova de estados subjectivos – Presunções e regras da experiência. Almedina, 2016.

⁷⁷ Acórdão do Tribunal da Relação de Guimarães, disponível em

<http://www.dgsi.pt/itrg.nsf/86c25a698e4e7cb7802579ec004d3832/36b07def5f5fc8bf80258472004d65d0>.

contradizer as provas apresentadas pela parte contrária ou suscitadas oficiosamente pelo tribunal bem como o direito à contraprova”⁷⁸.

Além disso, “o direito à prova é parte essencial do direito fundamental de acesso ao direito (artigo 20º da Constituição da República Portuguesa), na vertente do direito a um processo equitativo, constituindo-se como peça fundamental para a realização efetiva do direito de ação judicial, pois que, sem a possibilidade de oferecimento e produção de provas, o direito de ação judicial não passaria de uma concessão vazia de qualquer conteúdo, eventualmente sujeita aos humores e à sorte de um qualquer Bridoye”^{79 80}.

Em Portugal vigora o princípio da livre apreciação da prova, princípio que expressamente se consagra no art. 607º, nº 5 do CPC. “A livre apreciação traduz-se, na sua essência, em liberdade de formação da convicção do julgador, em que a forma de motivar a decisão de facto varia consoante o facto probando e o meio de prova utilizado”⁸¹. “O princípio da livre apreciação da prova nunca atribui ao juiz “o poder arbitrário de julgar os factos sem prova ou contra as provas”, ou seja, a livre apreciação da prova não pode confundir-se “com uma qualquer arbitrária análise dos elementos probatórios”, sendo “antes uma conscienciosa ponderação desses elementos e das circunstâncias que os envolvem”⁸².

Centremo-nos agora no tipo de provas que o sistema jurídico português admite.

Desde logo, todas as espécies de provas admissíveis em processo civil estão explanadas no Código Civil⁸³ e no CPC.

Assim, são admissíveis várias provas em processo civil, designadamente, as seguintes:

- i. Prova por documentos – art. 423º e ss do CPC;
- ii. Prova por confissão das partes – artº 452º e ss do CPC;
- iii. Prova por declarações de parte – artº 466º do CPC;
- iv. Prova pericial – art. 467º e ss CPC;
- v. Prova por inspeção judicial – art. 490º e ss CPC;
- vi. Prova testemunhal – art. 495º e ss CPC.

⁷⁸ Idem.

⁷⁹ Acórdão do Tribunal da Relação do Porto, disponível em

<http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/06545d2b7a5312a7802585c8002ea67a?OpenDocument>.

⁸⁰ Bridoye é um personagem do romance “A Vida de Gargântua e de Pantagruel” de François Rabelais. É um juiz que decide os casos lançando dados, simbolizando a arbitrariedade e a falta de lógica na justiça. Através de Bridoye, Rabelais critica a justiça da sua época, mostrando como as decisões judiciais podem ser influenciadas pelo acaso e pela falta de racionalidade.

⁸¹ RODRIGUES, André Marques, in A valorização da prova em processo civil: prova legal e livre apreciação da prova.

⁸² Acórdão do Tribunal da Relação de Coimbra, disponível em

<http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/d6b3d4a8a8754c69802584c400413edb?OpenDocument>

⁸³ HÖRSTER, Heinrich Ewald e MOREIRA DA SILVA, Eva Sónia. A Parte Geral do Código Civil Português. Almedina, 2019.

Vamos por partes:

Em primeiro lugar, cumpre dizer que todos estes tipos de prova têm como função única “formar a convicção do juiz a respeito dos factos que interessam à solução do litígio”⁸⁴.

1.1.1. Prova por documentos^{85 86 87}

Nos termos do art. 362º do CC, a “prova documental é a que resulta de documento; diz-se documento qualquer objeto elaborado pelo homem com o fim de reproduzir ou representar uma pessoa, coisa ou facto”.

Podemos afirmar que a prova documental é a “rainha das provas”, devido à grande segurança que a mesma alcança, quando comparada com as demais.

A prova por documentos consiste, precisamente, na apresentação de documentos. a prova documental é uma prova real que põe o juiz em presença dum objeto material que lhe representa o facto a averiguar, é a prova mediante um objeto material destinado a dar ao juiz a representação dum facto.

A prova documental engloba fotografias, papéis, plantas, documentos, etc.

Quanto ao momento de apresentação dos documentos, aplica-se o art. 423º, que indica que os documentos devem ser apresentados com o articulado em que se aleguem os factos correspondentes, isto é, devem ser apresentados logo com a petição inicial ou com a contestação, por serem estes os articulados mais relevantes, mas utilizando-se outros articulados em que se aleguem factos, também devem os documentos ser logo apresentados com esses articulados.

Porém, a lei admite que os documentos sejam apresentados posteriormente, nos termos dos arts. 423º, nº 2 do CPC “se não forem juntos com o articulado respetivo, os documentos podem ser apresentados até 20 dias antes da data em que se realize a audiência final, mas a parte é condenada em multa, exceto se provar que os não pôde oferecer com o articulado”. Posteriormente a este limite temporal, ainda se admitem documentos cuja apresentação não tenha sido possível até àquele momento e também documentos que apenas tenham sido necessários por força de ocorrência posterior – art. 423º, nº 3 do CPC.

⁸⁴ Acórdão do Tribunal da Relação de Coimbra, disponível em

<http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/21f0cf810efde0f9802586cf00354ccc?OpenDocument>.

⁸⁵ Fernandez, E. (2014). Um Novo Código de Processo Civil? Em busca das diferenças. Vida Económica; FERNANDEZ, Elisabeth. A prova difícil ou impossível. In Estudos em homenagem ao Prof. Doutor José Lebre de Freitas. 1.ª edição. Coimbra: Coimbra Editora, 2013.

⁸⁶ Freitas, J. L. de. (2019). Código de Processo Civil Anotado - Volume 2.º Artigos 362.º a 626.º. Coimbra: Coimbra Editora.

⁸⁷ Mendes, J. de C., & Sousa, M. T. de. (2023). Manual de Processo Civil. Vol. I & II. AAFDL Editora.

Também se admite, ao abrigo do art. 429º do CPC que se peçam documentos que estejam em poder da parte contrária: “1 - Quando se pretenda fazer uso de documento em poder da parte contrária, o interessado requer que ela seja notificada para apresentar o documento dentro do prazo que for designado; no requerimento, a parte identifica quanto possível o documento e especifica os factos que com ele quer provar.

2 - Se os factos que a parte pretende provar tiverem interesse para a decisão da causa, é ordenada a notificação”.

Para se pedir documentos em poder da parte contrária, “cabe ao requerente alegar a efetiva necessidade e da pertinência da junção dos documentos que estejam em poder da parte contrária (situação de necessidade probatória), cabendo-lhe individualizar tais documentos de molde a habilitar a contraparte a tomar posição sobre a existência do documento e sobre a proteção de que o mesmo possa eventualmente beneficiar”⁸⁸.

Na jurisprudência a propósito deste regime, ressaltam os seguintes arestos: Acórdão do Tribunal da Relação de Lisboa de 6.2.2020, Adeodato Brotas, 492/18, com este teor: «O deferimento da junção de documento em poder da parte contrária está dependente da efectiva necessidade e da pertinência da junção: impõe-se que a parte que pretenda a cooperação do tribunal justifique, de forma convincente, que não consegue obter esses elementos e, que deles carece efectivamente para uma finalidade processual.»⁸⁹. “Desse modo, cada documento deve ser concretamente indicado: “a razão de ser da indicação específica da coisa a exhibir reside, assim, na finalidade de evitar que uma parte se sirva do instituto da exibição com um escopo meramente exploratório, trazendo para o processo factos estranhos à causa, ou factos ainda nele não introduzidos. O limite mínimo do dever de específica descrição do documento deve, assim, ser dado pela ideia de que a exibição não pode ter um escopo meramente informativo, em ordem à eventual obtenção de novos elementos de prova, sem se saber previamente quais sejam, ou de novos fundamentos de ação ou exceção”⁹⁰. No mesmo sentido, deve ser concretamente indicado o documento que se requer, “para que a parte contrária possa tomar conscientemente qualquer atitude perante o despacho que requisitar a apresentação, é indispensável que ela saiba, ao certo, qual a espécie de documento que se lhe exige – se uma carta, se uma letra, se um relatório, se um balanço, se um título de arrendamento, etc. E não basta que se se indique a espécie, em abstrato, é necessário que se caracterize a espécie, que se individualize o documento,

⁸⁸ Acórdão do Tribunal da Relação de Lisboa, disponível em

<http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/3790fa22f0e0ef668025891a004b7119?OpenDocument>.

⁸⁹ Idem.

⁹⁰ Idem.

dizendo-se por exemplo, de que data é a carta e quem a expediu, a que prédio se refere o arrendamento e em que data se celebrou, etc”⁹¹.

1.1.2. Prova por confissão das partes

Dispõe o artigo 352º do CC que a “confissão é o reconhecimento que a parte faz da realidade de um facto que lhe é desfavorável e favorece a parte contrária”. A confissão constitui, portanto, uma modalidade de prova que tem como função demonstrar a realidade dos factos.

Nos termos do artº 452º nº 1 do CPC “o juiz pode, em qualquer estado do processo, determinar a comparência pessoal das partes para a prestação de depoimento, informações ou esclarecimentos sobre factos que interessem à decisão da causa” e o nº 2 estabelece que “quando o depoimento seja requerido por alguma das partes, devem indicar-se logo, de forma discriminada, os factos sobre que há de recair”.

Este meio de prova pode assumir as modalidades de confissão judicial e extrajudicial. A confissão judicial é feita em tribunal e pode ser espontânea ou provocada, enquanto a extrajudicial, por exclusão, realiza-se por modo diferente (artigo 355.º n.ºs 2 e 4 do CC).

A eficácia de confissão depende da circunstância de ser feita por pessoa com capacidade para poder dispor do direito a que o facto confessado se refira (artigo 353.º n.º 1 do do CC). A confissão é inadmissível como prova: a) se for declarada insuficiente por lei ou recair sobre facto cujo reconhecimento ou investigação a lei proíba; b) se recair sobre factos relativos a direitos indisponíveis; c) se o facto confessado for impossível ou notoriamente inexistente (artigo 354.º do CC).

1.1.3. Prova por declarações de parte

Dispõe o artº 466º nº 1 do CPC que “as partes podem requerer, até ao início das alegações orais em 1.ª instância, a prestação de declarações sobre factos em que tenham intervindo pessoalmente ou de que tenham conhecimento direto”. Com a entrada em vigor do atual CPC as declarações de parte foram introduzidas no nosso ordenamento jurídico-processual como um novo meio de prova, sujeito, em termos de força probatória, à livre apreciação do tribunal (salvo quando a parte em que se apresentem confessórias), e que não se confunde com o depoimento de parte.

São pressupostos legais da admissibilidade da prestação das declarações de parte: a) que elas sejam requeridas pela própria parte; b) que sejam requeridas até ao início da fase das alegações orais na

⁹¹ Acórdão do Tribunal da Relação de Coimbra, disponível em

<http://www.dgsi.pt/itrc.nsf/c3fb530030ea1c61802568d9005cd5bb/fdd10085d40d2c7c802588360031c23b?OpenDocument>.

audiência de discussão e julgamento em 1ª instância; c) que elas se reportem a factos em que a parte tenha intervindo pessoalmente ou de que tenha conhecimento direto; d) e que esses factos sejam indicados pelo requerente no requerimento em que formula esse seu pedido. A tomada das requeridas declarações de parte só pode ser recusada pelo tribunal quando os factos indicados no requerimento já estejam plenamente provados por documentos ou por outro meio de prova com força obrigatória plena.⁹²

1.1.4. Prova pericial

Dispõe o art. 388.º do CC que “a prova pericial tem por fim a percepção ou apreciação de factos por meio de peritos, quando sejam necessários conhecimentos especiais que os julgadores não possuem, ou quando os factos, relativos a pessoas, não devam ser objeto de inspeção judicial”.

A prova pericial é, assim, um meio de prova que recai, em regra, sobre factos que dependem de conhecimentos que, à partida, os juízes não dispõem. Para que sejam interpretados, analisados ou valorados de maneira correta, é necessário que seja um perito a apreciá-los.

No dizer de Lebre de Freitas⁹³, “o perito surge como intermediário entre a fonte da prova (pessoal ou real) e o tribunal quando, para plena apreensão da prova, haja necessidade de conhecimentos especializados. A prova pericial pode visar a percepção indiciária de factos por inspeção de pessoas (ex.: exame médico-legal) ou de coisas, móveis ou imóveis, (ex.: exame de uma máquina ou vistoria de um prédio), a avaliação de coisas ou direitos (determinação do valor de um prédio ou de um quadro, duma quota social), ou ainda a verificação da origem dum documento (assinatura, letra, data, genuinidade, alteração), a revelação do seu conteúdo (máxime os livros e documentos de escrita comercial e os documentos eletrónicos) ou a apreciação, de acordo com regras de especialidade, dos indícios a extrair de fontes de prova (para, nomeadamente, estabelecer um nexo de causalidade.”⁹⁴.

Para Fernando Pereira Rodrigues “a função da prova pericial não é apenas a de recolha de factos, mas também a da apreciação técnica dos factos observados. A função típica do perito é a da colheita de factos para depois produzir quanto aos mesmos uma apreciação técnica, mediante juízos de valor que se lhe ofereçam emitir com fundamento em critérios normativos, princípios científicos ou máximas da experiência”⁹⁵.

⁹² Acórdão do Tribunal da Relação de Coimbra, disponível em [Acórdão do Tribunal da Relação de Coimbra](#).

⁹³ Lebre de Freitas e Isabel Alexandre, Código de Processo Civil Anotado, Volume 2.º, 3.ª Edição, 2017.

⁹⁴ Acórdão do Tribunal da Relação de Lisboa, disponível em <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a69513a10885e338802584870053499f?OpenDocument>.

⁹⁵ Idem.

Há necessidade de prova pericial mediante os factos articulados pelas partes, sempre que para que sejam devidamente apreciados, se torne necessário um conhecimento técnico, conhecimentos de peritos, como é o caso de conhecimentos de engenheiros, médicos, etc.

“O âmbito e objeto da perícia configuram realidades conceptuais distintas: o âmbito deste meio de prova define-se pela matéria de facto articulada pelas partes e enunciada nos temas da prova; o objeto da perícia, por sua vez, é determinado pelas concretas questões de facto que a parte requerente da perícia pretende ver esclarecidas”⁹⁶.

A prova pericial pode ser requerida por qualquer uma das partes, devendo, nesse caso, ser deferida ou indeferida pelo juiz, mediante se relacione ou não com os factos invocados na peça processual – “A perícia pode ser requerida por uma ou mais partes, exigindo-se, todavia, sob pena de rejeição, que com o respetivo requerimento seja logo indicado o seu objeto e enunciadas as questões de facto cujo esclarecimento se pretende obter através da referida diligência, que tanto se pode reportar aos factos articulados pelo requerente, como aos alegados pela parte contrária”⁹⁷; ou pode ser ordenada oficiosamente pelo tribunal quando sobre o juiz recaiam dúvidas acerca de determinado facto – “E ainda que nenhuma das partes indique este meio probatório, pode o juiz, por sua exclusiva iniciativa, determinar a sua realização, como se retira directamente dos artigos 467.º, n.º 1 e 477.º, ambos do Código de Processo Civil”⁹⁸.

Também a prova pericial se encontra sujeita ao princípio da livre apreciação da prova, por força do disposto nos arts. 389º e 396º do CC: na verdade, a “prova pericial encontra-se sujeita ao princípio da livre apreciação da prova, o qual impõe ao julgador que decida os factos em julgamento segundo a sua íntima convicção, formada a partir do exame e avaliação da prova trazida ao processo e de acordo com a sua experiência de vida e do conhecimento das pessoas, utilizando, nessa avaliação, critérios objetivos, genericamente suscetíveis de motivação e controlo”, sendo que “os factos puramente descritivos que constam do relatório pericial, isto é, que não envolvam conhecimentos especializados para a sua perceção (compreensão) e/ou apreciação (valorização), não gozam de qualquer força probatória especial em relação à dos restantes meios de prova. Já os factos cuja perceção (compreensão) e/ou apreciação (valorização) reclame conhecimentos técnicos, científicos ou artísticos

⁹⁶ Idem.

⁹⁷ Acórdão do Tribunal da Relação do Porto, disponível em <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/fd9e948aaafe6a208025878f00596055>.

⁹⁸ Idem.

especializados, não acessíveis ao julgador médio, apenas podem ser infirmados ou rebatidos com fundamentos da mesma natureza aos utilizados pelos peritos”⁹⁹.”

1.1.5. Prova por inspeção judicial

Há certas situações em juízo que fazem com que o juiz tenha de aprofundar ou proceder oficiosamente à recolha de provas, pois as provas que foram carreadas para os autos não se demonstram suficientes para que o juiz possa decidir com base na solução mais adequada ao caso. É o que nos indica o art. 490º do CPC: “1 - O tribunal, sempre que o julgue conveniente, pode, por sua iniciativa ou a requerimento das partes, e com ressalva da intimidade da vida privada e familiar e da dignidade humana, inspecionar coisas ou pessoas, a fim de se esclarecer sobre qualquer facto que interesse à decisão da causa, podendo deslocar-se ao local da questão ou mandar proceder à reconstituição dos factos, quando a entender necessária”.

Nos termos do art. 390º do CC, “a prova por inspeção tem por fim a percepção direta de factos pelo tribunal”, e o art. 391º do CC indica que “o resultado da inspeção é livremente apreciado pelo tribunal”.

Luís Filipe Pires de Sousa¹⁰⁰ afirma que “a inspecção consiste na atividade (do juiz, acompanhado das partes) de percepção sensorial do estado ou condição de coisas ou pessoas que, por razões objetivas e intrínsecas à sua natureza, não podem ser adquiridas para o processo na sua corporeidade física, mas que assumem relevo na formulação de um juízo sobre a prova dos factos controversos no processo. Através da inspeção, permite-se ao juiz (co)fundamentar a decisão de facto numa observação direta das coisas ou pessoas, evitando-se os riscos inerentes à fundamentação da decisão num conhecimento indireto, veiculado por outras provas”.

Podemos afirmar que este tipo de prova é “um poder-dever, que só poderá deixar de ser exercido no caso da diligência requerida se mostrar de todo desnecessária ou inútil para a descoberta da verdade, o que deverá constar de despacho fundamentado e susceptível de recurso, sob pena de o direito à prova por inspecção, reconhecido no art. 390º do Cód. Civil, ficar na dependência da livre vontade do juiz”¹⁰¹.

⁹⁹ Acórdão do Tribunal da Relação do Porto, disponível em

<http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/c3017656e7d1723f802589d600323f16?OpenDocument>.

¹⁰⁰ SOUSA, Luís Filipe de, *Direito Probatório Material*, Coimbra, 2020, pág. 196.

¹⁰¹ Acórdão do Tribunal da Relação do Porto, de 26/11/2013, disponível em www.dgsi.pt.

Para que se ordene a realização de prova por inspeção judicial, essa produção de prova tem de ser útil para a decisão da causa e só deve ser indeferida quando se mostre desnecessária ou inútil, o que deverá constar de despacho fundamentado.

A prova por inspeção judicial permite ao juiz uma maior segurança na formação da sua convicção, que lhe servirá de base para a sentença, além de que permite perceber melhor o objeto do litígio, por se tratar de uma observação efetuada pelo próprio juiz em relação aos fatos, coisas e pessoas envolvidas no litígio e a inspeção judicial contribui de maneira diferenciada para a fase instrutória.

1.1.6. Prova testemunhal

Antunes Varela indica que “a prova testemunhal é considerada, sob vários aspectos, a prova mais importante de entre aquelas que são admitidas por lei”¹⁰².

A prova testemunhal baseia-se na testemunha, isto é, aquela pessoa que, não é parte na ação, mas é chamada a narrar aquilo que viu, ouviu e observou em relação aos factos chamados a juízo. Por isso, nos termos do art. 496º do CPC, se dispõe que “estão impedidos de depor como testemunhas os que na causa possam depor como partes”.

Nos termos do art. 495º, nº 1 do CPC, “têm capacidade para depor como testemunhas todos aqueles que tiverem aptidão mental para depor sobre os factos que constituam objeto da prova”. Para tanto, é ao juiz que incumbe a função de verificar a capacidade das pessoas arroladas como testemunhas para testemunhar, com vista a avaliar se o seu depoimento é admissível, credível, e, tanto quanto possível fiel à verdade.

A prova testemunhal, apesar de falível e precária, é aquela que, na prática, assume a maior importância, por ser a única a que pode recorrer-se na demonstração da realidade de muitos factos. É importante o «prudente senso crítico» - que o Tribunal, não podendo prescindir de tal meio de prova -, deve ter no interrogatório e na ponderação do depoimento testemunhal, lembrando o vetusto brocardo do Digesto «testium fides diligenter examinanda».”¹⁰³.

Contudo, não podemos olvidar que a prova testemunhal, na prática, será a mais difícil de valorar pelo juiz, no sentido em que é necessário uma grande experiência para perceber quem está a relatar os factos de acordo com a verdade - “a actividade judicatória na valoração dos depoimentos há-de atender a uma multiplicidade de factores, que têm a ver com as garantias de imparcialidade, as razões

¹⁰² Varela, Antunes, Manual de Processo Civil, 2ª edição, Coimbra: Coimbra Editora, 2006.

¹⁰³ Acórdão do tribunal da Relação de Coimbra, disponível em

<http://www.dgsi.pt/itrc.nsf/c3fb530030ea1c61802568d9005cd5bb/d6b3d4a8a8754c69802584c400413edb?OpenDocument>

de ciência, a espontaneidade dos depoimentos, a verosimilhança, a seriedade, o raciocínio, as lacunas, as hesitações, a linguagem, o tom de voz, o comportamento, os tempos de resposta, as coincidências, as contradições, o acessório, as circunstâncias, o tempo decorrido, o contexto sócio-cultural, a linguagem gestual (como por exemplo os olhares) e até saber interpretar as pausas e os silêncios dos depoentes, para poder perceber e aquilatar quem estará a falar a linguagem da verdade e até que ponto é que, consciente ou inconscientemente, poderá a verdade estar a ser distorcida, ainda que, muitas vezes, não intencionalmente”¹⁰⁴.

“A prova testemunhal não é, pois, para ser avaliada aritmeticamente. Ou como se o depoimento de uma testemunha fosse para ser considerada com o rigor de uma escritura de um notário”¹⁰⁵.

Também esta prova está sujeita a regras, previstas no CPC. Desde logo, não se podem oferecer testemunhas a juízo, sem mais. É necessário respeitar os limites das testemunhas: o autor, na petição inicial, pode oferecer até dez testemunhas, por seu turno, o réu, na contestação pode oferecer também um limite de dez testemunhas – art. 511º, nº 1 do CPC. Porém, nas ações de valor não superior à alçada do tribunal de primeira instância, o limite do número de testemunhas é metade, assim, cinco testemunhas – art. 511º, nº 1 in fine do CPC. Dispõe o nº 2 do art. 511º do CPC que “no caso de reconvenção, cada uma das partes pode oferecer também até 10 testemunhas, para prova dela e da respetiva defesa”. E o que acontece se as partes oferecerem mais testemunhas do que o previsto na lei? Para além de o juiz poder admitir a inquirição de mais testemunhas para além do limite – art. 511º, nº 4 do CPC, o rol de testemunhas que ultrapasse o limite previsto na lei, considera-se como não escrito – art. 511º, nº 3 do CPC.

Relativamente à ordem dos depoimentos, atentemos o art. 512º que nos indica que antes de se proceder à inquirição, recolhem-se as testemunhas a uma sala e são chamadas a depor pela ordem que estiverem mencionadas no rol de testemunhas. Isto é, primeiro são chamadas a depor as testemunhas do autor e depois as do réu, podendo, no entanto, o juiz determinar, ou as partes concordarem, na alteração da ordem de inquirição. Nos termos do art. 516º, nº 2 do CPC, “o interrogatório é feito pelo advogado da parte que ofereceu a testemunha, podendo o advogado da outra parte fazer-lhe, quanto aos factos sobre que tiver deposto, as instâncias indispensáveis para se completar ou esclarecer o depoimento”, porém, “sem prejuízo dos esclarecimentos pedidos pelo juiz ou de este poder fazer as perguntas que julgue convenientes para o apuramento da verdade” – art. 516º, nº 4 do CPC.

¹⁰⁴ Acórdão do Tribunal da Relação de Évora, disponível em <http://www.dgsi.pt/jtre.nsf/-/F202172FC5EE3ED18025821E005A046A>.

¹⁰⁵ Idem.

Antes da testemunha começar a ser inquirida em relação aos factos, tem de prestar juramento, sendo advertido das sanções aplicáveis às falsas declarações, nos termos do art. 459º do CPC. Posteriormente, o juiz inquirir a testemunha sobre a sua identidade “e pergunta-lhe se é parente, amigo ou inimigo de qualquer das partes, se está para com elas nalguma relação de dependência e se tem interesse, direto ou indireto, na causa” - art. 513º, nº 1 do CPC.

E agora questionamos: a testemunha pode-se recusar a depor? A resposta a esta questão é afirmativa. Diz-nos o art. 497º do CPC que sempre que haja uma relação de familiaridade entre a testemunha e uma das partes na ação: “Podem recusar-se a depor como testemunhas, salvo nas ações que tenham como objeto verificar o nascimento ou o óbito dos filhos: a) Os ascendentes nas causas dos descendentes e os adotantes nas dos adotados, e vice-versa; b) O sogro ou a sogra nas causas do genro ou da nora, e vice-versa; c) Qualquer dos cônjuges, ou ex-cônjuges, nas causas em que seja parte o outro cônjuge ou ex-cônjuge; d) Quem conviver, ou tiver convivido, em união de facto em condições análogas às dos cônjuges com alguma das partes na causa”.

Neste sentido, o juiz deve advertir as pessoas que se podem recusar a depor como testemunhas – art. 497º, nº 2 do CPC. Também quem estiver obrigado ao segredo profissional, deve recusar-se a depor como testemunha -art. 497º, nº 3 do CPC.

Se, por um lado, a prova testemunhal é uma das melhores provas no nosso sistema jurídico, a verdade é que ela nem sempre é admitida. Desta forma, a prova testemunhal não é admitida nos termos dos arts. 393º e 394º do CC: quando a declaração negocial tiver de ser reduzida a escrito ou tiver de ser, obrigatoriamente, provada por escrito, não se admite a prova testemunhal; o mesmo quando o facto estiver plenamente provado por documento ou outro meio que tenha força probatória plena (ex: documentos autênticos); também não se admite prova testemunhal nos casos em que existam convenções contrárias ou adicionais ao conteúdo de documento autêntico ou documento particular.

A prova testemunhal pode ser posta em causa através de dois incidentes: contradita e acareação.

A contradita encontra-se prevista no art. 521º do CPC e consiste na possibilidade de “a parte contra a qual for produzida a testemunha pode contraditá-la, alegando qualquer circunstância capaz de abalar a credibilidade do depoimento, quer por afetar a razão da ciência invocada pela testemunha, quer por diminuir a fé que ela possa merecer”. Para tanto, a parte contra a qual for produzida a testemunha, deduz contradita quando a testemunha termina o depoimento – art. 522º, nº 1 do CPC, ouvindo-se a testemunha sobre a matéria alegada, sendo que a parte a pode comprovar por documentos ou outras testemunhas, sendo estas apresentadas e inquiridas imediatamente – art. 522º, nºs 2 e 3 do CPC.

Relativamente à acareação, aplica-se o disposto no art. 523º do CPC, que nos indica que “se houver oposição direta, acerca de determinado facto, entre os depoimentos das testemunhas ou entre eles e o depoimento da parte, pode ter lugar, oficiosamente ou a requerimento de qualquer das partes, a acareação das pessoas em contradição”. Nos termos do art. 524º, nº 1, se as pessoas estiverem presentes, a acareação é feita imediatamente.

Podemos, assim, concluir que a prova testemunhal, para ser devidamente valorada, depende de um grau elevado de concentração do juiz, em relação à testemunha, no sentido em que este deve estar atento às suas expressões, contradições, à vontade da testemunha em depor e à forma como expõe os seus argumentos. Deste modo, também aqui se aplica o princípio da livre apreciação da prova, por força do art. 396º do CC que indica que “a força probatória dos depoimentos das testemunhas é apreciada livremente pelo tribunal”.

No campo do processo civil estão previstas situações de recusa no que diz respeito ao dever de cooperação para a descoberta da verdade, nos termos previstos no art. 417º do CPC, designadamente, no seu nº 3, nos termos do qual: “A recusa é, porém, legítima se a obediência importar: a) Violação da integridade física ou moral das pessoas; b) Intromissão na vida privada ou familiar, no domicílio, na correspondência ou nas telecomunicações; c) Violação do sigilo profissional ou de funcionários públicos, ou do segredo de Estado, sem prejuízo do disposto no n.º 4.”¹⁰⁶

1.2. Dever de cooperação

O princípio da cooperação tem consagração expressa no art. 7º do CPC. O princípio da cooperação é consagrado como a pedra angular de todo o direito processual civil. Indica-nos o art. 7º do CPC que: “1 - Na condução e intervenção no processo, devem os magistrados, os mandatários judiciais e as próprias partes cooperar entre si, concorrendo para se obter, com brevidade e eficácia, a justa composição do litígio. 2 - O juiz pode, em qualquer altura do processo, ouvir as partes, seus representantes ou mandatários judiciais, convidando-os a fornecer os esclarecimentos sobre a matéria de facto ou de direito que se afigurem pertinentes e dando-se conhecimento à outra parte dos resultados da diligência. 3 - As pessoas referidas no número anterior são obrigadas a comparecer sempre que para isso forem notificadas e a prestar os esclarecimentos que lhes forem pedidos, sem prejuízo do disposto no n.º 3 do artigo 417.º. 4 - Sempre que alguma das partes alegue justificadamente dificuldade séria em obter documento ou informação que condicione o eficaz exercício

¹⁰⁶ Acórdão do Tribunal da Relação de Lisboa, disponível em

<http://www.dgsi.pt/trl.nsf/33182fc732316039802565fa00497eec/1199fc63e203de4b80258845003b1236?OpenDocument>

de faculdade ou o cumprimento de ónus ou dever processual, deve o juiz, sempre que possível, providenciar pela remoção do obstáculo”.

Este princípio traduz a ideia de uma divisão de trabalhos entre as partes, devendo todos colaborar no processo.

O princípio da cooperação, plasmado no art. 7º do CPC, prevê que as partes, devem cooperar o mais possível com o Tribunal, e vice-versa, no sentido de haver entre eles uma interação, sendo que o objetivo final é comum a todos eles, que será o de obter, com brevidade e eficácia, a justa composição do litígio.

