

A JUSTIÇA NO MUNDO VIRTUAL

TOMO II

DESAFIOS DA PROVA DIGITAL

REVISTA JULGAR ONLINE

JULHO 2026

Índice

Rosa Lima Teixeira

9

O sistema e-Codex e a digitalização da cooperação judiciária em matéria civil e comercial: impactos nos ordenamentos jurídicos dos Estados-membros.

José Luís Lopes da Mota

20

As ordens europeias de produção e conservação de prova eletrónica em Processo Penal (Regulamento (UE) 2023/1543 e Diretiva (UE) 2023/1544): um novo caminho na resposta ao cibercrime.

Rui Cardoso

62

Regimes de conservação e utilização probatória penal de metadados de comunicações electrónicas: do passado distante ao futuro próximo, à beira do absurdo.

Luís Lemos Triunfante

141

A prova digital na jurisprudência do TJUE e portuguesa: constitucionalização, admissibilidade e dualidade de regimes.

Tiago Brandão de Pinho

172

A prova digital na jurisdição administrativa e fiscal: alguns casos decididos no TAF de Loulé.

Fernando Silva Pereira

213

A atividade de “navegação na internet” realizada pelo juiz.

Joel T. Ramos Pereira

236

Inteligência Artificial e prova em processo civil: nótulas exploratórias sobre a produção, a apresentação e a valoração da prova com conexão a sistemas de Inteligência Artificial.

Luís Paulo Reis

290

Inteligência Artificial e Estado de Direito: para uma justiça aumentada e juridicamente responsável.

Ficha Técnica

Julgar e-book

Julho 2026

Editor e proprietário

Associação Sindical dos Juizes Portugueses

Diretor

João Paulo Raposo

Diretor-adjunto

Eduardo Sousa Paiva

Coordenadores

Vitor Teixeira de Sousa

Mariana Coimbra Piçarra

Curador

Luís de Lemos Triunfante

Design

Vitor Teixeira de Sousa

Fotografia de capa

Steve A. Jonhson | Pexels

ISBN

978-989-34-0227-6

Editorial

«More people in the world now have internet access than access to justice»

Richard Susskind, *Online Courts and the Future of Justice* (2019)

A observação de Richard Susskind é, provavelmente, uma das mais citadas reflexões sobre os desafios atuais da administração da justiça — e não sem razão. Ela exprime um paradoxo que define o nosso tempo: numa sociedade cada vez mais digitalizada, a tecnologia encontra-se, com frequência, mais próxima dos cidadãos do que os próprios mecanismos institucionais criados para tutelar os seus direitos. É neste contexto que se inserem os oito estudos reunidos neste número da *Julgar*, dedicados às transformações que as tecnologias digitais vêm introduzindo na cooperação judiciária, na prova, na atividade jurisdicional e no exercício das profissões jurídicas.

A transformação digital da justiça deixou de ser uma perspectiva de futuro para se tornar uma realidade do quotidiano dos tribunais e das instituições responsáveis pela administração da justiça. A digitalização das relações económicas e sociais, a circulação global de dados, a desmaterialização dos procedimentos, a expansão da prova digital e a emergência da inteligência artificial alteraram profundamente os contextos em que o direito é produzido, interpretado e aplicado. A justiça contemporânea defronta-se, por isso, com um desafio que é simultaneamente tecnológico, jurídico e institucional: tirar partido das potencialidades da inovação sem comprometer as garantias fundamentais que constituem o núcleo do Estado de Direito. É em torno desta preocupação que convergem os estudos publicados neste segundo volume, também dedicado à digitalização, inteligência artificial e prova digital.

Uma primeira linha de reflexão respeita à construção de um espaço europeu de justiça progressivamente assente em infraestruturas digitais. Rosa Lima Teixeira analisa o sistema *e-CODEX* enquanto instrumento estruturante da cooperação judiciária digital europeia, pondo em evidência o seu papel na criação de canais seguros e interoperáveis para a comunicação entre autoridades judiciais dos Estados-Membros. Num registo complementar, José Luís Lopes da Mota debruça-se sobre o novo regime das Ordens Europeias de Produção e Conservação de Prova Eletrónica, introduzido pelo Regulamento (UE) 2023/1543 e pela Diretiva (UE) 2023/1544, mostrando como a União Europeia procura adaptar os mecanismos de cooperação judiciária às exigências da investigação criminal na era digital. Nos dois estudos ressalta uma conclusão comum: a modernização tecnológica da cooperação judiciária deixou de ser uma opção de política legislativa para se tornar uma necessidade imposta pela crescente transnacionalização da criminalidade e da informação.

No centro de vários dos trabalhos aqui publicados encontra-se a problemática da prova digital. Rui Cardoso examina os metadados das comunicações eletrónicas e os desafios que a sua conservação e utilização probatória levantam à luz da jurisprudência europeia e constitucional portuguesa. Por seu lado, Luís Lemos Triunfante percorre a evolução da jurisprudência do Tribunal de Justiça da União Europeia e dos tribunais portugueses em matéria de prova digital, identificando a progressiva constitucionalização deste domínio no processo penal e a consolidação de um regime diferenciado entre as jurisdições penal e civil. Ambos os artigos ilustram a tensão permanente entre as necessidades da investigação criminal e a proteção dos direitos fundamentais à privacidade, à proteção de dados pessoais e ao processo equitativo.

A transformação digital da prova não se manifesta, porém, apenas nos grandes debates jurisprudenciais e constitucionais. A experiência concreta dos tribunais revela uma realidade bem mais ampla e diversificada. É o que demonstra Tiago Brandão de Pinho, através da análise de casos decididos no Tribunal Administrativo e Fiscal de Loulé. O autor mostra como documentos eletrónicos, *screenshots*, ortofotomapas, sistemas de georreferenciação, perícias informáticas, inspeções a sistemas digitais e depoimentos por videoconferência passaram a integrar naturalmente a atividade instrutória dos tribunais. O estudo evidencia que muitos dos desafios colocados pela prova digital não exigem necessariamente novos institutos jurídicos, mas antes uma adaptação cuidadosa dos mecanismos probatórios tradicionais aos problemas específicos da autenticidade, integridade e fiabilidade da informação digital.

A utilização crescente da internet como instrumento auxiliar da atividade jurisdicional constitui igualmente um dos traços mais marcantes da justiça contemporânea. Fernando Silva Pereira analisa o fenómeno da chamada "cibernavegação judicial", refletindo sobre as possibilidades e os limites da utilização, pelos tribunais, de fontes de informação disponíveis em linha. O recurso a imagens de satélite, plataformas digitais, sistemas cartográficos ou bases de dados amplia significativamente os meios de que os tribunais dispõem para a reconstrução dos factos. Mas, como bem demonstra o autor, esta realidade exige uma reflexão permanente sobre o contraditório, a transparência dos métodos e a fiabilidade das fontes consultadas pelo julgador.

A etapa mais recente — e porventura mais desafiante — deste processo de transformação é representada pela inteligência artificial. Joel Timóteo Ramos Pereira analisa os múltiplos problemas que a inteligência artificial coloca ao sistema probatório contemporâneo: a autenticidade da prova digital, os riscos associados aos *deepfakes*, a explicabilidade dos sistemas algorítmicos e os novos critérios de valoração da prova produzida ou mediada por tecnologias inteligentes. O seu contributo deixa claro que a inteligência artificial não é apenas uma ferramenta tecnológica — é também uma fonte de novas interrogações jurídicas, epistemológicas e processuais.

Uma abordagem complementar é desenvolvida por Luís Paulo Reis, que propõe o conceito de "justiça aumentada" como modelo de integração equilibrada da inteligência artificial no universo jurídico. O autor destaca o potencial destes sistemas para apoiar magistrados, advogados e demais

profissionais em tarefas de pesquisa, análise documental, gestão processual e organização da informação. Ao mesmo tempo, chama a atenção para os riscos da opacidade algorítmica, do enviesamento dos dados e da erosão da responsabilidade humana nas decisões. O estudo recusa tanto a rejeição conservadora da tecnologia como o entusiasmo acrítico perante a inovação, defendendo uma utilização da inteligência artificial subordinada aos princípios fundamentais do Estado de Direito.

«Technology should be used to make the law and justice more accessible, not merely more efficient»

Richard Susskind

Esta afirmação mantém uma atualidade que vale a pena sublinhar, sobretudo num momento em que a eficiência tende a surgir como principal argumento legitimador da inovação tecnológica. Uma justiça mais rápida e mais organizada é, naturalmente, um objetivo desejável. Mas a legitimidade das transformações tecnológicas não se pode medir apenas por indicadores de produtividade ou de desempenho. A verdadeira questão é saber se essas transformações contribuem para uma justiça mais compreensível, mais transparente, mais acessível e mais efetiva na proteção dos direitos dos cidadãos. A inovação tecnológica será tanto mais valiosa quanto mais fortalecer — e não enfraquecer — a confiança das pessoas nas instituições jurídicas.

Os estudos reunidos neste número da *Julgar* mostram precisamente que a digitalização da justiça não é uma questão exclusivamente tecnológica. Trata-se, acima de tudo, de um desafio jurídico, institucional e democrático. A cooperação judiciária digital, a prova eletrónica, a utilização da internet na atividade probatória e a inteligência artificial são manifestações diversas de uma mesma transformação estrutural. E em todas elas ressurgue a mesma preocupação de fundo: garantir que o desenvolvimento tecnológico permaneça subordinado aos valores que legitimam a administração da justiça.

A justiça do futuro será, inevitavelmente, mais digital. Mas o seu sucesso não dependerá apenas da qualidade dos sistemas informáticos, da sofisticação dos algoritmos ou da rapidez das infraestruturas tecnológicas. Dependerá, sobretudo, da capacidade de preservar, nesse novo ambiente, os princípios que historicamente definem o Estado de Direito: a dignidade da pessoa humana, a proteção dos direitos fundamentais, o contraditório, a independência judicial, a transparência da decisão e a responsabilidade dos decisores. É nesse equilíbrio — sempre difícil, nunca garantido — entre inovação e garantia que reside, provavelmente, um dos maiores desafios da justiça do século XXI.

Luís Lemos Triunfante

O SISTEMA E-CODEX E A DIGITALIZAÇÃO DA COOPERAÇÃO JUDICIÁRIA EM MATÉRIA CIVIL E COMERCIAL: IMPACTOS NOS ORDENAMENTOS JURÍDICOS DOS ESTADOS-MEMBROS

Rosa Lima Teixeira: Juíza Desembargadora [\[i\]](#)

Sumário Executivo (*): (1) O artigo analisa o enquadramento jurídico do sistema **e-CODEX** no âmbito da digitalização da cooperação judiciária europeia em matéria civil e comercial, (2) examina as principais inovações introduzidas pelo pacote legislativo europeu da justiça digital e os instrumentos de cooperação abrangidos, (3) avalia os impactos do e-CODEX na organização e funcionamento dos sistemas judiciais nacionais, com destaque para a interoperabilidade, a segurança e a eficiência processual, (4) identifica os principais desafios jurídicos, tecnológicos e organizacionais associados à implementação do sistema pelos Estados-Membros, (5) analisa o estado de implementação em Portugal, evidenciando os progressos alcançados e as adaptações ainda necessárias e (6) conclui que o e-CODEX constitui a infraestrutura tecnológica central da construção de um espaço europeu de justiça digital, cuja plena concretização dependerá da implementação faseada prevista pelo direito da União e da adaptação dos sistemas nacionais.

Resumo: O presente artigo analisa o papel do sistema e-CODEX no processo de digitalização da cooperação judiciária europeia em matéria civil e comercial. Partindo do enquadramento normativo introduzido pelo pacote de digitalização da cooperação judiciária, examinam-se os seus efeitos estruturais, os principais instrumentos abrangidos, os impactos nos sistemas judiciais nacionais e os desafios de implementação. Dá-se particular atenção ao caso português, evidenciando o estado atual de implementação e as exigências de adaptação tecnológica. Conclui-se que o e-CODEX constitui um elemento central na construção de um ecossistema digital europeu da justiça, ainda que dependente de um processo progressivo de integração.

Palavras-Chave: e-CODEX; Cooperação judiciária europeia; Digitalização da justiça; interoperabilidade; Processo civil europeu.

Índice: (1) Introdução; (2) O pacote de digitalização da cooperação judiciária; (3) Instrumentos da cooperação judiciária mais afetados pela digitalização; (4) Impacto nos sistemas judiciais nacionais: reconfiguração da atividade jurisdicional; (5) Desafios de implementação, autonomia nacional e integração europeia; (6) O acesso dos particulares à justiça digital: o papel do EEAP; (7)

Calendarização e perspectivas de evolução; **(8)** A implementação em Portugal; **(9)** Condições estruturais e necessidade de adaptação tecnológica; **(10)** Conclusão.

1. Introdução

No âmbito das políticas desenvolvidas pela União Europeia com vista à simplificação e facilitação da cooperação judiciária transfronteiriça, surge o sistema e-CODEX (*e-Justice Communication via Online Data Exchange*[\[ii\]](#)), enquanto instrumento tecnológico estruturante.

Do ponto de vista organizativo, o e-CODEX assenta num modelo descentralizado, permitindo que os Estados-Membros mantenham os seus sistemas informáticos nacionais, interligados através de uma infraestrutura comum. Esta solução revela-se conforme ao princípio da autonomia processual nacional, tal como consolidado na jurisprudência do Tribunal de Justiça da União Europeia (TJUE), desde que respeitados os princípios da equivalência e da efetividade.[\[iii\]](#)

O e-CODEX constitui, assim, o principal instrumento atualmente existente para assegurar o intercâmbio eletrónico transfronteiriço de dados judiciais, de forma segura, interoperável e eficiente, evitando a substituição dos sistemas nacionais. Neste contexto, assume-se como elemento estruturante da digitalização da justiça europeia, promovendo a superação da fragmentação dos sistemas jurídicos nacionais.

Desde 3 de junho de 2024, a gestão do sistema encontra-se confiada à agência eu-LISA,[\[iv\]](#) reforçando a sua institucionalização no espaço europeu.[\[v\]](#)

Importa sublinhar que o e-CODEX não constitui um sistema processual autónomo, mas sim uma infraestrutura de interoperabilidade, baseada em componentes técnicos normalizados (*Connector e Gateway*[\[vi\]](#)). Este modelo assegura a transmissão de dados através de protocolos seguros e normalizados, mantendo os Estados-Membros o controlo sobre os seus sistemas internos.

Acresce que o sistema se caracteriza pela sua neutralidade quanto ao conteúdo, permitindo a sua utilização para múltiplos instrumentos jurídicos sem interferência na natureza dos dados transmitidos. Tal característica revela-se particularmente relevante num contexto de diversidade de regimes processuais nacionais, contribuindo para a construção de um modelo de cooperação baseado na interoperabilidade, mais do que na uniformização.

2. O pacote de digitalização da cooperação judiciária

O e-CODEX insere-se num quadro normativo mais amplo, consubstanciado no denominado pacote de digitalização da cooperação judiciária, composto, entre outros, pelo Regulamento (UE) 2023/2844 e pela Diretiva (UE) 2023/2843.

Este conjunto normativo consagra uma alteração paradigmática no funcionamento da cooperação judiciária europeia,[\[vii\]](#) ao estabelecer:

A obrigatoriedade, como regra, da comunicação eletrónica entre autoridades competentes em processos transfronteiriços;

O reconhecimento jurídico de documentos eletrónicos, assinaturas eletrónicas e selos digitais, em conformidade com o Regulamento (UE) n.º 910/2014 (eIDAS);

A admissibilidade da videoconferência em processos judiciais;[\[viii\]](#)

A criação do Ponto Europeu de Acesso Eletrónico (EEAP);

A imposição da aceitação de comunicações eletrónicas por parte dos Estados-Membros;

Pagamento eletrónico das custas (judiciais).

Este quadro representa uma evolução significativa no sentido da desmaterialização dos processos judiciais transfronteiriços, aproximando o modelo europeu das experiências mais avançadas de justiça digital.

A concretização do processo de digitalização da cooperação judiciária assenta, ainda, em mecanismos de operacionalização jurídica destinados a garantir a sua efetividade. Neste sentido, os Estados-Membros são obrigados a prestar informações à Comissão Europeia quanto aos meios de comunicação eletrónica disponíveis, as autoridades competentes e os canais utilizados para a tramitação dos procedimentos abrangidos. Esta obrigação de comunicação constitui um elemento essencial para assegurar a transparência, previsibilidade e acessibilidade do sistema, permitindo às autoridades e aos utilizadores conhecer os mecanismos disponíveis em cada jurisdição e assegurando a coerência na aplicação das normas europeias.

A relevância do processo de digitalização da justiça no espaço europeu é, aliás, expressamente sublinhada pela própria Comissão Europeia, a qual identifica a modernização digital dos sistemas judiciais como uma prioridade estratégica no âmbito da construção de uma “Europa preparada para a era digital”.[\[ix\]](#) Neste contexto, reconhece-se que os procedimentos judiciais - em particular nos casos transfronteiriços - permanecem ainda, em larga medida, dependentes de suporte em papel e de canais tradicionais de comunicação, o que compromete a eficiência do sistema e limita o acesso efetivo à justiça por parte de cidadãos e empresas.

Neste sentido, a iniciativa europeia de digitalização da justiça visa não apenas a introdução de ferramentas tecnológicas, mas antes uma transformação estrutural do modo de funcionamento dos sistemas judiciais, com particular incidência na cooperação judiciária transfronteiriça. O desenvolvimento de instrumentos como o e-CODEX insere-se, assim, numa estratégia mais ampla

destinada a promover uma justiça mais acessível, célere e adaptada às exigências de um contexto cada vez mais digitalizado.

3. Instrumentos da cooperação judiciária mais afetados pela digitalização

A digitalização promovida pelo e-CODEX incide transversalmente sobre diversos instrumentos fundamentais da cooperação judiciária em matéria civil e comercial.

Desde logo, assumem especial relevo os mecanismos relativos à citação e notificação de atos judiciais e à obtenção de prova, cuja tramitação tradicional revela frequentemente morosidades incompatíveis com as exigências de uma tutela jurisdicional efetiva.[\[x\]](#)

Por outro lado, os instrumentos destinados à execução transfronteiriça de decisões, como o título executivo europeu, a injunção europeia de pagamento e o processo europeu para ações de pequeno montante, serão particularmente beneficiados pela digitalização, permitindo uma redução significativa dos custos de transação e dos prazos processuais.[\[xi\]](#)

Igualmente relevantes são os domínios relativos às obrigações alimentares, responsabilidades parentais e regimes patrimoniais, nos quais a cooperação entre autoridades exige uma comunicação frequente e célere, sendo a digitalização determinante para a eficácia dos mecanismos previstos.[\[xii\]](#)

Por fim, os procedimentos de insolvência transfronteiriça e outros instrumentos de cooperação económica evidenciam uma forte dependência da circulação rápida e segura da informação, pelo que a implementação do e-CODEX surge como condição essencial para o seu pleno funcionamento.[\[xiii\]](#)

4. Impacto nos sistemas judiciais nacionais: reconfiguração da atividade jurisdicional

A implementação do e-CODEX implica uma transformação estrutural do funcionamento dos tribunais nacionais, inserindo-os numa rede digital europeia interligada.

Tal transformação traduz-se em ganhos ao nível da celeridade processual, da eficiência administrativa e da segurança das comunicações, contribuindo para uma maior efetividade do direito fundamental de acesso à justiça.[\[xiv\]](#)

Um dos aspetos estruturantes do e-CODEX reside nas garantias de segurança e fiabilidade das comunicações eletrónicas, assegurando a confidencialidade, integridade e autenticidade dos dados transmitidos. Este elemento é particularmente relevante no domínio da cooperação judiciária, no qual a troca de informações sensíveis exige níveis elevados de proteção jurídica e técnica.

Assim, o e-CODEX não se limita a promover a eficiência processual, antes contribuindo para a construção de um modelo de confiança digital entre autoridades nacionais, indispensável ao funcionamento do espaço judicial europeu.

5. Desafios de implementação, autonomia nacional e integração europeia

Apesar dos benefícios, a digitalização coloca desafios relevantes, nomeadamente: a adaptação das infraestruturas tecnológicas nacionais; a necessidade de assegurar a interoperabilidade entre sistemas; a formação dos operadores judiciais; a garantia de elevados padrões de proteção de dados pessoais, nos termos do Regulamento (UE) 2016/679 (RGPD).

A possibilidade de adoção de diferentes modelos de implementação (sistemas nacionais, soluções de referência ou modelos híbridos) contribui para uma maior flexibilidade, mas também impõe exigências acrescidas de coordenação. O modelo adotado permite conciliar a integração europeia com a autonomia dos Estados-Membros, evitando uma centralização excessiva.

Não estando em causa uma harmonização do direito substantivo, verifica-se, contudo, uma crescente convergência ao nível das práticas processuais e das infraestruturas tecnológicas, o que poderá, no futuro, influenciar também a evolução do direito processual interno.

O Portal de referência é fornecido pela Comissão a todos os Estados, embora os Estados possam optar por integrar no seu sistema nacional (sem usar o Portal de referência).

Portugal optou inicialmente pela implementação nacional, mas acabou por recorrer ao Portal de Referência. Ainda assim, a solução pretendida para o futuro continua a ser a implementação nacional (com a criação da respetiva infraestrutura para o adaptar no *Citius*), embora não exista, por agora, qualquer previsão para a sua concretização.

É neste Portal de Referência que são geridos os utilizadores e as permissões, bem como a estatística, o preenchimento dos formulários, e através do qual são anexados os documentos a enviar à autoridade competente de outro Estado.