Este princípio está intimamente ligado ao dever de gestão processual do art. 6º do CPC, “na medida em que, ao exercer os deveres de cooperação, o magistrado está, no fundo, a gerir o processo, eliminando os formalismos desnecessários, facilitando e estimulando o envolvimento das partes no procedimento, e esclarecendo dúvidas quanto às questões suscitadas, por forma a garantir a justa composição do litígio, em tempo breve e de modo eficaz”¹⁰⁷.

Nestes termos, todas as pessoas, sejam ou não partes na causa, trabalham em prol do mesmo objetivo e têm o dever de prestar a sua colaboração para a descoberta da verdade, praticando os atos que forem determinados e a omissão desse dever permite que a parte seja sancionada com o pagamento de uma multa.

Este princípio visa permitir à parte onerada com a prova de um facto a obtenção de esclarecimentos da parte contrária, em matéria do conhecimento desta, com vista a dar cumprimento ao ónus da prova que sobre a primeira incide.

O dever de cooperação encontra-se associado ao princípio da boa-fé e determina que as partes adotem uma conduta colaborante com o Tribunal no sentido da descoberta da verdade.

Miguel Teixeira de Sousa¹⁰⁸ assinala que, do ponto de vista do tribunal, o princípio da cooperação impõe quatro poderes-deveres ou deveres funcionais: de esclarecimento [artigo 7º, n.º 2, do CPC]; de prevenção [artigos 590º, n.º 2, alínea b) e artigo 591º, n.º 1, alínea c)]; de consulta [artigo 3º, n.º 3, do CPC]; e de auxílio das partes [artigo 7º, n.º 4, artigo 418º, n.º 1, e artigo 754º, n.º 1, alínea a), do CPC].

Como já vimos, “o princípio da cooperação impõe às partes e ao juiz uma atuação comprometida com a verdade com vista a obter-se com brevidade e eficácia a justa composição do litígio. Às partes compete prestar todos os esclarecimentos sobre a matéria de facto ou de direito que se afigurem

¹⁰⁷ Acórdão do Supremo Tribunal de Justiça, disponível em

<http://www.dgsi.pt/jsti.nsf/954f0ce6ad9dd8b980256b5f003fa814/e623a78cb415ef9c802582960031305e>.

¹⁰⁸ Miguel Teixeira de Sousa in “Introdução ao Processo Civil”, 2000, páginas 56/57.

pertinentes, devendo comparecer em juízo sempre que para isso sejam notificadas e a prestar os esclarecimentos que lhes forem pedidos”¹⁰⁹.

Para além deste princípio estar intimamente ligado ao princípio da gestão processual, previsto no art. 6º do CPC, encontra-se também ligado ao dever de boa-fé processual, previsto no art. 8º do CPC. “A boa-fé impõe uma norma de conduta das partes pautada pelos deveres de esclarecimento e lealdade. (...) O dever de boa-fé busca um interesse que excede o das partes, como seja o interesse público do Estado na prestação da tutela jurisdicional”¹¹⁰.

As partes que não cumpram o preceituado pelo art. 7º do CPC, em relação ao princípio da cooperação, encontram-se sujeitas a uma sanção, principalmente por este princípio estar relacionado com o princípio da boa-fé processual. Como nos ensina CARLOS DE OLIVEIRA REGO: as consequências jurídicas para o descumprimento deste dever de cooperação para a busca da verdade - que por força do art. 7º, nº 3 também são aplicáveis ao descumprimento do dever de esclarecimento (art. 7º, nº 2) - encontram-se elencadas no enunciado nº 2 do referido art. 417º. E são elas: a condenação ao pagamento de multa; a coerção do sujeito à realização da diligência; ou, em caso de recusa ilegítima no cumprimento da diligência que resulte na impossibilidade de produção de prova do fato - por se tratar de meio essencial para a mesma -, a inversão do ónus probatório; ou ainda, por último, a livre apreciação do valor probatório da recusa, quando essa não implicar a impossibilidade de prova do fato - por não se tratar de meio absoluto para tanto¹¹¹.

Por sua vez, o art. 417º do CPC prevê o dever de cooperação para a descoberta da verdade, tratando-se este de uma concretização do dever geral de cooperação, regulado pelo art. 7º do CPC. Nos termos do nº 1 do art. 417º do CPC, “todas as pessoas, sejam ou não partes na causa, têm o dever de prestar a sua colaboração para a descoberta da verdade, respondendo ao que lhes for perguntado, submetendo-se às inspeções necessárias, facultando o que for requisitado e praticando os atos que forem determinados”.

Assim, as partes devem cooperar entre si, esclarecendo todos os factos que forem solicitados, carreando para os autos as provas necessárias à boa decisão da causa, tudo em prol de uma célere e justa decisão do litígio, sob pena de aplicação de uma consequência jurídica.

¹⁰⁹ Acórdão do Supremo Tribunal de Justiça, disponível em

<http://www.dgsi.pt/jsti.nsf/954f0ce6ad9dd8b980256b5f003fa814/42aa9360a9d93bf98025847200319242?OpenDocument>.

¹¹⁰ Idem.

¹¹¹ REGO, Carlos Francisco de Oliveira do. Comentários ao código de processo civil. 2004, p. 453-455

1.3. Princípio do inquisitório

O princípio do inquisitório encontra a sua razão de ser no art. 411º do CPC. Nos termos deste princípio, “incumbe ao juiz realizar ou ordenar, mesmo oficiosamente, todas as diligências necessárias ao apuramento da verdade e à justa composição do litígio, quanto aos factos de que lhe é lícito conhecer”. Isto é, em relação aos factos instrumentais, ainda que não alegados pelas partes, nos termos do n.º 2, al a), do art. 5º, do CPC, e os factos essenciais que sejam complemento ou concretização de outros que as partes hajam alegado – art. 5º, n.º 2, al. b).

Por decorrência deste princípio, consagrado na lei processual civil, o juiz tem a iniciativa da prova, podendo realizar e ordenar oficiosamente todas as diligências necessárias para o apuramento da verdade. Trata-se de um dever de boa gestão processual, através do qual o juiz participa ativamente no processo.

Ao juiz é lícito ordenar a produção de prova, ainda que seja da competência das partes o ónus probatório, mas o juiz pode ordenar oficiosamente diversas diligências de instrução. É o caso da utilização de dados confidenciais (artigo 418º, n.º 1 do Código Civil); da requisição de documentos (artigo 436º n.º 1 do Código Civil); de determinar o depoimento de parte (artigo 452º n.º 1 do Código Civil); de ordenar a realização de prova pericial (artigo 477º e 487º, n.º 2 ambos dos Código Civil); de realizar inspeção judicial (artigo 490º, n.º 1 do Código Civil); de inquirir testemunhas no local da questão (artigo 501º do Código Civil); de ordenar a notificação e inquirir pessoa não oferecida como testemunha (artigo 526º n.º 1 do Código Civil); de ouvir as pessoas que entender e ordenar as diligências para o seu esclarecimento; de ordenar a verificações judiciais não qualificadas (artigo 494º do Código Civil); de ouvir o técnico designado em qualquer momento, antes das alegações orais (artigo 604º, n.º 7 do Código Civil), embora alguns destes atos se enquadrem no âmbito da gestão processual que incumbe ao juiz¹¹².

Através deste princípio, o juiz tem um papel ativo no processo. Afirmo mesmo BARBOSA MOREIRA que o juiz não se pode reduzir a um “convidado de pedra”¹¹³. Já ALBERTO DOS REIS, por sua vez, afirma que “o direito processual civil moderno substituiu ao tipo de juiz inerte o tipo de juiz ativo, concedeu ao órgão jurisdicional poderes de iniciativa em matéria de instrução do processo, poderes que têm sido sucessivamente alargados”¹¹⁴.

¹¹² Almeida, Francisco Manuel Lucas Ferreira de, *Direito Processual Civil*, Vol. I Coimbra, Edições Almedina, 2ª Edição, 2018, págs. 85 a 90

¹¹³ MOREIRA, José Carlos Barbosa, — *Processo Civil Contemporâneo - Um enfoque comparativo* in *Scientia Iuridica*, Revista de Direito Comparado Português e Brasileiro, Tomo LV, n.º 305, 2006, pág. 644.

¹¹⁴ REIS, José Alberto dos, *Código de Processo Civil Anotado*, vol. III, 3ª ed., Coimbra Editora, Coimbra, 2012, pág. 272.

Porém, “a amplitude de poderes/deveres decorrentes do princípio do inquisitório não significa que o juiz tenha a exclusiva responsabilidade pelo desfecho da causa, pois que, associada a ela está a responsabilidade das partes, sobre as quais a lei faz recair ónus, inclusive no domínio probatório, que se repercutem em vantagens ou desvantagens para as mesmas e que, por isso, aquelas têm interesse directo em cumprir”¹¹⁵. Contudo, este princípio plasmado no art. 411º do CPC, tem necessariamente de ser conjugado com outros princípios, podendo mesmo afirmar-se que “o princípio do inquisitório tem necessariamente de ser conjugado com outros ditames, designadamente com o da autorresponsabilidade das partes. Se a parte podia ter requerido, com toda a largueza e possibilidade, certa diligência probatória e não o fez, sibi imputet”¹¹⁶, pois que se a própria parte podia ter requerido aquele meio de prova, tendo decidido não o fazer, não incumbe ao juiz a responsabilidade do desfecho da causa, pois o ónus recai sobre as partes e não sobre o juiz. “A intervenção do juiz, em última instância, substituindo-se a ela, vai, em tese geral, acabar por violar o princípio da igualdade das partes no processo, pois estaria a permitir a prática de um acto já precludido e a esvaziar a aludida autorresponsabilidade de uma das partes, eventualmente favorecendo-a”¹¹⁷.

Assim, e ressalve-se, ainda que o juiz possa oficiosamente proceder à descoberta da verdade material, “a investigação oficiosa não deve ser exercida com a finalidade da parte poder contornar a preclusão processual decorrente da sua inércia, uma vez que o exercício dos poderes de investigação oficiosa do tribunal pressupõe que as partes cumpriram minimamente o ónus que sobre elas prioritariamente recai de indicarem tempestivamente as provas de que pretendem socorrer-se para demonstrarem os factos cujo ónus probatório lhes assiste”¹¹⁸. Se assim fosse, não havia necessidade de as partes carregarem prova para os autos e, nesse sentido, estariam de tal maneira “acomodadas” e a aguardar que o juiz, oficiosamente, procedesse à descoberta da verdade material e ordenasse a produção de prova.

Senão vejamos: “se o juiz tiver considerado pertinente e fundado para a realização da prova dos aludidos factos que lhe é lícito conhecer, nada obsta a que determine a produção de qualquer prova, pondo-se, assim, em evidência, o princípio geral da descoberta da verdade material, que sobressai do disposto nos citados artigo 411 e 436, do CPC, que, como se disse, permite ao Juiz realizar ou ordenar, mesmo oficiosamente, todas as diligências necessárias ao apuramento da verdade e à justa

¹¹⁵ Acórdão do Tribunal da Relação de Guimarães, disponível em <https://jurisprudencia.pt/acordao/197064/>.

¹¹⁶ Acórdão do Tribunal da Relação de Coimbra, disponível em <http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/dc64ca47f38eab8e8025885a004b59c9?OpenDocument>.

¹¹⁷ Idem.

¹¹⁸ Acórdão do Tribunal da Relação de Guimarães, de 19 de Novembro de 2020, disponível em <https://jurisprudencia.pt/acordao/197064/>.

composição do litígio, quanto aos factos de que lhe é lícito conhecer. Ora, parece-nos de todo evidente que os poderes que princípio do inquisitório, consagrado no art. 411 do CPC, confere ao juiz são para serem usados de forma direta pelo juiz, e não para suprir falhas das partes”¹¹⁹.

No fundo, nem faria sentido que se admitissem diligências probatórias que já não pudessem ser requeridas. Do mesmo modo, o princípio do inquisitório não visa que o juiz auxilie uma das partes, em prejuízo da outra, de tal modo que lhe permitisse introduzir quaisquer meios probatórios quando já não o podia fazer, ainda mais por não o ter feito dentro do prazo concedido por lei. De todo o modo, “não pode o juiz ao abrigo do inquisitório e da cooperação suprir o incumprimento de formalidades essenciais pelas partes, permitir o atropelo de normas legais e nem pode, obviamente, determinar oficiosamente a junção de documentos cuja junção já foi indeferida”¹²⁰.

É à luz do princípio do inquisitório, em conjunto com o princípio da oficialidade, que melhor se compreende o disposto no artigo 6.º, do CPC, no qual se consagra “um Dever de Gestão Processual, aí se prescrevendo, designadamente, que cumpre ao juiz, sem prejuízo do ónus de impulso especialmente imposto pela lei às partes, dirigir ativamente o processo e providenciar pelo seu andamento célere, promovendo oficiosamente as diligências necessárias ao normal prosseguimento da ação, recusando o que for impertinente ou meramente dilatório e, ouvidas as partes, adotando mecanismos de simplificação e agilização processual que garantam a justa composição do litígio em prazo razoável”¹²¹.

O princípio do inquisitório estabelece um “poder-dever” do juiz, que não se limita à prova de iniciativa oficiosa, incumbindo-lhe também realizar ou ordenar oficiosamente as diligências relativas aos meios de prova propostos pelas partes, na medida em que julgue que aquelas são necessárias ao apuramento da verdade e à justa composição do litígio relativamente a factos que o Tribunal pode (e deve) conhecer. Todavia, “o princípio do inquisitório deve ser interpretado como um poder-dever limitado, restringindo-se, em matéria probatória, na busca pelas provas dentro dos factos alegados pelas partes (factos essenciais), com vista à justa composição do litígio e ao apuramento da verdade”¹²².

Diz-nos Lopes do Rego que “o exercício dos poderes de investigação oficiosa do tribunal pressupõe que as partes cumpriram minimamente o ónus que sobre elas prioritariamente recai de indicarem tempestivamente as provas de que pretendem socorrer-se para demonstrarem os factos cujo ónus

¹¹⁹ Idem.

¹²⁰ Idem.

¹²¹ Idem.

¹²² Idem.

probatório lhes assiste - não podendo naturalmente configurar-se como uma forma de suprimento oficioso de comportamentos grosseira ou indesculpavelmente negligentes das partes. A inquirição por iniciativa do tribunal constitui um poder-dever complementar de investigação oficiosa dos factos, que pressupõe, no mínimo, que foram indicadas provas cuja produção implica a realização de uma audiência (...)"¹²³. No mesmo sentido, Nuno Lemos Jorge defende que se o juiz ordenar produção de prova que não seja justificada pelos elementos dos autos "a promoção de qualquer outra diligência resultará, apenas, da vontade da parte nesse sentido, a qual, não se tendo traduzido pela forma e no momento processualmente adequados, não deverá agora ser substituída pela vontade do juiz, como se de um seu sucedâneo se tratasse"¹²⁴.

Não se trata de uma obrigação do juiz ordenar uma produção de prova testemunhal, que a parte não indicou, mas posteriormente vem indicar que essa testemunha é importante para a descoberta da verdade material. Se assim fosse, "perdia sentido a obrigação de apresentação da prova em momentos processuais determinados, pois restaria sempre à parte a possibilidade de invocar esta norma do art. 526º, do C.P.C."¹²⁵

Em suma, o princípio do inquisitório não invalida nem descaracteriza o princípio do impulso processual das partes, sendo a elas que lhes cabe carrear para os autos as provas. Na mesma senda, este princípio não pode sobrepor-se aos outros princípios, nomeadamente ao princípio do dispositivo (que, na realidade, se contradiz com o princípio do inquisitório) e da autorresponsabilidade das partes, pois que estas estão obrigadas a cumprir os prazos legais, praticando os atos que entenderem por convenientes, tempestivamente, para a descoberta da verdade material e boa decisão da causa. Assim, pode o juiz fazer uso de outros meios probatórios não indicados pelas partes, sem nunca se substituir a elas, nem isentando as partes do ónus de prova que sobre elas recai.

1.4. Possibilidade de impugnação

Nos termos do art. 444º do CPC, pode-se impugnar a genuinidade de documentos: "1 - A impugnação da letra ou assinatura do documento particular ou da exatidão da reprodução mecânica (...) 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".

¹²³ Lopes do Rego, Carlos. *Comentários ao Código de Processo Civil*. Coimbra: Almedina, 1999, pág. 425.

¹²⁴ Idem.

¹²⁵ Acórdão do Tribunal da Relação de Guimarães, de 4/03/2013, Proc. 293/12.0TBVCT-J.G.I., disponível em www.dgsi.pt.

O art. 446º, nº 1 do CPC, indica que se pode ilidir a autenticidade ou força provatória de documentos: “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”.

Os documentos particulares que tenham sido impugnados deixam de fazer prova plena.

Estando em causa documentos particulares, o artº 374º, nº 1 do CC diz que “a letra e a assinatura, ou só a assinatura, de um documento particular consideram-se verdadeiras, quando reconhecidas ou não impugnadas pela parte contra quem o documento é apresentado, ou quando este declare não saber se lhe pertencem, apesar de lhe serem atribuídas, ou quando seja havidas legal ou judicialmente como verdadeiras”. A parte contra a qual o documento particular é apresentado pode impugnar a veracidade da letra ou da assinatura¹²⁶ ou declarar que não sabe se aquelas são verdadeiras, caso em que cabe à parte que ofereceu essa prova, fazer prova da veracidade da subscrição pela pessoa a cuja autoria é atribuído.

A impugnação da genuinidade do documento não carece de qualquer decisão judicial que seja subsequente a essa impugnação. Basta que a parte impugne a genuinidade do documento e não seja demonstrado pela parte que apresentou o documento, a sua veracidade. Esse documento passa a constituir apenas um meio de prova livremente apreciado pelo julgador, ficando arredada a sua força probatória plena.

Isto em relação à prova documental.

Admite-se também a impugnação da admissão de testemunhas, nos termos do art. 514º e 515º do CPC. O art. 514º do CPC indica que “a parte contra a qual for produzida a testemunha pode impugnar a sua admissão com os mesmos fundamentos por que o juiz deve obstar ao depoimento”.

A impugnação da admissão da testemunha só pode ser suscitada com base em fundamentos típicos, tais como não ter a testemunha capacidade para depor ou não ser a pessoa que foi indicada pela parte como testemunha. A admissão do incidente de impugnação de testemunha carece de decisão do juiz.

Seguindo à letra o disposto no art. 515º, nº 1 do CPC, havendo um dos indicados fundamentos para impugnação da testemunha, o incidente deve ser deduzido quando terminar o interrogatório preliminar.

A parte que suscita o incidente deve alegar os factos que integram o fundamento de inabilidade da

¹²⁶ No documento eletrónico com assinatura digital não é possível o incidente de falsidade. Cfr. artigo 3º nº 2 do DL 12/2021. A impugnação já seria possível se fosse utilizada a assinatura dinâmica. Cfr. Andrade, Francisco, “Consideração Jurídica das Assinaturas Dinâmicas no Ordenamento Jurídico Português” in *in Memórias do XVI Congresso Ibero Americano de Derecho e Informática*, Quito, 2012.

testemunha, caso esta os tenha omitido no interrogatório preliminar e se a testemunha os tiver mencionado e o juiz não tiver obstado ao seu depoimento, deve também a parte suscitar o incidente, após o qual o juiz ouve a parte que indicou a testemunha sobre os fundamentos invocados no incidente de impugnação, por força do princípio do contraditório, decidindo se admite ou rejeita o incidente.

“Admitido o incidente, o juiz deve convidar a testemunha a pronunciar-se sobre os fundamentos da impugnação. Se a testemunha os confirmar, sem impugnação pela parte que a arrolou, não deve ser admitido o depoimento; não sendo confirmados, inicia-se então uma fase de produção de prova com proposição de prova documental ou testemunhal pela parte que suscitou o incidente; inquirição das testemunhas (com o limite de três); decisão final sobre o incidente registada em acta – cf. art.ºs 515º e 153º do CPC”¹²⁷.

Como referem J. Lebre de Freitas e Isabel Alexandre¹²⁸ “os prazos que têm de mediar entre o oferecimento da testemunha e a sua inquirição (cf., designadamente, os arts. 598-2 e 510-1) visam assegurar à parte contrária tempo suficiente para indagar da admissibilidade – e também da credibilidade – da testemunha, pelo que é seu ónus de estar preparada, no momento da inquirição e antes de iniciado o depoimento, para impugnar a admissibilidade deste, oferecendo e produzindo as respectivas provas”.

1.5. Valor probatório

Entende-se por valor probatório a capacidade de um meio de prova demonstrar os factos.

O meio probatório pode ter um carácter abstrato e um carácter concreto. Desde logo, terá um carácter abstrato nos casos em que a lei não consegue fixar um valor ao meio probatório e este fica a cargo da livre apreciação da prova pelo juiz, como é o caso da prova testemunhal. Já o carácter concreto do meio de prova depende do contexto dos factos e do meio probatório, isto é, verifica-se o carácter concreto nos casos em que a lei estabelece o valor probatório daquele meio de prova, como acontece no caso da prova documental.

Daqui infere-se que o valor probatório se refere ao grau de certeza com que as provas demonstram a realidade dos factos, porquanto, quanto maior for o grau de certeza, maior será o valor probatório.

Entre nós, a regra é a livre apreciação da prova pelo tribunal, o que significa que o juiz deverá julgar a matéria de facto segundo a sua prudente convicção acerca de cada facto, conforme determina o artigo

¹²⁷Acórdão do Tribunal da Relação de Lisboa, disponível em

<http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/b47b9298b6d998b78025878b0033625b?OpenDocument>.

¹²⁸FREITAS, José Lebre de e ALEXANDRE, Isabel, Código de Processo Civil Anotado, 2º Vol., 3ª edição, pág. 392.

607º, nº 5 do CPC. Neste âmbito, desempenharão papel de relevo as máximas da experiência, “enquanto critérios de referência que orientam o juiz no desenvolvimento do raciocínio decisório”¹²⁹.

No sistema jurídico português há três tipos de valor probatório: prova bastante, prova plena e prova pleníssima.

A prova bastante é a de valor menor e é suficiente para fundamentar a convicção do juiz, mas que cede perante a contraprova – art. 346º do CC. Consiste na atividade da parte contrária em criar no julgador uma dúvida e incerteza acerca de um facto que foi objeto de prova.

A prova plena é apenas abalada pela prova em contrário. Nestes termos, para que o juiz não se baseie naquela prova para proferir decisão, basta que se invoque e prove que aquela prova não corresponde à verdade – art. 347º do CC. Para além de se criar a dúvida no Juiz é necessário provar que aquela prova é falsa, demonstrando outra prova. Para tanto só se admite em relação a presunções iuris tanto, ilidíveis, como sejam os documentos autênticos que fazem prova plena, porém são abaláveis com base na sua falsidade.

Por sua vez, a prova pleníssima é aquela que tem maior valor probatório. Este tipo de prova nem sequer admite prova em contrário, por se tratar de provas iure et de iure, por força do art. 350º, nº 2 in fine. Na prova pleníssima, o valor legal da prova é insuscetível de ser destruído, o que significa que a lei não permite que se produza qualquer prova em sentido contrário ao facto que resulta pleníssima provado do documento.

Conforme escreve Lebre de Freitas¹³⁰ “uma vez verificado o facto que serve de base à presunção (no sentido lato em que a entendemos), não é admissível a prova de que o facto presumido não se verificou (art. 350º-2 in fine). Prova pleníssima e presunção (naquele sentido lato) são conceitos sinónimos” e aponta como exemplos de presunções legais que gozam de prova pleníssima os arts. 243º, nº 3, 579º, nº 2 e 2198º, nº 2 do CC.

Já na “prova plena”, que constitui a regra no âmbito das presunções legais, é admissível a demonstração, através de outros meios de prova, de que o facto presumido pela lei não ocorreu, ainda que, em determinados casos, essa prova contrária apenas seja admissível quando se verificarem determinados requisitos legais (art. 350º, nº 2, 347º, nº 2, 372º, 376º, nº 1 e 393º, nº 2 do CC) constitutivos duma prova plena qualificada e se restrinja essa prova contrária a determinados meios de prova ou se admita estas apenas verificadas que sejam determinadas premissas. “Prova plena e

¹²⁹ PIMENTA, Paulo, *Processo Civil Declarativo*, 2.ª ed. Coimbra, Almedina, 2018, pág. 376.

¹³⁰ FREITAS, Lebre de; *A Ação Declarativa à Luz do Código de Processo Civil de 2013*, 3ª ed., Coimbra Editora, págs. 212 a 213. FREITAS, José Lebre de. *Introdução ao processo civil, conceitos e princípios gerais à luz do novo código*. 4ª Edição. Coimbra: Gestegal, 2017. FREITAS, José Lebre de. *A Falsidade no Direito Probatório*. Almedina, 2013.

presunção (em sentido lato) ilidível (art. 350º, n.º 2 do CC, 1ª parte) são conceitos sinónimos, sendo a essa presunção que se refere o art. 344º, n.º 1 ao estabelecer a inversão do ónus da prova”¹³¹.

Finalmente, “a prova bastante cede perante a simples dúvida que o julgador, confrontado com outros elementos de prova, tenha sobre a realidade do facto por ela em princípio provado (art. 346º do CC). Trata-se de presunção legal que não inverte o ónus da prova”, como acontece nos casos a que se reportam os arts. 1816º, n.º 3 e 1871º, n.º 2 do CC¹³².

Assim, nos casos em que estamos perante o carácter abstrato do meio de prova, maior é o livre arbítrio do juiz, que apreciará a prova de acordo com a sua convicção e regras de experiência, fixando a prova como bastante, plena ou pleníssima, de acordo com aquilo que entender ser aplicável à prova em concreto. Quanto mais concreto for o meio de prova, menor aplicabilidade terá o princípio da livre apreciação da prova.

CLÁUDIA TRINDADE afirma que para aumentar o grau de certeza da conclusão em relação à prova, é necessário conciliar a verificação do valor probatório, atribuído ao meio de prova livremente apreciado pelo juiz, com a ponderação quantitativa dos meios probatórios e recorrer às máximas de experiência¹³³.

Em relação aos tipos de prova, por exemplo um documento particular faz prova plena nos termos do art. 376º do CC, sem prejuízo de ser arguida e provada a nulidade desse documento. Porém, se se provar a força plena desse documento, já não se admite a prova testemunhal e, em consequência, também não se admite a prova por presunção judicial – art. 351º do CC.

Manuel de Andrade¹³⁴ escreve que “o documento constitui prova plena, só ilidível mediante arguição e prova de falsidade (prova do contrário) – quanto à veracidade das atestações do funcionário documentador (nos limites da sua competência), até onde versem sobre atos praticados por ele próprio, ou praticados na sua presença (declarações emitidas, entregas de dinheiro, etc.) – isto é, sobre ações ou percepções suas (quórum notitiam et scientiam habet propriis sensibus, visus et auditus). Os factos e declarações que o funcionário atesta como praticados, emitidas ou prestadas perante ele terão o valor jurídico que lhes competir, podendo ser impugnados pelos interessados, nos termos gerais de direito (erro na declaração ou erro-vício, coação, simulação, etc.) não importando isso arguição de falsidade. O documento faz assim prova plena quanto à materialização (prática, efetivação)

¹³¹ Idem, pág. 213.

¹³² Idem.

¹³³ TRINDADE, Cláudia, Prova, justificação e convicção racional – A propósito do conceito de verdade proposicional no processo decisório jurisprudencial, em Estudos em Homenagem ao Professor Doutor Alberto Xavier, Assuntos Europeus, Direito Privado, Direito Público e Vária, Vol III, Edições Almedina: Coimbra, 2013, pág. 184 e 185.

¹³⁴ ANDRADE, Manuel de; Noções elementares de processo civil, Coimbra Editora, 1979, págs. 226 e 227.

de tais atos e declarações; mas não quanto à sua sinceridade, à sua veracidade ou à falta de qualquer outro vício ou anomalia”.

Por sua vez, a prova por declarações de parte “deve merecer a mesma credibilidade das demais provas legalmente admissíveis e deverá ser valorada conforme se estabelece no art.º 466.º, n.º 3 do Código do Processo Civil, isto é, deverá ser apreciada livremente pelo tribunal. A credibilidade das declarações da parte tem de ser apreciada em concreto, numa perspectiva crítica, com vista à descoberta da verdade material, bem podendo suceder que as respectivas declarações, em concreto, possam merecer muita, pouca ou, mesmo, nenhuma credibilidade. Significa que a prova por declarações de parte é apreciada livremente pelo tribunal, na parte que não constitua confissão, sendo, porém, normalmente insuficiente para valer como prova de factos favoráveis à procedência da acção, desacompanhada de qualquer outra prova que a sustente, ou, sequer, indicie. (...) Logo, essas declarações, como princípio, não podem ser consideradas sem o auxílio de outros meios probatórios, sejam eles documentais ou testemunhais, já que se trata da versão da parte interessada - quem as produz tem um manifesto interesse na acção, sendo por isso de considerar, em regra, de irrazoável e insensato, que sem o auxílio de quaisquer outros meios probatórios, o Tribunal dê como provados os factos pela própria parte alegados e por ela, tão só, admitidos. ”¹³⁵.

Já “a prova testemunhal, a prova pericial e a prova por inspecção estão também sujeitas à livre apreciação do tribunal (Arts. 389, 391 e 396 do Código Civil), sem que se questione que o juiz possa considerar um facto provado só com base numa dessas provas singulares, no limite, só com base num depoimento”¹³⁶.

Assim, a regra é a da livre apreciação do juiz, porém, há certos casos em que a prova é de tal maneira inabalável que o juiz não pode apreciá-la de acordo com a sua livre convicção e regras de experiência, mas sim de acordo com o valor probatório que aquela prova concentra em si.

Quanto maior for o valor probatório da prova, menor será a liberdade do juiz em apreciar a prova e decidir com base nas regras de experiência e livre convicção. Ao contrário, quanto menor for o valor probatório trazido pela prova aos autos, maior será a discricionariedade do juiz, no sentido em que poderá atribuir muito valor ou pouco valor àquele meio probatório, atribuindo a essa prova valor de prova bastante, prova plena ou prova pleníssima. Por exemplo, a prova testemunhal, em regra, tem

¹³⁵Acórdão do Tribunal da Relação de Coimbra, disponível em

<http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/0476b9a4116061bd80258845003e396e?OpenDocument>.

¹³⁶Acórdão do Tribunal da Relação de Lisboa, disponível em

<http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/cb9177d619e94c5e8025812a003ee850?OpenDocument>.

valor de prova bastante. Porém, o juiz pode-lhe atribuir valor de prova plena, se, com recurso às suas regras de experiência, considerar que aquela prova merece mais valor.

1.6. Produção antecipada de prova

No direito processual civil português, a regra geral, é a de que a produção da prova é efetuada na audiência final, por força do disposto no art. 604º, n.º 3 do CPC, mas a título excecional, o Tribunal pode admitir a produção antecipada de prova – art. 419º do Código de Processo Civil.

“Através da produção antecipada de prova, visou o legislador salvaguardar a possibilidade de produzir prova quando a espera pelo momento processual próprio para o efeito coloque em risco a demonstração dos factos que da mesma serão objeto. Seja por que então tal prova será impossível de produzir, seja por que se tornará muito difícil. Em causa estará, portanto, e sempre o periculum in mora para a produção da prova”¹³⁷.

Vejam os que apenas se admite a produção antecipada de prova em relação a factos que posteriormente será difícil ou, até mesmo, impossível de provar. Senão, atentemos: diz-nos o acórdão do Tribunal de Coimbra que “a produção antecipada de prova tem a sua razão de ser no receio de que a mesma possa tornar-se impossível ou muito difícil, caso não seja produzida de imediato”¹³⁸.

Admite-se, portanto, que a prova seja produzida antes da audiência final, ou até mesmo antes da propositura da ação, por força do estatuído no art. 419º do CPC: “havendo 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, pode o depoimento, a perícia ou a inspeção realizar-se antecipadamente e até antes de ser proposta a ação”. Porém, são casos muito pontuais e escassos.

Como se trata de um instituto muito especial, está sujeito a regras ainda mais estreitas: para tanto, exige-se, nos termos do art. 420º, n.º 1 do CPC que aquele que requer este tipo de produção antecipada de prova, justifique “sumariamente a necessidade da antecipação, menciona com precisão os factos sobre que há de recair e identifica as pessoas que hão de ser ouvidas, quando se trate de depoimento de parte ou de testemunhas”. Nos casos em que se requeira a produção antecipada de prova, ainda antes da propositura da ação, o requerente tem, ao abrigo do n.º 2 do art. 420º do CPC, de indicar “sucintamente o pedido e os fundamentos da demanda e identifica-se a pessoa contra quem se pretende fazer uso da prova, a fim de ela ser notificada”.

¹³⁷Acórdão do Tribunal da Relação do Porto, disponível em

<http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/4dd140beb76352908025871a00547037?OpenDocument>.

¹³⁸Acórdão do Tribunal da Relação de Coimbra, disponível em

<http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/1c3befce6b1da08c8025739f00588a99>.

Infere-se assim que o legislador pretendeu através destes preceitos “salvaguardar a possibilidade de produzir prova quando a espera pelo momento processual próprio para o efeito coloque em risco a demonstração dos factos que da mesma serão objeto. Seja por que então tal prova será impossível de produzir, seja por que se tornará muito difícil, essencial é que se verifique o periculum in mora para a produção da prova”¹³⁹.

A razão que jaz a esta produção antecipada de prova é o “receio de que a mesma possa tornar-se impossível ou muito difícil, caso não seja produzida de imediato. 2) Tal receio tem que apresentar-se com foros de seriedade, apontando para um perigo efetivo e palpável e não ser apenas uma mera possibilidade. 3) A forma de aquilatar de tal perigosidade são os seus indícios patentes e as regras de senso comum, baseadas no conhecimento da vida e das expectativas procedimentais, tendo em linha de conta as peculiaridades de cada caso concreto. 4) Se assim não fosse, acabaria por tornar-se vulgar aquilo que só excepcionalmente deve permitir-se, com a consequente anarquia processual daí adveniente. Assim, a possibilidade de antecipação concedida, isto é a produção de prova antes do momento processual em que normalmente se produziria, é concebível quando estiver em risco a conservação da fonte da prova (impossibilidade) ou a facilidade de a produzir (grande dificuldade).”¹⁴⁰.

Se repararmos, a produção antecipada de prova assemelha-se em muito aos procedimentos cautelares, na medida em que ambos exigem que se verifique o periculum in mora, “porém, ao contrário do que acontece nos procedimentos cautelares não pressupõe o deferimento deste procedimento a alegação e demonstração da probabilidade séria da existência do direito (que para aqueles é exigida – vide artigo 368º do CPC), mas tão só do periculum in mora aferido pela prova que se pretende produzir¹⁴¹.”¹⁴² e, noutro sentido, as produções antecipadas de prova, também não tendem a obter providências a fim de evitar prejuízos que se anseiam.

Diz-nos Alberto dos Reis¹⁴³ que não se exige a certeza, mas apenas a probabilidade ou verosimilhança de que a fonte da prova venha a perder-se ou que a produção da prova se torne muito difícil. Poderá essa prova perder-se com o decurso do tempo, apagando-se os vestígios daquilo que se pretende provar, pelo desgaste natural das coisas, pelo uso, pela consistência dos materiais, se for em termos testemunhais, poderá a testemunha ser já de bastante idade, ou estado de saúde fragilizado e,

¹³⁹ Acórdão do Tribunal da Relação de Lisboa, disponível em <http://www.dgsi.pt/itrl.nsf/33182fc732316039802565fa00497eec/9cbcd312a201d3c68025896300415991?OpenDocument>.

¹⁴⁰ Idem.

¹⁴¹ José Lebre de Freitas e Isabel Alexandre in CPC Anotado, 2º volume, em anotação ao artigo 419º do Código de Processo Civil, pág. 231.

¹⁴² Idem.

¹⁴³ Código de Processo Civil anotado, Vol. III, pág. 337.

portanto, há receio de a mesma falecer. Porém, nunca se pode pretender uma produção antecipada de prova, tão só e apenas, por uma questão de celeridade processual.

A prova produzida através da produção antecipada de prova, tem o mesmo valor que aquela que seja produzida no momento processual apropriado.

1.7. Ónus da prova

Em Portugal, em termos de regras gerais sobre o ónus da prova, opera o preceituado no disposto no artigo 342º do Código Civil (doravante CC).

Nos termos do art. 342º, nº 1 do CC, “Àquele que invocar um direito cabe fazer a prova dos factos constitutivos do direito alegado”, e nos termos do nº 2, “a prova dos factos extintivos do direito, compete àquele contra quem a invocação é feita”, “garantindo o art. 346º, do mesmo Código o direito à contraprova: “(...) à prova que for produzida pela parte sobre quem recai o ónus probatório pode a parte contrária opor contraprova a respeito dos mesmos factos, destinada a torná-los duvidosos; se o conseguir, é a questão decidida contra a parte onerada com a prova”¹⁴⁴.

PIRES DE LIMA E ANTUNES VARELA defendem que “aquele que invoca determinado direito tem de provar os factos que normalmente o integram; a parte contrária terá de provar, por seu turno, os factos anormais que excluem ou impedem a eficácia dos elementos constitutivos”¹⁴⁵.

Assim, em direito processual, sendo a prova o acto ou série de actos processuais através dos quais há que convencer o juiz da existência ou inexistência dos dados lógicos que tem de se ter em consideração na causa, o ónus da prova (342º Código Civil), é a obrigação que recai sobre os sujeitos processuais da realidade de tais actos. A traduzir-se - haverá de dizer-se, agora e sempre -, “para a parte a quem compete, no encargo de fornecer a prova do facto visado, incorrendo nas desvantajosas consequências de se ter como líquido o facto contrário, quando omitiu ou não logrou realizar essa prova”¹⁴⁶.

O ónus da prova é a obrigação que recai sobre cada uma das partes, de demonstrar a ocorrência dos factos que invoca, para que as decisões sejam proferidas. O ónus da prova incumbe ao autor, quanto ao seu direito e, ao réu, relativamente à invocação da existência de factos impeditivos, modificativos ou extintivos do direito invocado pelo autor. Em caso de dúvida, os factos devem ser considerados como constitutivos do direito.

¹⁴⁴Acórdão do Tribunal da Relação de Lisboa, disponível em [Acórdão do Tribunal da Relação de Lisboa](#).

¹⁴⁵ CORREIRA, Têssia Matias, *in* A Prova no Processo Civil - Reflexões sobre o problema da (in)admissibilidade da prova ilícita; Coimbra, 2015.

¹⁴⁶Acórdão do Tribunal da Relação de Coimbra, disponível em [Acórdão do Tribunal da Relação de Coimbra](#).

A cada uma das partes compete, por um lado, o ónus de alegação dos factos que sustentam a sua pretensão e, por outro lado, o ónus da prova desses mesmos factos.

Pires de Lima e Antunes Varela¹⁴⁷ entendem que o art. 342º do CC assenta no critério da normalidade: aquele que invoca um direito tem de provar os factos que normalmente o integram, já a parte contrária tem de provar os factos anormais que excluem ou impedem a eficácia dos elementos constitutivos.

Se surgirem dúvidas sobre a quem incumbe o ónus da prova, isto é, em relação à parte a quem incumbe o ónus da prova, aplica-se o disposto no art. 414º do CPC que indica 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”.

A questão do ónus da prova é de suma importância, pois incide no processo como uma regra de julgamento, influenciando diretamente a decisão de mérito. Assim, se à parte cabia o ónus da prova e não o fez, verá o litígio ser julgado contra si. A importância do ónus da prova encontra-se na fixação das consequências que advêm por força da falta de prova de certo facto.

Há, porém, certos factos que não carecem de ser provados. Assim o indica o art. 412º do CPC: “1 - não carecem de prova nem de alegação os factos notórios, devendo considerar-se como tais os factos que são do conhecimento geral. 2 - Também não carecem de alegação os factos de que o tribunal tem conhecimento por virtude do exercício das suas funções; quando o tribunal se socorra destes factos, deve fazer juntar ao processo documento que os comprove”.

Há situações previstas na lei em que há um desvio à regra geral do ónus da prova, previsto no art. 342º do CC: são os casos especiais e a inversão do ónus da prova.

Há casos especiais de ónus da prova. Nos termos do artigo 343º, n.º 1 do CC, nas ações de simples apreciação negativa, é ao réu a quem compete a prova dos factos constitutivos do direito que se arroga. Nas ações de simples apreciação negativa, o autor pretende unicamente que o tribunal declare a inexistência de um direito ou de um facto (artigo 10.º, n.º 3, al. a)). Portanto, nestas ações é o réu que se arroga titular do direito controvertido e como tal, é a este que incumbe o ónus da prova dos factos que constituem o seu direito.

Presume-se que nestes casos seja mais fácil provar a existência de um facto, do que a sua inexistência. Defende RUI RANGEL¹⁴⁸, em relação a esta situação que “dada as naturais dificuldades de prova de qualquer facto negativo neste tipo de acções, a lei pensou que é mais fácil ao réu provar a existência

¹⁴⁷ Pires de Lima e Antunes Varela, Código Civil Anotado, Vol. I, 4ª ed., revista e atualizada, Coimbra Editora, 2011, pág. 306.

¹⁴⁸ RANGEL, Rui Manuel de Freitas, O Ónus da Prova no Processo Civil, 3.ª ed., Almedina, Coimbra, 2006, pág. 181.

de um direito ou de um facto, do que demonstrar a sua inexistência com a eliminação de todas as causas que justifiquem a sua produção”.

Nas ações como sejam a ação de preferência, que tem de ser proposta dentro de certo prazo a contar da data que o autor teve conhecimento da venda, cabe ao réu o ónus da prova de que o prazo já decorreu, salvo se for outra a solução especialmente prevista no art. 343º, nº 2 do CC.

A última situação especial é relativa às ações em que o direito está sujeito a condição ou termo. Assim, se o direito invocado pelo autor estiver sujeito a condição suspensiva ou termo inicial, cabe-lhe a prova de que a condição se deu ou que o termo se verificou. Porém, se o direito estiver sujeito a condição resolutiva ou termo final, incumbe ao réu provar a verificação da condição ou o vencimento do prazo.

Paralelamente a isto, há situações em que se inverte o ónus da prova.

Há inversão do ónus da prova quando se impõe a demonstração da realidade de um facto à parte que, seguindo-se o critério geral do ónus da prova, não teria tal ónus. Nos termos do art. 344º, nº 1 do CC, há inversão do ónus da prova “quando haja presunção legal, dispensa ou liberação do ónus da prova, ou convenção válida nesse sentido, e, de um modo geral, sempre que a lei o determine”. Já o nº 2 do mesmo art. determina que “há também inversão do ónus da prova, quando a parte contrária tiver culposamente tornado impossível a prova ao onerado, sem prejuízo das sanções que a lei de processo mande especialmente aplicar à desobediência ou às falsas declarações”.

Assim, o art. 344º, nº 2 “surge como consequência à atitude da parte que, com dolo ou mera culpa, impossibilitou o cumprimento do ónus da prova à parte contrária e que, como tal, não conseguiu provar o facto que lhe é favorável. Funciona como uma espécie de sanção civil à violação do dever de cooperação para a descoberta da verdade, exigindo uma atuação “culposa da parte que tenha tornado impossível ou particularmente difícil a produção de prova pela contraparte dos factos que lhe competiam””¹⁴⁹.

Há presunção legal nos termos do art. 349º do CC, isto é, quando se tem como assente um facto partindo de outro, tendo em conta o elevado grau de semelhança ou probabilidade de conexão entre eles. Assim, quem tem a seu favor a presunção legal escusa de provar o facto a que ela conduz – art. 350º, nº 1 do CC.

Nos termos do art. 350º, nº 2 do CC, “as presunções legais podem, todavia, ser ilididas mediante prova em contrário, exceto nos casos em que a lei o proibir”.

¹⁴⁹ Ana Raquel Barbosa, Márcia Passos e Susana Sousa Machado, A análise concetual da Prova em processo civil, ULP Law Review, Revista de Direito da ULP, Vol. 14, nº 1.

1.8. Princípio da igualdade das partes, da proporcionalidade e da razoabilidade

O princípio da igualdade das partes encontra abrigo no art. 4º do CPC. Nos termos deste artigo, “o tribunal deve assegurar, ao longo de todo o processo, um estatuto de igualdade substancial das partes, designadamente no exercício de faculdades, no uso de meios de defesa e na aplicação de cominações ou de sanções processuais”.

Relativamente à atuação do juiz durante o processo, este deve tratar com equidade situações semelhantes, independente da situação económica ou social da parte, principalmente no que concerne à produção de provas, pois a parte sobre a qual recai o dever de provar determinado fato pode estar em uma posição mais desvantajosa do que a outra parte que nada tem de provar para a decisão lhe ser favorável.

O princípio da igualdade das partes implica a paridade simétrica das posições das partes perante o tribunal. Isto é, o princípio da igualdade não proíbe tratamentos diferentes em relação a situações distintas, implica, isso sim, que se trate por igual o que é essencialmente igual e desigual o que é essencialmente desigual, de tal maneira que só haverá violação desse princípio da igualdade se houver tratamento diferenciado de situações essencialmente iguais.

Porém, nem sempre é fácil aplicar este princípio. Como sublinha Teixeira de Sousa¹⁵⁰. “um primeiro problema suscitado pelo artigo 3.º-A (atual artigo 4.º) e pela referida igualdade substancial entre as partes é o de que nem sempre é viável assegurar essa igualdade. Em certos casos, não é possível ultrapassar certas diferenças substanciais na posição processual das partes; noutras hipóteses não é possível afastar certas igualdades formais impostas pela lei. A posição processual das partes é, em muitos dos seus aspetos, substancialmente distinta. Por exemplo: o autor escolhe, normalmente segundo o seu arbítrio, o momento da propositura da ação e o réu tem sempre um prazo limitado para apresentação da sua defesa (...) o que origina uma desigualdade substancial entre as partes a favor do autor.”.

Teixeira de Sousa vai ainda mais longe e indica que este princípio tem um conteúdo positivo, no sentido de impor ao tribunal a igualdade das partes, mas tem também um conteúdo negativo, que proíbe o tribunal de criar desigualdade entre as partes - “a expressão do princípio da igualdade deve ser procurada fora daqueles poderes instrutórios ou inquisitórios, o que de modo algum exclui um amplo campo de aplicação desse princípio. Esta aplicação verifica-se tanto no conteúdo positivo, que

¹⁵⁰ SOUSA, Teixeira de; Estudos sobre o novo processo civil, 2ª edição, 1997, pág. 42.

impõe ao tribunal um dever de construir a igualdade das partes, como no conteúdo negativo, que o proíbe de originar, pela sua conduta, uma desigualdade entre as partes”¹⁵¹.

Violando-se o princípio preconizado no art. 4º do CPC, há uma nulidade.

O princípio da proporcionalidade, por sua vez, 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 especial relevância, sendo a sua aplicação mais usual a de um “instrumento capaz de restringir 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”¹⁵².

Daí que este princípio seja também de aplicação ao tema da admissibilidade da prova. Aliás, este princípio incide sobre quase todas as áreas do direito e não só o direito civil.

Se repararmos, este princípio torna-se importante quando há um conflito de direito, pois havendo colisão ou conflito de interesses entre direitos fundamentais, o juiz deve ponderar com base no princípio da proporcionalidade, colocando os direitos em conflito numa balança e fazendo uma justa escolha daquele que considera o que deverá ser menos restringido. No fundo, não se trata de aniquilar um direito em detrimento de outro, mas sim de restringir um para que o outro se possa expandir.

Por fim, o princípio da razoabilidade relaciona-se com os direitos fundamentais¹⁵³ que a lei atribui aos cidadãos. Há direitos, liberdades e garantias que jamais podem ser retirados aos cidadãos. Nos termos deste princípio, um cidadão não pode ficar numa situação de sacrifício intolerável, vendo-lhe ser restringidos direitos fundamentais à sua vida condigna, ainda que haja justificação para a restrição desses direitos. No fundo, esses direitos podem ser comprimidos em detrimento de outros direitos constitucionalmente protegidos e previstos, mas nunca anulados.

¹⁵¹ Idem, pág. 44.

¹⁵² NOVAIS, Jorge Reis, Os princípios constitucionais estruturantes da República Portuguesa, 1.ª Ed. (Reimpressão), Coimbra Editora, Coimbra, 2014, p.178

¹⁵³ ANDRADE, José Carlos Vieira de. Os Direitos Fundamentais na Constituição Portuguesa de 1976. Coimbra: Almedina, 2010.

2. Prova digital ^{154 155 156 157 158}

2.1. Definição

A prova digital refere-se a qualquer tipo de informação armazenada ou transmitida eletronicamente que pode ser usada em processos judiciais. Com o avanço da tecnologia, a prova digital tornou-se uma parte essencial dos litígios modernos, abrangendo uma ampla variedade de dados. Prova digital é, portanto, qualquer evidência que existe em formato electrónico. Pode incluir documentos criados digitalmente, comunicações eletrónicas¹⁵⁹, registos de transações digitais, entre outros.

A prova digital tem como características a imaterialidade, ou seja, diferente das provas físicas, a prova digital não possui uma forma física tangível; a facilidade de alteração, ou seja, a prova digital pode ser facilmente alterada, copiada ou apagada, o que levanta questões sobre a autenticidade e a integridade; os metadados, ou seja, além do conteúdo visível, os arquivos digitais contêm informações sobre o próprio arquivo, como data de criação, autor e histórico de modificações.

Existem diversos tipos de prova digital, designadamente, os documentos eletrónicos, como é o caso de e-mails (incluem conteúdo do e-mail, anexos e cabeçalhos que podem fornecer informações sobre remetente, destinatário e data) e documentos de texto (arquivos criados por software de processamento de texto, como Microsoft Word ou Google Docs); os registos de comunicação, como é o caso das mensagens instantâneas (conversas em plataformas como WhatsApp ou Telegram) e redes sociais (publicações, mensagens diretas e comentários em plataformas como Facebook, Twitter e LinkedIn); registos de transações; registos bancários, como é o caso de transações financeiras realizadas através de plataformas de banking online; registos de E-commerce (histórico de compras, vendas e transações em plataformas de comércio electrónico); arquivos de Media, como é o caso de

¹⁵⁴ BRANDÃO, Diogo. A prova digital no processo civil: repensar o sistema, Nova Causa Edições Jurídicas, 2020.

¹⁵⁵ GONÇALVES, João Gama. A prova digital em 2017 – Reflexões sobre algumas insuficiências processuais e dificuldades da investigação. Artigo da CEDIS Working Papers - Universidade Nova de Lisboa. Lisboa, 2017.

¹⁵⁶ MASSENO, Manuel David. A prova digital perante a protecção de dados pessoais – uma perspetiva Portuguesa e Europeia. Centro de Estudos Judiciários, 2018.

¹⁵⁷ MEIRELES, Isa. A prova digital no processo judicial. Universidade do Minho, Braga, 2022.

¹⁵⁸ CONDE CORREIA, João. "Prova digital: Enquadramento legal". Centro de Estudos Judiciários, 2018.

¹⁵⁹ ANDRADE, Francisco. Comunicações Eletrónicas e direitos humanos: o perigo do homo connectus" in MONTE, MÁRIO FERREIRA & TARSO, BRANDÃO, Direitos Humanos e a sua efetivação na Era da Transnacionalidade, 1.ª ed., Curitiba, Juruá Editora, 2012.

fotos e vídeos (arquivos de imagem e vídeo capturados digitalmente); e áudios (gravações de voz ou comunicações de áudio armazenadas digitalmente).

Implementar boas práticas, utilizar tecnologias avançadas e garantir a formação adequada das pessoas são passos fundamentais. À medida que a tecnologia continua a evoluir, a capacidade de lidar com provas digitais de maneira eficiente e eficaz é cada vez mais importante para a administração da justiça.

2.2. Neutralidade tecnológica

A neutralidade tecnológica é um princípio que procura garantir a imparcialidade e igualdade de tratamento de diferentes tecnologias em determinado contexto, sem favorecer ou discriminar uma tecnologia em relação a outras. Esse conceito é frequentemente aplicado em políticas governamentais, regulamentações e padrões técnicos para evitar restrições indevidas ou injustas no uso de tecnologias específicas.

A neutralidade tecnológica procura permitir que os utilizadores ou agentes envolvidos escolham livremente a tecnologia que melhor se adequa às suas necessidades e preferências, sem impor vantagens ou desvantagens a uma tecnologia em relação a outras. Isso promove a competição saudável, a inovação e a diversidade de opções tecnológicas, além de evitar monopólios ou oligopólios tecnológicos que possam restringir a escolha dos utilizadores. A Comissão Europeia defende a neutralidade tecnológica como parte de sua estratégia digital, procurando garantir que as políticas e regulamentações não favoreçam ou discriminem tecnologias específicas. A neutralidade tecnológica é considerada essencial para promover a concorrência equitativa, a inovação e o desenvolvimento tecnológico na UE. Ela visa garantir que as empresas e os consumidores tenham liberdade de escolha entre diferentes tecnologias e serviços digitais, sem obstáculos indevidos.

A União Europeia tem implementado medidas para assegurar a neutralidade tecnológica em várias áreas, incluindo telecomunicações, serviços online, proteção de dados e interoperabilidade. Essas medidas visam evitar práticas anticompetitivas, garantir a portabilidade de dados entre diferentes serviços e promover a interoperabilidade entre sistemas e plataformas digitais.

Existem várias leis e regulamentos que abordam a neutralidade tecnológica e promovem a igualdade de tratamento entre diferentes tecnologias. Alguns exemplos:

Regulamento Geral de Proteção de Dados (RGPD) ¹⁶⁰: O RGPD estabelece regras para o processamento de dados pessoais na UE e garante o direito das pessoas à portabilidade dos seus dados entre diferentes serviços. Isso promove a neutralidade tecnológica ao permitir que os utilizadores transfiram seus dados de um serviço para outro sem restrições indevidas. Já a anterior Diretiva 1999/93/CE assegurava a neutralidade tecnológica o que levou a que na alteração do DL 290-D/99 pelo DL 62/2003 o título do documento fosse alterado passando a referir “assinatura eletrónica” em vez de “assinatura digital”. A Diretiva 1999/93/CE foi, assim, a primeira a estabelecer uma estrutura comunitária para assinaturas eletrónicas, visando promover a segurança e a confiança nas transações eletrónicas entre Estados-membros. Um dos seus princípios era justamente a neutralidade tecnológica, permitindo que a legislação fosse aplicável a diversas tecnologias de assinatura, sem se limitar a uma única abordagem técnica. Essa neutralidade tecnológica foi uma das razões que levaram à alteração do Decreto-Lei 290-D/99 pelo Decreto-Lei 62/2003, em Portugal. A mudança permitiu que o título do decreto-lei passasse a referir “assinatura eletrónica” em vez de “assinatura digital”. Essa alteração foi significativa, pois "assinatura digital" refere-se tecnicamente a um tipo específico de assinatura baseada em criptografia¹⁶¹ assimétrica, enquanto "assinatura eletrónica" é um termo mais abrangente, que inclui qualquer método electrónico usado para assinar documentos. Essa mudança terminológica alinhou a legislação portuguesa com o conceito mais amplo e flexível da Diretiva 1999/93/CE, permitindo o uso de diferentes tecnologias de assinatura eletrónica, desde que assegurassem os requisitos de segurança, autenticidade e integridade estabelecidos pela legislação europeia¹⁶².

O Regulamento de Serviços Digitais ¹⁶³: foi adotado para estabelecer novas regras e responsabilidades para as plataformas online e serviços digitais na União Europeia. Ele tem como objetivo garantir condições equitativas para todas as empresas, independentemente da tecnologia que utilizem. Isso inclui regras para evitar tratamento discriminatório e para promover a concorrência justa.

Lei das Comunicações Eletrónicas¹⁶⁴: Esta lei regula o setor das comunicações eletrónicas em Portugal, incluindo serviços de internet e telecomunicações. Ela estabelece princípios de neutralidade de rede,

¹⁶⁰ Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)

¹⁶¹ VALENÇA, José Manuel. Sebenta da unidade curricular de Criptografia, do Mestrado de Direito e Informática da UM, 2016.

¹⁶² Almeida, João Gomes. *A Regulação das Assinaturas e Certificados Eletrónicos: Da Diretiva 1999/93/CE ao Regulamento eIDAS*. Lisboa: Leya, 2017.

¹⁶³ Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único de serviços digitais e que altera a Diretiva 2000/31/CE

¹⁶⁴ Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho de 11 de dezembro de 2018 e Lei n.º 16/2022, de 16 de Agosto

garantindo que os operadores de telecomunicações tratem todo o tráfego de dados de forma igual, sem discriminação indevida de conteúdo, aplicação ou serviço.

2.3. A prova digital e a natureza documental

A prova digital pode incluir uma vasta gama de dados, tais como e-mails, mensagens de texto, registos de chamadas, dados de GPS, arquivos de computador, imagens, vídeos, e até mesmo registos de atividades em redes sociais. Estas provas têm algumas características distintas:

1. Intangibilidade: Diferente dos documentos físicos, as provas digitais são intangíveis e podem ser duplicadas sem perda de qualidade.
2. Fragilidade: São suscetíveis a alterações e destruições acidentais ou intencionais, o que pode comprometer sua integridade e autenticidade.
3. Metadados: As provas digitais frequentemente contêm metadados que fornecem informações contextuais importantes, como data e hora de criação, autor, e histórico de modificações.

A prova digital, apesar de sua intangibilidade, tem características comuns aos documentos tradicionais:

1. Conteúdo Informativo: Assim como documentos em papel, as provas digitais contêm informações que podem ser cruciais para a resolução de um caso.
2. Autenticidade e Integridade: A natureza documental exige que a prova digital seja autêntica (não falsificada) e íntegra (não alterada desde sua criação ou captura).
3. Relevância: Para ser admissível, a prova digital deve ser relevante para o caso em questão, ajudando a estabelecer fatos materiais.

2.4. Cópia de documentos eletrônicos

A cópia de documentos eletrônicos é uma prática comum e necessária quando se lida com provas digitais. Quando se trata de documentos eletrônicos, a cópia geralmente envolve a criação de uma réplica exata ou parcial do documento original em formato digital.

Existem várias maneiras de fazer uma cópia de documentos eletrônicos, dependendo do contexto e dos requisitos legais ou forenses. Alguns métodos comuns incluem:

Cópia simples: Pode-se fazer uma cópia simples de um documento eletrônico, como copiar e colar o conteúdo em outro local ou salvar uma versão do arquivo em outro dispositivo de armazenamento.

Imagem forense: Em casos mais complexos, como investigações judiciais, pode ser necessário criar uma imagem forense do dispositivo ou sistema que contém os documentos eletrônicos. Essa imagem é

uma cópia bit a bit exata de todo o conteúdo do dispositivo, incluindo arquivos, metadados e informações de sistema.

É importante ressaltar que, ao fazer cópias de documentos eletrônicos para fins judiciais, é necessário seguir procedimentos adequados para garantir a autenticidade e a integridade da prova. Isso inclui o uso de ferramentas e métodos adequados de preservação de provas digitais, bem como a documentação adequada de todas as etapas do processo de cópia.

2.5. Prova mediante comunicação eletrônica

A prova mediante comunicação eletrônica refere-se à utilização de registros de comunicações eletrônicas como evidência em um processo judicial ou investigação. Isso inclui e-mails, mensagens de texto, mensagens instantâneas, chamadas telefônicas gravadas, entre outros meios de comunicação eletrônica.

Para que a comunicação eletrônica seja considerada como prova, geralmente é necessário cumprir certos requisitos legais, como a autenticidade e a integridade dos registros. Isso pode incluir a apresentação de metadados que comprovem a origem, o destino e a data/hora da comunicação, além de informações sobre a integridade do conteúdo.

Além disso, é importante levar em consideração as leis de privacidade e proteção de dados ao utilizar a comunicação eletrônica como prova. Em muitos casos, é necessário obter o consentimento das partes envolvidas ou cumprir exigências legais específicas para a obtenção e a utilização dessas comunicações como prova.

2.6. Valor probatório

O valor probatório refere-se à força ou peso que uma determinada evidência possui num processo judicial ou investigação para estabelecer a verdade ou os fatos relevantes do caso. Em outras palavras, é a capacidade da prova em convencer o tribunal ou autoridade competente sobre a veracidade ou a validade de um fato.

O valor probatório de uma prova pode variar de acordo com vários fatores, como a sua confiabilidade, autenticidade, integridade, admissibilidade legal, consistência com outras provas e a forma como foi obtida. Além disso, o valor probatório também pode ser influenciado pelo contexto específico do caso, a legislação aplicável e as regras de procedimento do tribunal.

No caso de evidências eletrônicas, como documentos digitais, registros de comunicações eletrônicas ou outras formas de prova digital, o valor probatório geralmente depende da autenticidade, integridade

e confiabilidade dessas evidências. Isso pode envolver a apresentação de metadados, testemunhos de especialistas em forense digital, conformidade com requisitos legais de preservação de evidências, entre outros elementos.

Em última análise, é responsabilidade do tribunal ou autoridade competente avaliar o valor probatório de cada evidência apresentada e decidir sua relevância e peso na decisão final.

2.7. Ônus da prova

O ônus da prova é um conceito jurídico que define quem tem a responsabilidade de apresentar evidências para comprovar a alegação feita num processo judicial. É o dever de uma das partes de produzir provas suficientes para sustentar seus argumentos e convencer o tribunal sobre a veracidade dos fatos alegados. Nos termos do artigo 342º do Código Civil “àquele que invocar um direito cabe fazer a prova dos factos constitutivos do direito alegado”.