Porém, para que o e-Codex funcione eficientemente em processos transfronteiriços o sistema apoia-se num diretório chamado *CDB (Court Database)*, o qual agrega informações que ajudam os utilizadores e os sistemas a, por exemplo, identificar e verificar qual é o tribunal ou autoridade competente num determinado Estado-Membro ou encaminhar e rastrear os dados do processo digitalmente.

O e-Codex será utilizado para encriptar os documentos, garantindo o seu envio seguro. Em termos práticos, o Portal de Referência liga-se ao e-Codex, que encripta a mensagem antes do envio; do lado do destinatário, o e-Codex procede à respetiva descodificação e entrega-a no Portal de

Referência (tendo o Instituto de Gestão Financeira e Equipamentos da Justiça - IGFEJ - disponibilizado um *link* próprio para o efeito).

6. O acesso dos particulares à justiça digital: o papel do EEAP

Como parte deste sistema informático descentralizado o Regulamento veio criar um «ponto de acesso eletrónico europeu» que será alojado no Portal Europeu da Justiça e que funcionará como um balcão único das informações e serviços judiciais da União. Desta forma, o Ponto Europeu de Acesso Eletrónico (EEAP) constitui um instrumento inovador, permitindo a interação direta entre particulares e autoridades judiciais de diferentes Estados-Membros. Significa isto que, é proporcionada a possibilidade de as pessoas singulares ou coletivas (bem como os seus representantes legais e autorizados) apresentarem um pedido ou comunicarem com as autoridades por via eletrónica (incluindo a citação/notificação). Embora, os meios tradicionais continuam sempre possíveis, os Estados-Membros estão obrigados a aceitar este tipo de comunicação.

Este mecanismo contribui, ademais, para a concretização do princípio do acesso efetivo à justiça, tal como consagrado no artigo 47.º da Carta dos Direitos Fundamentais da União Europeia, ao reduzir barreiras geográficas e facilitar o exercício de direitos em contexto transfronteiriço.

7. Calendarização e perspetivas de evolução

A implementação do e-CODEX seguirá uma lógica faseada, com a adoção progressiva de atos de execução e a integração gradual dos diversos instrumentos jurídicos (num total de 13 na área civil), dando-se prioridade aos instrumentos já preparados para o digital. Haverá um período transitório de 2 anos para cada implementação. A preparação começa aproximadamente 2 anos antes da data-limite para a adoção dos atos de execução.

Foi o que aconteceu nos Regulamentos de Citação/Notificação e Obtenção de Prova,[\[xv\]](#) cuja preparação se iniciou em Dezembro de 2022 e a implementação ocorreu em maio de 2025.

Em termos de calendário para integração no e-Codex dos restantes instrumentos comunitários de cooperação judiciária civil, encontra-se em fase de preparação, desde 17.01.2026, o instrumento referente ao *Procedimento europeu de injunção de pagamento*,[\[xvi\]](#) bem como o respeitante ao *Processo europeu para ações de pequeno montante*.[\[xvii\]](#) A respetiva implementação está prevista para 2028.

Seguidamente, entrarão em fase de preparação, a partir de 17 de janeiro de 2027, o instrumento comunitário relativo ao *Apoio Judiciário em processos transfronteiriços*,[\[xviii\]](#) o que instituiu o *Procedimento Europeu de Arresto de Contas Bancárias*[\[xix\]](#) e o que regula os *Processos de Insolvência Transfronteiriços*.[\[xx\]](#) A sua implementação está prevista para 2029.

Encontra-se igualmente calendarizado o início da preparação, para 17 de janeiro de 2028, do regulamento relativo às *Sucessões Internacionais*,^[xxi] bem como o relativo à *Cooperação reforçada no domínio da competência, da lei aplicável, do reconhecimento e da execução de decisões em matéria de regimes matrimoniais*^[xxii] e, ainda, o da *Cooperação reforçada em matéria de regimes matrimoniais e efeitos patrimoniais das parcerias registadas*,^[xxiii] prevendo-se a respetiva implementação em 2030.

Por sua vez, o instrumento comunitário que cria o *Título executivo europeu para créditos não contestados*,^[xxiv] bem como o relativo à *Competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial* (conhecido por *Bruxelas I - reformulado*),^[xxv] o relativo à *Competência, à lei aplicável, ao reconhecimento e à execução das decisões e à cooperação em matéria de obrigações alimentares*^[xxvi] e o relativo à *Competência, ao reconhecimento e à execução de decisões em matéria matrimonial e em matéria de responsabilidade parental e ao rapto internacional de crianças* (conhecido por *Bruxelas IIbis*)^[xxvii], têm como data de início da preparação 17 de janeiro de 2029, estando a sua implementação prevista para 2030.

Portanto, a médio prazo, é expectável a consolidação de um verdadeiro ecossistema digital europeu da justiça, no qual o e-CODEX assumirá o papel de infraestrutura nuclear.

8. A implementação em Portugal

Desde maio de 2025, a tramitação dos pedidos no âmbito dos regulamentos relativos à citação e notificação de atos judiciais e à obtenção de prova passou a ser obrigatoriamente efetuada por via eletrónica em todos os Estados-Membros, incluindo Portugal.

Para esse efeito, os Estados-Membros procederam à atualização da *Court Database*, com referência a 31 de dezembro de 2024, identificando todas as entidades requerentes e requeridas com competência para enviar e/ou receber pedidos de citação e notificação, bem como de obtenção de prova — designadamente, os tribunais de 1.ª instância. Consequentemente, as entidades não incluídas naquela base de dados deixaram de poder apresentar pedidos ao abrigo destes instrumentos.

Atualmente, os oficiais de justiça assumem um papel central na utilização do sistema informático descentralizado de transmissão e receção de pedidos de citação e notificação, no âmbito do Regulamento (UE) 2020/1784, bem como dos pedidos de obtenção de prova, ao abrigo do Regulamento (UE) 2020/1783.

Todavia, a ausência de uma infraestrutura devidamente integrada no sistema *Citius* — solução que tem sido apontada como objetivo pelo Estado Português — implica que, na prática, a tramitação destes procedimentos continue a assentar em operações de natureza manual. Com efeito, o acesso ao Portal de Referência, o descarregamento dos documentos e a subsequente inserção dos mesmos

no sistema *Citius* constituem etapas que exigem intervenção humana sucessiva, evidenciando uma persistente clivagem entre o modelo normativo de desmaterialização e a realidade operacional dos serviços judiciais.

A implementação do Ponto Europeu de Acesso Eletrónico (EEAP) constituirá uma das alterações mais relevantes para o sistema jurídico português, na medida em que permitirá a comunicação direta entre particulares e autoridades competentes de outros Estados-Membros.

Tal implicará a necessidade de adaptação dos mecanismos internos de receção e tramitação de comunicações eletrónicas provenientes do exterior, bem como a garantia da sua integração nos fluxos processuais nacionais.

Assim, no domínio da matéria civil e comercial, e não obstante o exposto, Portugal encontra-se ainda numa fase preparatória e de adaptação progressiva quanto à implementação do sistema e-CODEX, não se verificando, até ao momento, uma utilização generalizada e plenamente operacional deste mecanismo no âmbito dos instrumentos clássicos de cooperação judiciária europeia.

Este estado de desenvolvimento encontra-se em linha com a abordagem faseada adotada pela União Europeia, estando a concretização plena dependente da adoção de atos de execução e da subsequente integração técnica nos sistemas nacionais.

9. Condições estruturais e necessidade de adaptação tecnológica

Portugal apresenta, contudo, um contexto relativamente favorável à implementação do e-CODEX, em virtude do elevado grau de digitalização já alcançado na administração da justiça. Com efeito, sistemas como o *Citius*, nos tribunais judiciais, ou o *SITAF*, nos tribunais administrativos e fiscais, permitem a tramitação eletrónica dos processos, incluindo a prática de atos processuais e a gestão integral do processo em ambiente digital.

Não obstante, tais sistemas foram concebidos numa lógica predominantemente interna, carecendo de adaptações significativas para assegurar a sua interoperabilidade com infraestruturas europeias descentralizadas.

A integração plena no sistema e-CODEX implicará o desenvolvimento de soluções técnicas específicas, designadamente: a implementação dos módulos *Connector e Gateway*; a criação de interfaces de comunicação entre os sistemas nacionais e a rede europeia; a adoção de protocolos normalizados de troca de dados e o reforço das medidas de segurança e autenticação.

Este processo exigirá uma intervenção coordenada das entidades responsáveis pela gestão dos sistemas informáticos da justiça, designadamente o Instituto de Gestão Financeira e Equipamentos da Justiça (IGFEJ).

10. Conclusão

O e-CODEX representa uma transformação estrutural no domínio da cooperação judiciária europeia, contribuindo para a construção de uma justiça mais eficiente, acessível e integrada.

Embora coloque desafios significativos aos Estados-Membros, os benefícios associados à sua implementação justificam plenamente o esforço de adaptação, configurando-se este instrumento como um elemento central da evolução futura do espaço judicial europeu.

Portugal encontra-se numa fase de preparação e adaptação progressiva, à semelhança do que ocorre em todos os restantes Estados Membros, beneficiando de uma base tecnológica sólida, mas ainda distante de uma plena operacionalização do e-CODEX em matéria civil e comercial.

A sua integração efetiva dependerá, em larga medida, do calendário europeu de implementação e da capacidade de adaptação dos sistemas nacionais, sendo expectável que os efeitos mais significativos se façam sentir ao longo da presente década.

(*) O Sumário Executivo foi redigido com recurso ao www.chatgpt.com.

[i] As opiniões expressas neste artigo são exclusivamente da responsabilidade da autora e baseiam-se na experiência adquirida durante o período em que exerceu funções como Juiz Ponto de Contacto da Rede Judiciária Europeia em Matéria Civil e Comercial (de janeiro de 2022 a dezembro de 2025). Tais opiniões não comprometem nem vinculam a entidade em que exerceu essas funções, nem qualquer outra.

[ii] Regulamento (UE) 2022/850 do Parlamento Europeu e do Conselho de 30 de maio de 2022.

[iii] Acórdão do TJUE de 16 de dezembro de 1976, Rewe-Zentralfinanz, proc. 33/76, acessível para consulta em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:61976CJ0033&from=EN>.

[iv] https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-operational-management-large-scale-it-systems-area-freedom-security-and_pt.

[v] Sobre o papel da eu LISA, v. comunicação da Comissão COM(2020) 710 final, acessível para consulta em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020DC0710>.

[vi] <https://www.eulisa.europa.eu/activities/large-scale-it-systems/e-codex/technical-infrastructure>.

[vii] Importa sublinhar que a utilização obrigatória do sistema informático descentralizado admite exceções, designadamente em casos de perturbação do funcionamento do sistema, em razão da natureza do material a transmitir ou em situações de força maior. Nessas circunstâncias, deverá recorrer-se, em alternativa, ao meio mais rápido e adequado que assegure uma troca de informações segura e fiável. Por último, não pode ser desconsiderada a existência, em determinados domínios, de regimes que consagram uma maior flexibilidade na comunicação direta entre autoridades, designadamente com dispensa de formulários, como sucede, por exemplo, com os artigos 42.º, n.º 2, e 57.º, n.º 2, do Regulamento (UE) 2015/848 (Insolvência), bem como com o artigo 86.º do Regulamento (UE) 2019/1111 (Bruxelas II-B).

[viii] Importa salientar que este mecanismo não substitui a videoconferência tal como prevista no Regulamento relativo à obtenção de prova — já há muito utilizada —, antes a vem complementar e alargar o seu âmbito de aplicação. Com efeito, passa a abranger, designadamente, a participação das partes ou dos seus representantes legais, não se limitando, portanto, à obtenção de prova, mas estendendo-se também à simples participação em audiências, entre outros atos processuais

[ix] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_pt.

[x] Regulamento (UE) 2020/1784 (citação e notificação) e Regulamento (UE) 2020/1783 (obtenção de prova).

[xi] Regulamentos (CE) 805/2004, 1896/2006 e 861/2007.

[xii] Regulamentos (CE) 4/2009 e (UE) 2019/1111.

[xiii] Regulamento (UE) 2015/848 relativo aos processos de insolvência.

[xiv] Artigo 6.º CEDH e artigo 47.º da Carta dos Direitos Fundamentais da UE.

[xv] Regulamentos (UE) 2020/1784 e (UE) 2020/1783, do Parlamento Europeu e do Conselho de 25 de novembro de 2020.

[xvi] Regulamento (CE) 1896/2006, de 12.12.2006.

[xvii] Regulamento (CE) 861/2007 de 11.07.2007 – alterado pelo Regulamento (UE) 2015/2421.

[xviii] Diretiva 2003/8/CE, de 27.01.2003.

[xix] Regulamento (UE) 655/2014, de 15.05.

[xx] Regulamento (UE) 2025/848 de 20.05.

[xxi] Regulamento (UE) 650/2012.

[xxii] Regulamento (UE) 2016/1103 do Conselho, de 24 de junho de 2016.

[\[xxiii\]](#) Regulamento (UE) 2016/1104 do Conselho, de 24 de junho de 2016.

[\[xxiv\]](#) Regulamento (CE) 805/2004 do Parlamento Europeu e do Conselho, de 21 de Abril de 2004.

[\[xxv\]](#) Regulamento (UE) 1215/2012 do Parlamento Europeu e do Conselho de 25 de junho de 2019.

[\[xxvi\]](#) Regulamento (CE) 4/2009 do Conselho, de 18 de Dezembro de 2008.

[\[xxvii\]](#) Regulamento (UE) 2019/1111 do Conselho de 25 de junho de 2019.

AS ORDENS EUROPEIAS DE PRODUÇÃO E CONSERVAÇÃO DE PROVA ELETRÓNICA EM PROCESSO PENAL (REGULAMENTO (UE) 2023/1543 e DIRETIVA (UE) 2023/1544): UM NOVO CAMINHO NA RESPOSTA AO CIBERCRIME

José Luís Lopes da Mota: Juiz Conselheiro do Supremo Tribunal de Justiça & Ex-Presidente da EUROJUST

Sumário Executivo (*): (1) A criminalidade digital tornou a prova eletrónica indispensável na investigação penal transnacional. (2) Os mecanismos tradicionais de cooperação internacional revelaram-se demasiado lentos e ineficazes para a obtenção de prova digital. (3) O Regulamento (UE) 2023/1543 e a Diretiva (UE) 2023/1544, aplicáveis a partir de 18 de agosto de 2026, criam um novo regime europeu de prova eletrónica. (4) O regime assenta em duas novas medidas: i) Ordem Europeia de Produção de Prova (OEP); ii) Ordem Europeia de Conservação de Prova (OEC). (5) A principal inovação consiste na cooperação direta entre autoridades judiciais e prestadores de serviços, dispensando, em muitos casos, os mecanismos clássicos de auxílio judiciário. (6) Os prestadores de serviços passam a ter obrigações de colaboração, incluindo a designação de representantes legais na União Europeia. (7) O sistema funciona através de uma infraestrutura digital comum (e-CODEX), permitindo comunicações rápidas e seguras. (8) O Regulamento procura equilibrar eficácia da investigação e proteção dos direitos fundamentais, mediante controlo judicial, proporcionalidade, proteção de dados e direito a recurso. (9) O novo regime integra-se na evolução do direito internacional sobre cibercrime, articulando-se com a Convenção de Budapeste, o Segundo Protocolo Adicional, o CLOUD Act e a Convenção das Nações Unidas sobre o Cibercrime. (10) A implementação exige adaptações legislativas, organizativas e tecnológicas pelos Estados-Membros, permanecendo em aberto questões relativas à proteção de dados e à conservação de metadados.

Resumo ():** O artigo analisa o novo regime europeu de obtenção de prova eletrónica em processo penal, instituído pelo Regulamento (UE) 2023/1543 e pela Diretiva (UE) 2023/1544, cuja aplicação plena se inicia em agosto de 2026. O autor demonstra que a crescente transnacionalização da criminalidade e a dependência das investigações de dados armazenados por prestadores de serviços digitais tornaram insuficientes os mecanismos tradicionais de cooperação judiciária internacional. A principal inovação consiste na criação das Ordens Europeias de Produção e de Conservação de Prova (OEP e OEC), que permitem às autoridades judiciais obter ou preservar diretamente prova eletrónica junto de prestadores de serviços estabelecidos noutros Estados-Membros, através de um sistema digital seguro baseado no e-CODEX. Este modelo procura assegurar maior rapidez e eficácia na investigação criminal, sem comprometer as garantias processuais e os direitos fundamentais. O estudo examina detalhadamente o regime jurídico das

novas ordens, os respetivos pressupostos de emissão, as categorias de dados abrangidas, as obrigações impostas aos prestadores de serviços, os mecanismos de controlo judicial e os fundamentos de recusa, destacando o equilíbrio alcançado entre eficiência investigatória, proteção da privacidade, proteção de dados e direito a um processo equitativo. O autor enquadra ainda a reforma no contexto da evolução do direito internacional, analisando as suas relações com a Convenção de Budapeste, o Segundo Protocolo Adicional, o CLOUD Act norte-americano e a Convenção das Nações Unidas sobre o Cibercrime. Conclui identificando os desafios que permanecem, designadamente a adaptação da legislação nacional, a implementação tecnológica do sistema, a articulação com o regime europeu de proteção de dados e a necessidade de uma solução estável para a conservação de metadados, condição essencial para a eficácia futura da investigação criminal.

Palavras-Chave (***): Prova eletrónica; Processo Penal; Cooperação judiciária europeia; Cibercrime; Direitos fundamentais; Ordem Europeia de Produção de Prova (OEP).

Índice: (1) Introdução; (2) O “pacote” legislativo da União Europeia sobre prova eletrónica (“e-Evidence package”, 2023): a ordem europeia de produção de prova (OEP) e a ordem europeia de conservação de prova (OEC); (3) As ordens europeias de produção (OEP) e de conservação (OEC) de prova e o princípio do reconhecimento mútuo: a questão da proteção dos direitos fundamentais; (4) As ordens europeias de produção (OEP) e de conservação (OEC) de prova: elementos essenciais; (5) O processo legislativo: um longo e complexo processo negocial, um difícil compromisso; (6) Contexto internacional: o “CLOUD Act” e as negociações com os Estados Unidos da América, o Segundo Protocolo Adicional à Convenção de Budapeste (2022) e a Convenção das Nações Unidas sobre Cibercrime (Convenção de Hanói, 2025); (7) As condições de aplicação das ordens europeias de produção (OEP) e de conservação (OEC) de prova: obrigações dos Estados-membros; (8) Observações finais.

1. Introdução

Com a globalização, a realidade criminal mudou. O crime organizou-se e internacionalizou-se, tirando proveito das facilidades de circulação e da liberalização e expansão dos mercados de bens e serviços a nível mundial, da utilização intensiva das novas tecnologias de comunicação e informação e da redução ou eliminação de controlos de fronteiras. As comunicações eletrónicas e os sistemas informáticos, associados à explosão da *internet*, passaram a constituir instrumentos poderosos e, simultaneamente, alvo da criminalidade transfronteiriça, sobretudo quando organizada. São claramente visíveis os seus reconhecidos efeitos no aumento das dimensões das atividades criminosas, de natureza lucrativa, e na velocidade, sofisticação, dissimulação e ocultação do crime^{[1](#)}.

O *ciberespaço* emerge e afirma-se como o novo “território” do crime, onde se planificam, organizam e materializam as condutas ilícitas, se processam pagamentos e movimentam e branqueiam fundos gigantescos, se ocultam rastros e provas dos crimes e se exploram assimetrias e diferenças entre os sistemas nacionais de direito e justiça criminal. Um número cada vez mais elevado de investigações criminais depende atualmente de provas eletrónicas apenas disponíveis em infraestruturas privadas frequentemente localizadas fora do país onde é conduzida a investigação ou pertencentes a fornecedores de serviços estabelecidos fora desse país. O acesso transfronteiriço a textos, imagens, e-mails, mensagens e informações armazenados ou transmitidos através de sistemas e aplicações informáticas que possam constituir prova dos crimes em investigação é, nessas situações, absolutamente indispensável. De acordo com as informações recolhidas pela Comissão Europeia, entre 2013 e 2016, as solicitações de dados a grandes empresas tecnológicas americanas – como Google, Twitter, Facebook, Microsoft e Apple – aumentaram 70% durante esse período, sendo que mais da metade das investigações criminais na União Europeia («UE») envolvia pedidos transfronteiriços de dados eletrónicos. O acesso transfronteiriço a provas eletrónicas tornou-se necessário em 85% dessas investigações, ascendendo a 65% os pedidos dirigidos a prestadores de serviços situados em diferentes jurisdições^[ii].

Tornou-se evidente que as autoridades nacionais, de competência geograficamente limitada por critérios territoriais de soberania penal estadual, enfrentam sérias e inultrapassáveis dificuldades na obtenção dessas provas, que, pela sua reconhecida volatilidade e velocidade de circulação, requerem intervenção célere das instâncias formais de controlo, incompatível com os tempos e formalidades dos métodos de cooperação judiciária internacional concebidos antes da era da computação em nuvem e da disseminação de serviços *on line*, neles se incluindo, apesar dos progressos registados, os instrumentos adotados na UE em concretização do princípio de reconhecimento mútuo em que se funda a cooperação^[iii].