Em geral, a parte que alega um direito tem o ônus da prova. É essa parte que precisa apresentar provas suficientes para apoiar o seu direito. No entanto, em certos casos, o ônus da prova pode ser revertido para a contraparte quando há presunções legais ou fatos notórios que favorecem a contraparte¹⁶⁵.

O ônus da prova digital segue os mesmos princípios gerais do ônus da prova num processo judicial, mas com foco nas evidências digitais. Isso significa que a parte que alega algo e busca usar provas digitais para sustentar sua alegação terá o ônus de apresentar essas evidências. A este propósito veja-se o disposto no art. 3º nº 2 do DL Nº 12/2021, de 9 de fevereiro, que estabelece as seguintes presunções: *“A aposição de uma assinatura eletrónica qualificada a um documento eletrónico equivale à assinatura autógrafa dos documentos com forma escrita sobre suporte de papel e cria a presunção de que:*

- a) A pessoa que após a assinatura eletrónica qualificada é o titular desta ou é representante, com poderes bastantes, da pessoa coletiva em causa;*
- b) A assinatura eletrónica qualificada foi aposta com a intenção de assinar o documento eletrónico;*
- c) O documento eletrónico não sofreu alteração desde que lhe foi aposta a assinatura eletrónica qualificada.*

¹⁶⁵ Artº 344º do Código Civil: “1. As regras dos artigos anteriores invertem-se, quando haja presunção legal, dispensa ou liberação do ônus da prova, ou convenção válida nesse sentido, e, de um modo geral, sempre que a lei o determine. 2. Há também inversão do ônus da prova, quando a parte contrária tiver culposamente tornado impossível a prova ao onerado, sem prejuízo das sanções que a lei de processo mande especialmente aplicar à desobediência ou às falsas declarações.”

3 - A assinatura eletrônica qualificada deve referir-se inequivocamente a uma só pessoa singular ou representante da pessoa coletiva e ao documento ao qual é aposta."

No contexto de provas digitais, o ónus da prova pode envolver a apresentação de registos de comunicações electrónicas, documentos digitais, metadados, registos de atividade em sistemas ou redes, entre outros. A parte que busca usar essas provas digitais deve garantir sua autenticidade, integridade e confiabilidade.

No entanto, é importante destacar que o ónus da prova digital pode ser desafiador, uma vez que a natureza eletrónica das evidências pode apresentar desafios adicionais. Isso inclui a capacidade de rastrear a origem das evidências, a autenticidade dos registos, a preservação adequada dos dados e a conformidade com as leis de privacidade e proteção de dados.

Em alguns casos, pode ser necessário o envolvimento de especialistas forenses digitais para recolher, preservar e analisar as provas digitais de forma adequada. Esses especialistas podem ajudar a estabelecer a autenticidade e a confiabilidade das provas digitais, bem como a lidar com desafios técnicos e legais que possam surgir. Em última análise, o tribunal avaliará a força das provas digitais apresentadas, considerando sua autenticidade, integridade e relevância para tomar sua decisão.

2.8. Presunção de autoria, de vontade e de integridade

A presunção de autoria, de vontade e de integridade são conceitos jurídicos que podem ser aplicados nas situações em que não há provas diretas disponíveis sobre esses elementos, mas em que é possível inferir ou presumir sua existência com base em certas circunstâncias ou fatos conhecidos.

1. Presunção de autoria: A presunção de autoria é a suposição de que uma pessoa é a autora de um determinado ato ou documento. Isso significa que, na ausência de provas em contrário, presume-se, por exemplo, que a pessoa que assina um documento ou envia uma comunicação eletrónica é a autora ou remetente desse documento ou mensagem. Essa presunção pode ser refutada se houver provas que indiquem o contrário.

2. Presunção de vontade: A presunção de vontade refere-se à suposição de que, na ausência de provas em contrário, uma pessoa age de acordo com sua própria vontade e intenção. Isso significa que se presume que uma pessoa tem a intenção de realizar determinadas ações ou tomar determinadas decisões, a menos que haja provas que indiquem o contrário.

3. Presunção de integridade: A presunção de integridade é a suposição de que um documento ou registo é completo e não foi alterado, a menos que haja provas em contrário. Isso significa que, na ausência de provas que indiquem que, por exemplo, um documento foi alterado ou que seu conteúdo

não é confiável, presume-se que o documento seja íntegro. Essa presunção pode ser refutada se houver evidências de falsificação, edição ou manipulação do documento.

A recolha de prova digital implica a recolha forense (utilização de técnicas e ferramentas especializadas para garantir a integridade dos dados obtidos) e cadeia de custódia (manutenção de um registo detalhado de todas as pessoas que tiveram acesso à prova digital, para garantir sua integridade e autenticidade).

A preservação da prova digital é muito importante e pode ser feita através de notificações (instruções emitidas para assegurar que dados relevantes não sejam alterados ou deletados durante o litígio) ou cópias de segurança e arquivo (criação de cópias de segurança e arquivamento de dados para proteger contra perda ou corrupção).

2.9. Desafios da prova digital

A prova digital apresenta vários desafios, designadamente, a preservação porque devido à sua fragilidade, é essencial implementar métodos rigorosos de preservação e cadeia de custódia para assegurar que a prova digital não seja alterada; a admissibilidade porque os tribunais frequentemente enfrentam desafios ao determinar a admissibilidade de provas digitais¹⁶⁶, exigindo métodos de verificação da autenticidade e integridade das provas apresentadas; e a privacidade e segurança porque a recolha e uso de provas digitais devem equilibrar a necessidade de justiça com a proteção da privacidade dos indivíduos e a segurança dos dados.

Para garantir que a prova digital seja admissível e confiável, existem vários métodos de verificação podem ser utilizados, tais como:

1. Hashes Criptográficos: Utilizados para verificar a integridade dos dados, assegurando que não foram alterados.
2. Certificados Digitais: Podem atestar a autenticidade de documentos e comunicações eletrónicas.
3. Logs e Registos de Auditoria: Mantidos para documentar a cadeia de custódia e as ações realizadas sobre a prova digital.

No contexto do Regulamento eIDAS, os conceitos de admissibilidade, confiabilidade e valor probatório têm significados específicos e importantes para a utilização de documentos eletrónicos e serviços de confiança. Vamos explorar cada um deles:

¹⁶⁶ Cfr. Artigos 25°, 35°, 41°, 43°, 45°-B, 45°-I, 45°-K e 46° do Regulamento eIDAS (versão de 2024).

- **Admissibilidade:** refere-se à aceitação legal de um documento eletrónico como prova em processos judiciais ou administrativos. Segundo o eIDAS, documentos eletrónicos não podem ser negados como prova apenas por estarem em formato eletrónico. Isso significa que, desde que cumpram os requisitos legais, são admissíveis em tribunal.
- **Confiabilidade:** Relaciona-se com a segurança e a integridade dos documentos eletrónicos e dos serviços de confiança. O eIDAS estabelece que serviços como assinaturas eletrónicas qualificadas, selos eletrónicos e certificados de autenticação devem ser fornecidos por Prestadores Qualificados de Serviços de Confiança (QTSPs), garantindo um alto nível de segurança e confiabilidade. A confiabilidade é essencial para assegurar que os documentos não foram alterados e que a identidade do signatário é autêntica.
- **Valor Probatório:** Diz respeito à força que um documento eletrónico tem como prova em tribunal. O eIDAS especifica que assinaturas eletrónicas qualificadas têm o mesmo valor probatório que assinaturas manuscritas, criando uma presunção de integridade e autenticidade do documento. Isso significa que, em processos judiciais, um documento com uma assinatura eletrónica qualificada é considerado tão válido quanto um documento assinado à mão.

Estes conceitos são fundamentais para garantir que os documentos eletrónicos e os serviços de confiança sejam aceites e respeitados em todo o espaço jurídico da União Europeia, promovendo a interoperabilidade e a confiança nas transações digitais¹⁶⁷.

A autenticidade e integridade são essenciais ao risco de manipulação, a facilidade de alteração dos dados digitais exige métodos rigorosos para garantir sua autenticidade. A preservação dos metadados é crucial para estabelecer a autenticidade e o contexto da prova digital. A quantidade massiva de dados pode ser avassaladora, o que exige ferramentas avançadas de análise e revisão, sendo que a existência de dados em diferentes formatos e sistemas podem complicar a recolha e a análise dos mesmos. A necessidade de conformidade com leis de proteção de dados, como o RGPD, pode complicar a obtenção e uso de prova digital, sendo que é necessário garantir que informações pessoais e confidenciais sejam protegidas durante o processo de litígio.

Face aos desafios descritos, as boas práticas na gestão de prova digital são muito importantes. O planeamento antecipado, o protocolo de recolha para estabelecer procedimentos claros para a

¹⁶⁷ No Regulamento eIDAS, os conceitos de admissibilidade, confiabilidade e valor probatório são abordados nos artigos 24º e 25º.

obtenção e preservação de prova digital¹⁶⁸, o uso de tecnologia ou ferramentas de eDiscovery^{169 170 171} e a análise forense para garantir a integridade dos dados recolhidos.

A formação contínua ajuda a formar equipas jurídicas e técnicas sobre as melhores práticas e novas tecnologias em eDiscovery.

A atualização sobre Regulamentações deve ter a preocupação de manter actualizado sobre mudanças nas leis de proteção de dados e outras regulamentações relevantes.

A prova digital é, portanto, uma parte essencial dos litígios actuais, oferecendo uma riqueza de informações que podem ser cruciais para a resolução de casos. A prova digital representa um avanço significativo na forma como as evidências são recolhidas e apresentadas em processos judiciais. No entanto, devido à sua natureza única, apresenta desafios específicos que devem ser abordados para garantir sua eficácia e confiabilidade. A compreensão da natureza documental da prova digital e a implementação de práticas de preservação e verificação são essenciais para assegurar que essas provas possam ser utilizadas de forma justa e eficaz nos tribunais.

3. A descoberta eletrónica da prova

3.1. Definição

A descoberta eletrónica de prova é um componente essencial do processo jurídico moderno, especialmente em litígios e investigações que envolvem grandes volumes de dados digitais. A eDiscovery refere-se ao processo de identificação, recolha, preservação, análise, revisão e produção de dados eletrónicos que podem ser utilizados como prova em processos judiciais. Com o aumento da

¹⁶⁸ Early Case Assessment (ECA), i.e., avaliar rapidamente os dados disponíveis para definir a estratégia de litígio. Cfr. [The Basics of Early Case Assessment \(ECA\)](#), acesso em 28 de Outubro de 2024

¹⁶⁹ Exemplos de ferramentas:

- Relativity: é uma plataforma de ediscovery que facilita a revisão, produção e análise de grandes volumes de dados. É conhecida por sua escalabilidade e flexibilidade, permitindo que equipas jurídicas gerenciem casos complexos de forma eficiente. Cfr. [eDiscovery & Legal Search Software Solutions](#), acesso em 28 de Outubro de 2024
- Nuix: é uma ferramenta poderosa para processamento e análise de dados. É frequentemente utilizada para recolher, indexar e analisar grandes volumes de dados, sendo especialmente eficaz em avaliações iniciais de processos judiciais. Cfr. [Leading Provider of Investigative & Analytics Software | Nuix](#), acesso em 28 de Outubro de 2024
- Logikcull: é uma plataforma de ediscovery baseada na “nuvem” que simplifica o processo de revisão de documentos. É conhecida pela sua facilidade de uso e configuração rápida, sendo uma escolha popular para empresas que buscam uma solução eficiente e económica. Cfr. [Logikcull: eDiscovery & Legal Holds Software for Legal Teams](#), acesso em 28 de Outubro de 2024

¹⁷⁰ GRENIG, Jay E.; GLEISNER, William C. eDiscovery & Digital Evidence. Thomson West, 2023-2024.

¹⁷¹ GROSSMAN, M. R., & Cormack, G. V. (Eds.). The Grossman-Cormack Glossary of Technology-Assisted Review. Federal Judicial Center, 2015.

criação e armazenamento de dados digitais, a eDiscovery tornou-se uma prática indispensável, mas também complexa e desafiadora.

3.2. “Common Law” versus “Civil Law”

Os sistemas jurídicos do mundo geralmente dividem-se em dois: "Common Law" e "Civil Law". Embora ambos visem promover a justiça e a ordem, diferem significativamente em sua estrutura, fontes de direito, processos e práticas.

O sistema de Common Law tem suas raízes na Inglaterra medieval, desenvolvendo-se ao longo dos séculos através das decisões dos tribunais. Foi amplamente adotado em países que foram colônias britânicas, como Estados Unidos, Canadá, Austrália e Índia.

Tem como fontes de direito os precedentes judiciais, ou seja, as decisões judiciais anteriores (precedentes) desempenham um papel central e os juízes devem seguir os precedentes estabelecidos por tribunais superiores em casos semelhantes (princípio do stare decisis). A legislação embora exista e seja importante, muitas áreas do direito são predominantemente desenvolvidas através de decisões judiciais e os juízes têm o poder de alterar a regra aplicável.

O sistema de Civil Law tem suas raízes no direito romano, especialmente no Corpus Juris Civilis de Justiniano, e foi codificado em grande parte da Europa continental durante o século XIX. Um marco importante foi o Código Napoleônico de 1804, que consolidou muitas das leis civis na França e serviu de modelo para outros países europeus e suas colônias.

A principal fonte de direito são os códigos e estatutos elaborados por legisladores. O direito escrito é detalhado e abrangente, cobrindo todas as áreas de aplicação. Os precedentes têm um papel secundário, ou seja, as decisões judiciais anteriores têm menor peso. Os juízes interpretam e aplicam os códigos, mas não estão estritamente vinculados por precedentes.

Ambos os sistemas jurídicos têm impacto na Descoberta Eletrônica de Prova.

No Common Law temos o eDiscovery extensivo: grande ênfase na eDiscovery, com regras detalhadas para a preservação, recolha e produção de dados eletrônicos. Os precedentes são influentes, isto é, as decisões judiciais anteriores moldam significativamente as práticas e obrigações de eDiscovery.

No Civil Law há uma menor ênfase na descoberta porque a descoberta de provas é menos extensiva, com maior controle judicial sobre o processo de recolha de evidências. A codificação e regulamentação de eDiscovery são estabelecidas por estatutos específicos e regulamentações detalhadas.

Os sistemas de Common Law e Civil Law representam, portanto, abordagens distintas para a administração da justiça, cada um com suas próprias vantagens e desvantagens. Enquanto o Common Law oferece flexibilidade e capacidade de adaptação, o Civil Law proporciona previsibilidade e consistência. Na prática jurídica contemporânea, especialmente em áreas como a descoberta eletrônica de prova, esses sistemas estão cada vez mais convergindo, incorporando elementos um do outro para enfrentar os desafios do mundo digital e globalizado.

A compreensão das diferenças e semelhanças entre esses sistemas é crucial para advogados, juizes e legisladores, pois permite a aplicação de práticas jurídicas mais eficazes e justas, respeitando as tradições e os princípios subjacentes de cada sistema.

3.3. Dificuldades da descoberta eletrônica da prova

A descoberta eletrônica da prova é confrontada com diversas dificuldades, tais como:

a. Dificuldades Técnicas:

- Volume e Variedade de Dados: A enorme quantidade e diversidade de formatos de dados, como e-mails, documentos, mensagens de texto, e dados de redes sociais, dificultam a recolha e a análise eficaz.
- Preservação da Prova: Manter a integridade dos dados durante a recolha e a transferência é crucial para a sua utilização em processos judiciais. A corrupção ou perda de metadados pode comprometer a validade das provas.
- Complexidade Tecnológica: Diferentes sistemas e plataformas, cada um com suas próprias especificidades técnicas, exigem abordagens variadas para aceder e recolher dados.

b. Dificuldades legais:

- Conformidade com Regulamentos: As leis de proteção de dados, como o RGPD¹⁷², variam entre jurisdições, tornando a conformidade um desafio.
- Privacidade e Confidencialidade: A eDiscovery frequentemente envolve a manipulação de dados pessoais sensíveis, exigindo medidas rigorosas para proteger a privacidade dos indivíduos e a confidencialidade das informações.
- Admissibilidade de Provas: Garantir que as provas eletrônicas sejam admissíveis em tribunal implica manter uma cadeia de custódia rigorosa e provar a autenticidade dos dados.

c. Dificuldades Éticas:

¹⁷² O RGPD é um Regulamento Europeu e, como tal, direta e imediatamente aplicável, sem necessidade de transposição, em todos os estados-membros da União Europeia.

- Viés Algorítmico: Algoritmos de IA e ML utilizados na eDiscovery podem herdar vieses dos dados de treinamento¹⁷³, resultando em decisões injustas.

- Transparência e Explicabilidade: A complexidade dos algoritmos pode dificultar a explicação de como determinadas conclusões foram alcançadas, levantando questões sobre a justiça e a responsabilidade.

d. Custos e Recursos:

- Alto Custo: A implementação e manutenção de sistemas de eDiscovery eficientes são caros, tanto em termos de tecnologia quanto de recursos humanos.

- Necessidade de Especialização: Profissionais jurídicos e técnicos especializados são necessários para gerenciar os processos complexos de eDiscovery.

A operacionalização da descoberta eletrônica de prova comporta várias fases¹⁷⁴:

- Identificação: Determinação das fontes de dados que podem conter informações relevantes.

- Preservação: Garantia de que os dados identificados sejam protegidos contra alterações ou destruição.

- Recolha: Reunião dos dados de maneira forense, mantendo a integridade dos mesmos.

- Processamento: Conversão dos dados recolhidos num formato que possa ser facilmente revisado e analisado.

- Revisão: Avaliação dos dados para determinar sua relevância e confidencialidade.

- Análise: Exame dos dados para encontrar padrões, tópicos ou informações significativas.

- Produção: Entrega dos dados relevantes de acordo com os requisitos legais e formatados adequadamente.

- Apresentação: Uso das evidências recolhidas em audiências, julgamentos ou outros procedimentos legais.

Para esta operacionalização, tem de haver recurso a diversas tecnologias, designadamente:

- Software de eDiscovery: plataformas como Relativity, Nuix e Logikcull são usadas para gerir o processo de ponta a ponta.

¹⁷³ Que podem muito bem ser vieses resultantes do “Case Based Reasoning” ou dos estados cognitivos do software. Cfr. Giovanni Sartor “Cognitive automata and the law: electronic contracting and the intentionality of software agents”, *Artif Intell Law* (2009); Tina Balke, Paulo Novais, Francisco Andrade, Torsten Eymann “From Real-World Regulations to Concrete Norms for Software Agents – A case-based reasoning approach”, in proceedings of Legal and Negotiation Decision Support Systems Workshop at the 12th International Conference on Artificial Intelligence and Law, Barcelona, Junho 2009.

¹⁷⁴ Conforme descritas nos EUA pelo modelo EDRM (Electronic Discovery Reference Model). Cfr. Redgrave, J. D., & Moran, K. (2017). *The Electronic Discovery Reference Model (EDRM) and the Use of Technology in eDiscovery*. Duke Law Journal.

- Análise Forense: ferramentas como EnCase e FTK¹⁷⁵ ajudam na coleta e análise de dados de dispositivos.
- Tecnologias de Pesquisa e Indexação: soluções que permitem buscas rápidas e eficientes nos dados recolhidos.

Ora, no âmbito da descoberta eletrônica da prova há necessidade de estabelecer regras processuais, designadamente:

a. Atualização das normas existentes:

- Revisão de procedimentos: As normas processuais existentes devem ser revisadas e atualizadas para refletir a realidade digital atual.
- Diretrizes para eDiscovery: Criação de diretrizes específicas que regulamentem a identificação, recolha, preservação, análise e produção de dados eletrônicos.

b. Garantia de equidade e transparência:

- Transparência dos Algoritmos: Implementação de requisitos para que os algoritmos de IA utilizados na eDiscovery sejam transparentes e explicáveis¹⁷⁶.

¹⁷⁵ EnCase é uma ferramenta de computação forense utilizada para a recolha, preservação, análise e apresentação de evidências digitais. Desenvolvida pela Guidance Software, EnCase permite que os analistas forenses examinem cópias de conteúdos digitais sem recorrer a análises forenses ao vivo, garantindo a integridade das evidências. Forensic Toolkit (FTK), desenvolvido pela AccessData, é uma ferramenta de computação forense que facilita a análise de dados digitais. FTK é conhecido por seu processo de indexação robusto, que permite buscas rápidas e eficientes em grandes volumes de dados. Cfr. Bhosale, Narayan P. (2021). *Evidence Recovery using EnCase and FTK in Forensic Computing Investigation*. International Journal of Scientific Research in Computer Science and Engineering.

¹⁷⁶ A transparência dos algoritmos em sistemas de IA aplicados ao eDiscovery é uma questão cada vez mais relevante no campo da ciência da computação e do direito. Os algoritmos de eDiscovery são usados para automatizar o processo de busca, classificação e análise de dados eletrônicos para fins legais. No entanto, a sua transparência e explicabilidade são cruciais para garantir a confiança, a conformidade com os regulamentos e a proteção de direitos. Cfr. 1. Goodman, B., & Flaxman, S. (2017). "European Union regulations on algorithmic decision-making and a "right to explanation." *AI Magazine*; Este artigo explora os requisitos de transparência e de explicabilidade impostos pela União Europeia, especialmente em relação ao Regulamento Geral de Proteção de Dados (RGPD), e como estes impactam o desenvolvimento de algoritmos de IA. Destaca-se a ideia de "direito à explicação", que pode ser aplicada a processos de eDiscovery, impondo limites e normas para uma IA mais transparente. 2. Lepri, B., Oliver, N., Letouzé, E., Pentland, A., & Vinck, P. (2018). "Fair, transparent, and accountable algorithmic decision-making processes." *Philosophy & Technology*, 31(4), 611-627. Neste artigo, os autores discutem abordagens para garantir a equidade, transparência e responsabilização dos processos de tomada de decisão algorítmica, oferecendo um quadro teórico que pode ser útil na análise da implementação de IA em sistemas de eDiscovery. 3. Barfield, W., & Pagallo, U. (2020). "Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice." Springer Nature. Este livro oferece uma visão abrangente sobre o uso da IA no campo jurídico, incluindo eDiscovery, e discute a necessidade de explicabilidade dos algoritmos para que eles sejam confiáveis e legalmente válidos. Ele detalha como as regulamentações atuais, como o RGPD, exigem maior transparência. 4. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation." *International Data Privacy Law*, 7(2), 76-99. Este estudo examina as implicações do "direito à explicação" no contexto da tomada de decisões automatizadas e os desafios práticos na aplicação deste direito, especialmente em sistemas complexos como os algoritmos de eDiscovery. 5. Doshi-Velez, F., & Kim, B. (2017). "Towards a rigorous science of interpretable machine learning." Este artigo é uma referência importante sobre os métodos de aprendizagem de máquina interpretável, sendo útil para entender as técnicas aplicáveis ao eDiscovery, onde a transparência e a interpretabilidade são necessárias para auditorias e conformidade. 6. Surden, H. (2014). "Machine learning and law." *Washington Law Review*, 89, 87-115. Surden explora o impacto da aprendizagem da máquina no campo do direito e

- Proteção Contra Vieses: Medidas para garantir que os algoritmos sejam monitorados e ajustados para evitar vieses.

c. Proteção de dados e privacidade:

- Compliance com Leis de Proteção de Dados: as normas processuais devem garantir a conformidade com leis de proteção de dados, protegendo a privacidade dos indivíduos e a confidencialidade das informações.

- Segurança de dados: estabelecimento de padrões robustos para a segurança cibernética durante todo o processo de eDiscovery.

Embora a eDiscovery seja uma ferramenta poderosa na justiça moderna¹⁷⁷, ela enfrenta, portanto, desafios significativos que exigem soluções tecnológicas avançadas e uma cuidadosa gestão para serem superados.

3.4. A descoberta eletrônica da prova – Breve análise comparativa

O processo de descoberta eletrônica tem como objectivo maximizar a eficiência e minimizar os custos, garantindo que as provas eletrônicas relevantes sejam obtidas e apresentadas adequadamente no tribunal. É regulamentada por leis específicas em diversos países e pode ser um processo complexo e caro.

3.4.1. EUA

A descoberta eletrônica de prova é um componente crítico do sistema jurídico dos Estados Unidos, especialmente no contexto do Common Law, onde a descoberta de provas desempenha um papel central no processo litigioso. Com o aumento exponencial da criação e armazenamento de dados eletrônicos, a eDiscovery tornou-se essencial para a identificação, obtenção, preservação, análise e produção de dados eletrônicos que podem ser utilizados como evidência em processos judiciais.

os requisitos técnicos e éticos para que os algoritmos sejam explicáveis e transparentes. Este artigo é essencial para entender o cenário regulatório que impacta os algoritmos de eDiscovery. 7. Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). "The ethics of algorithms: Mapping the debate." *Big Data & Society*. Os autores discutem as questões éticas associadas ao uso de algoritmos, incluindo a necessidade de transparência, um ponto essencial para os sistemas de eDiscovery. O artigo explora os dilemas de implementação e as estratégias para manter a explicabilidade.

Estas referências oferecem uma base sólida sobre as preocupações e metodologias para garantir a transparência e explicabilidade dos algoritmos de IA em contextos legais como o eDiscovery. As publicações citadas tratam de uma combinação de princípios teóricos e de recomendações práticas, úteis para a implementação de algoritmos transparentes e auditáveis.

¹⁷⁷ COHEN, Adam I; LENDER, David J. "Electronic Discovery: Law and Practice". Wolters Kluwer in New York, 2017.

As Regras Federais de Processo Civil (Federal Rules of Civil Procedure - FRCP)¹⁷⁸ fornecem a estrutura legal para a eDiscovery nos Estados Unidos. As emendas de 2006 e 2015 às FRCP foram particularmente significativas na formalização dos procedimentos de eDiscovery.

Além disso, a Lei de Procedimentos de Descoberta Eletrônica (Electronic Discovery Procedures Act) de 2006 fornece orientações adicionais sobre o processo de ediscovery em casos federais. Cada Estado dos EUA também pode ter suas próprias leis de descoberta eletrônica para processos judiciais estaduais.

Um especial enfoque para um instituto de investigação e ensino nos EUA: The Sedona Conference. Este instituto tem publicado os chamados “The Sedona Principles”¹⁷⁹ e onde podemos analisar um conjunto de princípios fundamentais e recomendações das melhores práticas para abordar a produção de informações eletrônicas em litígios.

A eDiscovery nos EUA segue várias fases principais, conforme descritas pelo modelo EDRM (Electronic Discovery Reference Model):

- Identificação: Determinar as fontes de dados relevantes, como emails, documentos, mensagens de texto e dados de redes sociais.
- Preservação: Proteger os dados identificados contra alterações ou destruição. Isso pode incluir a implementação de notificações.
- Recolha: Reunir os dados identificados de maneira forense, garantindo a integridade dos mesmos.
- Processamento: Converter os dados obtidos em um formato que possa ser revisado e analisado. Inclui reduplicação e indexação.
- Revisão: Avaliar os dados para determinar sua relevância e confidencialidade. Ferramentas de TAR (Technology-Assisted Review) podem ser usadas.
- Análise: Examinar os dados para encontrar padrões, tópicos ou informações significativas.
- Produção: Entregar os dados relevantes à parte solicitante ou tribunal em um formato acordado.
- Apresentação: Usar as evidências em audiências, julgamentos ou outros procedimentos legais.

Contudo, levantam-se várias questões associadas à descoberta eletrônica de prova, nomeadamente, o grande volume e variedade de dados (a quantidade de dados gerados diariamente é enorme, tornando a recolha e revisão de todos os dados uma tarefa complexa); a diversidade de formatos (e-mails,

¹⁷⁸ [Federal Rules of Civil Procedure | Federal Rules of Civil Procedure | US Law | LII / Legal Information Institute \(cornell.edu\)](#)

¹⁷⁹ [The Sedona Principles Third Edition.19TSCJ1.pdf \(thesedonaconference.org\)](#)

documentos, mensagens de texto, bases de dados), cada um exigindo ferramentas e técnicas específicas para recolha e análise); os altos custos e recursos (a eDiscovery pode ser extremamente cara, devido aos recursos necessários para recolha, revisão e análise de grandes volumes de dados); a necessidade de especialização (profissionais jurídicos e técnicos especializados são necessários para gerir o processo de eDiscovery, o que pode aumentar os custos); a conformidade e regulamentação (a conformidade com leis de privacidade pode complicar a eDiscovery, especialmente em casos que envolvem dados internacionais); sanções por não preservação (a falha em preservar dados eletrónicos relevantes pode levar a sanções significativas, conforme estabelecido pela Regra 37(e) das FRCP); e a tecnologia e inovação (a aplicação de inteligência artificial e machine learning na eDiscovery^{180 181} melhora a eficiência e a precisão, mas também levanta questões sobre transparência e viés algorítmico); ferramentas de TAR - a revisão assistida por tecnologia (Technology-Assisted Review) - ajudam a gerir grandes volumes de dados, mas requer conhecimento técnico para ser implementada efetivamente.

A descoberta eletrónica de prova nos EUA é uma prática complexa e multifacetada, essencial para a administração da justiça no sistema de Common Law. As Regras Federais de Processo Civil fornecem uma estrutura forte para a eDiscovery, mas a prática enfrenta desafios significativos, incluindo o volume e a diversidade de dados, os custos elevados e a conformidade com regulamentações de privacidade.

A implementação de boas práticas, a colaboração entre as partes e a utilização de tecnologias avançadas são cruciais para o sucesso da eDiscovery. À medida que a tecnologia continua a evoluir, a comunidade jurídica nos EUA está a adaptar-se e adotar novas metodologias para garantir que a eDiscovery seja conduzida de maneira justa, eficiente e económica.

3.4.2. Canadá

No Canadá, as regras de processo civil do Canadá foram actualizadas em 2016 para incluir directrizes específicas sobre a descoberta eletrónica, incluindo a necessidade de cooperação entre as partes. A

¹⁸⁰ ZENG, R., & Xu, J. (2019). Machine Learning in Electronic Discovery: Foundations of a Comprehensive Workflow. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 13(2), 1-29.

¹⁸¹ BRUNDAGE, Miles; AVIN, Shahrar; CLARK, Jack; TONER, Helen; ECKERSLEY, Peter; GARFINKEL, Ben; DAFOE, Allan; SCHARRE, Paul; ZEITZOFF, Thomas; FILAR, Bobby; ANDERSON, Hyrum; ROFF, Heather; ALLEN, Gregory C.; STEINHARDT, Jacob; FLYNN, Carrick; HÉIGEARTAIGH, Seán Ó; BEARD, Simon; BELFIELD, Haydn; FARQUHAR, Sebastian; LYLE, Clare; CROOTOF, Rebecca; EVANS, Owain; PAGE, Michael; BRYSON, Joanna; YAMPOLSKIY, Roman; AMODEI, Dario. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. 1ª edição. Oxford: Oxford University, 2018.

descoberta eletrônica é regulamentada pelo Rules of Civil Procedure¹⁸² em cada província e território canadense.