As alternativas entretanto encontradas, assentes em bases de cooperação voluntária e informal entre as autoridades competentes e os prestadores de serviços (*service providers*)^[iv], enfrentam problemas bem conhecidos, relacionados, no essencial, com a fragmentação, lacunas e conflitos de normas aplicáveis, a legalidade do acesso às provas e a dados pessoais, a proteção de direitos fundamentais das pessoas visadas e, a final, com a própria licitude da intervenção e a admissibilidade das provas em julgamento.

Neste contexto, comumente reconhecido, impôs-se a necessidade de encontrar soluções para a obtenção célere e juridicamente sólida de provas eletrónicas essenciais para as investigações e processos penais. Perante a incapacidade de os Estados agirem isoladamente, face à dimensão transnacional do fenómeno e das questões envolvidas, a ação requerida teria necessariamente de convocar as instâncias de cooperação internacional, de âmbito global (Nações Unidas) ou regional (Conselho da Europa, União Europeia), apesar do atual contexto adverso, num mundo em conflito.

Os diagnósticos são conhecidos, pelo menos desde os anos 90 do século passado, a partir dos trabalhos da União Europeia, que conduziram à criação do “espaço de liberdade, segurança e justiça”[\[v\]](#), do Conselho da Europa e das Nações Unidas, devendo destacar-se, neste domínio, como marcos fundamentais, a aprovação e entrada em vigor da Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional (“Convenção de Palermo” 2000)[\[vi\]](#) e da Convenção do Conselho da Europa sobre o Cibercrime (“Convenção de Budapeste”, 2001)[\[vii\]](#).

A Convenção de Budapeste, de comprovada vocação universal[\[viii\]](#), constituiu o tratado internacional mais abrangente e coerente sobre cibercrime e provas eletrónicas, estruturante do direito penal e processual penal em desenvolvimento e do quadro da cooperação internacional. No plano processual, as medidas previstas na Convenção (artigos 16.º a 21.º) aplicam-se às infrações previstas na Convenção (crimes informáticos), a outras infrações cometidas por meio de sistema informático e à recolha de prova em suporte eletrónico de qualquer infração penal (provas eletrónicas). Incluem-se nestas medidas: a conservação expedita de dados informáticos armazenados (art.º 16.º), a conservação expedita e divulgação parcial de dados de tráfego (art.º 17.º), a injunção de comunicar (art.º 18.º)[\[ix\]](#), a busca e apreensão de dados informáticos armazenados (art.º 19.º), a recolha, em tempo real, de dados de tráfego (art.º 20.º) e a interceção de dados de conteúdo (art.º 21.º). Atendendo ao nível de interferência em direitos fundamentais, as medidas estão sujeitas a controlo judicial, no respeito pela Convenção Europeia dos Direitos Humanos, pelo Pacto Internacional sobre os Direitos civis e Políticos e por outros instrumentos internacionais na área dos direitos humanos, incorporando o princípio da proporcionalidade (art.º 15.º).

Estas medidas foram inseridas no direito interno pela Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime)[\[x\]](#), que o adaptou à Convenção sobre Cibercrime, sujeitando-as a controlo das autoridades judiciais – artigos 12.º (Preservação expedita de dados)[\[xi\]](#), 13.º (Revelação expedita de dados de tráfego)[\[xii\]](#), 14.º (Injunção para apresentação ou concessão do acesso a dados)[\[xiii\]](#), 15.º (Pesquisa de dados informáticos), 16.º (Apreensão de dados informáticos), 17.º (Apreensão de correio eletrónico e registos de comunicações de natureza semelhante) e 18.º (Interceção de comunicações).

No âmbito da cooperação internacional incluem-se medidas cautelares de auxílio mútuo – a conservação expedita de dados informáticos armazenados (art.º 29.º), mediante pedido, e a divulgação expedita de dados de tráfego conservados (art.º 30.º), no decurso da execução de um pedido de conservação de dados de tráfego relativos a uma determinada comunicação – e o auxílio mútuo no tocante aos poderes de investigação – auxílio mútuo para o acesso a dados informáticos armazenados (art.º 31.º) –, mediante pedido.

Nos termos da Convenção, as autoridades de um Estado-Parte apenas podem aceder a dados informáticos fora do seu território, sem autorização de outro Estado-Parte, se se tratar de dados informáticos acessíveis ao público (fonte aberta), independentemente da sua localização geográfica ou através de um sistema informático situado no seu território, e aceder a dados informáticos no

território de uma outra Parte, ou recebê-los, se obtiver o consentimento legal e voluntário da pessoa com legitimidade para lhe facultar os dados através desse sistema informático (artigos 32.º da Convenção e 29.º da Lei n.º 109/2009).

Os últimos anos marcaram, porém, um ponto de viragem na cooperação internacional em matéria de aquisição e transferência de prova eletrónica no processo penal. Destacam-se aqui, pelo carácter inovador, a aprovação do Segundo Protocolo Adicional à Convenção de Budapeste sobre Cibercrime (2022), que introduz novas bases jurídicas para a cooperação direta visando à obtenção de informações sobre o registo de nomes de domínio, e, pela sua dimensão, a negociação e adoção da Convenção das Nações Unidas sobre o Cibercrime (2024)[\[xiv\]](#), que, fortemente inspirada pela Convenção de Budapeste, define um quadro global de ação.

Paralelamente, após a aprovação do “CLOUD Act”, foram iniciadas negociações entre a União Europeia e os Estados Unidos, com o objetivo de conclusão de um acordo internacional para eliminar conflitos de leis e facilitar o acesso a provas eletrónicas[\[xv\]](#).

É neste quadro que é adotado e entra plenamente em vigor, em 16 de agosto de 2026, o designado “pacote legislativo” da União Europeia sobre prova eletrónica, que constitui as bases de cooperação direta transfronteiriça entre as autoridades judiciais e os prestadores de serviços com estabelecimento ou representados fora do país em que correm a investigação e o processo penal.

O presente artigo visa proporcionar um guia de leitura essencial destes novos instrumentos jurídicos, colocando-os no seu contexto, descrevendo-os nos seus aspetos essenciais e identificando os desafios de um longo e difícil processo de negociação que esteve na sua génese, evidenciando as diferenças relativamente ao regime vigente em matéria de cooperação judiciária para acesso e aquisição de prova eletrónica, na observância do princípio do reconhecimento mútuo das decisões judiciais e no respeito pelos direitos fundamentais consagrados no direito da União, perspetivando-os nas relações com outros instrumentos jurídicos emergentes ao nível internacional, e, finalmente, abordando as obrigações deles decorrentes para os Estados-membros e indicando, em observações finais, algumas questões ainda em aberto de cuja solução depende a constituição de bases sólidas no sentido de garantir a sua efetiva aplicação e funcionamento.

2. O “pacote” legislativo da União Europeia sobre prova eletrónica (“e-Evidence package”, 2023): a ordem europeia de produção de prova (OEP) e a ordem europeia de conservação de prova (OEC)

O desenvolvimento mais significativo em matéria de acesso transfronteiriço a provas eletrónicas é representado pela adoção do novo “pacote legislativo” da UE sobre provas eletrónicas (o chamado “e-Evidence package”[\[xvii\]](#)), constituído pelo Regulamento (UE) 2023/1543 do Parlamento e do Conselho de 12 de julho de 2023 relativo às ordens europeias de produção e às ordens europeias de conservação para efeitos de prova eletrónica em processos penais e para efeitos de execução de

penas privativas de liberdade na sequência de processos penais, e pela Diretiva (UE) 2023/1544 do Parlamento Europeu e do Conselho de 12 de julho de 2023 que estabelece regras harmonizadas aplicáveis à designação de estabelecimentos designados e à nomeação de representantes legais para efeitos de recolha de prova eletrónica em processos penais^[xvii].

A fim de assegurar uma aplicação coerente destas novas regras e de, entretanto, se poderem estabelecer condições para a sua implementação e cumprimento, o Regulamento apenas entra em vigor no dia 18 de agosto de 2026. Por sua vez, a Diretiva deveria ter sido transposta para a legislação nacional dos Estados-Membros UE até 18 de fevereiro de 2026^[xviii].

O sistema agora instituído:

(a) Cria uma “ordem europeia de produção de prova” («OEP»), que permite que uma autoridade judiciária de um Estado-Membro obtenha provas eletrónicas (como mensagens de correio eletrónico, mensagens de texto ou mensagens em aplicações móveis, bem como informações para identificar o autor) diretamente de um prestador de serviços ou do seu representante legal noutro Estado-membro^[xix];

(b) Cria uma “ordem europeia de conservação de prova” («OEC»), que permite que uma autoridade judiciária de um Estado-membro solicite a um prestador de serviços ou ao seu representante legal noutro Estado-membro que conserve dados específicos, tendo em vista um pedido subsequente de apresentação desses dados^[xx] através de auxílio judiciário mútuo, mediante uma decisão europeia de investigação («DEI»)^[xxi] ou de uma ordem europeia de produção de prova;

(c) Estabelece um “sistema informático descentralizado” através do qual todas as comunicações entre as autoridades e os prestadores de serviços possam ter lugar de forma segura e fiável, garantindo a autenticação de todos os participantes;

(d) Obriga os prestadores de serviços a designar um estabelecimento ou a nomear um representante legal na União para a receção, cumprimento e execução de decisões e ordens emitidas pelas autoridades competentes dos Estados-Membros, para efeitos de recolha de provas eletrónicas.

O Regulamento estabelece as regras segundo as quais uma autoridade de um Estado-Membro pode, num processo penal, emitir uma OEP ou uma OEC e, assim, ordenar a um prestador de serviços que ofereça serviços na União e que esteja estabelecido noutro Estado-Membro ou, caso não esteja estabelecido, que esteja representado por um representante legal noutro Estado-Membro, que produza ou que conserve provas eletrónicas constituída por dados de assinantes, dados de tráfego ou dados de conteúdo, conservados em formato eletrónico, por um prestador de serviços ou em seu nome^[xxii], no âmbito e para os efeitos de um processo penal, independentemente da localização dos dados^[xxiii].

A Diretiva estabelece as regras relativas à designação de estabelecimentos designados e à nomeação de representantes legais de determinados prestadores de serviços que oferecem serviços na União, para receberem, darem cumprimento e executarem decisões e ordens emitidas por autoridades competentes dos Estados-Membros para efeitos de recolha de prova eletrónica em processos penais^[xxiv].

A OEP e a OEC são decisões emitidas pela autoridade judiciária – um juiz, um tribunal, um juiz de instrução ou um magistrado do Ministério Público – do Estado-membro competente no processo em que as provas são necessárias ou validadas pela autoridade judiciária nos casos em que podem ser emitidas por outra autoridade competente, tal como definida pelo Estado de emissão, e que, no processo em causa, intervenha enquanto autoridade de investigação num processo penal com competência para ordenar a recolha de elementos de prova de acordo com a lei nacional, nos termos e condições especificadas no art.º 4.º do Regulamento. A OEP para obter dados de tráfego, com exceção dos dados solicitados com o único objetivo de identificar o utilizador, tal como definidos no artigo 3.º, n.º 10, ou para obter dados de conteúdo só pode ser emitida ou validada por um juiz, um tribunal ou um juiz de instrução que seja competente no processo^[xxv].

O que torna esse novo regime inovador é, pois, o mecanismo em que se baseia, isto é, num diálogo direto, no processo, entre autoridades judiciárias nacionais e “partes” privadas, com a finalidade de agilizar o processo de cooperação e de lhe conferir maior eficácia^[xxvi].

Seguindo o modelo de outros instrumentos de cooperação judiciária da UE baseados no princípio do reconhecimento mútuo, as OEP e OEC utilizam formulários próprios, para transmissão direta ao destinatário, ou seja, ao estabelecimento designado ou ao representante legal designado pelo prestador de serviços em causa, em todas as línguas da União – o “certificado de ordem europeia de produção” («COEP») para a produção de provas eletrónicas e o “certificado de ordem europeia de conservação” («COEC») para a conservação de provas eletrónicas^[xxvii].

É conferida particular atenção à proteção dos direitos fundamentais afetados^[xxviii], em particular do direito ao respeito pela vida privada e familiar e do direito à proteção das pessoas singulares relativamente ao tratamento dos dados pessoais (artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia – «Carta»^[xxix]), devendo ser assegurado que os dados pessoais sejam protegidos e tratados em conformidade com o Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados – «RGPD»)^[xxx] e com a Diretiva (UE) 2016/680, aplicável ao processamento e proteção de dados nas investigações e processos penais^[xxxi], bem como com a Diretiva 2002/58/CE^[xxxii], relativa à privacidade e às comunicações eletrónicas, nomeadamente no caso de utilização adicional, transmissão ou transferência posterior dos dados obtidos.

A fim de garantir o pleno respeito dos direitos fundamentais, o valor probatório das provas recolhidas deverá ser avaliado em julgamento pela autoridade judicial competente, em conformidade com o direito nacional e respeitando, em especial, o direito a um processo equitativo e o direito de defesa (artigo 47.º da Carta)^[xxxiii].

Nos procedimentos de emissão e execução das OEP e OEC deverão ser observados os direitos processuais em processo penal, nomeadamente os previstos nas Diretivas 2010/64/UE^[xxxiv] (direito à interpretação e tradução), 2012/13/UE^[xxxv] (direito à informação), 2013/48/UE^[xxxvi] (direito de acesso a um advogado), (UE) 2016/343^[xxxvii] (presunção de inocência e de comparecer em julgamento), (UE) 2016/800^[xxxviii] (garantias processuais para menores suspeitos ou arguidos em processo penal) e (UE) 2016/1919^[xxxix] (apoio judiciário), no seu âmbito de aplicação.

O Regulamento impõe a criação de canais adequados para assegurar que todas as partes possam cooperar de forma eficiente por meios digitais, através de um “sistema informático descentralizado”^[xl] que permita o intercâmbio eletrónico transfronteiriço rápido, direto, interoperável, sustentável, fiável e seguro de formulários, dados e informações relacionados com processos.

A fim de permitir uma comunicação escrita eficiente e segura entre as autoridades competentes e os estabelecimentos designados ou os representantes legais dos prestadores de serviços, esses estabelecimentos designados ou representantes legais deverão dispor de meios eletrónicos de acesso aos sistemas informáticos nacionais, parte do sistema informático descentralizado, operados pelos Estados-Membros.

O sistema informático descentralizado deverá incluir os sistemas informáticos dos Estados-Membros e das agências e organismos da União (Eurojust, Procuradoria Europeia) e os pontos de acesso interoperáveis através dos quais esses sistemas informáticos estão interligados^[xli].

Os pontos de acesso do sistema informático descentralizado deverão basear-se no sistema e-CODEX, criado pelo Regulamento (UE) 2022/850 do Parlamento Europeu e do Conselho^[xlii].

Cada Estado-Membro deve garantir que os estabelecimentos designados ou os representantes legais dos prestadores de serviços situados nesse Estado-Membro tenham acesso ao sistema informático descentralizado através dos respetivos sistemas informáticos nacionais. Os prestadores de serviços devem garantir que os seus estabelecimentos designados ou representantes legais possam utilizar o sistema informático descentralizado através do respetivo sistema informático nacional para receber COEP e COEC, enviar os dados solicitados à autoridade emissora e comunicar por qualquer outro meio com a autoridade emissora e a autoridade de execução, como previsto no Regulamento^[xliii].

Os prestadores de serviços que utilizam soluções informáticas concebidas especificamente para efeitos do intercâmbio de informações e dados relacionados com pedidos de provas eletrónicas deverão dispor de meios automatizados de acesso aos sistemas informáticos descentralizados através de uma norma comum de intercâmbio de dados^[xliv].

O Regulamento de Execução (UE) 2025/1550^[xlv] veio estabelecer as especificações técnicas e outros requisitos para o sistema informático descentralizado referido no Regulamento 2023/1543.

Deverá ser possível aos Estados-Membros utilizar software desenvolvido pela Comissão, nomeadamente a aplicação informática de referência, em vez de um sistema informático nacional. Essa aplicação informática de referência deve basear-se numa configuração modular, o que significa que são criados pacotes de software que são entregues independentemente das componentes do sistema e-CODEX necessárias para fazer a ligação ao sistema informático descentralizado. Essa configuração deverá permitir que os Estados-Membros reutilizem ou reforcem as respetivas infraestruturas nacionais de comunicação judicial existentes para efeitos da utilização transfronteiras^[xlv].

A Comissão é responsável pela criação, manutenção e desenvolvimento de uma aplicação informática de referência, financiados pelo orçamento geral da União, que os Estados-Membros podem optar por utilizar como sistema de retaguarda em vez de um sistema informático nacional. A conceção, desenvolvimento e manutenção da aplicação informática de referência são feitas em conformidade com os requisitos e princípios em matéria de proteção de dados estabelecidos no Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho^[xlvii], no Regulamento (UE) 2016/679^[xlviii] e na Diretiva (UE) 2016/680^[xlix], em especial os princípios da proteção de dados desde a conceção e por defeito, bem como um elevado nível de cibersegurança. É importante que a aplicação informática de referência também inclua medidas técnicas adequadas e permita a adoção das medidas organizativas necessárias para garantir um nível adequado de segurança e interoperabilidade^[l].

3. As ordens europeias de produção (OEP) e de conservação (OEC) de prova e o princípio do reconhecimento mútuo: a questão da proteção dos direitos fundamentais

Estabelece-se, pois, um novo modelo^[li], um sistema de cooperação direta entre autoridades nacionais e entidades privadas, que, indo além dos termos em que, por definição, a cooperação sempre foi concebida – como cooperação, através de “auxílio mútuo”, entre Estados ou entre autoridades estaduais –, introduz, decididamente, uma nova dimensão no princípio do reconhecimento mútuo em que se funda a cooperação na UE e no princípio da confiança mútua, que lhe subjaz, baseado na assunção da proteção equivalente dos direitos fundamentais no Estado de emissão e no Estado de execução das ordens de produção e de conservação de prova^[lii]. É esta assunção que o Regulamento afirma no preâmbulo^[liii]: “O mecanismo da ordem europeia de produção e da ordem europeia de conservação de provas eletrónicas em processos penais baseia-se no princípio da confiança mútua entre os Estados-Membros e na presunção do cumprimento pelos Estados-Membros do direito da União, do Estado de direito e, em especial, dos direitos fundamentais, que são elementos essenciais do espaço de liberdade, segurança e justiça da União. Tal mecanismo permite às autoridades nacionais competentes enviar essas ordens diretamente para os prestadores de serviços”.

Convém, todavia, a este propósito, lembrar as reservas iniciais que se suscitavam perante o quadro jurídico da cooperação judiciária no âmbito da UE, tendo em conta o direito primário (Tratados e Carta [\[liv\]](#)) e secundário da UE (decisões-quadro e diretivas), bem como a jurisprudência do Tribunal de Justiça da União Europeia («TJUE») nestas matérias.

De particular relevância, a observar na emissão e execução de ordens de produção e conservação de provas, são o artigo 6.º do TUE, segundo o qual a União reconhece os direitos, as liberdades e os princípios enunciados na Carta, a Declaração 21 anexa ao Tratado de Lisboa relativa à necessidade de disposições específicas sobre proteção de dados pessoais no domínio da cooperação judiciária em matéria penal [\[lv\]](#), e os artigos 7.º (“Respeito pela vida privada e familiar”, incluindo comunicações), 8.º (“Proteção de dados pessoais”), 47.º (“Direito à ação e a um tribunal imparcial”, incluindo o direito a um tribunal independente e a um processo equitativo) e 52.º (“Âmbito e interpretação dos direitos e dos princípios”, incluindo as exigências de legalidade e de respeito pelo princípio da proporcionalidade relativamente a restrições de direitos fundamentais) da Carta.

Da conjugação destas disposições resultaria, *prima facie*, de acordo com a abordagem tradicional, a necessidade de mecanismos de garantia de controlo judicial sistemático da obtenção de prova na posse de entidades privadas, por um juiz ou tribunal independente, quer no Estado de emissão, quer no Estado de execução [\[lvi\]](#), em conformidade com o regime e os ensinamentos da experiência de funcionamento do princípio do reconhecimento mútuo das decisões judiciais em matéria penal, baseado na confiança mútua. Nesse sentido concorreria também a jurisprudência do TJUE, em interpretação de atos legislativos [\[lvii\]](#) da União dando expressão ao princípio do reconhecimento mútuo, nomeadamente em casos de sério risco de sujeição de uma pessoa a tratamento desumano e degradante devido às graves condições das prisões no Estado de emissão, na sequência da entrega da pessoa em execução de um mandado de detenção europeu [\[lviii\]](#), cujo regime exige a intervenção de um juiz para verificar a presença de motivos de não execução e para ordenar a entrega, e em casos de execução de um mandado de detenção europeu por um juiz cuja independência se mostraria afetada por virtude de deficiências sistémicas e generalizadas de funcionamento do sistema judicial do Estado de emissão [\[lix\]](#).

Assim, tendo em conta que, para combater a criminalidade, é essencial que existam mecanismos eficazes de obtenção de provas eletrónicas, que esses mecanismos devem estar sujeitos a condições e salvaguardas que garantam o pleno respeito dos princípios e direitos fundamentais consagrados no TUE e na Carta – nomeadamente os princípios da necessidade e proporcionalidade, os direitos à tutela judiciária, ao processo equitativo e à proteção da privacidade e dos dados pessoais –, e que o impacto nos direitos fundamentais varia consoante as categorias de dados pessoais em causa, as soluções contidas no regulamento, na sequência de árduas discussões e afinamentos no decurso do processo legislativo [\[lx\]](#), refletem um delicado compromisso de equilíbrio entre as finalidades em conflito [\[lxi\]](#), assegurando que:

(a) Quando é emitida uma ordem europeia de produção ou uma ordem europeia de conservação, deverá estar sempre envolvida uma autoridade judiciária no processo de emissão ou no processo de validação da ordem;

(b) Tendo em conta a natureza mais sensível dos dados de tráfego, com exceção dos dados solicitados com o único objetivo de identificar o utilizador, e dos dados de conteúdo, a emissão ou a validação de uma ordem de produção para a obtenção dessas categorias de dados exigirá sempre o reexame por um juiz;

(c) A validação de ordens de produção ou de conservação por autoridades judiciárias deverá, em princípio, ser obtida antes da emissão;

(d) Tendo em conta a natureza mais sensível das ordens de produção para obter dados de tráfego, com exceção dos dados solicitados com o único objetivo de identificar o utilizador, ou para obter dados de conteúdo, prevê-se um mecanismo de notificação que deverá envolver uma autoridade de execução e consistir na transmissão da ordem a essa autoridade ao mesmo tempo de transmissão ao destinatário;

(e) A autoridade de execução deverá poder recusar uma ordem, em situações excecionais, quando existem motivos substanciais para crer, com base em elementos de prova específicos e objetivos, que a execução da ordem de produção implicaria, nas circunstâncias específicas do processo, uma violação manifesta de um direito fundamental relevante consagrado no artigo 6.º do TUE ou na Carta;

(f) Tendo em consideração que todas as pessoas cujos dados sejam solicitados em investigações criminais ou em processos penais têm acesso a vias de recurso efetivo, em conformidade com o artigo 47.º da Carta e sem prejuízo de outras vias disponíveis em conformidade com o direito interno, qualquer pessoa cujos dados tenham sido solicitados através de uma ordem de produção tem o direito a vias de recurso efetivo contra essa ordem e, caso se trate de uma pessoa suspeita ou arguida, o direito a vias de recurso efetivo durante o processo penal no âmbito do qual os dados são utilizados como prova;

(g) O direito a vias de recurso efetivo deverá ser exercido perante um tribunal do Estado de emissão em conformidade com o respetivo direito nacional, devendo incluir a possibilidade de contestar a legalidade da medida, incluindo a sua necessidade e proporcionalidade, sem prejuízo da garantia dos direitos fundamentais no Estado de execução, ou de outros recursos adicionais em conformidade com o direito nacional ou do direito de utilizar as vias de recurso previstas no Regulamento (UE) 2016/679 e na Diretiva (UE) 2016/680.

4. As ordens europeias de produção (OEP) e de conservação (OEC) de prova: elementos essenciais

Para efeitos do Regulamento, entende-se por prestador de serviços qualquer pessoa que preste uma ou mais das seguintes categorias de serviços (excluindo os serviços financeiros): serviços de comunicações eletrónicas, tais como serviços de acesso à *Internet*, serviços de comunicações interpessoais (por exemplo, serviços de mensagens, serviços de correio eletrónico e serviços de telefonia pela Internet); serviços de nomes de domínio na Internet e de numeração IP, tais como a atribuição de endereços IP, registos de nomes de domínio e serviços relacionados com a privacidade e proxy; outros serviços da sociedade da informação que permitem aos utilizadores comunicarem entre si ou armazenarem ou tratarem dados de outra forma, tais como redes sociais, mercados online e outros prestadores de serviços de alojamento [\[lxii\]](#).

Por «oferta de serviços na União» entende-se permitir que pessoas singulares ou coletivas num Estado-Membro utilizem os serviços acima referidos e ter uma ligação substancial, com base em critérios factuais específicos, ao Estado-Membro referido no primeiro ponto. Considera-se que existe essa ligação substancial quando o prestador de serviços possui um estabelecimento num Estado-Membro ou, na ausência de tal estabelecimento, quando existe um número significativo de utilizadores num ou mais Estados-Membros, ou quando as atividades são direcionadas para um ou mais Estados-Membros [\[lxiii\]](#).

A OEP e a OEC só podem ser emitidas no âmbito e para efeitos de processos penais, bem como para a execução de uma pena privativa de liberdade ou de uma ordem de detenção com duração mínima de quatro meses, na sequência de um processo penal.

As ordens podem ser emitidas relativamente a dados de assinantes, a dados de tráfego e a dados de conteúdo. Introduce-se uma quarta categoria de dados, ou seja, de «dados solicitados com o único objetivo de identificar o utilizador», definida como «endereços IP e, quando necessário, as portas de origem relevantes e o registo temporal, nomeadamente a data e a hora, ou equivalentes técnicos desses identificadores e informações relacionadas, quando solicitados pelas autoridades responsáveis pela aplicação da lei ou pelas autoridades judiciais com o único objetivo de identificar o utilizador no âmbito de uma investigação criminal específica» [\[lxiv\]](#).

O regulamento aplica-se apenas aos dados que já tenham sido armazenados, ou seja, não se aplica aos dados que permitam a monitorização em tempo real nem aos dados que venham a ser gerados no futuro.

Uma OEP para obter dados de assinantes ou dados solicitados com o único objetivo de identificar o utilizador pode ser emitida para todas as infrações penais e para a execução de uma pena privativa de liberdade ou de uma medida de detenção de, pelo menos, quatro meses [\[lxv\]](#). Uma OEP para obter de dados de tráfego ou de conteúdo pode ser emitida para infrações penais puníveis no Estado de emissão com uma pena privativa de liberdade de, no máximo, pelo menos três anos, ou, independentemente deste limiar, para um conjunto específico de infrações relacionadas com a cibercriminalidade [\[lxvi\]](#), a fraude relacionada com meios de pagamento que não sejam em numerário [\[lxvii\]](#), o terrorismo [\[lxviii\]](#) e o abuso sexual de crianças [\[lxix\]](#). Pode ser emitida uma OEC para

todas as infrações penais, «se pudesse ter sido emitida nas mesmas condições num caso nacional semelhante», e para a execução de uma pena privativa de liberdade ou de uma medida de detenção de, pelo menos, quatro meses^[lxx].

No que respeita à OEP, a autoridade emissora deve avaliar a necessidade e a proporcionalidade em relação ao caso em apreço e ter em conta os direitos processuais do suspeito ou do arguido, só podendo emitir uma ordem se tal ordem pudesse ter sido emitida nas mesmas condições num caso nacional semelhante^[lxxi].

No caso de uma OEP relativa a dados de tráfego e de conteúdo, a autoridade emissora deve notificar a autoridade de execução (ou seja, a autoridade competente no Estado em que o prestador de serviços está estabelecido ou em que reside o seu representante legal) se o titular dos dados ou o crime se encontrarem fora da jurisdição do Estado emissor.^[lxxii]

A autoridade emissora deve rever a OEP se o prestador de serviços invocar motivos para não dar cumprimento à ordem.^[lxxiii]

A autoridade emissora deve informar a pessoa visada, sem demora injustificada, sobre a apresentação dos dados, sendo possível adiar e restringir a informação por um período limitado, em conformidade com o artigo 13.º, n.º 3, da Diretiva 2016/680^[lxxiv].

O prestador de serviços deve apresentar os dados dentro dos prazos estabelecidos ou preservar os dados sem demora injustificada e mantidos durante o período estabelecido, garantir a confidencialidade, o sigilo e a integridade dos dados apresentados e preservados. O prestador de serviços pode solicitar esclarecimentos à autoridade emissora se a ordem de apresentação de provas europeia estiver incompleta, contiver erros manifestos ou informações insuficientes^[lxxv].

O prestador de serviços pode invocar dois fundamentos para não dar cumprimento a uma OEP: imunidades e privilégios ou interferência com regras sobre a determinação ou limitação da responsabilidade penal relacionadas com a liberdade de imprensa ou a liberdade de expressão noutros meios de comunicação social, ao abrigo do direito do Estado de execução e conflito com uma obrigação prevista na legislação aplicável de um país terceiro, casos em que deve informar a autoridade emissora e a autoridade de execução, utilizando formulários próprios^[lxxvi].

A autoridade de execução no Estado de execução tem o direito de avaliar as ordens emitidas pelo Estado de emissão e de decidir sobre o seu reconhecimento, quer quando estas tenham sido notificadas simultaneamente, quer quando tal tenha sido solicitado pelos prestadores de serviços, quer ainda durante o procedimento de execução (caso o prestador de serviços não cumpra uma ordem europeia de apresentação ou de conservação de dados)^[lxxvii].

A autoridade de execução pode invocar os seguintes motivos de recusa^[lxxviii], caso tenha sido notificada (ou seja, nos casos de ordens europeias de produção relativas a dados de tráfego e de conteúdo, em que o titular dos dados ou o crime se situam fora do Estado de emissão): imunidades e

privilégios concedidos ao abrigo da legislação do Estado de execução; dados solicitados estão abrangidos por regras em matéria de determinação ou limitação da responsabilidade penal relacionadas com a liberdade de imprensa ou a liberdade de expressão noutros meios de comunicação social; em situações excepcionais, violação manifesta dos direitos fundamentais consagrados no artigo 6.º do TUE ou na Carta; *ne bis in idem*; não preenchimento do requisito de dupla incriminação, a menos que a OEP diga respeito a um dos 32 crimes incluídos na lista puníveis no Estado de emissão com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos.

Um suspeito ou arguido (ou o seu advogado) pode solicitar a emissão de uma OEP ou uma OEC «no âmbito dos direitos de defesa aplicáveis, em conformidade com o direito processual penal nacional» [\[lxxix\]](#).

A pessoa cujos dados estão a ser solicitados (pessoa visada) tem o direito de ser informada da apresentação dos dados pela autoridade emissora, a menos que exista um motivo para adiar ou restringir a informação por parte da autoridade emissora [\[lxxx\]](#).

A pessoa visada tem direito a vias de recurso efetivo contra a ordem perante um tribunal no Estado de emissão, sem prejuízo de outras vias de recurso disponíveis em conformidade com o direito nacional ou ao abrigo do Regulamento (UE) 2016/679 e da Diretiva (UE) 2016/680, em conformidade com o direito nacional, devendo incluir a possibilidade de contestar a legalidade da medida, incluindo a sua necessidade e proporcionalidade, sem prejuízo das garantias dos direitos fundamentais no Estado de execução [\[lxxxi\]](#).

O Regulamento prevê um procedimento de revisão especial (artigo 17.º) caso um prestador de serviços considere que o cumprimento de uma OEP entraria em conflito com uma obrigação prevista na legislação de um país terceiro.

De acordo com o regulamento (artigo 12.º), os Estados-Membros devem estabelecer sanções pecuniárias caso os prestadores de serviços infringam as regras relativas à execução das ordens europeias de produção e de conservação de dados, devendo garantir-se que possam ser impostas sanções pecuniárias até 2 % do volume de negócios anual total a nível mundial do prestador de serviços.

As infrações às regras nacionais que transpõem a diretiva exigem que os Estados-Membros estabeleçam «sanções eficazes, proporcionadas e dissuasivas» e tomem todas as medidas necessárias para garantir a sua aplicação (artigo 5.º da diretiva).

5. O processo legislativo: um longo e complexo processo negocial, um difícil compromisso

O Regulamento e a Diretiva são o resultado de um compromisso difícil alcançado nas negociações tripartidas entre o Parlamento Europeu, o Conselho e a Comissão, refletindo a complexa tarefa de equilibrar adequadamente a aplicação harmoniosa e eficiente da lei no combate à criminalidade no mundo digital e a proteção adequada dos direitos fundamentais^[lxxxii]. Apresentadas pela Comissão Europeia em 17 de abril de 2018^[lxxxiii], após uma avaliação aprofundada e na sequência de discussões com os Estados-membros, seguiu-se um longo processo de negociação das propostas legislativas que só veio a terminar mais de 5 anos depois, em 12 de julho de 2023.

A negociação deparou-se com uma dificuldade adicional – a da necessidade de estabelecer e regular uma relação direta entre a autoridade judiciária de um Estado em que é exercida a ação penal (Estado de emissão das decisões) e entidades privadas (não estaduais) fora da sua jurisdição, ou seja, prestadores de serviços que detêm dados que podem conter vestígios de comunicações e atividades de autores de crimes que atuam através de meios informáticos, o que se afasta da relação tradicional entre autoridades estaduais baseada em pedidos de auxílio judiciário mútuo (através de cartas rogatórias) ou na execução de decisões judiciais emitidas com base no princípio do reconhecimento mútuo (DEI), que exigem a intervenção da autoridade judiciária do Estado onde o prestador de serviços está localizado. Suscitando, por isso, a questão fundamental de saber até que ponto a autoridade judiciária do Estado do prestador de serviços deveria estar ativamente envolvida na execução das ordens transfronteiriças de produção e conservação de provas.

Até à entrada em vigor do novo “pacote” legislativo, os instrumentos de cooperação judiciária internacional no quadro da UE para acesso e recolha transfronteiriça de provas eletrónicas incluíam: a Diretiva 2014/41/UE relativa à Decisão Europeia de Investigação em matéria penal («DEI»)^[lxxxiv]; a Convenção Europeia relativa ao Auxílio Judiciário Mútuo em Matéria Penal entre os Estados-Membros da União Europeia^[lxxxv]; o Regulamento (UE) n.º 2018/1727, de 14 de novembro de 2018, relativo à Agência da União Europeia para a Cooperação em matéria de Justiça Penal (Eurojust)^[lxxxvi]; a Decisão-Quadro 2002/465/JAI do Conselho relativa às equipas de investigação conjuntas^[lxxxvii]; acordos bilaterais entre a União e Estados terceiros, tais como os acordos de auxílio judiciário mútuo em vigor com os EUA^[lxxxviii]; a Convenção do Conselho da Europa sobre o Cibercrime (“Convenção de Budapeste”)^[lxxxix].

Estes instrumentos de cooperação judiciária, não conseguiram, porém, dar resposta adequada às dificuldades encontradas no acesso e obtenção de prova. Com as suas propostas, concebidas para complementar, e não para substituir, os instrumentos de cooperação judiciária existentes, em particular a DEI, a Comissão pretendia colmatar essas lacunas.

Desde o início, foi dada grande ênfase à questão de como contornar as dificuldades colocadas pelo princípio da territorialidade, o que foi conseguido ao consensualizar-se que a localização dos dados era irrelevante.

Outras questões se foram enfrentando, entre as quais a de como solucionar potenciais conflitos com obrigações decorrentes da legislação de países terceiros (em particular a da relação com lei norte-americana “CLOUD Act”), a de uma possível extensão do âmbito de aplicação do regulamento para incluir o acesso direto por via de interceções em tempo real e a de saber se as ordens deveriam também ser notificadas à autoridade competente do Estado de execução ou de outro Estado que tenha uma ligação com o caso em apreço^[xc].

No seu parecer, de 12 de julho de 2018^[xci], o Comité Económico e Social Europeu, saudando a iniciativa da Comissão e a importância das medidas propostas para a recolha de provas para combater o crime grave transnacional, salientou a necessidade de assegurar o respeito pelos direitos fundamentais das pessoas visadas e o controlo judicial para garantir esses direitos.

Por sua vez, a Autoridade Europeia para a Proteção de Dados («AEPD»), no seu longo e detalhado parecer de 6 de novembro de 2019^[xcii], apoiando o objetivo de colocar à disposição das autoridades instrumentos eficazes para investigar e julgar infrações penais num mundo transformado pelas novas tecnologias e de acelerar e facilitar o acesso aos dados em casos transfronteiriços, simplificando os procedimentos no seio da UE, sublinhou a necessidade de respeitar plenamente a Carta dos Direitos Fundamentais da União Europeia e o *aquis* em matéria de proteção de dados pessoais, em particular os direitos ao respeito pela vida privada e à proteção de dados pessoais, garantidos pelos artigos 7.º e 8.º da Carta e as condições de restrição desses direitos impostos pelos critérios de necessidade e proporcionalidade estabelecidos no artigo 52.º, n.º 1, da Carta. Nesta conformidade, defendia a AEPD um efetivo envolvimento das autoridades judiciais no processo, o mais cedo possível, a fim de poderem verificar a conformidade das ordens com a Carta e poderem invocar motivos de recusa com base nessa avaliação. Para além disso, pronunciou-se pela necessidade de clarificar as definições das categorias de dados, no sentido de as tornar coerentes com outras definições na legislação europeia, recomendando uma reavaliação do equilíbrio entre os tipos de infrações para as quais podem ser emitidas ordens europeias e as categorias de dados em causa, à luz da jurisprudência relevante do Tribunal de Justiça da UE.

Na qualidade de colegislador, o Parlamento Europeu («PE») apresentou um vasto conjunto de alterações, que divergiam significativamente da abordagem geral do Conselho, suscitando dúvidas quanto à adequação da sua base jurídica. O texto da posição final do PE, adotado em dezembro de 2020^[xciii], assumiu uma abordagem bastante mais restritiva em várias matérias, nomeadamente no respeitante aos requisitos para a emissão das ordens, à necessidade de notificação ao Estado de execução, ao alargamento dos motivos de não execução, incluindo motivos obrigatórios, e à fusão da diretiva com o regulamento.

As negociações interinstitucionais entre a Comissão, o Conselho e o Parlamento Europeu (o chamado «trílogo»^[xciv]), que se revelaram particularmente difíceis e complexas devido às profundas diferenças entre o texto da abordagem geral do Conselho e a posição do PE, tiveram início em janeiro de 2021, sob a presidência portuguesa do Conselho^[xcv], tendo abrangido mais quatro

presidências do Conselho (Eslovénia, França, República Checa e Suécia), que, na sequência de uma abordagem diferente iniciada no segundo semestre de 2021^[xcvi], conduziram a textos de compromisso sob a presidência sueca^[xcvii], em janeiro de 2023. O diálogo entre o PE e o Conselho foi retomado em maio de 2022 e os intensos esforços de negociação permitiram registar progressos significativos nas discussões bilaterais. No final de 2022, a presidência do Conselho solicitou aos Estados-Membros que lhe fosse concedido um mandato para a reunião de trílogo de 29 de novembro, a fim de apresentar um pacote de compromisso global, que acabou por ser acordado pelas delegações dos Estados-Membros e pelo PE.

6. Contexto internacional: o “CLOUD Act” e as negociações com os Estados Unidos da América, o Segundo Protocolo Adicional à Convenção de Budapeste (2022) e a Convenção das Nações Unidas sobre Cibercrime (Convenção de Hanói, 2025)

O avanço alcançado com a adoção das novas regras internas da UE relativas ao acesso direto às provas eletrónicas pelas autoridades judiciais dos Estados-membros deve também ser compreendido no contexto internacional, em que, no respeito pelos princípios e regras do Estado de Direito e dos direitos fundamentais e com idênticos objetivos de fazer face à criminalidade atual num mundo sem fronteiras, outros instrumentos jurídicos vêm sendo desenvolvidos e em cuja negociação a UE tem participado ativamente, tendo como quadro de referência o direito europeu.

Neste contexto, merecem particular referência as negociações de um acordo com os Estados Unidos da América, a aprovação do Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime (2022) e a conclusão da Convenção das Nações Unidas sobre Cibercrime («Convenção de Hanói», 2025) .

O Conselho JAI de 6 e 7 de junho de 2019 aprovou a Decisão que autoriza a Comissão Europeia, em representação da União, a iniciar negociações com os Estados Unidos relativamente ao acesso direto transfronteiriço a provas eletrónicas no contexto da cooperação judiciária em matéria penal^[xcviii] e a Adenda a essa Decisão contendo os objetivos e as diretrizes de negociação relevantes, com respeito pelo direito da União^[xcix], entre os quais o de, nas relações externas, complementar^[c] o quadro legal de acesso à prova eletrónica definido pelo “pacote” sobre prova eletrónica em discussão (proposta de regulamento e de diretiva sobre os quais o Conselho tinha adotado posição em dezembro de 2018 e março de 2019)^[cii], bem como o denominado *Umbrella Agreement* (“Acordo-Quadro”) entre a União Europeia e os Estados Unidos sobre proteção de dados no quadro da cooperação transatlântica^[cii], com salvaguardas adicionais tendo em conta o nível de sensibilidade das categorias de dados em questão e a circunstância de a transferência de dados ocorrer entre autoridades judiciais e entidades privadas (“service providers”).

A abertura de negociações^[ciii] de um acordo com os Estados Unidos surge na sequência da adoção do “CLOUD Act” (*Clarifying Lawful Overseas Use of Data*)^[civ], aprovada pelo Congresso dos

Estados Unidos em 23 de março de 2018, que, alterando o *Stored Communications Act*, de 1986, esclarece que os fornecedores de serviços dos EUA são obrigados a cumprir ordens norte-americanas para fornecer dados de conteúdo e dados que não sejam de conteúdo, independentemente do lugar onde tais dados estejam armazenados, inclusive na União Europeia[cvi]. A segunda parte do "CLOUD Act" cria um novo mecanismo para que outros países possam aceder ao conteúdo de comunicações mantidas por fornecedores de serviços dos EUA, permitindo que os EUA firmem "acordos executivos" com determinados governos estrangeiros "qualificados", possibilitando a suspensão de restrições impostas pelo 'Electronic Communications Privacy Act' e que as autoridades de aplicação da lei desses países solicitem o acesso ao conteúdo de comunicações de cidadãos e residentes não americanos diretamente aos fornecedores de serviços[cvii].