A descoberta eletrônica de prova no Canadá, é uma prática fundamental no sistema jurídico canadense, refletindo a importância crescente dos dados eletrônicos em litígios e investigações. O sistema jurídico canadense, que combina elementos de Common Law e Civil Law, tem adaptado suas práticas de eDiscovery para lidar com a crescente prevalência de informações digitais. Este capítulo examina a estrutura, os procedimentos e os desafios da eDiscovery no Canadá.

Cada província e território canadense tem suas próprias regras de procedimento civil que regem a eDiscovery, com algumas variações regionais. No entanto, existem diretrizes comuns que são amplamente seguidas:

- Proporcionalidade: Um princípio central na eDiscovery canadense é a proporcionalidade, que exige que o escopo da descoberta eletrônica seja proporcional à importância das questões em disputa, ao valor do litígio e à capacidade das partes de produzir as informações.
- Código de Procedimento Civil: As regras de eDiscovery são especificadas no Código de Procedimento Civil de cada província, como o Código de Procedimento Civil de Ontário (Rules of Civil Procedure).

A Sedona Canada, uma subdivisão da Sedona Conference, desenvolveu diretrizes específicas para a eDiscovery no Canadá, conhecidas como "The Sedona Canada Principles Addressing Electronic Discovery"¹⁸³. Estas diretrizes oferecem uma estrutura para a condução da eDiscovery e são amplamente aceitas e aplicadas nos tribunais canadenses:

- Princípio 1 - Planeamento antecipado e cooperação: As partes devem planejar e cooperar antecipadamente para a eDiscovery.
- Princípio 2 - Proporcionalidade: A eDiscovery deve ser conduzida de forma proporcional à natureza e à importância do litígio.
- Princípio 3 - Preservação: As partes devem tomar medidas razoáveis para preservar os dados eletrônicos relevantes.
- Princípio 4 - Recolha e produção: A obtenção e produção de dados devem ser feitas de maneira eficiente e económica.

¹⁸² [R.R.O. 1990, Reg. 194: REGRAS DE PROCESSO CIVIL \(ontario.ca\)](#)

¹⁸³ [The Sedona Canada Principles third edition January 2022 0.pdf \(thesedonaconference.org\)](#)

A descoberta eletrónica de prova no Canadá é uma prática bem estabelecida, com diretrizes claras e princípios que garantem a eficiência e a equidade do processo. A combinação de regras de procedimento civil provinciais e os princípios da Sedona Canada proporcionam uma base sólida para a condução da eDiscovery.

Apesar dos desafios, como o volume de dados e os custos, as boas práticas de planeamento, cooperação e utilização de tecnologias avançadas ajudam a mitigar essas dificuldades. À medida que a tecnologia continua a evoluir, a comunidade jurídica no Canadá continua a adaptar-se e a adotar novas metodologias para garantir que a eDiscovery seja conduzida de maneira justa, eficiente e económica.

3.4.3. Reino Unido

No Reino Unido, a descoberta eletrónica da prova é uma parte importante do processo judicial, mas é menos comum do que nos Estados Unidos. As regras de processo civil do Reino Unido foram actualizadas em 2019 para incluir orientações específicas sobre a descoberta eletrónica, incluindo a necessidade de cooperação entre as partes no processo de descoberta.

A descoberta eletrónica de provas é regulamentada pelo Civil Procedure Rules Parte 31¹⁸⁴, que estabelece as diretrizes para a condução de processos civis, incluindo a descoberta de provas:

- Part 31 do Civil Procedure Rules¹⁸⁵: Trata da divulgação de documentos, incluindo dados eletrónicos. As partes são obrigadas a divulgar documentos que estejam na sua posse, custódia ou controlo e que sejam relevantes para as questões em discussão.

- Practice Direction 31B¹⁸⁶: Especificamente aborda a divulgação de dados eletrónicos (Electronic Documents). Define obrigações e procedimentos detalhados para a eDiscovery, incluindo a necessidade de um "Document Preservation Notice" para garantir que os documentos relevantes sejam preservados.

3.4.4. Austrália

A eDiscovery na Austrália é regulamentada principalmente pelas regras de procedimento civil dos tribunais federais e estaduais. As Federal Court Rules 2011¹⁸⁷ (Regras do Tribunal Federal de 2011) e

¹⁸⁴ Civil Procedure Rules Parte 31

¹⁸⁵ [PART 31 – DISCLOSURE AND INSPECTION OF DOCUMENTS – Civil Procedure Rules \(justice.gov.uk\)](https://www.justice.gov.uk/civil-procedure-rules/part-31)

¹⁸⁶ [PRACTICE DIRECTION 31B – DISCLOSURE OF ELECTRONIC DOCUMENTS – Civil Procedure Rules \(justice.gov.uk\)](https://www.justice.gov.uk/civil-procedure-rules/practice-direction-31b)

¹⁸⁷ [FEDERAL COURT RULES 2011 \(austlii.edu.au\)](https://www.austlii.edu.au/au/other/auflii/au/other/auflii/au/other/federal-court-rules-2011)

as Uniform Civil Procedure Rules 2005¹⁸⁸ (Regras Uniformes de Procedimento Civil de 2005) são particularmente importantes.

Na Federal Court Rules 2011 as regras estabelecem os procedimentos para a eDiscovery no Tribunal Federal da Austrália. Incluem diretrizes específicas para a divulgação de documentos eletrônicos.

As Uniform Civil Procedure Rules 2005 são utilizadas nos tribunais estaduais de Nova Gales do Sul, Queensland e outros estados, essas regras também fornecem diretrizes detalhadas para a eDiscovery.

Os tribunais australianos frequentemente adotam um protocolo de descoberta eletrônica que define as obrigações das partes em relação à preservação, recolha e produção de dados eletrônicos. O "Practice Note CM 6"¹⁸⁹ do Tribunal Federal da Austrália é um exemplo significativo. O Practice Note CM 6 estabelece diretrizes para a gestão de eDiscovery, enfatizando a necessidade de planejamento antecipado e cooperação entre as partes.

3.4.5. Brasil

Já no Brasil, a descoberta eletrônica de prova está prevista no Código de Processo Civil de 2015¹⁹⁰, que estabelece regras para a produção e utilização de provas eletrônicas em processos judiciais civis.

A descoberta eletrônica de prova, ou eDiscovery, está a ganhar cada vez mais relevância no Brasil devido à crescente digitalização dos dados e à complexidade dos litígios actuais. Embora o sistema jurídico brasileiro, baseado no Civil Law, não tenha uma tradição tão forte de descoberta de provas como o Common Law, o uso de tecnologias digitais está a transformar a forma como as provas são obtidas, preservadas e apresentadas em processos judiciais.

O Código de Processo Civil de 2015 trouxe inovações significativas para o processo civil brasileiro, incluindo disposições que facilitam a utilização de provas eletrônicas:

- Artigo 369: Estabelece que as partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, para provar a verdade dos fatos em que se funda a ação ou a defesa.
- Artigo 373: Trata do ônus da prova, determinando que cabe ao autor provar os fatos constitutivos de seu direito e ao réu os fatos impeditivos, modificativos ou extintivos do direito do autor.
- Artigo 422: Autoriza o juiz a determinar a exibição de documento ou coisa em poder da parte contrária ou de terceiro, desde que relevante para o processo.

Além do Código de Processo Civil de 2015, existem outras leis relevantes:

¹⁸⁸ [Uniform Civil Procedure Rules 2005 - NSW Legislation](#)

¹⁸⁹ [Practice Note CM 6 | ALRC](#)

¹⁹⁰ [L13105 \(planalto.gov.br\)](#)

- Lei de Acesso à Informação (Lei nº 12.527/2011) ¹⁹¹: Regula o acesso a informações públicas, o que pode incluir dados eletrónicos.
- Marco Civil da Internet (Lei nº 12.965/2014) ¹⁹²: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, incluindo a obrigação de provedores de serviços de Internet de manter registos de acesso.

3.4.6. Portugal

Em Portugal, a descoberta eletrónica da prova em processo civil¹⁹³ ainda é relativamente nova e não é tão amplamente utilizada quanto em outros países. O art.º 362º Código Civil português, estipula que os documentos têm de ser gerados pelo homem, ou seja, o documento é o resultado de uma actividade humana. A descoberta eletrónica de prova é regulamentada pelo Código Civil e pelo Código de Processo Civil por analogia com outros meios de prova. O art 411º do Código de Processo Civil estabelece o princípio do inquisitório e o artº 413º do Código de Processo Civil define as provas atendíveis. A descoberta eletrónica de prova em Portugal segue, assim, os princípios gerais de produção de provas no processo civil e as partes devem cooperar e tomar medidas para garantir a protecção da privacidade e dos dados pessoais durante o processo de descoberta eletrónica de provas.

A descoberta eletrónica de prova em Portugal, é um conceito emergente, especialmente importante no contexto do aumento da digitalização e do uso de tecnologias de informação. Embora o sistema jurídico português, baseado no Civil Law, não tenha uma tradição tão robusta de descoberta de provas como o sistema de Common Law, a crescente relevância dos dados eletrónicos está a moldar novas práticas jurídicas.

O Código de Processo Civil¹⁹⁴ tem várias disposições que permitem a utilização de provas eletrónicas:

- Artigo 417.º: Estabelece que as partes podem requerer a exibição de documentos ou coisas que estejam na posse de outras partes ou terceiros.
- Artigo 423.º: Define que os documentos devem ser apresentados como prova juntamente com o articulado em que se aleguem factos correspondentes.

Além do Código de Processo Civil, temos outras leis relevantes:

¹⁹¹ [L12527 \(planalto.gov.br\)](http://L12527.planalto.gov.br)

¹⁹² [L12965 \(planalto.gov.br\)](http://L12965.planalto.gov.br)

¹⁹³ MAURÍCIO, Rui. O paradigma do processo eletrónico no Direito Processual Civil português. In ASCENÇÃO, José Oliveira - Direito da Sociedade da Informação – Separata do Volume IX. 1ª edição. Coimbra: Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2011.

¹⁹⁴ [Lei n.º 41/2013, de 26 de Junho \(pgdlisboa.pt\)](http://Lei n.º 41/2013, de 26 de Junho (pgdlisboa.pt))

- Lei da Proteção de Dados Pessoais (Lei n.º 58/2019) ¹⁹⁵: Transpõe o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia para a legislação portuguesa, regulamentando o tratamento de dados pessoais.

- Lei do Comércio Eletrónico (Decreto-Lei n.º 7/2004) ¹⁹⁶: Estabelece o regime jurídico do comércio eletrónico, incluindo disposições sobre a validade jurídica dos documentos eletrónicos¹⁹⁷.

A descoberta eletrónica de prova em Portugal está em fase de desenvolvimento, impulsionada pela digitalização crescente e pela necessidade de lidar com dados eletrónicos em litígios. O Código de Processo Civil e outras legislações avulsas fornecem uma base jurídica, mas a prática de eDiscovery ainda enfrenta desafios significativos, incluindo custos elevados, necessidade de especialização e conformidade com a Lei de Proteção de Dados Pessoais.

A regulação e implementação de boas práticas, como o planeamento antecipado e a utilização de tecnologias avançadas, é essencial para a condução eficiente e justa da eDiscovery em Portugal. À medida que a tecnologia continua a evoluir, a comunidade jurídica portuguesa deve adaptar-se e adotar novas metodologias para garantir que a eDiscovery seja conduzida de maneira justa, eficiente e económica.

3.5. Direito Norte Americano (Federal Rules Civil Procedure)¹⁹⁸

As Regras Federais de Processo Civil (Federal Rules of Civil Procedure) foram alteradas em 2006 para confirmar que a descoberta de informação armazenada eletronicamente está em igualdade com a descoberta de documentos em papel.

Esta clarificação pôs fim ao argumento de que a descoberta apenas se aplicava à informação que tinha sido intencionalmente criada ou intencionalmente criada ou visualizada por utilizadores humanos - excluindo os metadados e outras informações do sistema geradas automaticamente por computadores. Assim, a informação armazenada eletronicamente está geralmente sujeita ao mesmo âmbito de descoberta relevante para as reivindicações e defesas que rege os registos em papel. Mas a informação armazenada eletronicamente apresenta questões especiais em pelo menos três áreas.

¹⁹⁵ ::: [Lei n.º 58/2019, de 08 de Agosto \(pgdlisboa.pt\)](#)

¹⁹⁶ ::: [DL n.º 7/2004, de 07 de Janeiro \(pgdlisboa.pt\)](#)

¹⁹⁷ Cfr. Art. 3º nº 1 do DL nº 12/2021, de 09 de Fevereiro e Art. 3º nº 35 do Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho de 11 de Abril de 2024.

¹⁹⁸ As Regras Federais de Processo Civil regem os processos civis nos tribunais distritais dos Estados Unidos. O seu objetivo é "assegurar a determinação justa, rápida e económica de todas as acções e procedimentos". As regras foram adoptadas pela primeira vez por ordem do Supremo Tribunal em 20 de dezembro de 1937, transmitidas ao Congresso em 3 de janeiro de 1938 e entraram em vigor em 16 de setembro de 1938. As Regras Civis foram alteradas pela última vez em 2022.

Em primeiro lugar, algumas regras dos tribunais estão expressamente limitadas quanto à informação armazenada eletronicamente. Por exemplo, a Regra 26(b)(2)(B) prevê "limitações específicas" "que a parte identifique como não razoavelmente acessível devido a pôr causa de encargos ou custos indevidos".

Em segundo lugar, algumas regras judiciais não se limitam expressamente à informação armazenada eletronicamente, mas são mais importantes para a informação armazenada eletronicamente do que para os registos em papel. Por exemplo, a Regra 26(b)(1) limita explicitamente o âmbito da descoberta da informação que seja relevante e "proporcional às necessidades do caso". A regra especifica os factores para determinar a proporcionalidade: "a importância das questões em causa na ação, o montante em litígio, o acesso relativo das partes a informação relevante, os recursos das partes, a importância da descoberta na resolução das questões, e se o ónus ou despesa da descoberta proposta supera o seu provável benefício".

Em terceiro lugar, o volume de informação armazenada eletronicamente que é criado e distribuído dentro e entre organizações está a crescer exponencialmente. A possibilidade de descoberta e a proliferação de informação armazenada eletronicamente significa que as organizações podem beneficiar ainda mais de programas eficazes de governação da informação que reduzam o custo e o risco de cumprir as obrigações de descoberta.

Eis os pontos-chave sobre as regras de descoberta eletrónica nos EUA¹⁹⁹:

¹⁹⁹ Cfr. 1. Sedona Conference. (2019). "The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production." Sedona Conference Journal, 20th Anniversary Edition. Este documento é uma das referências mais amplamente aceites sobre melhores práticas de eDiscovery, oferecendo princípios e recomendações sobre questões jurídicas e técnicas em relação à preservação e produção de documentos eletrónicos.

2. Federal Rules of Civil Procedure, especialmente as Regras 16, 26, 33, 34, 37 e 45. Estas regras estabelecem as obrigações de eDiscovery, incluindo a obrigação de preservar provas eletrónicas, os processos de solicitação e produção, e as sanções aplicáveis em caso de falhas de preservação (como a destruição de provas). 3. Scheindlin, S. A., & Capra, D. J. (2009). "The Electronic Discovery and Digital Evidence Casebook." Thomson West. Um guia abrangente para a eDiscovery, escrito pela juíza Shira Scheindlin, uma autoridade em eDiscovery. O livro abrange as obrigações de preservação de provas, recolha de dados eletrónicos e as sanções decorrentes da não conformidade. 4. Losey, R. (2009). "Introduction to eDiscovery: New Cases, Ideas, and Techniques." American Bar Association. O autor explora as técnicas e práticas mais comuns de eDiscovery, com base nas regulamentações e nas práticas judiciais dos EUA, incluindo a proteção de informações privilegiadas e os desafios técnicos do processo de descoberta. 5. Redgrave, J., & Redgrave, M. (2017). "eDiscovery: Current Trends and Cases." Law Journal Press. Este livro explora tendências modernas na eDiscovery, incluindo a gestão de dados massivos e as tecnologias de análise preditiva (TAR) e inteligência artificial, cada vez mais utilizadas em eDiscovery. 6. Ball, C. (2016). "The Data Detective's Toolkit: A Guide to the Effective Use of eDiscovery." Self-published. Um guia prático para advogados sobre como lidar com a eDiscovery em processos judiciais, abrangendo desde a preservação inicial até a revisão e produção de documentos eletrónicos, com exemplos práticos e orientações. 7. Gensler, S., & Rosenthal, L. (2018). "Rule 26(b)(1) and the Proportionality Revolution." The Review of Litigation, 37(2), 185-241. Este artigo examina a evolução da Regra 26(b)(1) do FRCP, discutindo a importância da proporcionalidade na eDiscovery, que determina que o acesso a provas deve ser equilibrado com o custo e o esforço de obtenção.

Estes recursos fornecem uma visão ampla e detalhada das práticas de eDiscovery nos EUA, abordando tanto os aspetos teóricos e jurídicos quanto as metodologias práticas para a preservação e análise de documentos eletrónicos.

1. Federal Rules of Civil Procedure (FRCP) ²⁰⁰: As regras federais de procedimento civil nos EUA abordam a descoberta eletrônica no contexto de litígios federais. A Regra 26(f) exige que as partes se reúnam para discutir questões relacionadas à descoberta eletrônica e cheguem a um acordo sobre os detalhes do processo.

2. ESI (Electronically Stored Information)²⁰¹: A descoberta eletrônica abrange informações armazenadas eletronicamente, como e-mails, documentos digitais, mensagens de texto, arquivos em nuvem, registros de chamadas, meios de comunicação, entre outros.

3. Preservação de evidências: As partes envolvidas num litígio têm a obrigação de preservar adequadamente as evidências eletrônicas relevantes assim que tiverem conhecimento da ação legal iminente ou pendente.

4. Solicitação de produção: As partes podem solicitar a produção de documentos eletrônicos relevantes através de intimações, pedidos de produção ou outras medidas legais.

5. Privacidade e sigilo: As informações protegidas por sigilo legalmente reconhecido, como o sigilo advogado-cliente, podem ser excluídas da descoberta eletrônica. Além disso, questões de privacidade podem surgir e exigir a proteção adequada das informações pessoais.

Existem vários artigos e regras que são aplicáveis à descoberta eletrônica nos Estados Unidos, dependendo da jurisdição e do tribunal em questão.

No contexto federal, as regras mais relevantes são as Federal Rules of Civil Procedure (FRCP), que incluem os seguintes artigos que tratam da descoberta eletrônica:

FRCP 16: Este artigo aborda as conferências de planeamento pré-julgamento, onde as partes discutem questões relacionadas à descoberta eletrônica.

FRCP 16(b): Esta regra estabelece a obrigação das partes de fornecer informações sobre as formas de armazenamento de dados eletrônicos relevantes durante a conferência de planeamento.

FRCP 26: A Regra 26(f) exige que as partes se reúnam para discutir questões de descoberta, incluindo a descoberta eletrônica, e cheguem a um acordo quanto ao processo, o que inclui questões como a forma de produção, o formato dos documentos eletrônicos e como lidar com informações potencialmente privilegiadas. Esta regra impõe uma reunião prévia entre o juiz e as partes para definir quais os procedimentos de descoberta eletrônica de prova que as partes pretendem produzir, o que reveste particular importância para o próprio princípio da igualdade das partes, evitando vantagens

²⁰⁰ [Normas Federais de Processo Civil | Tribunais dos Estados Unidos \(uscourts.gov\)](https://www.uscourts.gov/normas-federais-de-processo-civil-tribunais-dos-estados-unidos)

²⁰¹ OLSON, Bruce A. Electronic Discovery for Small Cases: Managing Digital Evidence and ESI. Chicago, Ill.: American Bar Association, Law Practice Management Section, 2012.

processuais desleais. Esse planejamento conjunto é fundamental para que as partes possam participar do processo de descoberta de modo equilibrado, promovendo uma igualdade de armas.

FRCP 33: Embora principalmente relacionado a interrogatórios escritos, este artigo também pode abranger perguntas relacionadas à descoberta eletrônica.

FRCP 34: Esta regra trata dos pedidos de produção de documentos, incluindo informações eletrônicas.

Regra 34(a): Autoriza a solicitação de documentos, incluindo dados eletrônicos, que estejam sob a posse, custódia ou controle da parte solicitada.

Regra 34(b): Especifica que a solicitação deve descrever com razoável particularidade os itens a serem inspecionados e permitir que a parte solicitante escolha o formato de produção dos dados eletrônicos.

FRCP 37: O artigo 37 aborda as sanções que podem ser impostas a uma parte que não cumpre com as obrigações de descoberta eletrônica.

Regra 37(e): Estabelece medidas corretivas e sanções para a falha em preservar informações eletrônicas relevantes. As sanções variam, dependendo da gravidade da falha.

FRCP 45: Esta regra trata das intimações para produção de documentos, incluindo informações eletrônicas, por parte de terceiros.

FRCP 55: Este artigo aborda a produção de evidências eletrônicas em casos de execução de sentença.

Além das FRCP, muitos Estados têm suas próprias regras de procedimento civil que podem ser aplicadas à descoberta eletrônica em litígios estaduais.

O processo judicial de descoberta eletrônica nos Estados Unidos geralmente segue algumas etapas comuns, embora os detalhes possam variar dependendo da jurisdição e do tribunal específico. A visão geral do processo é a seguinte:

1. Conferência inicial: As partes envolvidas num litígio reúnem-se para uma conferência de organização, geralmente conforme exigido pela Regra 26(f)²⁰² das Federal Rules of Civil Procedure

²⁰² **Rule 26(f) Conference of the Parties; Planning for Discovery**

1. **Conference Timing:** *Except in a proceeding exempted from initial disclosure under Rule 26(a)(1)(B) or when the court orders otherwise, the parties must confer as soon as practicable—and in any event at least 21 days before a scheduling conference is to be held or a scheduling order is due under Rule 16(b).*
2. **Conference Content; Parties' Responsibilities:** *In conferring, the parties must consider the nature and basis of their claims and defenses and the possibilities for promptly settling or resolving the case; make or arrange for the disclosures required by Rule 26(a)(1); discuss any issues about preserving discoverable information; and develop a proposed discovery plan. The attorneys of record and all unrepresented parties that have appeared in the case are jointly responsible for arranging the conference, for attempting in good faith to agree on the proposed discovery plan, and for submitting to the court within 14 days after the conference a written report outlining the plan. The court may order the parties or attorneys to attend the conference in person.*
3. **Discovery Plan:** *A discovery plan must state the parties' views and proposals on:*

(FRCP). Durante essa conferência, as partes discutem questões relacionadas à descoberta eletrônica, como a natureza e o escopo das informações eletrônicas relevantes.

2. Identificação e preservação²⁰³: As partes têm a obrigação de identificar e preservar adequadamente qualquer evidência eletrônica relevante assim que tiverem conhecimento da ação legal iminente ou pendente. Isso inclui tomar medidas para evitar a destruição acidental ou intencional de evidências eletrônicas.

3. Solicitação de produção²⁰⁴: As partes podem enviar solicitações de produção de documentos eletrônicos relevantes à outra parte. Essas solicitações geralmente são feitas por meio de intimações,

-
- (A) what changes should be made in the timing, form, or requirement for disclosures under Rule 26(a), including a statement of when initial disclosures were made or will be made;
 - (B) the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused on particular issues;
 - (C) any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced;
 - (D) any issues about claims of privilege or of protection as trial-preparation materials, including—if the parties agree on a procedure to assert these claims after production—whether to ask the court to include their agreement in an order under Federal Rule of Evidence 502;
 - (E) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed; and
 - (F) any other orders that the court should issue under Rule 26(c) or under Rule 16(b) and (c).

²⁰³ **Rule 26(b)(1) Scope in General:**

"Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable".

Rule 37(e) Failure to Preserve Electronically Stored Information

"If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

- (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
- (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
 - (A) presume that the lost information was unfavorable to the party;
 - (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
 - (C) dismiss the action or enter a default judgment"

²⁰⁴ **Rule 34. Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes**

(a) **In General.** A party may serve on any other party a request within the scope of Rule 26(b):

1. to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control:
 - (A) any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form; or
 - (B) any designated tangible things; or

-
2. to permit entry onto designated land or other property possessed or controlled by the responding party, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

(b) Procedure.

1. **Contents of the Request.** The request:

- (A) must describe with reasonable particularity each item or category of items to be inspected;
- (B) must specify a reasonable time, place, and manner for the inspection and for performing the related acts; and
- © may specify the form or forms in which electronically stored information is to be produced.

2. **Responses and Objections.**

- (A) **Time to Respond.** The party to whom the request is directed must respond in writing within 30 days after being served or—if the request was delivered under Rule 26(d)(2)—within 30 days after the parties' first Rule 26(f) conference. A shorter or longer time may be stipulated to under Rule 29 or be ordered by the court.
- (B) **Responding to Each Item.** For each item or category, the response must either state that inspection and related activities will be permitted as requested or state with specificity the grounds for objecting to the request, including the reasons. The responding party may state that it will produce copies of documents or of electronically stored information instead of permitting inspection. The production must then be completed no later than the time for inspection specified in the request or another reasonable time specified in the response.
- (C) **Objections.** An objection must state whether any responsive materials are being withheld on the basis of that objection. An objection to part of a request must specify the part and permit inspection of the rest.
- (D) **Responding to a Request for Production of Electronically Stored Information.** The response may state an objection to a requested form for producing electronically stored information. If the responding party objects to a requested form—or if no form was specified in the request—the party must state the form or forms it intends to use.
- (E) **Producing the Documents or Electronically Stored Information.** Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:
 - (i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;
 - (ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and
 - (iii) A party need not produce the same electronically stored information in more than one form.

(C) **Nonparties.** As provided in Rule 45, a nonparty may be compelled to produce documents and tangible things or to permit an inspection.

Rule 45. Subpoena

(a) In General.

1. **Form and Contents.**

- (A) **Requirements—In General.** Every subpoena must:
 - (i) state the court from which it issued;
 - (ii) state the title of the action and its civil-action number;
 - (iii) command each person to whom it is directed to do the following at a specified time and place: attend and testify; produce designated documents, electronically stored information, or tangible things in that person's possession, custody, or control; or permit the inspection of premises; and
 - (iv) set out the text of Rule 45(d) and (e).
- (B) **Command to Attend a Deposition—Notice of the Recording Method.** A subpoena commanding attendance at a deposition must state the method for recording the testimony.
- (C) **Combining or Separating a Command to Produce or to Permit Inspection; Specifying the Form for Electronically Stored Information.** A command to produce documents, electronically stored information, or tangible things or to permit the inspection of premises may be included in a subpoena commanding attendance at a deposition, hearing, or trial, or may be set out in a separate subpoena. A subpoena may specify the form or forms in which electronically stored information is to be produced.

-
- **(D) Command to Produce; Included Obligations.** A command in a subpoena to produce documents, electronically stored information, or tangible things requires the responding person to permit inspection, copying, testing, or sampling of the materials.
2. **Issuing Court.** A subpoena must issue from the court where the action is pending.
 3. **Issued by Whom.** The clerk must issue a subpoena, signed but otherwise in blank, to a party who requests it. That party must complete it before service. An attorney also may issue and sign a subpoena if the attorney is authorized to practice in the issuing court.
 4. **Notice to Other Parties Before Service.** If the subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, then before it is served on the person to whom it is directed, a notice and a copy of the subpoena must be served on each party.
- (b) Service.**
1. **By Whom and How; Tendering Fees.** Any person who is at least 18 years old and not a party may serve a subpoena. Serving a subpoena requires delivering a copy to the named person and, if the subpoena requires that person's attendance, tendering the fees for 1 day's attendance and the mileage allowed by law. Fees and mileage need not be tendered when the subpoena issues on behalf of the United States or any of its officers or agencies.
 2. **Service in the United States.** A subpoena may be served at any place within the United States.
 3. **Service in a Foreign Country.** 28 U.S.C. §1783 governs issuing and serving a subpoena directed to a United States national or resident who is in a foreign country.
 4. **Proof of Service.** Proving service, when necessary, requires filing with the issuing court a statement showing the date and manner of service and the names of the persons served. The statement must be certified by the server.
- (c) Place of Compliance.**
1. **For a Trial, Hearing, or Deposition.** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:
 - (A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or
 - (B) within the state where the person resides, is employed, or regularly transacts business in person, if the person
 - (i) is a party or a party's officer; or
 - (ii) is commanded to attend a trial and would not incur substantial expense.
 2. **For Other Discovery.** A subpoena may command:
 - (A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and
 - (B) inspection of premises at the premises to be inspected.
- (d) Protecting a Person Subject to a Subpoena; Enforcement.**
1. **Avoiding Undue Burden or Expense; Sanctions.** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.
 2. **Command to Produce Materials or Permit Inspection.**
 - (A) **Appearance Not Required.** A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.
 - (B) **Objections.** A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:
 - (i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.
 - (ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.
 3. **Quashing or Modifying a Subpoena.**

pedidos de produção ou outros mecanismos legais. As solicitações devem ser específicas e direcionadas às informações eletrônicas relevantes para o caso.

4. Recolha e preservação de informações ou dados armazenados em formato digital: A parte contrária deve recolher e preservar as informações eletrônicas solicitadas (também conhecidas como ESI -

-
- (A) **When Required.** *On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:*
 - (i) *fails to allow a reasonable time to comply;*
 - (ii) *requires a person to comply beyond the geographical limits specified in Rule 45©;*
 - (iii) *requires disclosure of privileged or other protected matter, if no exception or waiver applies; or*
 - (iv) *subjects a person to undue burden.*
 - (B) **When Permitted.** *To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:*
 - (i) *disclosing a trade secret or other confidential research, development, or commercial information; or*
 - (ii) *disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.*
 - © **Specifying Conditions as an Alternative.** *In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:*
 - (i) *shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and*
 - (ii) *ensures that the subpoenaed person will be reasonably compensated.*

(e) Duties in Responding to a Subpoena.

1. **Producing Documents or Electronically Stored Information.** *These procedures apply to producing documents or electronically stored information:*
 - (A) **Documents.** *A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.*
 - (B) **Form for Producing Electronically Stored Information Not Specified.** *If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.*
 - © **Electronically Stored Information Produced in Only One Form.** *The person responding need not produce the same electronically stored information in more than one form.*
 - (D) **Inaccessible Electronically Stored Information.** *The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)©. The court may specify conditions for the discovery.*
2. **Claiming Privilege or Protection.**
 - (A) **Information Withheld.** *A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:*
 - (i) *expressly make the claim; and*
 - (ii) *describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.*
 - (B) **Information Produced.** *If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information.*

Electronically Stored Information). Isso envolve a identificação, aquisição e armazenamento seguro das evidências eletrônicas para garantir sua autenticidade e integridade.

5. Revisão e produção: Após a recolha, as evidências eletrônicas são revistas para determinar sua relevância e possíveis sigilos. A parte contrária deve apresentar as evidências eletrônicas relevantes conforme acordado pelas partes ou conforme determinado pelo tribunal.