Na mesma reunião, o Conselho adotou a decisão que autorizou a participação da União Europeia nas negociações para a adoção de um Segundo Protocolo adicional à Convenção de Budapeste sobre o Cibercrime e que conferiu à Comissão Europeia um mandato para a representar ao nível do Conselho da Europa, bem como a Adenda a essa Decisão, com definição de objetivos e diretrizes sobre as negociações, em particular sobre relações e compatibilização com o direito da União Europeia e outros acordos, simplificação e reforço da cooperação, cooperação direta com fornecedores de serviços, reforço de salvaguardas no âmbito transferência internacional de dados e dos requisitos de proteção de dados pessoais[cviii]. Finalizado em dezembro de 2021 e aberto à assinatura a 12 de maio de 2022, o Segundo Protocolo[cix] entrará em vigor após a ratificação por cinco Estados Partes da Convenção[cix].

Tendo em conta que as disposições do Protocolo se inserem num domínio abrangido, em grande medida, por regras comuns na aceção do artigo 3.º, n.º 2, do TFUE, e que a União não pode ratificar o Protocolo, por não ser Parte da Convenção, após o parecer favorável do Parlamento Europeu, o Conselho adotou uma Decisão[cx], em 14.02.2023, que autoriza os Estados-Membros da UE a ratificar o Segundo Protocolo, no interesse da UE, e indica várias reservas, declarações, notificações e comunicações relativamente ao Protocolo, consideradas necessárias para assegurar a compatibilidade deste com o direito da União ou importantes para assegurar a aplicação uniforme do Protocolo pelos Estados-Membros da União que são Parte no Protocolo (Partes que são Estados-Membros) nas suas relações com países terceiros que são Partes no Protocolo (Partes que são países terceiros), bem como a aplicação efetiva do Protocolo. Aqui se incluem reservas relativas ao direito de não aplicar o artigo 7.º (divulgação de dados relativos aos assinantes) e ao direito de não o aplicar a determinados tipos de números de acesso, que deve ser limitada em relação a números de acesso diferentes dos necessários para fins exclusivos de identificação do utilizador, bem como a declaração relativa ao artigo 7.º, n.º 1, no sentido de que a injunção referida aí referida deve ser emitida por um procurador ou outra autoridade judicial, ou sob a sua supervisão, ou ainda sob supervisão independente, bem como ao artigo 9.º, quanto à divulgação expedita de dados informáticos armazenados em caso de emergência, a omitir no caso de se tratar de executar pedidos cuja finalidade seja apenas a divulgação de dados relativos aos assinantes, e a notificações de

emissão de injunção a prestadores de serviços em território nacional (art.º 7.º, n.º 5), sobre informações adicionais para execução da injunção prevista no art.º 8.º, n.º 1. Inclui-se ainda uma indicação aos Estados-membros de transmissão de comunicação[[cxi](#)] às autoridades competentes dos Estados Unidos para efeitos do artigo 14.º, n.º 1.b, do Protocolo, de que o “*Umbrella Agreement*” (“Acordo-Quadro”) se aplica às transferências recíprocas de dados pessoais efetuadas ao abrigo do Protocolo entre as autoridades competentes, tendo em conta que o “Acordo-Quadro” deve ser complementado por salvaguardas adicionais que integrem os requisitos próprios da transferência de provas eletrónicas diretamente pelos prestadores de serviços, e não entre autoridades, tal como previsto no Protocolo.

Na parte que agora releva, o Segundo Protocolo fornece instrumentos para reforçar a cooperação e a obtenção de provas eletrónicas, estabelecendo a obrigação de criar canais específicos para uma cooperação rápida e direta entre as autoridades estatais e entre estas autoridades e entidades privadas estabelecidas no território de outro Estado Parte, incluindo as seguintes medidas: um procedimento que prevê a cooperação direta entre as autoridades de uma Parte e uma entidade que presta serviços de registro de nomes de domínio no território de outra Parte, para a obtenção de informações sobre registros de nomes de domínio na Internet (artigo 6.º); um procedimento que prevê a cooperação direta entre as autoridades de uma Parte e um prestador de serviços no território de outra Parte para obter informações sobre subscritores (artigo 7.º); uma disposição que permite que uma Parte requerente emita uma ordem a ser apresentada como parte de uma solicitação a outra Parte e que a Parte requerida possa dar cumprimento a essa ordem, obrigando um provedor de serviços em seu território a fornecer informações sobre assinantes ou dados de tráfego que estejam em posse ou sob o controle desse provedor (artigo 8.º)[[cxii](#)].

A regulamentação das provas eletrónicas tem também concentrado os esforços e a atenção das Nações Unidas.

Através da Resolução 74/247, adotada em 27.12.2019, relativa ao combate à utilização das tecnologias da informação e das comunicações para fins criminosos[[cxiii](#)], a Assembleia Geral da ONU criou um Comité Intergovernamental de Peritos (*ad hoc committee*) com representantes de todas as regiões “para elaborar uma convenção internacional abrangente sobre o combate ao uso de tecnologias da informação e comunicação para fins criminosos, levando em consideração os instrumentos internacionais existentes e os esforços ao nível nacional, regional e internacional para combater o uso de tecnologias da informação e comunicação para fins criminosos, em particular os trabalhos do “*open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime*”[[cxiv](#)], criado em 2010.

Seguindo largamente a Convenção do Conselho da Europa de 2001 (Convenção de Budapeste)[[cxv](#)] e não contendo disposições sobre obtenção direta de provas eletrónicas detidas por fornecedores de serviços no território de outro Estado, diversamente do que sucede com o Segundo Protocolo Adicional à Convenção de Budapeste[[cxvi](#)] e com a legislação da União Europeia, a

Convenção das Nações Unidas contra o Cibercrime («Convenção de Hanói»)[[cxvii](#)], na sequência de um complexo processo negocial, foi adotada pela Assembleia Geral das Nações Unidas, pela resolução 79/243[[cxviii](#)], em 24.12.2024.

A UE participou nas negociações e esteve presente na cerimónia de assinatura, onde apresentou uma declaração conjunta com os Estados-membros, sublinhando a importância da Convenção no combate e na cooperação internacional contra o cibercrime e na obtenção de provas eletrónicas, em linha com a Convenção de Budapeste e com outros instrumentos internacionais de âmbito universal, no quadro do Estado de direito e do respeito pelos direitos fundamentais[[cxix](#)].

Uma vez que a Convenção prevê procedimentos que visam melhorar o acesso transfronteiriço a provas em formato eletrónico e um elevado nível de garantias e reconhecendo que tornar-se parte na Convenção promoverá a coerência dos esforços da União na luta contra a cibercriminalidade e contra outras formas de criminalidade a nível mundial, o Conselho, por Decisão 4.6.2026[[cxx](#)], aprovou a Convenção e as reservas relevantes para assegurar a compatibilidade da Convenção com o direito da União, a aplicação uniforme da Convenção entre os Estados-Membros nas suas relações com os Estados Partes que não são membros da UE, bem como a aplicação efetiva da Convenção, a apresentar em nome da União Europeia, tendo em conta as competências partilhadas entre os Estados-membros e a União[[cxxi](#)], na medida que a Convenção possa afetar regras comuns ou alterar o seu âmbito de aplicação, definindo ainda o âmbito da sua competência no que diz respeito às matérias regidas pela Convenção na “Declaração de competência da União Europeia feita em conformidade com o artigo 64.º, n.ºs 3 e 4, da Convenção”.

7. As condições de aplicação das ordens europeias de produção (OEP) e de conservação (OEC) de prova: obrigações dos Estados-membros

O Regulamento 2022/1543, em vigor desde agosto de 2023, é aplicável a partir de 18 de agosto de 2026 (artigo 34.º).

Nos termos do artigo 33.º, a Comissão deverá realizar uma avaliação do Regulamento até 18 de agosto de 2029 (seis anos após a sua entrada em vigor), transmitindo o respetivo relatório ao Parlamento Europeu, ao Conselho, à Autoridade Europeia para a Proteção de Dados e à Agência dos Direitos Fundamentais da União Europeia incluindo uma análise da aplicação e dos resultados alcançados no que diz respeito aos seus objetivos, bem como uma análise de impacto nos direitos fundamentais.

No que diz respeito à Diretiva, que constitui uma condição prévia necessária ao funcionamento do regulamento, o artigo 7.º prevê que os Estados-Membros ponham em vigor as leis, regulamentos e disposições administrativas necessárias para dar-lhe cumprimento até 18 de fevereiro de 2025, devendo a Comissão levar a efeito a sua avaliação até 18 de agosto de 2029 (artigo 8.º), em paralelo com a avaliação do Regulamento.

O funcionamento do sistema agora instituído assenta, como se viu, num conjunto de condições e obrigações da responsabilidade dos Estados-membros, que requerem, por um lado, a adequação e aprovação de legislação interna para a aplicação do Regulamento e para a transposição da Diretiva e do estabelecimento, em coordenação com a Comissão Europeia, da infraestrutura tecnológica necessária à transmissão e execução das OEP e OEC e, por outro, ao estabelecimento dos pontos de acesso ao sistema informático descentralizado previsto no Regulamento [\[cxxii\]](#). Trata-se obviamente, de um projeto ambicioso, integrado na estratégia e medidas de digitalização da justiça na União Europeia [\[cxxiii\]](#), envolvendo significativos recursos financeiros e tecnológicos e a organização e gestão adequadas ao nível interno, em coordenação e com a participação dos vários intervenientes no complexo sistema de justiça penal, no âmbito das suas atribuições e competências.

Em 1.6.2026, o Governo apresentou à Assembleia da República a Proposta de Lei n.º 83/XVII/1.^a visando transpor a Diretiva (UE) 2023/1544 e estabelecer o regime sancionatório aplicável às infrações das normas constantes da Diretiva e do Regulamento (UE) 2023/1543 [\[cxxiv\]](#), tendo sido atribuída urgência ao processo legislativo. A proposta prevê: (a) a designação da Autoridade Nacional de Comunicações (ANACOM) como autoridade central para efeitos de recolha, organização e tratamento da informação relativa aos estabelecimentos designados e aos representantes legais, em cooperação com as autoridades nacionais e de outros Estados-membros, prestando informações e apoio em sede de execução do Regulamento e da Diretiva; (b) as regras aplicáveis à designação de estabelecimentos designados e à nomeação de representantes legais; (c) o regime sancionatório requerido pelo Regulamento e pela Diretiva; (d) a designação da Procuradoria-Geral da República como autoridade central para efeitos do disposto no n.º 6 do artigo 4.º do Regulamento (transmissão administrativa dos COEP e COEC).

8. Observações finais

O funcionamento adequado da OEP e da OEC exige soluções legislativas e de organização que garantam um sistema robusto e seguro de proteção de dados pessoais, em conformidade com os requisitos e exigências impostos pelo Regulamento Geral sobre a Proteção de Dados (“RGPD”) e pela Diretiva (UE) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados na UE. Como já se observou noutro local [\[cxxv\]](#), subsistem, neste domínio, questões em aberto que não podem ser negligenciadas.

Em primeiro lugar, a da adaptação da legislação processual penal aos princípios e regras de tratamento de dados pessoais. Sendo a área de mais profunda interferência na privacidade, no direito à proteção de dados pessoais e em outros direitos fundamentais, a atividade de recolha e obtenção de prova no processo penal traduz-se, por definição, em atos («operações») de tratamento de dados pessoais necessários à realização das finalidades do processo, nas suas várias fases, desde

as medidas cautelares e de polícia (artigos 248.º e segs. do CPP), ao inquérito (artigo 262.º, n.º 1, e 267.º e segs. do CPP), à instrução (artigo 286.º, n.º 1, e segs. do CPP), ao julgamento (artigos 339.º, n.º 4, 340.º e segs., 368.º, 369.º e 370.º do CPP), ao recurso (artigo 399.º e segs. do CPP), à execução da pena, e, de modo geral, a todos os atos processuais. A adequação do Código de Processo Penal e legislação complementar à Lei n.º 59/2019, que transpõe a Diretiva 2016/680, visaria, nomeadamente, garantir a observância dos critérios de limitação material e temporária e de minimização dos dados e de operações e regras de tratamento em função das finalidades do tratamento com referência a cada uma das fases do processo, e de necessidade, adequação e proporcionalidade, que conformam todo o processo. A consideração destas exigências, no respeito pelos direitos fundamentais das pessoas sobre as quais são recolhidas informações (muitas delas sem interesse após o encerramento do inquérito), imporão que devam equacionar-se alterações no sentido de limitar e impedir o acesso a dados que, findo o inquérito, não constituam objeto ou meio de prova, por quem nisso não possa ter interesse (na decorrência do já estabelecido no n.º 7 do art.º 86.º do CPP).

Em segundo lugar, as questões relacionadas com garantias dos direitos dos titulares dos dados conferidos pelo RGPD e pela Diretiva 680. Sendo os direitos de informação, acesso, retificação, apagamento e limitação do tratamento exercidos “nos termos da lei” processual e demais legislação aplicável^[cxxvii], importaria esclarecer a necessidade de assegurar a garantia e o exercício efetivo dos direitos dos titulares dos dados e a sua tutela jurisdicional efetiva, relativamente a atos de magistrados praticados na “função jurisdicional”^[cxxviii] e quanto a atos praticados fora dessa função, bem como a de definir a atribuição de competências do “responsável pelo tratamento” relativamente a tais atos. Sendo que o respeito pelos princípios sempre seria inconciliável com a atribuição de estatuto e competências de “responsável pelo tratamento” de dados no exercício de “funções jurisdicionais” a órgãos de gestão das magistraturas, sem competências jurisdicionais. Isto sem prejuízo da participação destes órgãos de gestão em órgão ou órgãos do sistema judicial que, assegurando a independência deste, como previsto no RGPD e na Diretiva 680, possam exercer funções de autoridade de controlo^[cxxviii]. A conceção, organização e poderes de autoridade de controlo continua a ser uma das questões em aberto, quer no que se refere ao tratamento de dados pelos magistrados no exercício de «funções jurisdicionais», quer no que diz respeito ao tratamento de dados «não jurisdicionais». A situação atual evidencia uma carência de lei, em resultado da regulamentação incompleta do RGPD a nível interno (no que respeita ao tratamento de dados no sistema judicial) e da transposição, também incompleta, da Diretiva 2016/680^[cxxix].

A perseguição e o controlo da criminalidade, nomeadamente da criminalidade no ciberespaço, constituem dever do Estado, ao qual compete assegurar a preservação dos valores essenciais do Estado de Direito e proteger os direitos fundamentais das pessoas, nomeadamente das vítimas e dos agentes do crime. Por definição, a intervenção penal é uma tarefa do Estado que constitui sempre uma ingerência nos direitos fundamentais, admissível por razões de necessidade, adequação e proporcionalidade, com divisão de tarefas entre o legislador e os órgãos encarregados de julgar e

aplicar o direito, por imposição do princípio da independência e separação dos poderes, vinculados a idênticos critérios.

O grande desafio que aqui se impõe é o de garantir sempre o desejável equilíbrio entre as necessidades de combate ao crime, garantindo a paz social e a segurança, e o respeito pelos direitos fundamentais das pessoas, reconhecidos constitucionalmente e nos instrumentos internacionais vigentes na ordem interna.

Quanto maior a gravidade, a sofisticação e invisibilidade do crime, mais elevada tende a ser a interferência nos direitos fundamentais, através de medidas de investigação mais intrusivas, mas necessárias, nomeadamente, para a recolha de prova digital, elevando a tensão máxima entre as finalidades do processo penal em conflito, entre a liberdade e a segurança. Por isso mesmo, mais intensa deve ainda ser a intervenção do juiz, desde as fases mais precoces e ao longo de todo o processo, para garantia dos direitos das pessoas e para assegurar a sua proteção judicial efetiva.

Um caso exemplar desta tensão é o decorrente da declaração de invalidade, pelo Tribunal de Justiça da União Europeia, da Diretiva 2006/24/CE^[cxxx], relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações e que alterou a Diretiva 2002/58/CE. A Diretiva era aplicável unicamente aos dados de tráfego e dados conexos necessários para identificar o assinante ou o utilizador registado e aos dados de localização (aos denominados “metadados”). A obrigação imposta era a de conservar e proteger, de forma segura, por período entre 6 meses e 2 anos, os dados necessários para encontrar e identificar a fonte e o destino de uma comunicação, data, hora, duração e tipo de comunicação, o equipamento de telecomunicações, a localização do equipamento de comunicação móvel, mas sem acesso ao conteúdo das comunicações. A conservação tinha por finalidade a deteção, investigação e repressão do terrorismo e de crimes graves e o acesso dependeria sempre de ordem ou autorização judicial, caso a caso, nos termos da lei do processo relativa à aquisição de prova, permitindo restrições, por lei, à confidencialidade das comunicações (privacidade) e ao direito à proteção de dados pessoais (incluindo eliminação ou apagamento e anonimização de dados de tráfego e de localização ou consentimento para conservação de dados de localização).

Apesar de visar garantir o respeito dos princípios e dos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, o Tribunal de Justiça da União Europeia, no acórdão *Digital Rights Ireland*,^[cxxx] de 8.4.2014, declarou a invalidade da Diretiva, afirmando que “o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta”.

Ora, convém salientar, o Regulamento 2023/1543 e a Diretiva 2023/1544 regulam o acesso e a obtenção de dados como prova, o que significa que pressupõem a existência desses dados; não regulam as obrigações de conservação de dados, igualmente importante em matéria de prova eletrónica. A necessidade de uma regulamentação adequada em matéria de conservação de dados

é inegável, pois que um crime é frequentemente descoberto apenas após ter decorrido um período de tempo considerável desde a sua prática. Se, nesses casos, os dados não forem conservados ou forem conservados por um período demasiado curto, todas as regras que regem a sua obtenção correm o risco de ter uma aplicação limitada.

A questão permanece^[cxxxii], sem resposta uniforme e coerente na União e, na falta de acordo, corre-se o risco de não se dispor nem de meios de investigação nem de meios de defesa das pessoas e da sociedade contra as formas de crime grave e mais sofisticado, tendo como resultado uma indesejável e inquietante negação do próprio Estado de direito.

(*) O Sumário Executivo foi redigido com recurso ao www.chatgpt.com.

(**) O Resumo foi redigido com recurso ao www.chatgpt.com.

(***) As Palavras-Chave foram redigidas com recurso ao www.chatgpt.com.

[i] Como se sublinhou na intervenção «A Cooperação Judiciária e Policial Internacional: A importância de uma rede de cooperação judiciária em matéria penal», em *Cooperação Judiciária e Policial - Seminário Internacional realizado nos dias 3 e 4 de maio de 2017 em Bissau*, Guiné-Bissau, AAVV, Camões, I.P. - Projeto de Apoio à Consolidação do Estado de Direito (Lisboa, 2017, em https://www.paced-paloptl.com/uploads/publicacoes_ficheiros/paced_confgb.pdf).

[ii] Informação extraída do documento de trabalho da Comissão “Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings” [SWD(2018) 118, 17.4.2018], que acompanhou a proposta da Comissão Europeia que esteve na origem do Regulamento (UE) 2023/1543 e da Diretiva (UE) 2023/1544 («e-Evidence package»), em <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018SC0118>.

[iii] Instrumentos que, possibilitando a transmissão de pedidos e os contactos diretos entre as autoridades judiciárias competentes na União Europeia, e no princípio do reconhecimento mútuo das decisões judiciais [artigo 82.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia («TFUE»)], adaptaram à União Europeia, desenvolvendo-os e substituindo-os, os instrumentos de cooperação clássica baseados no pedido, os quais, note-se, ainda hoje, com maior ou menor intervenção das autoridades políticas e administrativas, continuam a ser dominantes na cooperação internacional, apesar de inadequados à obtenção de provas eletrónicas. Dispõe o artigo 82.º do TFUE: “1. A cooperação judiciária em matéria penal na União assenta no princípio do

reconhecimento mútuo das sentenças e decisões judiciais e inclui a aproximação das disposições legislativas e regulamentares dos Estados-Membros (...). O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, adotam medidas destinadas a: a) Definir regras e procedimentos para assegurar o reconhecimento em toda a União de todas as formas de sentenças e decisões judiciais; (...) d) Facilitar a cooperação entre as autoridades judiciárias ou outras equivalentes dos Estados-Membros, no âmbito da investigação e do exercício da ação penal, bem como da execução de decisões”.

[iv] Cfr. o preâmbulo do Regulamento (UE) 2023/1543 e “Sirius EU Electronic Evidence Situation Report 2024”, Europol-Eurojust, em <https://www.europol.europa.eu/publications-events/publications/sirius-eu-electronic-evidence-situation-report-2024>.

[v] O elevado grau de integração e de cooperação no quadro dos Tratados, permitiu realizar o “espaço de liberdade, segurança e justiça”, enquanto objetivo da União no Tratado de Amesterdão (1997), consolidado no Tratado de Lisboa (2007), com realizações extraordinárias neste domínio (artigos 29.º do TUE (Amesterdão) e 3.º, n.º 2, e Título V do TFUE (Lisboa)). (Tratado de Amesterdão, artigo 29.º: “(...) será objectivo da União facultar aos cidadãos um elevado nível de protecção num espaço de liberdade, segurança e justiça, mediante a instituição de acções em comum entre os Estados-Membros no domínio da cooperação policial e judiciária em matéria penal e a prevenção e combate do racismo e da xenofobia”. Tratado de Lisboa, artigo 3.º TUE: “2. A União proporciona aos seus cidadãos um espaço de liberdade, segurança e justiça sem fronteiras internas, em que seja assegurada a livre circulação de pessoas, em conjugação com medidas adequadas em matéria de controlos na fronteira externa, de asilo e imigração, bem como de prevenção da criminalidade e combate a este fenómeno”. Artigo 67.º: “1. A União constitui um espaço de liberdade, segurança e justiça, no respeito dos direitos fundamentais. (...) 3. A União envida esforços para garantir um elevado nível de segurança, através de medidas de prevenção da criminalidade, do racismo e da xenofobia e de combate contra estes fenómenos, através de medidas de coordenação e de cooperação entre autoridades policiais e judiciárias e outras autoridades competentes, bem como através do reconhecimento mútuo das decisões judiciais em matéria penal e, se necessário, através da aproximação das legislações penais”.

[vi] Ratificação: RAR n.º 32/2004, de 02/04, e DPR n.º 19/2004, de 02/04 (DR I-A de 02/04/2004). Informação em <https://www.ministeriopublico.pt/instrumento/convencao-das-nacoes-unidas-contracriminalidade-organizada-transnacional-0>.

[vii] Ratificação: RAR n.º 88/2009, de 15/09, e DPR n.º 91/2009, de 15/09 (DR I de 15/09/2009). Informação em <https://www.ministeriopublico.pt/instrumento/convencao-sobre-o-cibercrime-0>.

[viii] A Convenção (ETS 185) é complementada pelo Primeiro Protocolo Adicional, que trata da criminalização de atos de natureza racista e xenófoba cometidos por meio de sistemas informáticos (CETS 189), e pelo Segundo Protocolo Adicional, relativo ao reforço da cooperação internacional e à divulgação de provas eletrónicas (CETS 224) (*infra*). Entrou em vigor em 1.7.2004, estando ratificada

por todos os Estados-membros do Conselho da Europa, à exceção da Irlanda, e 37 Estados não membros, no total de 82 ratificações e adesões (informação em <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty-num=185>, acesso em 1.7.2026).

[ix] “Production order”, no original, em inglês, terminologia usada no “e-Evidence package” da União Europeia (“ordem de produção”, na versão em língua portuguesa).

[x] Alterada pela Lei n.º 79/2001, de 24/11, que transpõe a Diretiva (UE) 2019/713, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, e pelo Decreto-Lei n.º 125/2025, de 4/12, que transpõe a Diretiva (UE) 2022/2555, de 14 de dezembro de 2022 (Lei da Cibersegurança).

[xi] O artigo 12.º transpõe parcialmente os artigos 16.º e 17.º da Convenção, quanto à “conservação” de dados.

[xii] O artigo 13.º transpõe a segunda parte do artigo 17.º da Convenção.

[xiii] O artigo 14.º transpõe o artigo 18.º da Convenção (“injunção de comunicação, na tradução portuguesa de “production order”).

[xiv] *Infra*, 15.

[xv] *Infra*, 13.

[xvi] Informação em https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en.

[xvii] Publicados no JO L 191/118 e no JO L 191/191 de 28.7.2023. O Regulamento, obrigatório e de aplicação direta (artigo 288.º do TFUE), funda-se no artigo 82.º, n.º 1, do TFUE, relativo à cooperação judiciária em matéria penal, assentando no princípio do reconhecimento mútuo das sentenças e decisões judiciais. Por sua vez, a Diretiva, que vincula os Estados-membros destinatários quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios (artigo 288.º do TFUE), tem sua base jurídica nos artigos 53.º e 62.º do TFUE, que dizem respeito à prestação de serviços na União.

[xviii] Em 27.3.2026, a Comissão Europeia anunciou ter decidido iniciar procedimentos de infração, enviando cartas de notificação formal a 22 Estados-membros, entre os quais Portugal, por não terem comunicado a transposição integral da Diretiva (UE) 2023/1544 até essa data (nota de imprensa em https://ec.europa.eu/commission/presscorner/detail/en/inf_26_679). Em 1.6.2026, foi apresentada na Assembleia da República a Proposta de Lei n.º 83/XVII/1.ª, que transpõe a Diretiva (UE) 2023/1544 e estabelece o regime sancionatório aplicável às infrações das normas constantes da referida Diretiva e do Regulamento (UE) 2023/1543 (*infra*, 16), tendo sido atribuída urgência ao processo legislativo

(em <https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetailIniciativa.aspx?BID=356842>, acesso em 2.7.2026).

[xix] Artigo 3.º, n.º 1, do Regulamento.

[xx] Artigo 3.º, n.º 2, do Regulamento.

[xxi] Diretiva 2014/41/UE, de 3 de abril de 2014, relativa à decisão europeia de investigação em matéria penal, transposta pela Lei n.º 88/2017, de 21 de agosto.

[xxii] O artigo 3.º do Regulamento oferece as definições de “prova eletrónica” (dados de assinantes, dados de tráfego ou dados de conteúdo, conservados em formato eletrónico, por um prestador de serviços ou em seu nome, no momento da receção de um certificado de ordem europeia de produção (COEP) ou de um certificado de ordem europeia de conservação (COEC)), de “dados de assinantes” (dados na posse de um prestador de serviços relacionados com a adesão aos seus serviços, que especifica), de «dados de tráfego» (dados relacionados com a prestação de um serviço por um prestador de serviços que servem para fornecer contexto ou informações adicionais sobre esse serviço e que são gerados ou tratados por um sistema de informação do prestador de serviços, que também especifica), e de «dados de conteúdo» (dados num formato digital, como texto, voz, vídeos, imagens e som, que não sejam dados de assinantes ou de tráfego) – art.º 3.º, n.ºs 8, 9, 10 e 11.

[xxiii] Artigos 1.º, 2.º, n.º 2, e 3.º do Regulamento.

[xxiv] Artigo 1.º da Diretiva.

[xxv] Artigo 4.º do Regulamento, que especifica quais são as “autoridades emissoras”, em função da finalidade e das categorias dos dados e do correspondente nível de interferência em direitos fundamentais.

[xxvi] Cfr. os artigos 10.º e 11.º do Regulamento que dispõem sobre a execução dos COEP e COEC.

[xxvii] Artigos 7.º e 9.º do Regulamento.

[xxviii] Sobre restrições aos direitos fundamentais (legalidade e proporcionalidade) importa ter presente o artigo 52.º, n.º 1, da Carta que dispõe: “1. Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.” A anotação a este artigo (“anotações” à Carta, JO C 303 de 14.12.2007) esclarece: “O n.º 1 trata do regime de restrições. A fórmula utilizada inspira-se na jurisprudência do Tribunal de Justiça: «... segundo jurisprudência bem assente, podem ser introduzidas restrições ao exercício desses direitos, (...) desde que essas restrições correspondam, efectivamente, a objectivos de interesse geral prosseguidos pela Comunidade [agora: União] e não constituam, face a esses

objectivos, uma intervenção desproporcionada e intolerável, susceptível de atentar contra a própria essência desses direitos» (acórdão de 13 de Abril de 2000, processo C-292/97, ponto 45)”.

[xxix] Publicada no JO C 202/389, de 7.6.2016. Dispõe o artigo 7.º (Respeito pela vida privada e familiar): “Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações”. E o artigo 8.º (Proteção de dados pessoais) “1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente”. Quanto à interpretação da “Carta”, estabelece o artigo 6.º, n.º 2, TUE: “Os direitos, as liberdades e os princípios consagrados na Carta devem ser interpretados de acordo com as disposições gerais constantes do Título VII da Carta que regem a sua interpretação e aplicação e tendo na devida conta as anotações a que a Carta faz referência, que indicam as fontes dessas disposições”.

As “anotações” à Carta (JO C 303 de 14.12.2007), auxiliando na interpretação, referem: (a) em anotação ao artigo 7.º: “Os direitos garantidos no artigo 7.º correspondem aos garantidos pelo artigo 8.º da CEDH. Para ter em conta a evolução técnica, o termo «correspondência» foi substituído por «comunicações». Nos termos do n.º 3 do artigo 52.º, este direito tem um sentido e um âmbito iguais aos do artigo correspondente da CEDH. Por conseguinte, as restrições susceptíveis de lhe serem legitimamente impostas são idênticas às toleradas no quadro do artigo 8.º em questão: «1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.»”: (b) em anotação ao artigo 8.º: “Este artigo baseou-se no artigo 286.º do Tratado que institui a Comunidade Europeia e na Directiva 95/46/CE do Parlamento Europeu e do Conselho, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31), bem como no artigo 8.º da CEDH e na Convenção do Conselho da Europa para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, de 28 de Janeiro de 1981, ratificada por todos os Estados-Membros. O artigo 286.º do Tratado CE é substituído pelo artigo 16.º do Tratado sobre o Funcionamento da União Europeia e pelo artigo 39.º do Tratado da União Europeia. É também feita referência ao Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).”

[xxx] Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (...) JO L 119/1, de 4.5.2016.

[xxxi] Diretiva (UE) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, JO L 119/89, de 4.5.2016. A Diretiva foi transposta para o direito interno pela Lei n.º 59/2019, de 8 de agosto.

[xxxii] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37). A Diretiva foi transposta para o direito interno pela Lei n.º 41/2004, de 18 de agosto (alterada pela Lei n.º 46/2012, de 29 de agosto, que transpõe a Diretiva n.º 2009/136/CE, na parte que altera a Diretiva n.º 2002/58/CE, e pela Lei n.º 16/2022, de 16 de agosto, que aprova a Lei das Comunicações Eletrónicas).

[xxxiii] Preâmbulo, 16.

Artigo 47.º da Carta ("Direito à ação e a um tribunal imparcial): "Toda a pessoa cujos direitos e liberdades garantidos pelo direito da União tenham sido violados tem direito a uma ação perante um tribunal nos termos previstos no presente artigo. Toda a pessoa tem direito a que a sua causa seja julgada de forma equitativa, publicamente e num prazo razoável, por um tribunal independente e imparcial, previamente estabelecido por lei. Toda a pessoa tem a possibilidade de se fazer aconselhar, defender e representar em juízo (...)." Anotação ao artigo 47.º (em "anotações", supra, 29): "O primeiro parágrafo baseia-se no artigo 13.º da CEDH: «Qualquer pessoa cujos direitos e liberdades reconhecidos na presente Convenção tiverem sido violados tem direito a recurso perante uma instância nacional, mesmo quando a violação tiver sido cometida por pessoas que actuarem no exercício das suas funções oficiais.» Porém, no direito da União, a protecção é mais alargada, dado que garante um direito a acção em tribunal. O Tribunal de Justiça consagrou este direito como princípio geral do direito da União no seu acórdão de 15 de Maio de 1986 (processo 222/84, Johnston, Colect. 1986, p. 1651; ver também os acórdãos de 15 de Outubro de 1987, processo 222/86, Heylens, Colect. 1987, p. 4097, e de 3 de Dezembro de 1992, processo C-97/91, Borelli, Colect. 1992, p. I-6313). Segundo o Tribunal de Justiça, este princípio geral do direito da União aplica-se também aos Estados-Membros quando estes aplicam o direito da União. (...)"

[xxxiv] Diretiva 2010/64/UE, de 20 de outubro de 2010, relativa ao direito à interpretação e tradução em processo penal (JO L 280 de 26.10.2010, p. 1).

[xxxv] Diretiva 2012/13/UE, de 22 de maio de 2012, relativa ao direito à informação em processo penal (JO L 142 de 1.6.2012, p. 1).

[xxxvi] Diretiva 2013/48/UE, de 22 de outubro de 2013, relativa ao direito de acesso a um advogado em processo penal e nos processos de execução de mandados de detenção europeus, e ao direito de informar um terceiro aquando da privação de liberdade e de comunicar, numa situação de privação de liberdade, com terceiros e com as autoridades consulares (JO L 294 de 6.11.2013, p. 1).

[xxxvii] Diretiva (UE) 2016/343, de 9 de março de 2016, relativa ao reforço de certos aspetos da presunção de inocência e do direito de comparecer em julgamento em processo penal (JO L 65 de 11.3.2016, p. 1).

[xxxviii] Diretiva (UE) 2016/800, de 11 de maio de 2016, relativa a garantias processuais para os menores suspeitos ou arguidos em processo penal (JO L 132 de 21.5.2016, p. 1).

[xxxix] Diretiva (UE) 2016/1919, de 26 de outubro de 2016, relativa ao apoio judiciário para suspeitos e arguidos em processo penal e para as pessoas procuradas em processos de execução de mandados de detenção europeus (JO L 297 de 4.11.2016, p. 1).

[xl] Capítulo V do Regulamento (artigos 19.º-26.º).

[xli] Cada Estado-Membro deve suportar os custos de instalação, funcionamento e manutenção dos pontos de acesso do sistema informático descentralizado pelo qual esse Estado-Membro é responsável, bem como os custos de criação e adaptação dos respetivos sistemas informáticos nacionais pertinentes, a fim de os tornar interoperáveis com os pontos de acesso, assim como os custos de gestão, funcionamento e manutenção desses sistemas (artigo 23.º do Regulamento).

[xlii] Regulamento (UE) 2022/850, de 30 de maio de 2022, relativo a um sistema informatizado de intercâmbio eletrónico transfronteiriço de dados no domínio da cooperação judiciária em matéria civil e penal (sistema e-CODEX) (JO L 150 de 1.6.2022, p. 1). Nos termos do art.º 10.º, n.º 4, do Regulamento e-CODEX, a eu-LISA (Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça, criada pelo Regulamento (UE) 2018/1726 de 14 de novembro de 2018), assumiu a responsabilidade pelo sistema e-CODEX em 3 de junho de 2024, nos termos da Decisão de Execução (UE) 2024/1272 da Comissão de 7 de maio de 2024 sobre a declaração da conclusão do processo de transferência e tomada de controlo do sistema e-CODEX (JO L de 14.5.2024).

[xliii] Artigo 19.º, n.ºs 2 e 3, do Regulamento.

[xliv] Preâmbulo, 81-84.

[xlv] Regulamento de Execução (UE) 2025/1550 da Comissão, de 28 de julho de 2025, que estabelece as especificações técnicas e outros requisitos para o sistema informático descentralizado referido no Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho, JO L de 29.7.2025, em <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32025R1550>.

[xlvi] Preâmbulo, 89-90.

[xlvi] Regulamento (UE) 2018/1725, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados ((JO L 295 de 21.11.2018, p. 39).

[xlviii] *Supra*, 30.

[xlix] *Supra*, 31.

[l] Artigo 22.º do Regulamento.

[li] Havendo autores que, a este propósito, falam mesmo de uma “revolução”, de uma “mudança de paradigma” ou da “privatização” da cooperação”. A alegada fragilização da proteção dos direitos fundamentais, decorrente do afastamento da autoridade judiciária de execução no território do Estado-membro de localização dos dados, constituiu um dos temas mais controversos ao longo do processo legislativo.

[lii] Sobre o princípio do reconhecimento mútuo de decisões judiciais em matéria penal, sua dimensão e alcance, cfr. J. Lopes da Mota, «Reconhecimento mútuo de decisões judiciais em matéria penal na União Europeia», *Comentário da Convenção Europeia dos Direitos Humanos e dos Protocolos Adicionais*, Paulo Pinto de Albuquerque (Org.), Universidade Católica Editora, Vol. II, Lisboa, 2019, pp. 1142ss.

[liii] Preâmbulo, ponto 13.

[liv] A Carta tem a força jurídica dos Tratados (art.º 6.º, n.º 1, do TUE).

[lv] Declaração 21 anexada à Ata Final da Conferência Intergovernamental que adotou o Tratado de Lisboa: “21. Declaração sobre a proteção de dados pessoais no domínio da cooperação judiciária em matéria penal e da cooperação policial. A Conferência reconhece que, atendendo à especificidade dos domínios em causa, poderão ser necessárias disposições específicas sobre proteção de dados pessoais e sobre a livre circulação desses dados, nos domínios da cooperação judiciária em matéria penal e da cooperação policial, com base no artigo 16.º do Tratado sobre o Funcionamento da União Europeia” (JO C 326/347, de 26.10.2012).

[lvi] Sobre este ponto, cfr. Marco Stefan and Gloria González Fuster, «Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters», CEPS Paper in Liberty and Security in Europe No. 2018-07, November 2018, www.ceps.eu.

[lvii] Artigo 267.º do TFUE (recurso prejudicial).

[lviii] Interpretação de disposições da Decisão-Quadro 2002/584/JAI, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros, o primeiro ato legislativo da União a dar expressão a este princípio. Cfr. acórdãos de 5.4.2016, nos processos C-404/15 e C-659/15 (*Aranyosi e Căldăraru*), ECLI:EU:C:2016:198, de 25.7.2016, no

processo C-220/18 (*ML*), ECLI:EU:C:2018:589, e de 15.10.2019, no processo C-128/18 (*Dorobantu*), ECLI:EU:C:2019:857.

[lix] Interpretando disposições da mesma decisão-quadro. Cfr. acórdãos de 25.7.2018, no processo C-216/18 PPU (*LM*), 2018 ECLI:EU:C:2018:586, e de 17.12.2020, nos processos C-354/20 PPU (*L*) e 412/20 PPU (*P*), 2020 ECLI:EU:C:2020:1033.

[lx] *Infra*, 10-11.

[lxi] Cfr. considerandos 34, 36, 37, 51, 64 e 80 do preâmbulo e artigos 4.º, 5.º, 6.º, 8.º, 10.º, 12.º e 18.º do Regulamento 2023/1543.

[lxii] Artigo 3.º, n.º 3, do Regulamento.

[lxiii] Artigo 3.º, n.º 4, do Regulamento.

[lxiv] Os artigos 5.º e 6.º do Regulamento especificam as condições em que pode ser emitida uma OEP e uma OEC;

[lxv] Artigo 5.º, n.º 3, do Regulamento.

[lxvi] Artigos 3.º a 8.º da Diretiva 2013/40/UE, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação.

[lxvii] Artigos 3.º a 8.º da Diretiva 2019/713 de 17 de abril de 2019 relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário.

[lxviii] Artigos 3.º a 12.º e 14.º da Diretiva (UE) 2017/541, de 15 de março de 2017, relativa à luta contra o terrorismo.

[lxix] Artigos 3.º a 7.º da Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil.

[lxx] Artigo 5.º, n.º 4, do Regulamento.

[lxxi] Artigo 5.º, n.º 2, do Regulamento.

[lxxii] Artigo 8.º do Regulamento.

[lxxiii] Artigos 10.º e 17.º do Regulamento.

[lxxiv] Que permite o adiamento, a limitação ou a não prestação aos titulares dos dados das informações a que se refere o n.º 2 (informações sobre o fundamento jurídico do tratamento; o prazo de conservação dos dados pessoais ou, se tal não for possível, os critérios usados para definir esse período; as categorias de destinatários dos dados pessoais, inclusive nos países terceiros ou nas

organizações internacionais; informações adicionais, especialmente se os dados pessoais forem recolhidos sem conhecimento do seu titular) “se e enquanto tais medidas constituírem medidas necessárias e proporcionadas numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de: a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais; b) Evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais; c) Proteger a segurança pública; d) Proteger a segurança nacional; e) 4. Proteger os direitos e as liberdades de terceiros”. Artigo 13.º do Regulamento.

[lxxv] Artigos 10.º e 11.º do Regulamento.

[lxxvi] Artigos 10.º, n.º 5, e 17.º, n.ºs 1 e 2, do Regulamento.

[lxxvii] Artigos 8.º e 16.º do Regulamento.

[lxxviii] Artigo 12.º e anexo IV do Regulamento.

[lxxix] Artigo 1.º, n.º 2, do Regulamento.

[lxxx] Artigo 13.º do Regulamento.

[lxxxi] Artigo 18.º do Regulamento

[lxxxii] Para informação detalhada sobre o processo negocial e sobre o conteúdo e sentido das disposições acordadas ver G. Forlani, “The E-evidence Package”, 2023, Vol. 18(2), eucrim, pp174–181. DOI: <https://doi.org/10.30709/eucrim-2023-013>, publicado por Max Planck Institute for the Study of Crime, Security and Law.

[lxxxiii] Proposta de Regulamento: COM(2018) 225 final, em <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN>. Proposta de Diretiva: COM(2018) 226 final, (em <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN>). Para uma visão sumária das propostas, ver T. Wahl, “Commission Proposes Legislative Framework for E-evidence”, (2018) eucrim, 35, em <https://eucrim.eu/news/commission-proposes-legislative-framework-e-evidence/>.

[lxxxiv] Diretiva 2014/41/UE, de 3 de abril de 2014, relativa à decisão europeia de investigação em matéria penal, JO L 130, 1.5.2014, 1, alterada pela Diretiva (UE) 2022/228, de 16 de fevereiro de 2022, no que diz respeito à sua harmonização com as regras da União em matéria de proteção de dados pessoais. A Diretiva foi transposta para o direito interno pela Lei n.º 88/2017, de 21 de agosto, alterada pela Lei n.º 42/2023, de 10 de agosto, que transpõe a Diretiva (UE) 2022/228, estabelecendo que ao tratamento de dados pessoais realizados no âmbito da aplicação da DEI é aplicável a Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, e a Lei n.º 34/2009, de 14 de julho, que estabelece o regime jurídico aplicável ao tratamento

de dados referentes ao sistema judicial. Sem prejuízo da sua aplicação entre Estados-membros e Estados terceiros, a Diretiva substitui as disposições correspondentes das seguintes convenções aplicáveis às relações entre os Estados-Membros vinculados à presente diretiva: a) Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal, do Conselho da Europa, de 20 de abril de 1959, e os seus dois Protocolos Adicionais, bem como os acordos bilaterais celebrados nos termos do artigo 26.º dessa Convenção; b) Convenção de Aplicação do Acordo de Schengen; c) Convenção relativa ao Auxílio Judiciário Mútuo em Matéria Penal entre os Estados-Membros da União Europeia, e o respetivo Protocolo (art.º 34.º).