6. Privacidade e sigilo: Questões de privacidade e sigilo legalmente reconhecido, como o sigilo advogado-cliente, podem surgir durante a descoberta eletrônica. A parte pode solicitar a proteção de informações confidenciais ou privilegiadas.

7. Sanções e contestações²⁰⁵: Se uma parte não cumprir com suas obrigações de descoberta eletrônica ou se surgirem contestações sobre a produção ou autenticidade das evidências eletrônicas, o tribunal pode impor sanções ou resolver a contestação por meio de audiências ou outras medidas legais.

²⁰⁵ **Rule 37. Failure to Make Disclosures or to Cooperate in Discovery; Sanctions**

(b) Failure to Comply with a Court Order.

1. **Sanctions Sought in the District Where the Deposition Is Taken.** *If the court where the discovery is taken orders a deponent to be sworn or to answer a question and the deponent fails to obey, the failure may be treated as contempt of court. If a deposition-related motion is transferred to the court where the action is pending, and that court orders a deponent to be sworn or to answer a question and the deponent fails to obey, the failure may be treated as contempt of either the court where the discovery is taken or the court where the action is pending.*
2. **Sanctions Sought in the District Where the Action Is Pending.**
 - **(A) For Not Obeying a Discovery Order.** *If a party or a party's officer, director, or managing agent—or a witness designated under Rule 30(b)(6) or 31(a)(4)—fails to obey an order to provide or permit discovery, including an order under Rule 26(f), 35, or 37(a), the court where the action is pending may issue further just orders. They may include the following:*
 - *(i) directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims;*
 - *(ii) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence;*
 - *(iii) striking pleadings in whole or in part;*
 - *(iv) staying further proceedings until the order is obeyed;*
 - *(v) dismissing the action or proceeding in whole or in part;*
 - *(vi) rendering a default judgment against the disobedient party; or*
 - *(vii) treating as contempt of court the failure to obey any order except an order to submit to a physical or mental examination.*
 - **(B) For Not Producing a Person for Examination.** *If a party fails to comply with an order under Rule 35(a) requiring it to produce another person for examination, the court may issue any of the orders listed in Rule 37(b)(2)(A)(i)–(vi), unless the disobedient party shows that it cannot produce the other person.*
 - **(C) Payment of Expenses.** *Instead of or in addition to the orders above, the court must order the disobedient party, the attorney advising that party, or both to pay the reasonable expenses, including attorney's fees, caused by the failure, unless the failure was substantially justified or other circumstances make an award of expenses unjust.*

(e) *"If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:*

- (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or*
- (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:*

(A) presume that the lost information was unfavorable to the party;

Os dados eletrônicos são produzidos de acordo com os formatos acordados pelas partes ou determinados pelo tribunal. As partes devem garantir que os dados produzidos sejam completos e acessíveis.

Nos processos de descoberta eletrônica, especialmente sob as Federal Rules of Civil Procedure (FRCP), as partes envolvidas devem discutir e acordar os formatos de produção de informações armazenadas eletronicamente (ESI), ou, na ausência de acordo, o tribunal pode determinar esses formatos. Esse processo é regulamentado principalmente pelas Regras 26 e 34:

1. Regra 26(f) – Conferência de Planeamento de Descoberta

- Durante a conferência de planeamento da descoberta (Rule 26(f)), as partes devem discutir e tentar chegar a um acordo sobre o formato de produção de ESI. Esse acordo cobre detalhes como:

- Formato nativo: Produção de documentos no formato em que foram originalmente criados (como arquivos docx para documentos do Word ou xlsx para folhas de cálculo).

- Formato PDF ou TIFF: Produção de documentos em formatos estáticos que são legíveis e preservam o conteúdo visual.

- Metadados: Inclusão ou exclusão de metadados, como a data de criação e o autor, o que pode ser importante para a integridade dos dados.

2. Regra 34(b)(1)(C) – Solicitação de formato específico para apresentação

- Regra 34(b)(1)(C) permite que a parte solicitante especifique o formato desejado para a produção de ESI na própria solicitação. A parte solicitada deve cumprir essa especificação, a menos que apresente uma objeção razoável.

3. Regra 34(b)(2)(E) – Apresentação de documentos Eletrônicos

- Caso não haja acordo entre as partes sobre o formato, a Regra 34(b)(2)(E)(ii) determina que, por padrão, o ESI deve ser produzido em um formato "razoavelmente utilizável". Isso significa que o tribunal pode exigir que o ESI seja apresentado de forma acessível e legível, evitando formatos obsoletos ou difíceis de manipular e de difícil utilização por alguma das partes. Também aqui está em causa o princípio da igualdade das partes

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment"

Estas normas garantem que as partes negociem o formato de produção de forma transparente e que, caso não haja acordo, o tribunal possa intervir para assegurar que o ESI seja entregue em um formato adequado e funcional para o processo de descoberta.

A questão dos formatos na produção de documentos eletrônicos e dados em processos legais é crucial, especialmente na descoberta eletrônica (eDiscovery), onde as partes devem partilhar as provas digitais. O formato escolhido para apresentar essas informações pode afetar significativamente a igualdade das partes no processo judicial, com implicações de custos, tempo e facilidade de análise. Vejamos qual a importância dos formatos na igualdade das partes²⁰⁶:

1. Custos Associados ao Formato:

- Diferentes formatos de dados podem exigir tecnologias, softwares ou até especialistas específicos para serem lidos e analisados. Por exemplo, fornecer dados em formato original (como uma folha Excel ou um banco de dados) pode ser mais fácil e econômico para uma parte, enquanto um formato estático (como PDF ou TIFF) pode ser mais acessível para a outra. Se uma parte é obrigada a produzir documentos em um formato mais complexo ou custoso, isso pode criar uma desigualdade financeira que afeta sua capacidade de participação justa.

2. Acessibilidade e Legibilidade:

- A legibilidade dos dados em formatos específicos pode favorecer uma parte em detrimento de outra. Formatos que preservam metadados (como autor, data de modificação, etc.) podem oferecer mais contexto e transparência, enquanto formatos sem essas informações limitam a análise completa dos dados. Se uma parte não tem acesso a certos elementos dos dados, pode enfrentar desvantagens na interpretação e uso das provas.

²⁰⁶ Cfr. 1. Redgrave, J. D., & Moran, K. (2017). "The Electronic Discovery Reference Model (EDRM) and the Use of Technology in eDiscovery." Este artigo examina o Modelo de Referência de Descoberta Eletrônica (EDRM) e discute a importância dos formatos de produção de dados e os desafios de acessibilidade e custos envolvidos. Ele explora como os formatos podem impactar a igualdade entre as partes. 2. Sedona Conference. (2018). "The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production." Os Sedona Principles são uma das principais fontes sobre melhores práticas em eDiscovery. O documento destaca a importância de acordos sobre formatos de produção para garantir a equidade e a acessibilidade das provas entre as partes envolvidas. 3. Losey, R. (2016). "eDiscovery: Current Trends and Cases." Losey discute as tendências de eDiscovery, incluindo o impacto dos formatos de produção de dados e as questões de custos e acessibilidade, abordando como a imposição de formatos específicos pode prejudicar a igualdade de condições entre as partes. 4. Bordone, R. C., & Barrett, J. W. (2007). "The Negotiation Within: The Impact of Internal Conflict Over the Format of Electronic Discovery on the Fairness of Litigation." Este artigo examina como as escolhas de formato de eDiscovery podem criar conflitos internos e externos, afetando a eficiência do processo e a justiça entre as partes. 5. Moore, S. (2014). "Predictive Coding and the Future of eDiscovery." Este artigo explora o papel de formatos e tecnologias, como predictive coding, em processos de eDiscovery, discutindo como as escolhas de formato afetam a acessibilidade e a igualdade entre as partes no uso de dados complexos.

3. Tempo e Eficiência no Processamento de Dados:

- Formatos mais complexos podem exigir mais tempo para processamento e revisão, o que afeta o calendário do processo. A imposição de formatos específicos pode, assim, beneficiar uma das partes, especialmente se esta tiver mais recursos tecnológicos para lidar com o processamento rápido e análise de grandes volumes de dados.

4. Impacto na Equidade Processual:

- A equidade depende do acesso igualitário às provas. Formatos que criam barreiras adicionais podem comprometer a igualdade, pois uma das partes pode ficar em desvantagem ao precisar gastar mais tempo e recursos para adequar ou entender os dados fornecidos. Para evitar isso, as partes devem concordar com formatos que sejam mutuamente acessíveis e razoáveis, ou o tribunal deve intervir para garantir um tratamento justo.

Portanto, a oneração dos formatos representa um potencial risco à igualdade entre as partes, pois pode afetar custos, acesso à informação e a capacidade de análise de provas.

Isto posto,

As evidências eletrônicas são apresentadas durante os procedimentos judiciais, com a necessidade de comprovar a autenticidade e a integridade dos dados.

Existem desafios e considerações na eDiscovery, nomeadamente, no volume e complexidade dos dados (o grande volume de dados eletrônicos pode complicar a recolha e a revisão, aumentando os custos e o tempo necessário para completar a eDiscovery); conformidade com a preservação (a preservação adequada de dados é crítica. A falha em preservar pode resultar em sanções severas, conforme a Regra 37(e)); privacidade e confidencialidade (a eDiscovery deve equilibrar a necessidade de informações com a proteção da privacidade e confidencialidade, especialmente em relação a dados pessoais e informações privilegiadas); custos elevados (o custo da eDiscovery pode ser elevado devido ao volume de dados, necessidade de tecnologia avançada e mão de obra especializada) e uso de tecnologia (a aplicação de tecnologias pode aumentar a eficiência, mas também levanta questões sobre transparência e viés algorítmico).

As boas práticas em eDiscovery sob as FRCP são fundamentais para garantir que o processo de descoberta eletrônica seja eficiente, eficaz e em conformidade com as regulamentações legais. Algumas das principais boas práticas são:

1. Planeamento e preparação antecipada

- Plano de Preservação: desenvolver um plano de preservação de dados assim que a possibilidade de litígio surgir, garantindo que todas as informações relevantes sejam retidas.
- Consulta com especialistas: envolver especialistas em eDiscovery desde o início para aconselhamento sobre estratégias, tecnologias e procedimentos.

2. Comunicação e colaboração:

- Reuniões iniciais: realizar reuniões iniciais entre as partes para discutir e acordar os aspectos da eDiscovery, incluindo escopo, formatos de produção e cronogramas.
- Transparência: manter uma comunicação clara e contínua entre as partes para evitar mal-entendidos e disputas sobre o processo de descoberta.

3. Uso de tecnologia avançada

- Software de eDiscovery: Utilizar ferramentas de software especializadas para gestão de documentos, análise de dados e revisão de informações eletrônicas.
- Inteligência Artificial e Machine Learning: Implementar tecnologias de IA e aprendizagem da máquina para melhorar a eficiência na triagem e análise de grandes volumes de dados.

4. Documentação e auditoria:

- Registo de atividades: manter registos detalhados de todas as etapas do processo de eDiscovery, incluindo decisões sobre preservação, recolha, revisão e produção de dados.
- Auditoria regular: realizar auditorias periódicas para garantir que os processos de eDiscovery estejam sendo seguidos conforme planejado e estejam em conformidade com as normas da FRCP.

5. Gestão de Dados:

- Recolha proporcional: recolher apenas os dados que sejam razoavelmente necessários para o caso, evitando a sobrecarga de informações irrelevantes.

- Formatação e produção: acordar sobre os formatos de produção dos dados eletrônicos para facilitar a revisão e a utilização nos procedimentos legais.

6. Educação:

- Formação: garantir que a equipe envolvida na eDiscovery conheça as ferramentas e processos específicos utilizados.
- Atualização contínua: manter-se atualizado sobre as mudanças nas regulamentações e melhores práticas em eDiscovery.

7. Proteção de dados e privacidade

- Medidas de segurança: implementar medidas rigorosas de segurança cibernética para proteger os dados sensíveis durante todo o processo de eDiscovery.
- Gestão de privacidade: Respeitar as leis de privacidade e as diretrizes de proteção de dados, especialmente ao lidar com informações confidenciais ou pessoais.

8. Resolução de Disputas:

- Mediação e arbitragem: Considerar métodos alternativos de resolução de disputas para resolver conflitos sobre questões de eDiscovery de forma eficiente e econômica.
- Conformidade com ordens judiciais: seguir rigorosamente as ordens judiciais e os prazos estabelecidos para evitar sanções e penalidades.

Implementar essas boas práticas ajuda a mitigar riscos, reduzir custos e melhorar a eficiência geral do processo de eDiscovery, garantindo ao mesmo tempo conformidade com as FRCP e promovendo uma resolução justa e equitativa das disputas jurídicas.

A descoberta eletrônica de prova sob as Federal Rules of Civil Procedure nos Estados Unidos é um processo complexo e detalhado, essencial para garantir a justiça e a equidade nos litígios federais. As FRCP fornecem uma estrutura que orienta as partes na obtenção, preservação e produção de informações eletrônicas, garantindo que as evidências sejam tratadas de maneira eficiente e justa.

Apesar dos desafios, como o volume de dados, os custos elevados e as questões de conformidade, a aplicação de boas práticas e o uso de tecnologias avançadas podem ajudar a mitigar essas dificuldades. A colaboração entre as partes e a adesão às diretrizes das FRCP são cruciais para o sucesso da eDiscovery, garantindo que o processo seja conduzido de maneira justa, eficiente e econômica.

3.6. The Sedona Conference²⁰⁷

A Sedona Conference é uma organização dos Estados Unidos da América, sem fins lucrativos, que promove o desenvolvimento de melhores práticas e diretrizes para a resolução de disputas jurídicas complexas. Fundada em 1997, é conhecida pelas suas contribuições significativas nas áreas de eDiscovery, privacidade de dados e propriedade intelectual.

A missão da Sedona Conference é promover o diálogo entre os profissionais do direito e fomentar o desenvolvimento de práticas jurídicas eficientes e justas. Os objetivos da organização incluem:

- Desenvolvimento de melhores práticas: Criar e promover diretrizes que ajudem a comunidade jurídica a lidar com questões complexas de forma eficaz.
- Formação: fornecer recursos educacionais e oportunidades de capacitação para advogados, juizes e outros profissionais do direito.
- Fomento ao diálogo: Facilitar o diálogo entre diferentes partes interessadas para promover a cooperação e a compreensão mútua.

A Sedona Conference realiza várias atividades para alcançar os seus objetivos, incluindo:

a. Publicação de Guias e Princípios:

- The Sedona Principles: Um conjunto de diretrizes amplamente respeitadas que aborda a produção de documentos eletrônicos na eDiscovery. Esses princípios são atualizados regularmente para refletir as mudanças tecnológicas e jurídicas.
- Relatórios e Comentários: A organização publica relatórios detalhados sobre tópicos específicos, como privacidade de dados, proteção de informações confidenciais e o uso de tecnologia na prática jurídica.

b. Workshops e Conferências:

- Eventos Educacionais: A Sedona Conference organiza workshops, seminários e conferências que reúnem especialistas para discutir e debater questões jurídicas complexas.
- Grupos de Trabalho: Esses grupos são formados por profissionais do direito, acadêmicos e especialistas em tecnologia que colaboram para desenvolver melhores práticas e diretrizes.

c. Programas de formação:

²⁰⁷ [The Sedona Conference®](#), acesso em 28 de Outubro de 2024.

- Formação: Oferecem formação especializada em eDiscovery, proteção de dados e outros tópicos relevantes para advogados²⁰⁸, juízes e profissionais de tecnologias de informação.
- Certificações: Programas de certificação que reconhecem a competência e o conhecimento em áreas específicas do direito e da tecnologia.

As publicações da Sedona Conference são amplamente utilizadas como referência na prática jurídica. Algumas das principais incluem:

a. The Sedona Principles²⁰⁹:

- Conteúdo: Os princípios oferecem diretrizes sobre a preservação, recolha, revisão e produção de documentos eletrônicos. Eles abordam questões como a proporcionalidade, a integridade dos dados e a privacidade.
- Impacto: Estes princípios são utilizados por tribunais e advogados para orientar a eDiscovery e garantir que o processo seja justo e eficiente.

b. The Sedona Guidelines:

- Proteção de Dados e Privacidade: Diretrizes sobre a proteção de dados pessoais e a conformidade com leis de privacidade.
- Confidencialidade de Informações: Recomendações sobre como proteger informações confidenciais e privilegiadas durante a eDiscovery.

c. Relatórios específicos:

- Inteligência Artificial e eDiscovery: Relatórios que exploram o uso de IA e ML na eDiscovery, discutindo os benefícios, desafios e considerações éticas.
- eDiscovery transfronteiriço: Publicações que abordam as complexidades da eDiscovery em contextos internacionais, incluindo questões de jurisdição e conformidade com regulamentos de diferentes países.

A Sedona Conference tem um impacto significativo na área eDiscovery. O seu trabalho influencia a forma como os tribunais interpretam e aplicam as leis relacionadas à produção de documentos

²⁰⁸ WAISBERG, Noah; HUDEK, Alexander. "AI for Lawyers: How Artificial Intelligence Is Transforming the Legal Profession". JOHN WILEY & SONS INC: 2021.

²⁰⁹ Cfr. 1. THE SEDONA CONFERENCE. Commentary on Legal Holds, Second Edition: The Trigger & The Process, 20 SEDONA CONF. J. 341, 2019. 2. THE SEDONA CONFERENCE. The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production. The Sedona Conference Journal, 2018.

eletrônicos e à privacidade de dados. Os tribunais frequentemente citam as publicações da Sedona Conference nas suas decisões, utilizando seus princípios e diretrizes como base para decisões sobre eDiscovery e outras questões tecnológicas. As diretrizes da Sedona Conference servem como modelos para a criação de melhores práticas em escritórios de advogados e departamentos jurídicos corporativos. Esta organização mantém a comunidade jurídica atualizada sobre as últimas tendências e desenvolvimentos em tecnologia e direito.

Por sua vez, os "Sedona Principles for Third-Party Data and Litigation Hold Obligations, Third Edition"²¹⁰ são uma parte integral do conjunto de diretrizes desenvolvidas pela Sedona Conference para orientar a prática jurídica na era digital. Esta edição específica aborda questões críticas relacionadas à retenção de dados e às obrigações de preservação de evidências, especialmente no contexto de dados mantidos por terceiros. Estas instruções são projetadas para ajudar advogados, empresas e tribunais a navegar pelas complexidades legais e práticas da descoberta eletrônica de prova.

Os princípios da Sedona Conference foram inicialmente desenvolvidos para proporcionar um quadro de melhores práticas para a eDiscovery, refletindo a evolução tecnológica e as mudanças nas práticas comerciais e jurídicas. A terceira edição dos princípios especificamente focados em dados de terceiros e obrigações de litígios reflete a crescente importância e prevalência de dados armazenados por terceiros, como provedores de serviços em nuvem, fornecedores de tecnologia e outras entidades externas.

A necessidade de diretrizes específicas surge devido à complexidade dos dados de terceiros: a terceirização e o armazenamento em nuvem complicam a identificação, preservação e obtenção de dados relevantes; a responsabilidade legal: empresas e advogados precisam entender as suas obrigações legais em relação à preservação de dados mantidos por terceiros para evitar sanções e garantir um processo justo; e a proporcionalidade e o custo: A busca de dados de terceiros pode ser onerosa e desafiadora, exigindo um equilíbrio cuidadoso entre a necessidade de informações e os custos envolvidos.

A terceira edição dos princípios da Sedona Conference aborda várias áreas chave:

I. Identificação e preservação de dados de terceiros:

- Princípio 1: Dever de preservação - As partes têm a obrigação de identificar e preservar dados relevantes mantidos por terceiros quando há uma expectativa razoável de litígio.

²¹⁰ The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 19 Sedona Conf. J. 1 (2018).

- Princípio 2: Notificação e Colaboração - É essencial notificar os terceiros relevantes sobre a necessidade de preservar dados e colaborar para garantir a conformidade.

II. Implementação de notificações

- Princípio 3: Adequação das Notificações, que devem ser claras e específicas, detalhando os tipos de dados a serem preservados e os procedimentos para garantir a preservação adequada.
- Princípio 4: Monitorização e Cumprimento - As partes devem monitorar a conformidade com as hold notices e tomar medidas corretivas quando necessário.

III. Proporcionalidade e razoabilidade

- Princípio 5: Avaliação de proporcionalidade - A extensão da preservação e recolha de dados de terceiros deve ser proporcional às necessidades do caso, levando em conta o custo e o benefício.
- Princípio 6: Minimização de custos e esforços - Devem ser feitas tentativas razoáveis para minimizar os custos e os esforços associados à preservação e recolha de dados de terceiros.

Transparência e Boa Fé

- Princípio 7: Transparência no processo - As partes devem ser transparentes sobre os processos de preservação e recolha de dados de terceiros, compartilhando informações relevantes com a outra parte e o tribunal.
- Princípio 8: Boa-fé - Todas as partes envolvidas devem agir de boa-fé durante todo o processo de eDiscovery, evitando práticas obstrutivas ou de má-fé.

Em termos exemplificativos, uma empresa que utiliza um provedor de serviços em nuvem para armazenar e-mails e documentos corporativos. Quando surge um litígio, a empresa deve:

- Identificar quais dados mantidos pelo provedor são relevantes para o caso.
- Notificar o provedor de serviços em nuvem sobre a necessidade de preservar esses dados.
- Implementar notificações adequadas e específicas para garantir que os dados sejam preservados.
- Colaborar com o provedor para recolher os dados relevantes de maneira eficiente e económica.
- Monitorizar a conformidade e tomar medidas corretivas se necessário.

O uso de ferramentas tecnológicas avançadas pode facilitar a aplicação desses princípios, como:

- Software de eDiscovery: Plataformas que ajudam na gestão de notificações, preservação de dados e recolha.

- Análise Forense: Ferramentas que garantem a integridade dos dados coletados e ajudam na análise detalhada.
- Automação e IA: Tecnologias que podem automatizar partes do processo de eDiscovery, melhorando a eficiência e a precisão.

Em suma, os "Sedona Principles for Third-Party Data and Litigation Hold Obligations, Third Edition" fornecem uma estrutura essencial para lidar com os desafios complexos da preservação e recolha de dados mantidos por terceiros. Ao seguir esses princípios, advogados, empresas e tribunais podem garantir que o processo de eDiscovery seja conduzido de maneira justa, eficiente e económica, minimizando riscos legais e garantindo a integridade das provas.

A implementação eficaz dessas diretrizes requer uma compreensão clara das obrigações legais, uma colaboração estreita com terceiros e o uso de tecnologias avançadas para facilitar a identificação, preservação e recolha de dados. Com a evolução contínua das tecnologias e práticas de eDiscovery, a adaptação e a adesão a princípios como os desenvolvidos pela Sedona Conference²¹¹ são cada vez mais cruciais para a prática jurídica moderna.

3.7. A descoberta eletrónica da prova – Princípio da igualdade das partes ^{212 213 214 215 216}

O princípio da igualdade das partes na descoberta eletrónica da prova é fundamental para garantir que todas as partes envolvidas num litígio têm as mesmas oportunidades e recursos para aceder e apresentar evidências eletrónicas. Esse princípio busca assegurar um processo justo e equilibrado:

a) Acesso igualitário às provas

- Transparência: as partes devem ter igual acesso às provas eletrónicas relevantes. Isso significa que todas as informações recolhidas e preservadas devem ser compartilhadas de maneira justa.
- Equidade no processo de recolha: A obtenção de provas deve ser feita de maneira uniforme, garantindo que nenhum dos lados tenha vantagem injusta devido à forma como os dados foram recolhidos.

²¹¹ THE SEDONA CONFERENCE. Commentary on Proportionality in Electronic Discovery. 2013. SEDONA CONFERENCE. The Sedona Canada Principles Addressing Electronic Discovery, Third Edition, 2021.

²¹² Michels, D. (2015). eDiscovery: An Introduction to Digital Evidence. American Bar Association.

²¹³ Sedona Conference (2018). The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production. The Sedona Conference Journal.

²¹⁴ Redgrave, J. D., & Moran, K. (2017). The Electronic Discovery Reference Model (EDRM) and the Use of Technology in eDiscovery. Duke Law Journal.

²¹⁵ Ball, C. E. (2012). The eDiscovery Primer: The Essentials of eDiscovery Law. Jones McClure Publishing.

²¹⁶ Scheindlin, S. A., & Capra, D. J.(2009). Electronic Discovery and Digital Evidence in a Nutshell. West Academic Publishing.

b) Direito à preservação de prova

- Preservação de dados: as partes têm a responsabilidade de preservar provas relevantes. Isso inclui evitar a destruição ou alteração de dados que podem ser significativos para o caso.
- Notificação: se uma parte perceber que determinados dados podem ser importantes, ela deve notificar a outra parte para garantir que esses dados sejam preservados.

c) Proporcionalidade

- Relevância e necessidade: a descoberta eletrônica deve ser proporcional ao valor do litígio. Solicitações excessivamente amplas ou onerosas podem ser contestadas para garantir que a recolha de provas não imponha um ônus indevido a qualquer das partes.
- Custos Razoáveis: os custos associados à descoberta eletrônica devem ser equilibrados, e, se necessário, o tribunal pode ordenar a divisão dos custos para evitar desvantagens financeiras significativas.

d) Confidencialidade e privacidade

- Proteção de dados sensíveis: as partes devem proteger dados confidenciais e informações pessoais durante o processo de descoberta eletrônica. Acordos de confidencialidade e medidas de proteção de dados devem ser implementados para evitar o uso indevido de informações sensíveis.
- Proteção de informações privadas: informações que não são relevantes para o litígio, mas que contêm dados privados ou sensíveis, devem ser protegidas.

e) Capacidade técnica

- Assistência técnica igualitária: as partes devem ter acesso a recursos técnicos e expertise para lidar com a complexidade da descoberta eletrônica. Isso pode incluir o uso de peritos ou consultores de eDiscovery.
- Formação: A formação sobre eDiscovery devem estar disponíveis para garantir que ambas as partes possam efetivamente participar do processo.

f) Procedimentos justos e eficientes

- Normas e protocolos: Estabelecer normas e protocolos claros para a condução da descoberta eletrônica, garantindo que as regras sejam aplicadas de maneira uniforme e justa.

-Resolução de disputas: Mecanismos para resolver disputas relacionadas à descoberta eletrónica devem estar disponíveis, permitindo que questões sejam resolvidas de forma rápida e justa, sem causar atrasos desnecessários no processo.

g) Supervisão judicial

-Intervenção do Tribunal: O tribunal deve supervisionar o processo de descoberta eletrónica para garantir que seja conduzido de maneira justa e equitativa. Decisões judiciais podem ser necessárias para resolver disputas ou impor sanções em casos de má-fé.

h) Responsabilidade e sanções

- Responsabilidade por condutas inadequadas: as partes devem ser responsabilizadas por qualquer conduta inadequada, como a destruição intencional de provas ou a ocultação de informações relevantes.

- Sanções apropriadas: Sanções proporcionais devem ser aplicadas em casos de violação dos princípios de igualdade, preservação e transparência.

O princípio de igualdade das partes na descoberta eletrónica da prova é essencial para garantir um processo justo e equilibrado, onde todas as partes têm a mesma oportunidade de aceder, preservar e apresentar provas eletrónicas. Esse princípio ajuda a manter a integridade do processo legal e assegura que nenhuma das partes tenha uma vantagem indevida.

A descoberta eletrónica de prova é um componente indispensável do processo jurídico actual, oferecendo benefícios significativos em termos de eficiência e precisão na análise de grandes volumes de dados. No entanto, enfrenta desafios técnicos, legais e éticos que precisam ser cuidadosamente geridos.

A operacionalização eficaz da eDiscovery exige uma combinação de tecnologias avançadas e práticas bem definidas, desde a identificação e preservação até a produção e apresentação das provas. Além disso, a necessidade de novas regras processuais é evidente para garantir a justiça, a equidade e a conformidade com as leis de proteção de dados.

Para maximizar os benefícios da eDiscovery e mitigar seus desafios, é crucial que a comunidade jurídica se adapte continuamente às mudanças tecnológicas e adote práticas que assegurem a justiça e a integridade no processo de descoberta eletrônica. A formação contínua, a adaptação a novas metodologias e a criação de normas regulatórias específicas são passos essenciais nesse caminho.

3.7. eDiscovery: O Direito português em comparação com os EUA

No âmbito dos processos judiciais que envolvem descoberta eletrônica, a distribuição do ónus da prova, os formatos de produção de documentos e a igualdade entre as partes assumem uma relevância fundamental.

Estes elementos influenciam diretamente a eficácia e a equidade do processo judicial, particularmente em litígios que exigem gestão de grandes volumes de dados digitais, como disputas comerciais complexas ou investigações de responsabilidade corporativa. Assim, face a tudo o exposto, é importante a concretização de um exame crítico de como esses fatores são abordados no sistema jurídico português em comparação com o dos Estados Unidos, oferecendo sugestões para possíveis adaptações no direito português.

I. O ónus da prova no contexto de eDiscovery

No sistema jurídico português, o ónus da prova recai geralmente sobre a parte que alega o fato (artº 342º CC). No entanto, em processos que envolvem descoberta eletrônica, a capacidade de provar a existência e relevância de documentos eletrônicos depende frequentemente da infraestrutura tecnológica e da capacidade de gestão documental das partes envolvidas. A falta de regulamentação específica para eDiscovery em Portugal pode, assim, gerar dificuldades, especialmente quando uma das partes precisa exigir a produção de documentos eletrônicos em posse de outra.

Em contrapartida, o sistema americano tem um enquadramento bem mais detalhado para o ónus da prova em eDiscovery. A Regra 37(e) do FRCP, por exemplo, prevê sanções para as partes que falhem em preservar dados relevantes, atribuindo-lhes uma responsabilidade ativa sobre a gestão e integridade dos dados, e promovendo maior transparência processual. Assim, o ónus de provar que os dados foram preservados e produzidos de forma adequada recai na parte que detém esses dados.

A introdução de normas específicas para o ónus da prova em eDiscovery no direito português traria maior segurança jurídica às partes, incentivando a conformidade na produção de dados e promovendo

a transparência. Definir responsabilidades claras sobre a preservação e produção de dados, incluindo penalidades para o incumprimento, tornaria o sistema mais eficaz em litígios que envolvem documentos eletrônicos.

II. Formatos de produção de documentos e dados eletrônicos

A escolha dos formatos de produção de documentos em eDiscovery afeta diretamente a acessibilidade e a eficácia do tratamento de dados. Formatos complexos podem impor custos e prolongar o tempo de análise, colocando uma das partes em desvantagem.