[\[lxxxv\]](#) Acto do Conselho de 29 de maio de 2000 que estabelece, em conformidade com o artigo 34.º do Tratado da União Europeia, a Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia (JO C 197, 12.7.2000) com o objetivo de completar as disposições e facilitar a aplicação entre os Estados-membros da União Europeia: a) Da Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal, de 20 de Abril de 1959 (Conselho da Europa); b) Do Protocolo Adicional à Convenção Europeia de Auxílio Judiciário Mútuo, de 17 de Março de 1978; c) Das disposições sobre auxílio judiciário mútuo em matéria penal da Convenção de 19 de Junho de 1990, de aplicação do Acordo de Schengen de 14 de Junho de 1985. A Convenção foi aprovada para ratificação pela RAR n.º 63/2001, de 16/10 e ratificada pelo DPR n.º 53/2001, de 16/10, DR I-A, de 16/10/2001.

[\[lxxxvi\]](#) Regulamento (UE) 2018/1727 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, que cria a Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust), e que substitui e revoga a Decisão 2002/187/JAI do Conselho, JO L 295, 21.11.2018, 138 (alterado pelo Regulamento (UE) 2022/838 do Parlamento Europeu e do Conselho, de 30 de maio de 2022, no que se refere à preservação, análise e armazenamento, pela Eurojust, de provas relacionadas com genocídio, crimes contra a humanidade, crimes de guerra e infrações penais conexas, JO L 148, 1, de 31.05.2022, pelo Regulamento (UE) 2023/2131 do Parlamento Europeu e do Conselho de 4 de outubro de 2023, no que respeita ao intercâmbio de informações digitais em casos de terrorismo, JO L 2131 de 11.10.2023, e pelo Regulamento (UE) 2025/2082 de 8 de outubro de 2025 no que diz respeito à prorrogação do prazo para a criação do sistema de gestão de processos da Eurojust, JO L 2082 de 15.10.2025). A Lei n.º 36/2003, de 22 de agosto, alterada pela Lei n.º 20/2014, de 15/04, estabelece normas de execução da decisão do Conselho da União Europeia que cria a Eurojust, a fim de reforçar a luta contra as formas graves de criminalidade, e regula o estatuto e competências do respetivo membro nacional.

[\[lxxxvii\]](#) Decisão-Quadro do Conselho, de 13 de junho de 2002, relativa às equipas de investigação conjuntas, JO L 162, 20.06.2002 (alterada pela Diretiva (UE) 2022/211 do Parlamento Europeu e do Conselho de 16 de fevereiro de 2022 no que diz respeito à sua harmonização com as regras da União em matéria de proteção de dados pessoais, JO L 37 de 18.02.2022). Transposta pela Lei n.º 48/2003, de 22 de agosto, que aditou os artigos 145.º-A e 145.º-B à Lei n.º 144/99, que aprova a lei de

cooperação internacional em matéria penal (o art.º 145.º-A foi alterado pela Lei n.º 42/2023, de 10 de agosto, que transpõe a Diretiva (UE) 2022/228).

[lxxxviii] Acordo entre a União Europeia e os Estados Unidos da América sobre auxílio judiciário mútuo JO L 181, 19.7.2003, 34, e Instrumento entre a República Portuguesa e os Estados Unidos da América, feito em Washington em 14 de Julho de 2005, conforme o n.º 3 do artigo 3.º do Acordo entre a União Europeia e os Estados Unidos da América sobre Auxílio Judiciário Mútuo, assinado em Washington em 25 de Junho de 2003, aprovado pela RAR n.º 44/2007, de 10/09; e ratificado pelo DPR n.º 94/2007, de 10/09 (DR I de 10/09/2007).

[lxxxix] Convenção sobre o Cibercrime, adotada em Budapeste em 23 de Novembro de 2001 (ETS n.º 185), aprovada pela RAR n.º 88/2009, de 15/09; e ratificada pelo DPR n.º 91/2009, de 15/09 (DR I de 15/09/2009), complementada pelo Protocolo Adicional Relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, adotado em Estrasburgo em 28 de Janeiro de 2003 (ETS n.º 189).

[xc] A Presidência austríaca do Conselho apresentou um texto de compromisso (que refletia os esforços dos Estados-Membros para chegar a um acordo) ao Conselho «Justiça e Assuntos Internos» (JAI) em dezembro de 2018, em que foi adotada a abordagem geral do Conselho sobre o projeto de regulamento, sendo a abordagem geral sobre o projeto de diretiva alcançada em março de 2019. Apesar do apoio ao texto de compromisso da Presidência austríaca, alguns Estados sugeriram a introdução de um procedimento mais incisivo de notificação das autoridades nos Estados das pessoas afetadas enquanto outros teriam preferido um procedimento mais simplificado que não envolvesse a notificação.

[xci] Em https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PI_EESC:EESC-2018-02737-AC.

[xcii] Opinion 7/2019, EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters, https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf.

[xciii] European Parliament Report A9-0256/2020, https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html>, E-Evidence Package - The Position of the European Parliament, Update 9/08/2021, <https://www.eurojust.europa.eu/sites/default/files/assets/e-evidence-package-the-position-of-the-european-parliament.pdf>> e Report on the proposal for a directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, https://www.europarl.europa.eu/doceo/document/A-9-2020-0257_EN.html

[xciv] No contexto do processo legislativo ordinário da União Europeia, um trólogo é uma negociação interinstitucional informal entre representantes do Parlamento Europeu, do Conselho da União

Europeia e da Comissão Europeia, que tem como objetivo alcançar acordos provisórios sobre propostas legislativas, aceites quer pelo Parlamento, quer pelo Conselho, os legisladores, os quais têm depois de ser adotados através dos procedimentos formais de cada uma destas instituições. Em 2007, o Parlamento e o Conselho emitiram uma declaração comum sobre as regras práticas do processo de codecisão (JO C 145/5 de 30.06.2007), reconhecendo que «o sistema de trilogos demonstrou a sua vitalidade e flexibilidade, aumentando significativamente as possibilidades de acordo na fase de primeira ou segunda leitura e contribuindo para a preparação do Comité de Conciliação».

[xcv] Sobre os avanços dos trabalhos durante a Presidência Portuguesa do Conselho no 1.º semestre de 2021, cfr. o «Report by the Portuguese Presidency on the state of play on the negotiations on the draft Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (e-evidence)», Interinstitutional File 2018/0108 (COD), Council doc. 10316/21, de 30.06.2021 (<https://statewatch.org/news/2021/july/eu-outgoing-portuguese-presidency-report-on-e-evidence-state-of-play/>).

[xcvi] Cfr. «EU: E-evidence: Council note on state of play and possible ways forward», Interinstitutional File: 2018/0108(COD), Council doc. 11681/21, de 16.09.2021 (<https://statewatch.org/news/2021/september/eu-e-evidence-council-note-on-state-of-play-and-possible-ways-forward/>).

[xcvii] Cfr. press release “Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence” (<https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/>).

[xcviii] “Negotiations should be opened with a view to concluding an agreement between the Union and the United States of America on cross-border access by judicial authorities in criminal proceedings to electronic evidence held by a service provider” (do preâmbulo da Decisão, ponto 2). Tal acordo virá, assim, a completar os instrumentos de cooperação policial e judiciária em vigor, nomeadamente o acordo entre os Estados Unidos e a Europol (2001) e o respetivo acordo adicional sobre intercâmbio de dados pessoais (2002), em <https://www.europol.europa.eu/partners-collaboration/agreements/united-states-of-america>, o Acordo entre a União Europeia e os Estados Unidos da América sobre extradição (2003), em [https://eur-lex.europa.eu/eli/agree_internation/2003/516\(1\)/oj/eng](https://eur-lex.europa.eu/eli/agree_internation/2003/516(1)/oj/eng), o Acordo entre a União Europeia e os Estados Unidos da América sobre auxílio judiciário mútuo (2003), em [https://eur-lex.europa.eu/eli/agree_internation/2003/516\(2\)/oj/eng](https://eur-lex.europa.eu/eli/agree_internation/2003/516(2)/oj/eng), o Acordo entre os Estados Unidos e a Eurojust (2006), em <https://www.eurojust.europa.eu/document/agreement-between-eurojust-and-united-states-america>, o Acordo entre a União Europeia e os Estados Unidos da América sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua transferência da União

Europeia para os Estados Unidos para efeitos do Programa de Detecção do Financiamento do Terrorismo (2009), em <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=LEGISSUM:jl0039>, o Acordo entre os Estados Unidos da América e a União Europeia sobre a utilização e a transferência dos registos de identificação dos passageiros para o Departamento da Segurança Interna dos Estados Unidos (2011), em https://eur-lex.europa.eu/eli/agree_internation/2012/472/oj/eng, e o Acordo entre os Estados Unidos da América e a União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, deteção e repressão de infrações penais ('Umbrella Agreement') (2016), em https://eur-lex.europa.eu/eli/agree_internation/2016/2220/oj/eng>.

[xcix] "The agreement should include the necessary safeguards for fundamental rights and freedoms and observe the principles recognised by the Charter of Fundamental rights of the European Union, in particular the right to private and family life, home and communications recognised in article 7 of the Charter, the right to protection of personal data recognised in Article 8 of the Charter, the right to effective remedy and fair trial recognised in Article 47 of the Charter, the presumption of innocence and right of defence recognised in Article 48 of the Charter and principles of legality and proportionality of criminal offences and penalties recognised in Article 49 of the Charter. The agreement should be applied in accordance with those rights and principles" (do preâmbulo da Decisão, ponto 3).

[c] Cfr. press release do Conselho em <https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/>.

[cii] European Commission "Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters", 5.2.2019, COM(2019) 70 final (em <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52019PC0070>) e "Addendum to the Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters", Council doc. ST 10128 2019 ADD 1, de 12.06.2019 (<https://www.consilium.europa.eu/pt/documents/public-register/public-register-search/?AllLanguagesSearch=false&OnlyPublicDocuments=false&DocumentNumber=10128%2F19&DocumentLanguage=EN>). Cfr. também T. Wahl, "E-Evidence: Commission obtains Mandates for EU-US agreement and Negotiations in Council of Europe" (2019) eucrim, 113

[ciii] "Acordo entre os Estados Unidos da América e a União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, deteção e repressão de infrações penais", JO L 336/3 de 10.12.2016.

[ciiv] As negociações iniciaram-se formalmente em 25 de setembro de 2019, tendo sido suspensas em março de 2020, em virtude do Covid-19.

[civ] Sobre o CLOUD Act: informação detalhada em <https://www.eurojust.europa.eu/publication/cloud-act> (Sirius Project Europol-Eurojust, em <https://www.eurojust.europa.eu/sirius>).

[cv] Questão então discutida no conhecido caso *Microsoft v. United States*, em que a Microsoft contestou uma ordem judicial do Federal Bureau of Investigation (FBI) para o fornecimento de e-mails de uma conta-alvo armazenados na Irlanda, argumentando que uma ordem emitida com base no artigo 2703 ("Required disclosure of customer communications or records") do 'Stored Communications Act' não poderia obrigar empresas americanas a fornecer dados armazenados em servidores fora dos Estados Unidos.

[cvi] Para uma visão das divergências e questões a negociar ver Theodore Christakis e Fabien Terpan, «EU-US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options», em *International Data Privacy Law*, 2021, Vol. 11, No. 2, p. 81ss, Oxford University Press, em <https://academic.oup.com/idpl/article/11/2/81/6133744>.

[cvii] Council Decision authorising the European Commission to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), Council Doc. ST-9116/19, 21 de maio de 2019, e Adenda a essa decisão (ver *press release* do Conselho <<https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/>>) e Recomendação de Decisão do Conselho que autoriza a participação nas negociações respeitantes ao Segundo Protocolo Adicional (STCE-185), em <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019PC0071&qid=1774646365891>.

[cviii] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e da divulgação de provas sob a forma eletrónica) (CETS 224).

[cix] Art.º 16.º, n.º 3, do Protocolo. Até agora foi ratificado por quatro Estados (cfr. informação no site do Conselho da Europa, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224>, acesso em 27.6.2026).

[cx] Decisão (UE) 2023/436 do Conselho de 14.2.2023 que autoriza os Estados-Membros a ratificar, no interesse da União Europeia, o Segundo Protocolo Adicional à Convenção sobre o Cibercrime, relativo ao reforço da cooperação e da comunicação de provas eletrónicas (JO L 63/48 28.2.2023). Cfr. ainda a Proposta da Comissão de Decisão do Conselho de 25.11.2021 [COM(2021) 719 final 2021/0383 (NLE)].

[cxi] Os Estados-membros deverão transmitir a seguinte comunicação: "Para efeitos do artigo 14.º o, n.º 1.b, do Segundo Protocolo Adicional à Convenção do Conselho da Europa sobre o Cibercrime ("Protocolo"), [Estado-Membro] considera que o Acordo entre os Estados Unidos da América e a

União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, deteção e repressão de infrações penais ("Acordo-Quadro") se aplica às transferências recíprocas de dados pessoais efetuadas ao abrigo do Protocolo entre as autoridades competentes. No que respeita às transferências realizadas ao abrigo do Protocolo entre prestadores de serviços e autoridades, o Acordo-Quadro só é aplicável em conjugação com outro acordo específico na aceção do artigo 3.º, n.º 1, do Acordo-Quadro que integre os requisitos próprios da transferência de provas eletrónicas diretamente pelos prestadores de serviços, e não entre autoridades. Na falta de um acordo de transferência específico, as referidas transferências podem ser efetuadas ao abrigo do Protocolo, caso em que se aplica o artigo 14.º, n.1.a, em conjugação com o artigo 14.º, n.ºs 2 a 15, do Protocolo".

[cxii] Para informação mais detalhada ver texto, com tradução em português, e relatório explicativo da convenção em <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224>.

[cxiii] Resolution 74/247 "Countering the use of information and communications technologies for criminal purposes", em <https://docs.un.org/en/a/res/74/247>.

[cxiv] Grupo de peritos criado na sequência da Resolução n.º 65/230 da Assembleia Geral das Nações Unidas, em 21.12.2010. O primeiro estudo foi publicado em fevereiro de 2013 (acessível em <https://www.icnl.org/post/report/unodc-comprehensive-study-on-cybercrime>). Para informação detalhada sobre os trabalhos subsequentes que conduziram à elaboração da Convenção, ver o "Explanatory Memorandum" constante da Recomendação da Comissão Europeia ao Conselho para adoção de uma decisão autorizando a participação da União nas negociações da Convenção [COM(2022) 132 final, de 29.3.2022].

[cxv] Para uma análise comparada das Convenções ver "From Budapest to Hanoi: Comparing the Council of Europe and United Nations Cybercrime Conventions", Kenneth Propp e DeBrae Kennedy-Mayo, em <https://www.crossborderdataforum.org/lawfare-comparing-the-council-of-europe-and-united-nations-cybercrime-conventions/>.

[cxvi] O Segundo Protocolo à Convenção de Budapeste vai além da Convenção da ONU ao prever ferramentas inovadoras para a cooperação transfronteiriça, especificamente para divulgação e produção de informações sobre assinantes (artigos 7 e 8) e de dados armazenados em situações de emergência (artigo 9).

[cxvii] United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, em https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-16&chapter=18&clang=en (Convenção das Nações Unidas contra o Cibercrime: Reforço da Cooperação Internacional para o Combate a Crimes Cometidos através de Sistemas de Tecnologias da Informação e Comunicação e

para a Partilha de Prova em Suporte Eletrónico de Crimes Graves – versão em língua portuguesa no JO L 19.6.2026, em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202601348). Também conhecida por Convenção de Hanói (Vietname), onde teve lugar a cerimónia de assinatura, em 25 e 26.10.2025. Até esta data (acesso em 28.6.2026), a Convenção foi assinada por 78 e ratificada por três Estados Partes (em https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-16&chapter=18&clang=_en).

[cxviii] Nos termos do artigo 64.º, a Convenção ficou aberta à assinatura de todos os Estados e organizações de integração económica regional em Hanói, Vietname, de 25 a 26 de outubro de 2025, e, posteriormente, na sede das Nações Unidas, em Nova York, até 31 de dezembro de 2026. Uma análise detalhada da Convenção encontra-se disponível em <https://www.eurojust.europa.eu/publication/united-nations-convention-against-cybercrime> (Eurojust, Projeto Sirius).

[cxix] Cfr. declaração do representante da UE na cerimónia de assinatura, em Hanói, em <https://hanoiconvention.org/statement/european-unions-statement/>.

[cxx] Decisão (UE) 2026/1347 do Conselho de 4.6.2026, JO L de 19.6.2026. Pela Decisão (UE) 2025/2307 do Conselho de 13.10.2025 (JO L de 11.11.2025) foi aprovada a assinatura da Convenção em nome da União. Cfr. a Proposta da Comissão [COM(2025) 417 final 2025/0231 (NLE)] sobre a celebração, em nome da União Europeia, da Convenção das Nações Unidas contra o Cibercrime, em <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0417>.

[cxxi] Art.º 4.º, n.º 2, al. j), do TFUE: “2. As competências partilhadas entre a União e os Estados-Membros aplicam-se aos principais domínios a seguir enunciados: ...j) Espaço de liberdade, segurança e justiça;”.

[cxxii] Sobre estes pontos, cfr. Stanislaw Tosza, “Eletronic Evidence after E-evidence Package’s Adotion: Challenges for Application and Unsolved Roblems”, Sudia Iuridica Lublinensia vol. 33, 5, 2014, em https://www.researchgate.net/publication/388203812_Electronic_Evidence_after_E-evidence_Package's_Adoption_Challenges_for_Application_and_Unresolved_Problems.

[cxxiii] Cfr. Regulamento (UE) 2023/2844 de 13 de dezembro de 2023 relativo à digitalização da cooperação judiciária e do acesso à justiça em matéria civil, comercial e penal com incidência transfronteiriça, e que altera determinados atos no domínio da cooperação judiciária, e Diretiva (UE) 2023/2843 de 13 de dezembro de 2023 que altera as Diretivas 2011/99/UE e 2014/41/UE do Parlamento Europeu e do Conselho, a Diretiva 2003/8/CE do Conselho e as Decisões-Quadro 2002/584/JAI, 2003/577/JAI, 2005/214/JAI, 2006/783/JAI, 2008/909/JAI, 2008/947/JAI, 2009/829/JAI e 2009/948/JAI do Conselho no que diz respeito à digitalização da cooperação judiciária, JO L 27.12.2023, bem como o “Pacote Justiça Digital 2030”, que inclui a Estratégia Justiça Digital@2030 e a Estratégia Europeia de Formação Judiciária 2025-2030, em https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2754.

[cxxiv] <https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetailheIniciativa.aspx?BID=356842>. (acesso em 3.7.2026).

[cxxv] Livro Digital *Dia da Proteção de Dados 2025, 6 anos de RGPD, Balanço da (des)Aplicação da Lei Nacional de Execução e da Lei sobre o Tratamento de Dados no Sistema Judicial*, «Tratamento e Proteção de dados Pessoais no Sistema Judicial: Observações e Perspetivas», Supremo Tribunal de Justiça, fevereiro de 2026, p. 60-80, Livros Digitais do Supremo, em <https://www.stj.pt/publicacoes/> e <https://www.ministeriopublico.pt/destaque/livro-digital-6-anos-de-rgpd-balanco-da-desaplicacao-da-lei-de-execucao-e-da-lei-sobre-o>.

[cxxvi] Artigo 23.º da Lei n.º 34/2009, de 14 de julho, que estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial.

[cxxvii] Caso os dados pessoais sejam tratados no âmbito de uma investigação criminal ou de um processo judicial em matéria penal, o exercício do direito à informação, ao acesso aos dados pessoais e à sua retificação ou apagamento, bem como à limitação do tratamento, pode ser feito nos termos das regras nacionais aplicáveis aos processos judiciais (preâmbulo da Diretiva 2016/680, n.º 49).

[cxxviii] A competência das autoridades de controlo não abrange o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional (competências processuais – artigo 43.º, n.º 2, da Lei n.º 59/2019), a fim de assegurar a independência do poder judicial no exercício da sua função jurisdicional, nomeadamente a tomada de decisões (preâmbulo do RGPD, n.º 20), sem prejuízo de o cumprimento das regras da Diretiva ficar sempre sujeito a uma fiscalização independente nos termos do artigo 8.º, n.º 3, da Carta dos Direitos Fundamentais (n.ºs 80 a 82 do preâmbulo da Diretiva 2016/680 e artigo 43.º da Lei n.º 59/2019).

[cxxix] Como é conhecido, a Proposta de Lei n.º 126/XIII/3.^a (DAR II Série-A n.º 104, de 26.04.2018), de que resultou o Decreto da Assembleia da República n.º 333/XIII (DAR II Série-A n.º 131, de 22-07.2019) devolvido pelo Presidente da República à Assembleia da República, em 26.7.2019 (veto (leitura) DAR I Série n.º 109, de 12.09.2019), para reapreciação, visava completar o RGPD e a Lei n.º 59/2019, complementando a transposição da Diretiva 680, introduzindo, para isso, um conjunto de alterações à Lei n.º 34/2009.

[cxxx] Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis, JO L 105, de 13.4.2006, p. 54, <https://eur-lex.europa.eu/eli/dir/2006/24/oj>.

[cxxxi] Tribunal de Justiça da União Europeia, Acórdão de 8 de abril de 2014, *Digital Rights Ireland Ltd* (C-293/12) e *Kärntner Landesregierung* (C-594/12), EU:C:2014:238, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A62012CJ0293>.