O Código de Processo Civil português não oferece normas específicas sobre os formatos de produção de documentos em eDiscovery, deixando uma lacuna que pode resultar em disputas ou desigualdade processual. Em contraste, as Regras 26 e 34 do FRCP dos EUA estabelecem que as partes devem discutir e concordar sobre os formatos de produção durante a fase de conferência. Caso não haja acordo, o tribunal pode determinar um formato adequado, assegurando que as informações sejam produzidas de maneira acessível para ambas as partes.

Implementar normas semelhantes às dos EUA no sistema português garantiria que os formatos de produção fossem mutuamente acessíveis, promovendo um processo mais eficiente e justo. Uma norma que exija uma conferência inicial para decidir os formatos de produção, ou, na falta de acordo, a determinação do tribunal, poderia evitar disputas e assegurar um tratamento equitativo entre as partes.

III. Igualdade das partes e proporcionalidade em eDiscovery

A igualdade das partes é um princípio central do sistema jurídico português (artº 4º do CPC), mas pode ser comprometida em processos de eDiscovery, onde as partes não dispõem da mesma infraestrutura e recursos tecnológicos. Esta disparidade de recursos pode dificultar a produção de documentos eletrônicos para uma das partes, comprometendo a equidade processual.

Nos Estados Unidos, o conceito de proporcionalidade, presente na Regra 26(b)(1) do FRCP, considera a relação entre o custo e a relevância das provas, evitando que as partes sofram encargos desproporcionais. Este princípio ajuda a manter um equilíbrio processual, especialmente para as partes com acesso limitado a tecnologia e recursos.

Incorporar o princípio da proporcionalidade em eDiscovery, inspirado no sistema americano, permitiria ao tribunal avaliar a razoabilidade dos pedidos de produção de dados, considerando a capacidade de

cada parte. Esse ajuste beneficiaria a igualdade das partes e evitaria sobrecargas processuais para as partes menos capacitadas tecnologicamente, promovendo uma justiça mais acessível e justa.

Capítulo III – A inteligência artificial, o machine learning e a descoberta eletrônica da prova

1. Definição

A inteligência artificial é um campo da ciência da computação que se concentra no desenvolvimento de sistemas e programas capazes de realizar tarefas que normalmente exigem inteligência humana. Essas tarefas incluem raciocínio, aprendizagem, reconhecimento de padrões, tomada de decisões e resolução de problemas. A IA busca simular e replicar a capacidade cognitiva humana por meio de algoritmos e técnicas específicas. A IA é um termo abrangente para software de computador que imita a cognição humana para realizar tarefas complexas e aprender com elas.

O machine learning, por sua vez, é um subcampo da IA que usa algoritmos treinados em dados para produzir modelos adaptáveis que podem executar uma variedade de tarefas complexas.

Analisemos os dois conceitos²¹⁷:

- A inteligência artificial²¹⁸ é um campo amplo que se refere à criação de sistemas e máquinas capazes de executar tarefas que normalmente exigiriam inteligência humana. A IA engloba várias técnicas, metodologias e abordagens para desenvolver sistemas que possam perceber o ambiente, raciocinar, tomar decisões e resolver problemas complexos de forma autônoma.

- O machine learning é uma subárea específica da inteligência artificial que se concentra no desenvolvimento de algoritmos e modelos que permitem que as máquinas aprendam a partir de dados, sem serem explicitamente programadas. Em vez de seguir instruções específicas, os modelos de machine learning são treinados para reconhecer padrões nos dados e fazer previsões ou tomar decisões com base nesses padrões. O machine learning é uma técnica-chave utilizada na construção de sistemas de inteligência artificial.

Em resumo, o machine learning é uma abordagem específica dentro do campo mais amplo da inteligência artificial, onde os sistemas aprendem com os dados para realizar tarefas específicas,

²¹⁷ Russell, S., & Norvig, P. (2009). "Artificial Intelligence: A Modern Approach." Prentice Hall.

²¹⁸ Cfr. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de Junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial): Art. 3° n° 1: "«Sistema de IA», um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais;"

enquanto a inteligência artificial engloba uma variedade de técnicas para criar sistemas inteligentes capazes de realizar uma ampla gama de tarefas.

Os mecanismos de inteligência artificial e de machine learning²¹⁹ desempenham um papel cada vez mais importante na descoberta eletrônica da prova, também conhecida como eDiscovery. A eDiscovery refere-se ao processo para identificar, recolher, preservar e analisar dados eletrônicos relevantes para um litígio ou investigação forense num contexto jurídico.

Na descoberta eletrônica da prova, a inteligência artificial e o machine learning desempenham um papel essencial na análise e gestão de dados eletrônicos relevantes para processos judiciais. A IA e o ML são usadas na descoberta eletrônica da prova para automatizar e otimizar várias etapas do processo. Isso inclui a triagem e a classificação automatizadas de documentos eletrônicos, a identificação de informações relevantes e a descoberta de padrões e insights ocultos nos dados. A IA e o ML também podem ser aplicados na análise de linguagem natural, processamento de imagem e reconhecimento de voz para auxiliar na revisão e na extracção de informações relevantes.

2. Algoritmos

O ML, na descoberta eletrônica da prova, envolve o uso de algoritmos²²⁰ e técnicas para automatizar e otimizar a análise e a gestão de dados eletrônicos relevantes em processos judiciais, com o objectivo de tornar o processo mais eficiente, preciso e económico.

Existem vários algoritmos utilizados na aplicação da inteligência artificial na descoberta eletrônica da prova. Esses algoritmos são projectados para realizar tarefas particulares. Aqui estão alguns exemplos de algoritmos utilizados nessa área:

1. Algoritmo de aprendizagem supervisionada: É um tipo de algoritmo que aprende a partir de exemplos rotulados, ou seja, dados de treino que já foram classificados previamente por humanos. Alguns exemplos de algoritmos de aprendizagem supervisionada incluem Naive Bayes, Support Vector Machines (SVM) e Redes Neurais Artificiais²²¹.

²¹⁹ KACEM, A.; BELACEL, N. Electronic Discovery: A Machine Learning Approach. In Proceedings of the 6th International Conference on Control, Decision and Information Technologies (CoDIT), 2019.

²²⁰ No livro Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). "Introduction to Algorithms." MIT Press, um algoritmo é definido como uma sequência bem definida de instruções computacionais que transformam uma entrada em uma saída.

²²¹ Três técnicas de aprendizagem da máquina, cada uma com suas próprias características e aplicações ideais.

2. Algoritmo de aprendizagem não supervisionada: Este tipo de algoritmo é usado quando não há rótulos ou categorias pré-definidas nos dados. Ele procura identificar padrões, agrupamentos ou similaridades nos dados. Alguns exemplos de algoritmos de aprendizagem não supervisionada incluem o algoritmo de agrupamento K-means e o algoritmo de redução de dimensionalidade PCA (Principal Component Analysis)²²².

3. Algoritmo de aprendizagem por reforço: Este tipo de algoritmo é usado para tomar decisões sequenciais em um ambiente dinâmico. Ele aprende através de tentativa e erro, recebendo feedback positivo ou negativo com base nas suas acções. O algoritmo Q-Learning é um exemplo comum de aprendizagem por reforço.

4. Algoritmo de processamento de linguagem natural (NLP): Estes algoritmos são projectados para processar, analisar e compreender a linguagem humana. Podem ser usados para realizar tarefas como identificação de entidades, extracção de informações, análise de sentimentos e tradução automática. Algoritmos como o algoritmo de Markov Hidden Model (HMM) e o algoritmo de análise sintáctica (parsing) são amplamente utilizados em NLP.

Esses são apenas alguns exemplos de algoritmos que se usam na descoberta eletrónica da prova.

1. Naive Bayes: Baseado em probabilidade, este método aplica o teorema de Bayes, assumindo que os preditores são independentes entre si. Embora esta seja uma suposição simplista (daí o "naive" ou "ingénuo"), muitas vezes resulta em um bom desempenho, especialmente em grandes conjuntos de dados. É conhecido pela eficácia e velocidade em grandes conjuntos de dados, sendo frequentemente usado para classificação de textos e filtragem de spam. Aplicações: classificação de documentos e e-mails; análise de sentimentos; diagnóstico médico baseado em sintomas.

2. Support Vector Machines (SVM): Classificador de Margem Máxima, o SVM busca encontrar o hiperplano que maximiza a margem entre as classes nos dados de treinamento. Isso é feito transformando os dados para um espaço dimensional superior onde as classes possam ser separadas linearmente. Aplicações: reconhecimento de padrões, como reconhecimento facial e de voz; classificação de textos e imagens; problemas de bioinformática, como classificação de proteínas.

3. Redes Neurais Artificiais (ANNs): Modelagem Complexa, capazes de modelar relações não-lineares complexas aprendendo padrões diretamente dos dados sem a necessidade de especificações manuais de características, através de camadas que imitam os neurónios humanos. Redes neurais com muitas camadas (deep learning) podem aprender características em múltiplos níveis de abstração, tornando-as poderosas para tarefas como reconhecimento de fala e imagem. Aplicações: visão computacional; processamento de linguagem natural; previsão financeira e análise de séries temporais.

Cfr. Artigo "Naive Bayes: applications, variations and vulnerabilities: a review of literature with code snippets for implementation" publicado na revista *Soft Computing*, Livro "An Introduction to Statistical Learning: with Applications in R" por Gareth James, Daniela Witten, Trevor Hastie e Robert Tibshirani.

²²² Técnica estatística utilizada para redução de dimensionalidade em conjuntos de dados com múltiplas variáveis. PCA transforma o conjunto de dados original em um novo sistema de eixos (ou componentes principais), onde cada componente principal captura a maior variação possível dos dados com um número menor de dimensões, enquanto minimiza a perda de informação. Cfr. Jolliffe, I. T. (2002). "Principal Component Analysis." *Springer Series in Statistics*.

Cada um possui suas próprias características e aplicabilidades, e a escolha do algoritmo mais adequado dependerá das necessidades e objectivos específicos do caso concreto, bem como das regras de cada ordenamento jurídico.

3. Integração da Inteligência Artificial²²³ e o Machine Learning²²⁴ na descoberta eletrónica da prova ²²⁵

A integração de tecnologias avançadas como a Inteligência Artificial e o Machine Learning na descoberta eletrónica da prova está a transformar significativamente o campo jurídico. Estas tecnologias permitem a análise eficiente de grandes volumes de dados, melhorando a precisão e a velocidade na identificação de evidências relevantes. Vejamos o impacto da IA e do ML na descoberta eletrónica da prova, discutindo suas aplicações, benefícios, desafios e implicações éticas.

Como aplicações da IA e do ML na descoberta eletrónica da prova, temos:

I. Revisão de documentos assistida por tecnologia (TAR)²²⁶

A TAR utiliza algoritmos de IA para classificar e rever grandes volumes de documentos eletrónicos, sendo um dos avanços mais significativos na descoberta eletrónica da prova. Existem duas abordagens principais:

- TAR 1.0: Baseada em técnicas de recuperação de informações e requer uma fase inicial de treinamento supervisionado por humanos. Os documentos são classificados por relevância com base no feedback fornecido pelos revisores humanos durante o treinamento inicial. O algoritmo então aplica esses critérios a um conjunto maior de documentos.

O TAR 2.0 utiliza algoritmos de aprendizagem contínua que melhoram a precisão conforme mais dados são revisados. Esta abordagem é mais dinâmica e adapta-se em tempo real às novas informações e padrões identificados nos dados, permitindo uma análise mais refinada e precisa.

²²³ ROCHA, Manuel Lopes; PEREIRA, Rui Soares Pereira. *Inteligência artificial & Direito*. Almedina, 2022.

²²⁴ SARTOR, G., & Sartor, C. The Impact of Machine Learning on Electronic Discovery. *International Journal of Law and Information Technology*. 2017.

²²⁵ - MICHELS, D. *eDiscovery: An Introduction to Digital Evidence*. American Bar Association, 2015.

- SEDONA CONFERENCE. *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*. The Sedona Conference Journal, 2018.

- REDGRAVE, J. D.; MORAN, K. *The Electronic Discovery Reference Model (EDRM) and the Use of Technology in eDiscovery*. Duke Law Journal, 2017.

- BALL, C. E. *The eDiscovery Primer: The Essentials of eDiscovery Law*. Jones McClure Publishing, 2012.

- SCHEINDLIN, S. A.; CAPRA, D. J. *Electronic Discovery and Digital Evidence in a Nutshell**. West Academic Publishing, 2009.

²²⁶ Cfr. "eDiscovery for Corporate Counsel" (2022) da Thomson Reuters.

II. Análise preditiva

Algoritmos de ML são usados para prever quais documentos serão relevantes para um caso específico. Isso reduz significativamente o tempo e o custo associados à revisão manual. A análise preditiva envolve a criação de modelos baseados em dados históricos e a aplicação desses modelos para identificar documentos pertinentes de forma automatizada. Estes modelos podem identificar padrões complexos e relações subtis nos dados que podem não ser evidentes para revisores humanos.

III. Extração de entidades e análise semântica

Ferramentas de IA podem extrair entidades específicas (como nomes, datas, locais) e realizar análises semânticas para entender o contexto dos documentos, facilitando a identificação de informações cruciais. A análise semântica vai além das palavras-chave, capturando o significado subjacente e as relações entre os termos. Isso é particularmente útil em casos complexos onde o contexto e as nuances dos documentos são críticos.

IV. Análise de comunicação

IA e ML podem ser usados para mapear redes de comunicação e identificar padrões de interação entre indivíduos, revelando relacionamentos e fluxos de informação que podem ser relevantes para um caso. Isso inclui a análise de e-mails, mensagens instantâneas e outros registros de comunicação.

4. Benefícios da IA e do ML na descoberta eletrônica

São vários os benefícios da IA e do ML na descoberta eletrônica da prova.

a. Eficiência e Economia de Tempo

- Automação: A automação de tarefas repetitivas acelera o processo de descoberta, permitindo que advogados e equipas legais se concentrem em tarefas mais estratégicas.
- Escalabilidade: Capacidade de lidar com grandes volumes de dados sem comprometer a qualidade da análise. Algoritmos de ML podem processar terabytes de informações em frações do tempo necessário para uma revisão manual.

b. Precisão e consistência

- Redução de Erros Humanos: Minimiza a possibilidade de erros associados à revisão manual, como a omissão de documentos relevantes ou a inclusão de documentos irrelevantes.

- Consistência: Garante uma aplicação uniforme dos critérios de revisão em todos os documentos, eliminando a variabilidade humana.

c. Custo-Benefício

- Redução de Custos: Diminui a necessidade de equipes grandes para revisão manual, resultando em economias significativas. As economias podem ser reinvestidas em outras áreas, como a preparação do caso ou a análise estratégica.

d. Melhoria na gestão de processos

- Organização: Ferramentas de IA ajudam a organizar grandes volumes de documentos e a manter o controle sobre prazos e tarefas, melhorando a gestão do processo e a coordenação das equipes.

Contudo, também existem desafios e limitações:

a. Complexidade dos Algoritmos

- Formação: Os algoritmos de IA e ML requerem formação extensa e adaptação contínua para diferentes tipos de dados e casos. A eficácia desses sistemas depende da qualidade dos dados de treinamento e da experiência dos analistas que supervisionam o processo.

b. Transparência e explicabilidade

- Caixa Preta: Muitos algoritmos de IA são complexos e difíceis de explicar, o que pode ser problemático num contexto jurídico, onde a transparência é essencial. É crucial que os profissionais jurídicos entendam como e porque um algoritmo chegou a uma determinada conclusão.

c. Viés e Preconceito

- Dados de treinamento: Algoritmos podem herdar vieses dos dados de treinamento, levando a decisões injustas ou imprecisas. É essencial monitorizar e mitigar esses vieses para garantir a equidade no processo de descoberta.

d. Segurança de dados

- Proteção Contra Violações: Garantir que os dados sensíveis sejam protegidos contra acessos não autorizados e violações. Medidas de segurança cibernética são essenciais para proteger a integridade dos dados.

5. Implicações éticas e legais

Falar de IA e ML, leva-nos à discussão das várias implicações éticas e legais, tais como:

1. Privacidade e Proteção de Dados

- Compliance: A implementação de IA e ML deve estar em conformidade com leis de proteção de dados, como o RGPD. O uso de dados sensíveis²²⁷ deve ser cuidadosamente regulado para evitar violações de privacidade.
- Segurança: Garantir que os dados sensíveis sejam protegidos contra acessos não autorizados e violações. Medidas de segurança informática são essenciais para proteger a integridade dos dados.

2. Responsabilidade e Accountability

- Responsabilidade Legal: Determinar quem é responsável pelas decisões tomadas por sistemas de IA²²⁸ em contextos legais. É necessário estabelecer claramente as responsabilidades dos criadores de algoritmos e dos profissionais que utilizam essas ferramentas.
- Auditoria e Supervisão: Implementar mecanismos de auditoria para monitorar o desempenho e a imparcialidade dos sistemas de IA. Auditorias regulares ajudam a garantir que os sistemas operem conforme esperado e não introduzam vieses inadvertidos.

3. Transparência²²⁹ e explicabilidade

- Justificação das Decisões: Em contextos jurídicos, é essencial que as decisões tomadas por algoritmos de IA possam ser explicadas e justificadas de forma compreensível para todas as partes envolvidas.
- Desenvolvimento Ético: Garantir que os desenvolvedores de IA sigam diretrizes éticas e considerem o impacto de suas tecnologias em questões de justiça e equidade.

6. Futuro da IA²³⁰ e do ML na Descoberta Eletrónica da Prova

O futuro da IA²³¹ e do ML na descoberta eletrónica de prova abarca as inovações Tecnológicas. Por um lado, os desenvolvimentos futuros levam-nos a previsões sobre como as tecnologias emergentes

²²⁷ Cfr. Art.9 do Regulamento Geral de Proteção de Dados.

²²⁸ Cfr. Proposta de Diretiva Do Parlamento Europeu e do Conselho relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial: eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52022PC0496

²²⁹ Cfr. Artigo 52 e 60 do Regulamento de Inteligência Artificial.

²³⁰ ASHLEY, Kevin D. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age. Cambridge University Press, 2017. ASHLEY, Kevin D. An Introductory Guide to Artificial Intelligence for Legal Professionals. Kluwer Law International, 2020.

continuarão a evoluir e influenciar a descoberta eletrônica. A integração de IA com outras tecnologias, como blockchain, pode oferecer novas formas de garantir a integridade e a autenticidade dos dados. Por outro lado, podemos ter soluções híbridas de combinação de IA com técnicas tradicionais para criar abordagens híbridas que maximizem os benefícios de ambas as metodologias.

Será também necessário a adaptação e formação. Por um lado, a formação contínua para advogados e profissionais jurídicos para acompanhar as mudanças tecnológicas é essencial. Por outro lado, programas de formação e certificação em eDiscovery e tecnologias associadas são essenciais para manter a competência profissional.

Preciso também é a educação interdisciplinar, ou seja, é necessário fomentar a colaboração entre advogados, cientistas de dados e engenheiros informáticos para desenvolver soluções mais eficazes e éticas.

Por último, a regulação e as políticas públicas. É essencial a criação de normas e diretrizes específicas para o uso de IA e ML na descoberta eletrônica da prova, garantindo que essas tecnologias sejam utilizadas de maneira justa e transparente. Além disso, deve ser feita uma análise de como as políticas públicas podem influenciar a adoção e a regulação de tecnologias de IA no campo jurídico.

O futuro da eDiscovery está intrinsecamente ligado aos avanços contínuos em IA e ML. À medida que essas tecnologias evoluem, espera-se que elas se tornem ainda mais integradas e essenciais para os processos legais. Inovações futuras podem incluir:

1. Sistemas mais Intuitivos: Ferramentas de eDiscovery que são mais fáceis de usar, com interfaces intuitivas e capacidade de auto-aprendizagem, democratizando ainda mais o acesso a essas tecnologias.
2. Melhorias em Precisão e Velocidade: Algoritmos mais avançados que podem processar dados em tempo real e com precisão ainda maior.
3. Integração de Dados Multimodais: processo de analisar e integrar dados de diversas fontes e formatos, incluindo texto, vídeo e áudio, oferecendo uma visão mais completa e contextual das provas.

²³¹ Cfr. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento Inteligência Artificial): <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689>

7. A autenticidade e integridade

A prova digital obtida por meio da IA e ML deve ser tratada com cuidado e submetida a procedimentos adequados para garantir sua autenticidade e integridade.

A autenticidade e integridade são duas questões essenciais na descoberta eletrónica da prova. Há que distinguir entre a função de autenticidade, i.e., a prova provém da fonte que é indicada, da função de integridade, i.e., a prova não sofreu qualquer modificação posterior. A autenticidade refere-se à garantia de que uma evidência eletrónica é genuína e não foi modificada ou manipulada. É fundamental garantir que os dados eletrónicos não tenham sido adulterados, para que possam ser considerados confiáveis e aceitáveis como prova em um processo legal. Para garantir a autenticidade, podem ser utilizadas técnicas como assinaturas digitais, carimbos de data e hora, criptografia e registos de auditoria.

A nova versão do Regulamento eIDAS (Regulamento de Identificação Eletrónica e Serviços de Confiança) amplia e atualiza os tipos de serviços de confiança contemplados, designadamente:

1. Assinaturas Eletrónicas: Inclui assinaturas eletrónicas qualificadas, que têm o mesmo valor legal que as assinaturas manuscritas.
2. Selos Eletrónicos: Utilizados para garantir a integridade e a origem dos dados, semelhantes às assinaturas eletrónicas, mas para entidades jurídicas.
3. Carimbos de Tempo Eletrónicos: Fornecem uma prova confiável da data e hora em que um documento foi criado ou modificado.
4. Serviços de Entrega Eletrónica Registrada: Garantem a entrega segura e rastreável de documentos eletrónicos, fornecendo provas de envio e receção.
5. Certificados de Autenticação de Websites: Verificam a autenticidade dos websites, assegurando uma comunicação segura entre o navegador e o site.
6. Serviços de Arquivo Eletrónico: Novos serviços qualificados para o armazenamento seguro e a longo prazo de documentos eletrónicos.
7. Gestão de Assinaturas e Selos à Distância: Serviços que permitem a criação de assinaturas e selos eletrónicos de forma remota e segura.

Esses serviços²³² visam aumentar a confiança e a segurança nas transações eletrónicas em toda a União Europeia, promovendo a interoperabilidade e a aceitação mútua entre os Estados-Membros.

²³² Cfr. Artigos 22º, 24º, 34º, 35º, 40º, 43º e 45º do do Regulamento eIDAS.

A integridade envolve a protecção dos dados eletrónicos contra modificações não autorizadas. É importante garantir que os dados eletrónicos permaneçam intactos e não tenham sido alterados ao longo do tempo. Para garantir a integridade dos dados, podem ser utilizadas técnicas como códigos de hash, que são valores numéricos únicos gerados a partir dos dados e que podem ser usados para verificar se houve alterações nos dados originais.

No contexto da descoberta eletrónica da prova, tanto a autenticidade quanto a integridade são fundamentais para garantir a confiabilidade das evidências eletrónicas apresentadas num processo judicial. É importante que as ferramentas e técnicas utilizadas na descoberta eletrónica sejam capazes de preservar a autenticidade e integridade dos dados, garantindo a sua validade como prova. Além disso, é necessário seguir procedimentos adequados para a recolha, preservação e manipulação das evidências eletrónicas, a fim de evitar qualquer suspeita de manipulação ou adulteração.

A integração da IA e do ML na descoberta eletrónica da prova oferece uma série de benefícios, incluindo maior eficiência, precisão e redução de custos. as técnicas de IA e ML podem desempenhar um papel importante no apoio à tomada de decisão. Ao analisar grandes volumes de dados e identificar padrões, o machine learning pode fornecer informações valiosas que auxiliam na tomada de decisões mais informadas e precisas.

No entanto, esses avanços também trazem desafios técnicos, éticos e legais que precisam ser cuidadosamente geridos. À medida que a tecnologia continua a evoluir, a comunidade jurídica deve adaptar-se e adotar práticas que garantam a justiça e a equidade no processo de descoberta eletrónica. Contudo, a IA e ML na descoberta eletrónica da prova não substitui os profissionais jurídicos. A interpretação legal e a tomada de decisões finais continuam a ser responsabilidade humana. A IA e ML devem actuar como uma ferramenta auxiliar, fornecendo informações e agilizando o trabalho dos profissionais, mas a supervisão humana é essencial para garantir a precisão²³³ e a conformidade com as leis e regulamentos aplicáveis.

²³³ Cfr. Art. 22 do Regulamento Geral de Proteção de Dados.

Capítulo IV - Exemplos práticos

Exemplo 1: Uso de IA no Caso Enron²³⁴

O caso Enron é um dos mais conhecidos de aplicação de eDiscovery nos EUA. Neste processo a IA foi utilizada para processar milhões de e-mails e documentos internos. Através de algoritmos de aprendizagem supervisionada, os investigadores puderam identificar rapidamente padrões de fraude e comunicação suspeita. A tecnologia de análise preditiva ajudou a priorizar documentos relevantes, acelerando o processo de revisão e reduzindo significativamente os custos.

O processo Enron, que veio a público no início dos anos 2000, é um dos exemplos mais significativos de insolvência corporativa e fraude contabilística na história dos Estados Unidos. A Enron Corporation, uma gigante no setor de energia, foi descoberta a manipular os seus relatórios financeiros para esconder dívidas e inflacionar os lucros. A queda da empresa levou à perda de bilhões de dólares em investimentos e à destruição de milhares de empregos.

No caso Enron, a quantidade de dados eletrónicos a ser analisada era enorme. Aproximadamente 1,6 milhão de e-mails, documentos financeiros, e outros registos eletrónicos precisavam ser analisados. A aplicação de eDiscovery foi crucial para gerir e processar essa vasta quantidade de informações.

A aplicação de eDiscovery no caso Enron envolveu várias etapas críticas e o uso de tecnologias avançadas para garantir a eficiência e a precisão na análise dos dados:

- Recolha e preservação de dados: A primeira etapa envolveu a recolha e a preservação de dados relevantes. Equipas de peritos em forense digital foram mobilizadas para garantir que todos os registos eletrónicos fossem capturados e preservados de maneira segura, evitando qualquer risco de adulteração ou perda de dados.
- Indexação e catalogação: Com o uso de softwares de eDiscovery, os dados foram indexados e catalogados para facilitar a busca e a recuperação. Ferramentas como o EnCase²³⁵ foram utilizadas para criar uma estrutura organizada dos dados recolhidos.
- Revisão Assistida por Tecnologia (TAR): Devido ao volume massivo de dados, a Revisão Assistida por Tecnologia (TAR) desempenhou um papel crucial. Algoritmos de aprendizagem supervisionada foram

²³⁴ [Pesquisar | Distrito Sul do Texas \(uscourts.gov\)](https://www.uscourts.gov/research-and-publications)

²³⁵ EnCase é uma ferramenta de análise forense digital utilizada para conduzir investigações forenses digitais em computadores, dispositivos móveis e redes. Desenvolvida pela Guidance Software (agora parte da OpenText), a EnCase é reconhecida por sua capacidade de recolher, preservar, analisar e apresentar dados eletrónicos de maneira forensicamente sólida.

treinados para identificar padrões e classificar documentos com base na relevância para o caso. Isso incluiu a análise de linguagem natural para identificar palavras-chave e contextos importantes.

Um dos aspectos mais críticos do eDiscovery no caso Enron foi a análise de comunicação. Ferramentas de IA e ML foram usadas para mapear redes de comunicação interna e identificar padrões de interação entre os funcionários da Enron. Isso ajudou a revelar como os executivos da empresa estavam a colaborar para manipular os dados financeiros.

A análise de e-mails internos revelou comunicações entre executivos-chave discutindo estratégias para esconder dívidas através de entidades com um propósito específico. Essas evidências foram fundamentais para demonstrar a intenção fraudulenta e a colaboração entre os envolvidos.

A extração de entidades e a análise semântica foram utilizadas para identificar e relacionar nomes, datas, locais e eventos importantes. Isso ajudou a contextualizar as ações dos executivos da Enron dentro da cronologia do escândalo.

Através da análise semântica, foi possível correlacionar documentos financeiros adulterados com e-mails internos, discutindo a necessidade de "ajustes" contábilísticos, proporcionando uma visão clara de como e quando as fraudes foram executadas.

As provas recolhidas e analisadas foram produzidas de acordo com os requisitos legais e apresentadas em tribunal. O uso de eDiscovery garantiu que as provas fossem organizadas de maneira lógica e acessível, facilitando sua compreensão e utilização pelos advogados e pelo tribunal.

A aplicação de eDiscovery no caso Enron teve um impacto significativo na resolução do caso:

- Revelação de fraudes: A análise detalhada dos e-mails e documentos internos revelou a extensão da fraude contábil e a conivência dos executivos da Enron, incluindo o CEO Jeffrey Skilling e o CFO Andrew Fastow.
- Provas cruciais: As provas obtidas através do eDiscovery foram cruciais para as condenações dos executivos envolvidos. A capacidade de correlacionar comunicações internas com documentos financeiros adulterados foi fundamental para construir o caso contra os acusados.
- Precedente legal: O caso Enron estabeleceu um importante precedente para o uso de eDiscovery em litígios complexos, demonstrando como a tecnologia pode ser usada para gerir e analisar grandes volumes de dados eletrônicos de forma eficaz.

Recorrendo ao processo Enron destacamos a importância do eDiscovery em litígios corporativos complexos. A capacidade de recolher, preservar, analisar e apresentar grandes volumes de dados eletrônicos foi crucial para a resolução do caso e para a obtenção de justiça. O uso de IA na revisão e análise de documentos não só acelerou o processo, mas também garantiu a precisão e a integridade

das provas apresentadas. Este caso serve como um exemplo claro do potencial transformador do eDiscovery no campo jurídico.

Exemplo 2: Revisão de documentos no Caso de Antitruste da Microsoft²³⁶

O caso antitruste contra a Microsoft, iniciado em 1998, é um dos litígios mais significativos da história da tecnologia e do direito empresarial. O Departamento de Justiça dos Estados Unidos (DOJ) e 20 estados processaram a Microsoft, acusando a empresa de práticas monopolistas e anticompetitivas, especialmente em relação ao seu sistema operacional Windows e ao navegador Internet Explorer.

No caso Microsoft, a quantidade de dados eletrônicos a ser analisada foi imensa. Milhões de e-mails, documentos internos, comunicações empresariais e códigos de software foram analisados. A aplicação de eDiscovery foi essencial para gerir e processar essa vasta quantidade de informações de maneira eficiente e precisa.

A aplicação de eDiscovery no caso Microsoft envolveu várias etapas e o uso de tecnologias avançadas para garantir a eficiência e a precisão na análise dos dados:

- Recolha e preservação de dados: A primeira etapa envolveu a recolha e preservação de dados relevantes. Equipas de peritos em forense digital garantiram que todos os registos eletrónicos fossem capturados e preservados de maneira segura, evitando qualquer risco de adulteração ou perda de dados.
- Indexação e catalogação: Utilizando softwares de eDiscovery, como o Concordance²³⁷ e o Summation²³⁸, os dados foram indexados e catalogados para facilitar a busca e a recuperação. Esses softwares permitiram a criação de uma estrutura organizada dos dados recolhidos, agilizando a análise subsequente.
- Revisão Assistida por Tecnologia (TAR): Devido ao volume massivo de dados, a Revisão Assistida por Tecnologia (TAR) desempenhou um papel crucial. Algoritmos de aprendizagem supervisionada foram

²³⁶ [Antitrust Division | U.S. V. Microsoft: Court's Findings Of Fact \(justice.gov\)](#)

²³⁷ Concordance é uma ferramenta de software utilizada para a revisão e análise de documentos, principalmente em contextos de eDiscovery. Desenvolvida para ajudar advogados, revisores de documentos e profissionais de compliance, Concordance facilita a organização, indexação, busca e revisão de grandes volumes de dados eletrónicos. Concordance permite a indexação de documentos de diferentes formatos, incluindo emails, PDFs, documentos do Microsoft Office e outros arquivos eletrónicos. A indexação facilita a rápida recuperação de informações durante a revisão de documentos.

²³⁸ Summation é uma solução de software de eDiscovery desenvolvida pela AccessData, projetada para ajudar advogados, revisores de documentos e profissionais de compliance a gerir, rever e analisar grandes volumes de dados eletrónicos durante processos judiciais e investigações. A ferramenta é amplamente utilizada para organizar, pesquisar, rever e produzir documentos eletrónicos de maneira eficiente e eficaz. Summation permite a indexação de uma ampla variedade de formatos de documentos, incluindo emails, PDFs, documentos do Microsoft Office e outros arquivos eletrónicos. A indexação facilita a rápida recuperação de informações e a revisão de documentos durante investigações e litígios.

treinados para identificar padrões e classificar documentos com base na relevância para o caso. Isso incluiu a análise de linguagem natural para identificar palavras-chave e contextos importantes.

A análise de comunicação foi um aspecto crítico do eDiscovery no caso Microsoft. Ferramentas de IA e ML foram usadas para mapear redes de comunicação interna e identificar padrões de interação entre os funcionários da Microsoft. Isso ajudou a revelar como os executivos da empresa estavam colaborando para implementar práticas anticompetitivas.

A análise de e-mails internos revelou comunicações entre executivos da Microsoft discutindo estratégias para integrar o Internet Explorer ao Windows, dificultando a instalação de navegadores concorrentes. Essas evidências foram fundamentais para demonstrar a intenção monopolista da Microsoft.

A extração de entidades e a análise semântica foram utilizadas para identificar e relacionar nomes, datas, locais e eventos importantes. Isso ajudou a contextualizar as ações dos executivos da Microsoft dentro da cronologia do caso.

Através da análise semântica, foi possível correlacionar documentos internos a discutir a exclusividade do Internet Explorer com as práticas de licenciamento da Microsoft que impediam a instalação de navegadores concorrentes em computadores novos.

As evidências obtidas e analisadas foram produzidas de acordo com os requisitos legais e apresentadas em tribunal. O uso de eDiscovery garantiu que as provas fossem organizadas de maneira lógica e acessível, facilitando sua compreensão e utilização pelos advogados e pelo tribunal.

A aplicação de eDiscovery no caso Microsoft teve um impacto significativo na resolução do caso:

- Revelação de práticas anticompetitivas: A análise detalhada dos e-mails e documentos internos revelou a extensão das práticas anticompetitivas da Microsoft, incluindo estratégias para integrar o Internet Explorer ao Windows e excluir navegadores concorrentes.
- Provas cruciais: As provas obtidas através do eDiscovery foram cruciais para as condenações. A capacidade de correlacionar comunicações internas com ações estratégicas foi fundamental para construir o caso contra a Microsoft.
- Precedente legal: O caso Microsoft estabeleceu um importante precedente para o uso de eDiscovery em litígios antitruste, demonstrando como a tecnologia pode ser usada para gerir e analisar grandes volumes de dados eletrônicos de forma eficaz.

O caso antitruste contra a Microsoft destaca a importância do eDiscovery em litígios corporativos complexos. A capacidade de recolher, preservar, analisar e apresentar grandes volumes de dados eletrônicos foi crucial para a resolução do caso e para a obtenção de justiça. O uso de IA e ML na revisão e análise de documentos não só acelerou o processo, mas também garantiu a precisão e a

integridade das provas apresentadas. Este caso serve como um exemplo claro do potencial transformador do eDiscovery no campo jurídico. No caso antitruste contra a Microsoft, a TAR 1.0 foi usada para analisar um enorme volume de e-mails e documentos internos. Utilizando técnicas de recuperação de informações, os documentos foram classificados por relevância com base em um conjunto inicial de documentos previamente analisados por revisores humanos. Isso permitiu que a equipa jurídica concentrasse os esforços nos documentos mais pertinentes, economizando tempo e recursos.

Conclusão

A prova digital tornou-se uma peça-chave nos processos judiciais modernos, refletindo a crescente digitalização das nossas vidas e transações. Em Portugal, a descoberta eletrónica de provas tem evoluído significativamente, acompanhando as tendências globais e as exigências locais do sistema judiciário. Este avanço permite uma abordagem mais eficiente e precisa na recolha, análise e apresentação de informações eletrónicas, facilitando a resolução de litígios complexos que envolvem grandes volumes de dados digitais.

A descoberta eletrónica, ou ediscovery, refere-se ao processo de identificação, recolha e análise de informações digitais para serem usadas como evidência legal. Este processo é crucial para a investigação e resolução de litígios, permitindo que informações armazenadas eletronicamente (ESI - Electronically Stored Information) sejam recuperadas e apresentadas em tribunal. Em Portugal, a adoção de práticas de eDiscovery tem permitido maior eficiência na recolha e gestão de provas digitais, embora ainda existam desafios quanto à padronização e regulamentação desses processos. A adaptação a esses desafios é essencial para assegurar que as provas digitais sejam recolhidas de maneira ética e legal, preservando a integridade e a autenticidade das informações.

A integração de tecnologias de IA e ML na descoberta eletrónica tem potencializado a eficácia e a precisão na análise de grandes volumes de dados. Estas tecnologias oferecem diversas vantagens que transformam a forma como as evidências são geridas. Algoritmos de IA podem automatizar a triagem e classificação de dados, reduzindo significativamente o tempo e o esforço necessários para analisar grandes quantidades de informações. Além disso, ferramentas de ML podem identificar padrões e prever a relevância de dados específicos, auxiliando na localização de provas cruciais que poderiam ser negligenciadas por métodos tradicionais. A capacidade de detectar comportamentos anómalos e possíveis fraudes aumenta a segurança e a confiabilidade das provas digitais, tornando o processo judicial mais robusto.

Apesar dos benefícios, a utilização de IA e ML na descoberta eletrónica apresenta desafios importantes. É essencial que os sistemas de IA sejam transparentes e suas decisões explicáveis para garantir que as partes envolvidas compreendam como as provas foram selecionadas e analisadas. A recolha e análise de grandes volumes de dados pessoais devem ser conduzidas em conformidade com as

regulamentações de privacidade, como o Regulamento Geral de Proteção de Dados (RGPD). Os algoritmos de IA devem ser rigorosamente testados e monitorizados para evitar vieses que possam comprometer a imparcialidade e a justiça do processo judicial. Assim, a adoção de IA e ML na descoberta eletrônica exige um equilíbrio cuidadoso entre inovação tecnológica e responsabilidade ética.

Em Portugal, a adoção de IA e ML na descoberta eletrônica está ainda em fase de crescimento, com um potencial significativo para transformar o sistema judiciário. A formação de profissionais do direito em tecnologias digitais e a criação de regulamentações específicas para a utilização dessas ferramentas serão fundamentais para maximizar os benefícios e mitigar os riscos associados. A formação contínua e a colaboração entre juristas e tecnólogos são cruciais para a implementação bem-sucedida dessas tecnologias. O desenvolvimento de uma infraestrutura legal que suporte a integração de IA e ML garantirá que o sistema judicial português possa enfrentar os desafios e aproveitar as oportunidades oferecidas pela era digital.

A evolução da prova digital e a incorporação de tecnologias avançadas como IA e ML representam um marco significativo no sistema judicial português. Essas inovações têm o potencial de aumentar a eficiência, precisão e justiça nos processos judiciais. No entanto, é crucial que a implementação dessas tecnologias seja acompanhada de regulamentações adequadas e considerações éticas para garantir que a integridade e a equidade do sistema judicial sejam mantidas. A harmonização entre progresso tecnológico e princípios éticos será a chave para assegurar que a justiça continue a ser servida de maneira justa e eficaz no contexto de um mundo cada vez mais digitalizado.

Assim, a descoberta eletrônica de provas e a utilização de IA e ML não apenas aprimoram a capacidade de lidar com dados complexos e volumosos, mas também destacam a necessidade de uma abordagem prudente e equilibrada na aplicação dessas tecnologias. A jornada de Portugal rumo a um sistema judicial mais moderno e eficiente dependerá da capacidade de integrar essas inovações de maneira responsável, garantindo que o avanço tecnológico seja sempre guiado pelos valores fundamentais de justiça e equidade.

A adoção de regulamentações específicas para o processo de eDiscovery no sistema jurídico português, inspiradas em práticas americanas, poderia garantir uma gestão mais eficaz e equitativa de

processos que envolvem documentos eletrônicos. Normas que definam claramente o ônus da prova, os formatos de produção e a proporcionalidade no tratamento de dados podem fortalecer a conformidade e preservar a igualdade das partes, respondendo de forma adequada às demandas jurídicas da era digital.

Seria importante incluir uma norma específica no Código de Processo Civil que defina o ônus da prova em processos que envolvem eDiscovery. Esta norma estabeleceria que a parte detentora de documentos eletrônicos relevantes tem a obrigação de preservá-los e produzi-los conforme solicitado, sob pena de sanções. Inspirada na Regra 37(e) do FRCP, esta norma poderia prever sanções graduadas, aplicadas caso a parte responsável pela preservação falhe em mantê-los. Sanções poderiam variar desde advertências e presunções adversas até a exclusão de defesas ou provas, conforme a gravidade da violação. Assim, seria possível promover uma gestão responsável e transparente de documentos eletrônicos, assegurando que as partes preservem informações que podem ser cruciais para a resolução do litígio.

Seria também importante incluir um procedimento de conferência obrigatória inicial no Código de Processo Civil, em que as partes, à semelhança da Regra 26 (f) do FRCP, devem discutir e tentar chegar a um acordo sobre as diligências de descoberta eletrônica da prova e os formatos de produção de documentos eletrônicos, de modo a garantir acessibilidade, eficiência e igualdade das partes. Caso as partes não cheguem a um consenso, o juiz poderá determinar o formato de produção com base em critérios de razoabilidade e acessibilidade, semelhantes às práticas da Regra 34 do FRCP. Assim, seria possível evitar disputas relacionadas a formatos e garantir que as partes não sejam oneradas desnecessariamente devido à complexidade dos dados ou à necessidade de conversão de formatos. Isso asseguraria uma produção de dados que respeita a igualdade das partes.

Seria ainda importante incorporar o princípio da proporcionalidade diretamente no Código de Processo Civil português em casos de eDiscovery, inspirando-se na Regra 26(b)(1) do FRCP. Esse princípio permitiria que o tribunal avalie o esforço, custo e recursos de uma parte em relação ao valor e importância dos documentos eletrônicos para o caso. O tribunal teria a autoridade para limitar pedidos de produção que imponham uma carga desproporcional a uma das partes, considerando a relevância do dado solicitado, a possibilidade de acesso e os custos envolvidos. Assim, seria possível assegurar que as partes não sejam sobrecarregadas injustamente com obrigações de produção excessivas, mantendo uma igualdade processual e favorecendo o acesso à justiça de maneira equitativa.

Por fim, seria importante incluir uma norma específica que defina padrões de segurança e privacidade para o tratamento de dados eletrónicos em processos judiciais. Esta norma garantiria que as partes implementem medidas adequadas de segurança e confidencialidade, especialmente quando dados sensíveis estão envolvidos. Inspirada na legislação europeia de proteção de dados, como o Regulamento Geral de Proteção de Dados (RGPD), essa norma garantiria que os dados em eDiscovery sejam protegidos contra acessos não autorizados e manipulação. Assim, seria possível proteger a privacidade e a integridade dos dados eletrónicos, evitando que informações sensíveis ou confidenciais sejam expostas ou manipuladas durante o processo de eDiscovery.

Estas sugestões permitiriam adaptar o direito processual português aos desafios da era digital. A inclusão de normas específicas para eDiscovery que abordem o ónus da prova, formatos de produção, proporcionalidade e privacidade dos dados pode contribuir para uma prática jurídica mais eficiente e justa, garantindo que a gestão de documentos eletrónicos em processos judiciais respeite os princípios de igualdade e acesso aos tribunais.

Bibliografia

- ALEXANDRE, Isabel. Provas Ilícitas em Processo Civil. 1ª edição. Coimbra: Almedina, 1998.
- ALMEIDA, Francisco Manuel Lucas Ferreira de, Direito Processual Civil, Vol. I Coimbra, Edições Almedina, 2ª Edição, 2018
- ALMEIDA, João Gomes. *A Regulação das Assinaturas e Certificados Eletrónicos: Da Diretiva 1999/93/CE ao Regulamento eIDAS*. Lisboa: Leya, 2017.
- ANDRADE, Francisco. Da contratação eletrónica - em particular da contratação eletrónica Inter-sistémica inteligente. Universidade do Minho, Braga, 2008.
- ANDRADE, Francisco. Derecho, nuevas tecnologías e Inteligencia Artificial. Editorial DYKINSON, 2023.
- ANDRADE, Francisco. Identificação eletrónica, assinatura e serviço de confiança. UNIO - EU Law Journal. Vol. 4, No. 2, 2018.
- ANDRADE, Francisco (2019). O documento eletrónico revisitado face ao Regulamento (EU) nº 910/2014 (Regulamento EIDAS). In Jornadas Comemorativas dos 25 anos EDUM, Direito e Pessoa no Mundo Digital.
- ANDRADE, Francisco, “Consideração Jurídica das Assinaturas Dinâmicas no Ordenamento Jurídico Português” in *in Memórias do XVI Congresso Ibero Americano de Derecho e Informática*, Quito, 2012.
- ANDRADE, Francisco e Silva, Marina. O documento eletrónico: suporte e formato. Revista da Ordem dos Advogados (ROA), Ano 81, Vol. III/IV, Jul./Dez, 2021.
- ANDRADE, Francisco. Assinatura digital: conceito e risco futuro. In Joana Covelo de Abreu et al. (Coords.), O Contencioso da União Europeia e a cobrança transfronteiriça de créditos: compreendendo as soluções digitais à luz do paradigma da Justiça eletrónica europeia (e-Justice), Volume III, Coleção UNIO E-book, Escola de Direito, 2022.
- ANDRADE, Francisco e Bacelar Almeida, José Carlos (2024). Digital Signatures and Quantum Computing. In Legal Developments in Cybersecurity and Related Fields, Springer.
- ANDRADE, Francisco. Comunicações Eletrónicas e direitos humanos: o perigo do homo connectus” in MONTE, MÁRIO FERREIRA & TARSO, BRANDÃO, Direitos Humanos e a sua efetivação na Era da Transnacionalidade, 1.ª ed., Curitiba, Juruá Editora, 2012.
- ANDRADE, José Carlos Vieira de. Os Direitos Fundamentais na Constituição Portuguesa de 1976. Coimbra: Almedina, 2010.

- ANDRADE, Manuel de. Noções elementares de processo civil, Coimbra Editora, 1979.
- ASCENSÃO, José Oliveira. O Direito: Introdução e Teoria Geral. 10ª edição. Coimbra: Almedina, 1997
- ASCENSÃO, José Oliveira de. Direito Civil: Teoria Geral, Vol. III. Coimbra: Coimbra Editora, 2002.
- ASHLEY, Kevin D. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age. Cambridge University Press, 2017.
- ASHLEY, Kevin D. An Introductory Guide to Artificial Intelligence for Legal Professionals. Kluwer Law International, 2020.
- BALL, C. E. The eDiscovery Primer: The Essentials of eDiscovery Law. Jones McClure Publishing, 2012.
- Ball, C. (2016). "The Data Detective's Toolkit: A Guide to the Effective Use of eDiscovery." Self-published.
- BALKE, Tina; NOVAIS, Paulo; ANDRADE, Francisco, Torsten Eymann "From Real-World Regulations to Concrete Norms for Software Agents – A case-based reasoning approach", in proceedings of Legal and Negotiation Decision Support Systems Workshop at the 12th International Conference on Artificial Intelligence and Law, Barcelona, Junho 2009.
- BARBOSA, Ana Raquel; PASSOS, Márcia Passos; MACHADO, Susana Sousa, A análise concetual da Prova em processo civil, ULP Law Review, Revista de Direito da ULP, Vol. 14, nº 1.
- BARFIELD, W., & Pagallo, U. (2020). "Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice." Springer Nature
- BHOSALE, Narayan P. (2021). *Evidence Recovery using EnCase and FTK in Forensic Computing Investigation*. International Journal of Scientific Research in Computer Science and Engineering.
- Bordone, R. C., & Barrett, J. W. (2007). "The Negotiation Within: The Impact of Internal Conflict Over the Format of Electronic Discovery on the Fairness of Litigation."
- BRANDÃO, Diogo. A prova digital no processo civil: repensar o sistema, Nova Causa Edições Jurídicas, 2020.
- BRUNDAGE, Miles; AVIN, Shahrar; CLARK, Jack; TONER, Helen; ECKERSLEY, Peter; GARFINKEL, Ben; DAFOE, Allan; SCHARRE, Paul; ZEITZOFF, Thomas; FILAR, Bobby; ANDERSON, Hyrum; ROFF, Heather; ALLEN, Gregory C.; STEINHARDT, Jacob; FLYNN, Carrick;

- HÉIGEARTAIGH, Seán Ó; BEARD, Simon; BELFIELD, Haydn; FARQUHAR, Sebastian; LYLE, Clare; CROOTOF, Rebecca; EVANS, Owain; PAGE, Michael; BRYSON, Joanna; YAMPOLSKIY, Roman; AMODEI, Dario. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. 1ª edição. Oxford: Oxford University, 2018.
- CANOTILHO, J. J. Gomes. *Direito Constitucional e Teoria da Constituição*. 7ª Edição. Coimbra: Almedina, 2018.
 - CASTRO, Anselmo de. *Lições de processo civil*, vol. IV. 1ª Edição. Coimbra: Atlântida, 1969.
 - CASTRO, Catarina Semedo de. *Direito da Informática, Privacidade e Dados Pessoais*. Almedina, 2005.
 - CASTRO, Catarina Sarmiento e. 40 anos de 'Utilização da Informática' - o artigo 35.º da Constituição da República Portuguesa. ePública: Revista Eletrónica de Direito Público. Lisboa. ISSN 2183-184X. vol. 3. nº 3, 2016.
 - COHEN, Adam I; LENDER, David J. "Electronic Discovery: Law and Practice". Wolters Kluwer in New York, 2017.
 - CONDE CORREIA, João. "Prova digital: Enquadramento legal". Centro de Estudos Judiciários, 2018.
 - CORREIRA, Têssia Matias, *in* A Prova no Processo Civil - Reflexões sobre o problema da (in)admissibilidade da prova ilícita; Coimbra, 2015.
 - CORMEN, T. H., Leiserson, C. E., RIVEST, R. L., & Stein, C. (2009). "Introduction to Algorithms." MIT Press
 - Doshi-Velez, F., & Kim, B. (2017). "Towards a rigorous science of interpretable machine learning."
 - DUMORTIER, Jos e Vandezande, Niels. "Critical observations on the proposed Regulation for electronic identification and trust services for electronic transactions in the internal market", 2013.
 - FERNANDEZ, Elisabeth. *Um Novo Código de Processo Civil? Em busca das diferenças*. Vida Económica, 2014.
 - FERNANDEZ, Elisabeth. *A prova difícil ou impossível*. In *Estudos em homenagem ao Prof. Doutor José Lebre de Freitas*. 1.ª edição. Coimbra: Coimbra Editora, 2013.
 - FREITAS, J. L. de. *Código de Processo Civil Anotado - Volume 2.º Artigos 362.º a 626.º*. Coimbra: Coimbra Editora, 2019.

- FREITAS, José Lebre de. Introdução ao processo civil, conceitos e princípios gerais à luz do novo código. 4ª Edição. Coimbra: Gestegal, 2017.
- FREITAS, José Lebre de. A Falsidade no Direito Probatório. Almedina, 2013.
- FREITAS, Lebre de. A Ação Declarativa à Luz do Código de Processo Civil de 2013, 3ª ed., Coimbra Editora.
- FREITAS, José Lebre de; ALEXANDRE, Isabel. Código de Processo Civil Anotado, Volume 2.º, 3.ª Edição, 2017.
- GENSLER, S., & Rosenthal, L. (2018). "Rule 26(b)(1) and the Proportionality Revolution." *The Review of Litigation*
- GONÇALVES, João Gama. A prova digital em 2017 – Reflexões sobre algumas insuficiências processuais e dificuldades da investigação. Artigo da CEDIS Working Papers - Universidade Nova de Lisboa. Lisboa, 2017.
- GONÇALVES, Marco Carvalho. Notas sobre o regime transitório de aplicação do novo Código de Processo Civil, in *Cadernos de Direito Privado*, n.º 44, Outubro-Dezembro de 2013;
- GOODMAN, B., & Flaxman, S. (2017). "European Union regulations on algorithmic decision-making and a "right to explanation." *AI Magazine*;
- GREINIG, Jay E.; GLEISNER, William C. *eDiscovery & Digital Evidence*. Thomson West, 2023-2024.
- GROSSMAN, M. R., & Cormack, G. V. (Eds.). *The Grossman-Cormack Glossary of Technology-Assisted Review*. Federal Judicial Center, 2015.
- HÖRSTER, Heinrich Ewald e MOREIRA DA SILVA, Eva Sónia. *A Parte Geral do Código Civil Português*. Almedina, 2019.
- JOLLIFFE, I. T. (2002). "Principal Component Analysis." *Springer Series in Statistics*.
- KACEM, A.; BELACEL, N. Electronic Discovery: A Machine Learning Approach. In *Proceedings of the 6th International Conference on Control, Decision and Information Technologies (CoDIT)*, 2019.
- LOSEY, R. (2009). "Introduction to eDiscovery: New Cases, Ideas, and Techniques." *American Bar Association*.
- LA TORRE, Maria Enza. *Contributo Alla Teoria Giuridica Del Documento*, Giuffrè 2004.
- LIMA, Pires de; Varela, ANTUNES, Código Civil Anotado, Vol. I, 4ª ed., revista e atualizada, Coimbra Editora, 2011.

- LEITÃO, Hélder Martins. A prova no código de processo civil – Como a requerer (anotado e comentado). Librum Editora, 2017.
- LEITÃO, Hélder - Da instrução em processo civil das provas. 3ª edição. Coimbra: Librum Editora/Almedina, 2016.
- Lepri, B., Oliver, N., Letouzé, E., Pentland, A., & Vinck, P. (2018). "Fair, transparent, and accountable algorithmic decision-making processes."* Philosophy & Technology.
- REGO, Carlos Lopes do. *Comentários ao Código de Processo Civil*. Coimbra: Almedina, 1999
- LOSEY, R. (2016). "eDiscovery: Current Trends and Cases."
- MASSENO, Manuel David. A prova digital perante a protecção de dados pessoais – uma perspetiva Portuguesa e Europeia. Centro de Estudos Judiciários, 2018.
- MAURÍCIO, Rui. O paradigma do processo eletrónico no Direito Processual Civil português. In ASCENÇÃO, José Oliveira - Direito da Sociedade da Informação – Separata do Volume IX. 1ª edição. Coimbra: Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2011.
- MEIRELES, Isa. A prova digital no processo judicial. Universidade do Minho, Braga, 2022.
- MENDES, João de Castro. Do conceito de Prova. 1ª edição. Lisboa: Ática, 1961.
- MENDES, J. de C.; SOUSA, M. T. de. (2023). Manual de Processo Civil. Vol. I & II. AAFDL Editora.
- MICHELS, D. eDiscovery: An Introduction to Digital Evidence. American Bar Association, 2015.
- MITTELSTADT, B., Allo, P., TADDEO, M., Wachter, S., & Floridi, L. (2016). "The ethics of algorithms: Mapping the debate." Big Data & Society
- MOREIRA, José Carlos Barbosa, — Processo Civil Contemporâneo - Um enfoque comparativo” in Scientia Iuridica, Revista de Direito Comparado Português e Brasileiro, Tomo LV, n.º 305, 2006
- Moore, S. (2014). "Predictive Coding and the Future of eDiscovery."
- 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 (e-book). 2ª Edição. Lisboa: Centro de Estudos Judiciários (CEJ), 2013.
- NOVAIS, Jorge Reis, Os princípios constitucionais estruturantes da República Portuguesa, 1.ª Ed. (Reimpressão), Coimbra Editora, Coimbra, 2014.
- O Novo Processo Civil - Contributos da doutrina para a compreensão do novo código de processo civil. Centro de Estudos Judiciários, Caderno I, 2ª Ed., 2013.

- OLSON, Bruce A. Electronic Discovery for Small Cases: Managing Digital Evidence and ESI. Chicago, Ill.: American Bar Association, Law Practice Management Section, 2012.
- ORLANDO, de Carvalho. Teoria Geral do Direito Civil. 3ª Ed. Coimbra: Coimbra Editora, 2012.
- PIMENTA, Paulo. Processo Civil Declarativo, 2.ª ed. Coimbra, Almedina, 2018.
- PINTO, Carlos Alberto da Mota. Teoria Geral do Direito Civil. 4ª Ed., 2005.
- PIRES DE SOUSA, Luís Filipe. O valor probatório do documento eletrónico em processo civil. Almedina, 2017.
- Miguel Pupo Correia, *in* "Assinatura eletrónica e certificação digital", in "Direito da Sociedade da Informação", vol. VI, Coimbra Editora, 2006.
- RANGEL, Rui Manuel de Freitas. O Ónus da Prova no Processo Civil. 3ª Edição. Almedina, 2006.
- REDGRAVE, J. D., & Moran, K. The Electronic Discovery Reference Model (EDRM) and the Use of Technology in eDiscovery. Duke Law Journal, 2017.
- REGO, Carlos Francisco de Oliveira do. Comentários ao código de processo civil. 2004
- REIS, José Alberto dos. Código de Processo Civil Anotado, vol. III. 3ª edição. Coimbra: Coimbra Editora, 2012.
- ROCHA, Manuel Lopes; PEREIRA, Rui Soares Pereira. Inteligência artificial & Direito. Almedina, 2022.
- RODRIGUES, André Marques, in A valoração da prova em processo civil: prova legal e livre apreciação da prova.
- RODRIGUES, Fernando Pereira. Os meios da prova em processo civil. 3ª edição. Almedina, 2017.
- Russell, S., & Norvig, P. (2009). "Artificial Intelligence: A Modern Approach." Prentice Hall.
- SARTOR, G., & Sartor, C. The Impact of Machine Learning on Electronic Discovery. International Journal of Law and Information Technology. 2017.
- SARTOR, Giovanni, "Cognitive automata and the law: electronic contracting and the intentionality of software agents ", Artif Intell Law (2009)
- SCHEINDLIN, S. A.; Capra, D. J. Electronic Discovery and Digital Evidence in a Nutshell. West Academic Publishing, 2009.
- SEDONA CONFERENCE. The Sedona Canada Principles Addressing Electronic Discovery, Third Edition, 2021.
- SOUSA, Luís Filipe de, Direito Probatório Material, Coimbra, 2020, pág. 196.

- SOUSA, Miguel Teixeira de. As partes, o objecto e a Prova em processo declarativo. 1ª edição. Lisboa: Lex-Edições Jurídicas, 1995.
- SOUSA, Teixeira de; Estudos sobre o novo processo civil, 2ª edição, 1997.
- SOUSA, Miguel Teixeira de in “Introdução ao Processo Civil”, 2000.
- SOUSA, Miguel Teixeira de. O Valor Probatório dos Documentos Eletrónicos. In Direito da Sociedade da Informação – Volume II. 1ª Edição. Coimbra: Coimbra Editora, 2001.
- Surden, H. (2014). "Machine learning and law." Washington Law Review
- THE SEDONA CONFERENCE. Commentary on ESI Evidence & Admissibility. 2021.
- THE SEDONA CONFERENCE. Best Practices Addressing Data Security and Privacy in Civil Litigation, 2020
- THE SEDONA CONFERENCE. Commentary on Legal Holds, Second Edition: The Trigger & The Process, 20 SEDONA CONF. J. 341, 2019.
- THE SEDONA CONFERENCE. The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production. The Sedona Conference Journal, 2018.
- THE SEDONA CONFERENCE. Commentary on Proportionality in Electronic Discovery. 2013.
- TRINDADE, Cláudia Sofia Alves. A prova de estados subjectivos – Presunções e regras da experiência. Almedina, 2016.
- TRINDADE, Cláudia, Prova, justificação e convicção racional – A propósito do conceito de verdade proposicional no processo decisório jurisprudencial, em Estudos em Homenagem ao Professor Doutor Alberto Xavier, Assuntos Europeus, Direito Privado, Direito Público e Vária, Vol III, Edições Almedina: Coimbra, 2013.
- VALENÇA, José Manuel. Sebenta da unidade curricular de Criptografia, do Mestrado de Direito e Informática da UM, 2016.
- Varela, Antunes, Manual de Processo Civil, 2ª edição, Coimbra: Coimbra Editora, 2006.
- VARELA, Antunes - Manuel de Andrade e o ensino do processo Civil. Boletim da Faculdade de Direito. Coimbra. vol. 35, 2005.
- VARELA, Antunes; BEZERRA, J. Miguel; NORA, Sampaio E. - Manual de processo Civil. 2ª edição (reimpressão), Coimbra: Coimbra Editora, 2006.
- VASCONCELOS, Pedro Pais de. Teoria Geral do Direito Civil. 7ª Ed. Coimbra: Almedina, 2012.
- VAZ, Alexandre Pessoa- Direito Processual Civil – Do antigo ao novo Código. 2ª edição, Coimbra: Almedina, 2002.

- VENÂNCIO, Pedro. A Tutela Jurídica do Formato de Ficheiro Electrónico. Tese de doutoramento, Universidade do Minho, Braga, 2013.
- WAISBERG, Noah; HUDEK, Alexander. "AI for Lawyers: How Artificial Intelligence Is Transforming the Legal Profession". JOHN WILEY & SONS INC: 2021.
- WACHTER, S., Mittelstadt, B., & Floridi, L. (2017). "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation." *International Data Privacy Law*
- ZENG, R., & Xu, J. (2019). Machine Learning in Electronic Discovery: Foundations of a Comprehensive Workflow. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 13(2), 1-29.