[cxxxii] Em 17.09.2025, a Presidência do Conselho da União dirigiu às delegações nacionais do Grupo COPEN um questionário para identificação e troca de opiniões em vista da definição de normas futuras («Future rules on data retention in the European Union»), aguardando-se os passos seguintes nesta matéria (WK 11640/2025 INT, <https://data.consilium.europa.eu/doc/document/WK-11640-2025-INIT/en/pdf>).

REGIMES DE CONSERVAÇÃO E UTILIZAÇÃO PROBATÓRIA PENAL DE METADADOS DE COMUNICAÇÕES ELECTRÓNICAS: DO PASSADO DISTANTE AO FUTURO PRÓXIMO, À BEIRA DO ABSURDO

Rui Cardoso: Procurador-Geral-Adjunto

Sumário Executivo (*): (1) A digitalização da sociedade tornou os metadados das comunicações eletrónicas um elemento central da investigação criminal, colocando em tensão permanente as necessidades de investigação e a proteção dos direitos fundamentais. (2) O regime jurídico português evoluiu de forma fragmentada, através da sucessiva sobreposição do Código de Processo Penal, da Lei n.º 41/2004, da Lei n.º 32/2008, da Lei do Cibercrime e, mais recentemente, da Lei n.º 18/2024, originando dificuldades de articulação e insegurança interpretativa. (3) A jurisprudência europeia e constitucional alterou profundamente o quadro normativo, em especial através da invalidação da Diretiva 2006/24/CE pelo Tribunal de Justiça da União Europeia e da declaração de inconstitucionalidade de normas essenciais da Lei n.º 32/2008 pelo Tribunal Constitucional. (4) A Lei n.º 18/2024 procurou reconstruir o regime da conservação de metadados, distinguindo entre dados de identificação e endereços IP, sujeitos a conservação obrigatória, e dados de tráfego e localização, cuja conservação depende agora de autorização do Supremo Tribunal de Justiça. (5) Persistem numerosas questões interpretativas relevantes, designadamente quanto ao âmbito de aplicação do artigo 189.º, n.º 2, do Código de Processo Penal, da Lei do Cibercrime e da própria Lei n.º 32/2008, bem como quanto ao regime de acesso aos dados conservados. (6) O autor procede a uma clarificação conceptual rigorosa, distinguindo categorias de dados (dados de base, de tráfego, de localização e de conteúdo) e separando três realidades frequentemente confundidas: conservação, preservação e interceção de dados. (7) É igualmente diferenciada a natureza jurídica dos metadados, demonstrando-se que estes constituem meios de prova documentais, distintos quer dos meios de obtenção de prova quer dos mecanismos destinados apenas à sua conservação. (8) Sustenta-se que os acórdãos do Tribunal Constitucional não proibiram a utilização probatória dos metadados, tendo incidido exclusivamente sobre determinados regimes de conservação, e não sobre a admissibilidade dos metadados enquanto prova penal. (9) A preservação expedita prevista na Lei do Cibercrime não equivale à conservação nem à interceção de comunicações, funcionando apenas como medida cautelar destinada a impedir a destruição de dados já existentes. (10) O novo modelo de conservação seletiva autorizado pelo Supremo Tribunal de Justiça procura responder às exigências constitucionais e europeias, substituindo a anterior conservação geral e indiferenciada por mecanismos dirigidos e proporcionais. (11) O Regulamento (UE) 2023/1543 introduzirá uma transformação estrutural do sistema, criando mecanismos europeus de produção e preservação de prova eletrónica que obrigarão a reinterpretar o direito interno e a harmonizar conceitos atualmente divergentes. (12) A conclusão central do estudo é que o regime português continua longe da

estabilidade, mantendo-se um quadro jurídico complexo, com múltiplas zonas de incerteza interpretativa e novos desafios decorrentes da futura aplicação do direito da União Europeia.

Resumo ():** O artigo analisa a evolução e o estado atual do regime jurídico da conservação e da utilização probatória dos metadados de comunicações eletrónicas em processo penal, à luz das profundas alterações introduzidas pela jurisprudência do Tribunal de Justiça da União Europeia, do Tribunal Constitucional e pela Lei n.º 18/2024. Partindo da reconstrução histórica do enquadramento legislativo português, o autor clarifica conceitos frequentemente confundidos, distinguindo entre categorias de dados, conservação, preservação, interceção, meios de prova e meios de obtenção de prova. O estudo examina criticamente os diferentes regimes de conservação atualmente existentes, bem como os fundamentos legais de acesso e utilização probatória previstos na Lei n.º 32/2008, no Código de Processo Penal e na Lei do Cibercrime, identificando as principais dificuldades interpretativas que subsistem. Analisa igualmente o novo modelo de conservação seletiva de dados e avalia o impacto que decorrerá da entrada em aplicação do Regulamento (UE) 2023/1543, concluindo que o direito português permanece num período de transição, marcado por significativa incerteza normativa e pela necessidade de compatibilizar a eficácia da investigação criminal com a proteção dos direitos fundamentais.

Índice: I. Introdução. 1. Contexto. 2. Breve história legislativa. 3. Questões actuais. 4. Plano. II. Clarificações Necessárias. 1. Categorias de dados. 2. Meio de prova, meio de obtenção de prova e conservação de (possível) meio de prova. 3. *Metadados*: conservação, preservação e intercepção. III. Conservação. 1. Lei 32/2008. 2. Lei 41/2004. 3. Lei das Comunicações Electrónicas. IV. Acesso e Utilização Probatória. 1. Artigo 9.º da Lei 32/2008. 2. Artigo 189.º, n.º 2, do CPP. 3. Artigo 14.º da LCC. Artigo 18.º da LCC? 5. Regulamento (UE) 2023/1543. V. Síntese Conclusiva.

I. Introdução

1. Contexto

Com a sempre crescente digitalização da vida social, a conservação e utilização de *metadados* de comunicações electrónicas^[1] continuam a ser assuntos de crucial importância para a prova em processo penal.

Volto ao tema, depois de, no final de 2022, ter publicado “A conservação e a utilização probatória de *metadados* de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – *o que nasce torto...*”, na Revista do Ministério Público (RMP), n.º 172.

A alteração legislativa entretanto ocorrida (Lei 18/2024, que alterou a Lei 32/2008) e a muito próxima entrada em aplicação do Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho de 12 de Julho de 2023 [doravante, apenas Regulamento (UE) 2023/1543], que impactará de forma muito significativa nesta matéria, aqui me trazem de novo, não só para analisar o regime em vigor (para o que continua imprescindível conhecer bem a sua história), como para perspectivar o que se avizinha.

No que ainda se mantém actual, o texto da RMP será aproveitado sem pudor.

2. Breve história legislativa

2.1.

Quando, em 1987, foi aprovado o actual CPP, já os fornecedores de serviço (FS), apesar de não haver lei que expressamente o previsse (isso não sucedia com o DL 188/81, então em vigor, que estabelecia os princípios gerais das comunicações, incluindo as telecomunicações), conservavam os dados de base e os dados de tráfego então disponíveis^[ii], pois a “factura do telefone” dependia das concretas chamadas realizadas, do seu tipo (zonas geográficas de chamador e chamado), momento do dia e duração^[iii]. De qualquer forma, não havia previsão legal expressa que permitisse ao utilizador o acesso a esses dados (à “factura detalhada”). O CPP, por seu lado, não continha qualquer preceito que expressamente dispusesse sobre o acesso a esses dados e a sua utilização probatória.

A Lei 88/89, que revogou e substituiu o DL 188/81, embora continuasse a nada prever sobre a conservação desses dados pelos FS, já atribuía ao consumidor o direito de poder controlar o preço cobrado pela utilização dos serviços de telecomunicações de uso público, nos termos a definir nos respectivos regulamentos de exploração dos serviços – artigo 15.º, n.º 4. Ou seja, o direito de acesso à “factura detalhada”. Esta lei foi revogada e substituída pela Lei 91/97, que, não obstante, manteve preceito idêntico no artigo 17.º, n.º 4.

2.2.

Com a Lei 67/98 (que transpôs para a ordem jurídica portuguesa a Directiva 95/46/CE, do Parlamento Europeu e do Conselho), foi pela primeira vez definido um regime jurídico sobre a *conservação e tratamento dos dados pessoais*, embora não especificamente sobre os dados das telecomunicações.

Foi a Lei 41/2004 (que transpôs para a ordem jurídica nacional a Directiva 2002/58/CE, do Parlamento Europeu e do Conselho) o primeiro diploma a definir um regime próprio sobre o tratamento de dados pessoais no contexto da prestação de serviços de comunicações electrónicas, especificando e complementando as disposições da Lei 67/98, que permitia aos FS a conservação

de *metadados* em determinadas situações. Também pela primeira vez, aí se previa a possibilidade de utilização probatória desses dados em processo judicial.

2.3.

Só com a revisão introduzida pela Lei 48/2007 o CPP passou a ter disposições específicas sobre *acesso e utilização probatória* dos *metadados*: o n.º 2 do artigo 189.º. Fê-lo, porém, sobre o catálogo de crimes das intercepções telefónicas (artigo 187.º, n.º 1), não permitindo assim a obtenção de alguns dados de acesso (como o endereço IP) imprescindíveis à prova de alguns crimes informáticos e de crimes cometidos através de meios informáticos que não admitiam essas intercepções^[iv].

2.4.

Cerca de um ano depois, entrou em vigor a Lei 32/2008 (que transpôs para a ordem jurídica interna a Directiva 2006/24/CE, do Parlamento Europeu e do Conselho), regulando a conservação e a transmissão dos dados de tráfego e de localização, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves. Porém, para além disso, e ultrapassando o escopo da directiva, a lei prescreveu também sobre o regime de acesso e utilização probatória desses dados (o artigo 9.º). Fê-lo de forma desastrosa: incoerente com o regime das intercepções telefónicas (aquele que permite ter acesso à mais importante das categorias dos dados: os dados de conteúdo) e não articulada com o artigo 189.º, n.º 2, do CPP, que manteve inalterado, gerando problemas interpretativos de difícil solução^[v]. As eventuais necessárias alterações ao quadro legal em matéria de acesso e utilização dos dados deveriam ter sido feitas apenas no CPP.

2.5.

Novo marco legal ocorreu um ano depois, com a entrada em vigor da Lei 109/2009, conhecida como Lei do Cibercrime (doravante, LCC), transpondo para a ordem jurídica interna a Decisão Quadro 2005/222/JAI, do Conselho, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa (doravante, CCiber). Também nesse momento não fez o legislador uma correcta integração normativa entre os regimes já em vigor no CPP e na Lei 32/2008. Não obstante a LCC não ter preceitos sobre a conservação dos dados, os que tem sobre o acesso e utilização agravaram ainda mais os problemas interpretativos existentes. Formaram-se diferentes correntes doutrinárias e jurisprudenciais que se mantiveram até ao Ac. do Tribunal Constitucional (TC) 268/2022^[vi], e mesmo até hoje.

2.6.

Por acórdão de 08.04.2014, nos processos apensos C-293/12 (Digital Rights Ireland) e C-594/12 (Irish Human Rights Commission)[\[vii\]](#), o Tribunal de Justiça da União Europeia (TJUE), em Grande Secção, declarou a invalidade da Directiva 2006/24/CE, do Parlamento Europeu e do Conselho, que em Portugal foi transposta pela Lei 32/2008.

2.7.

Conhecendo de requerimento de fiscalização sucessiva abstracta apresentado pela Provedora de Justiça sobre algumas normas da Lei 32/2008, o TC, no Ac. 268/2022, declarou a inconstitucionalidade com força obrigatória geral:

- De todas as normas do artigo 4.º (que define quais as categorias de dados que devem ser conservadas), em conjugação com o artigo 6.º (que define o prazo de conservação – um ano), com fundamento em violação do disposto nos números 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo n.º 18.º, todos da Constituição da República Portuguesa (CRP), em concreto:

- quanto aos “*dados de base e IP (da fonte da comunicação)*”

- § porque a lei não prescreve a *obrigatoriedade de os dados serem conservados em território da UE*;

- quanto aos “*dados de tráfego e de localização*”

- § porque a lei não prescreve a *obrigatoriedade de os dados serem conservados em território da UE*;

- § devido à *universalidade da medida* (todos os utilizadores e assinantes)[\[viii\]](#).

- Da norma do artigo 9.º (que define as condições de acesso e de utilização dos dados), na parte *em que não prevê uma notificação ao visado de que os dados conservados foram acedidos* pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja susceptível de comprometer as investigações nem a vida ou integridade física de terceiros, por violação do disposto no n.º 1 do artigo 35.º e do n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º, todos da CRP.

2.8.

Procurando “ressuscitar” a Lei 32/2008, alterando-a para a deixar conforme às exigências do TJUE e do TC, a Assembleia da República (AR) aprovou o Decreto n.º 91/XV, que, em síntese, e para além do mais ora não relevante:

- alterava o artigo 4.º, obrigando os FS a conservar os dados em Portugal ou no território de outro Estado-Membro da União Europeia;
- alterava o artigo 4.º, conjugado com o n.º 2 do artigo 6.º, determinando a conservação dos dados de tráfego e de localização pelo período de três meses a contar da data da conclusão da comunicação, considerando-se esse período prorrogado até seis meses, salvo oposição do titular à prorrogação;
- alterava o artigo 6.º, obrigando à conservação dos dados de base e IP’s fonte da ligação, pelo período de um ano (n.º 1);
- alterava o artigo 9.º, criando um regime de notificação ao visado.

2.9.

Conhecendo de requerimento do Presidente da República (PR) em fiscalização preventiva sobre essas normas do artigo 2.º do Decreto n.º 91/XV da AR, o TC, no Ac. 800/2023, pronunciou-se:

· pela *inconstitucionalidade*:

o na parte em que altera o artigo 4.º da Lei 32/2008, conjugado com o artigo 6.º da mesma lei, quanto aos dados previstos no n.º 2 do mencionado artigo 6.º (dados de tráfego e de localização), devido à *universalidade da medida* (conservação geral e indiferenciada), e ao período de conservação (três meses a contar da data da conclusão da comunicação, considerando-se esse período prorrogado até seis meses, salvo se o seu titular se tivesse oposto perante os FS à prorrogação dessa conservação), por violação do disposto nos números 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição.

· pela *não inconstitucionalidade*:

o na parte em que altera o artigo 4.º da Lei 32/2008 (*localização dos dados a conservar – em Portugal ou no território de outro Estado-Membro da União Europeia*);

o na parte em que altera o artigo 6.º quanto a conservação dos *dados de base* e *IP’s* fonte da ligação (estáticos ou dinâmicos) pelo período de um ano (artigo 6.º, n.º 1);

o na parte em que altera o artigo 9.º da Lei 32/2008 (*condições de acesso e utilização – notificação ao visado*).

2.10.

O PR devolveu o decreto à AR, que o reformulou, eliminando a obrigação de conservação dos dados de tráfego e de localização pelo período de três meses a contar da data da conclusão da comunicação, e sua possibilidade de prorrogação. No seu lugar, inseriu a possibilidade de tais dados de tráfego e de localização serem conservados por decisão do Supremo Tribunal de Justiça (STJ), a requerimento do Ministério Público (MP). Tal decreto não foi submetido a fiscalização preventiva, vindo a ser promulgado pelo PR. Foi publicado como Lei 18/2024, que alterou a Lei 32/2008 e a Lei da Organização do Sistema Judiciário (LOSJ). Até à presente data, o TC não fez qualquer apreciação, em fiscalização concreta, das novas normas desta lei.

3. Questões actuais

A Lei 18/2024 de modo algum constitui um “fim da história” em matéria de *metadados*, como está patente na muito divergente jurisprudência superior publicada desde a sua entrada em vigor. Há novas e velhas questões por resolver. Para que tipo de autorização é agora competente o STJ (artigo 6.º, n.º 2, da Lei 32/2008)? Como se processa a comunicação ao visado, após o acesso aos dados (n.ºs 7 e 8 do artigo 9.º)? Os dados conservados pelos FS ao abrigo da Lei 41/2004 podem ser acedidos e utilizados para prova em processo penal? Somente dados de tráfego ou também dados de localização? Outros dados respeitantes ao subscritor do serviço conservados pelos FS podem ser utilizados como prova? O n.º 2 do artigo 189.º do CPP continua a ser fundamento normativo para acesso e utilização probatória de *metadados*? Em que medida? Para dados conservados com que fundamento? A LCC contém fundamento normativo para acesso e utilização probatória de *metadados*? Que tipo de dados? Em que artigos? Somente 14.º ou também 18.º?

Por outro lado, a 18.08.2026 será aplicável o Regulamento (UE) 2023/1543, que estabelece as regras segundo as quais uma autoridade de um Estado-Membro pode, num processo penal, emitir uma Ordem Europeia de Produção ou uma Ordem Europeia de Conservação e, assim, ordenar a um prestador de serviços que ofereça serviços na União e que esteja estabelecido noutro Estado-Membro ou, caso não esteja estabelecido, que esteja representado por um representante legal noutro Estado-Membro, que produza ou que conserve provas electrónicas, independentemente da localização dos dados. Ainda que não exista para já alteração da legislação nacional^[ix], esse regulamento obrigará a interpretar a existente de acordo com o mesmo^[x].

4. Plano

A estas e outras questões procurarei dar resposta. Antes, porém, e face aos muitos equívocos que subsistem – quer para o legislador, quer para os aplicadores – é necessário clarificar alguns aspectos essenciais. Feito isso, analisarei os diferentes (possíveis) regimes de conservação de *metadados* de comunicações electrónicas: a Lei 32/2008, a Lei 41/2004 e a Lei das Comunicações Electrónicas (LCE), aprovada pela Lei 16/2002. Após, analisarei os actuais diferentes possíveis fundamentos normativos de acesso e utilização probatória de tais dados (na Lei 32/2008, na LCC e no CPP) e as implicações que decorrerão da entrada em vigor do Regulamento (UE) 2023/1543. Terminarei com uma síntese conclusiva sobre o actual e o futuro próximo do regime de conservação e utilização probatória de *metadados* de telecomunicações.

II. Clarificações Necessárias

1. Categorias de dados

1.1.

Os “*metadados* das telecomunicações” são os dados das mesmas que não são comunicados: são os dados sobre os dados comunicados; são os dados gerados antes e durante o processo de comunicação, que, para o que releva neste estudo, estão na posse dos fornecedores desses serviços (FS). Não são o conteúdo comunicado: o som (incluindo a voz), a imagem (estática ou dinâmica), o texto, os dados informáticos em geral.

Com estes dados não se confundem os *dados na posse dos fornecedores de serviços online* (vulgarmente designados por OSP – *Online Service Providers*). Os FS permitem a comunicação; tratando-se de acesso a serviços *online*, v. g., na internet, os OSP fornecem os serviços a que se acede (correio electrónico, motores de pesquisa, comércio electrónico e tudo o mais que aí se pode encontrar)^[xi].

1.2.

A Lei 32/2008 contém, directamente, apenas a definição de “dados”: os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador [artigo 2.º, n.º 1, alínea a)]. Assim é desde a sua versão original. Nessa versão, a menção a dados de tráfego e a dados de localização no artigo 1.º (definição do objecto da lei) e depois nesse artigo 2.º (definições) era até inconsequente, pois a lei não voltava a utilizar tais conceitos.

Na versão original, o n.º 2 do artigo 2.º dispunha que, «[p]ara efeitos da presente lei, são aplicáveis, sem prejuízo do disposto no número anterior, as definições constantes das Leis n.ºs 67/98, de 26 de Outubro, e 41/2004, de 18 de Agosto». Após a alteração pela Lei 18/2024, dispõe o mesmo preceito que «[p]ara efeitos da presente lei, são aplicáveis, sem prejuízo do disposto no número

anterior, as definições constantes do Regulamento (UE) 2016/679 [...], e das Leis n.ºs 41/2004 [...], que transpõe para a ordem jurídica nacional a Diretiva 2002/58/CE [...], relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, e 58/2019 [...], que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 [...], relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados».

Nem a Lei 67/98, nem a Lei 58/2019 (que a revogou e substituiu), nem tão pouco o RGPD contém qualquer definição de “dados de tráfego” ou de “dados de localização”. Tal apenas sucede com a Lei 41/2004, que o faz nestes termos (artigo 2.º, n.º 1): “Dados de tráfego” quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma [alínea d)]; “Dados de localização” quaisquer dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público [alínea e)]. Deste modo, desde o primeiro momento, a Lei 41/2004 e a Lei 32/2008 partilham a mesma definição de “dados de tráfego” e de “dados de localização”, por remissão da segunda para a primeira.

1.3.

Desde os Pareceres do Conselho Consultivo da Procuradoria-Geral da República (CCPGR) n.ºs 16/94 e 21/2000^[xii], que a importaram de países próximos na Europa, que em Portugal é utilizada uma classificação tripartida dos dados respeitantes às telecomunicações, depois seguida pela jurisprudência (incluindo a constitucional, com início no Ac. TC 241/2002): dados de base^[xiii], dados de tráfego^[xiv] e dados de conteúdo^[xv]. Só as duas primeiras categorias integram os *metadados* ora tratados^[xvi].

A utilidade da classificação – feita de acordo com um critério que assenta na potencialidade crescente de, com o acesso a esses dados, haver ofensa a direitos fundamentais, *v. g.*, à privacidade e ao sigilo das telecomunicações – era a de definir a admissibilidade, face ao princípio da proporcionalidade, da utilização de tais dados em diferentes tipos de processos^[xvii] ou, na área penal, para a prova de diferentes tipos de crimes, por um lado, e para a determinação de quais as entidades competentes para ordenar ou autorizar a sua produção, por outro. É, pois, uma classificação que *apenas releva ao nível do acesso aos dados, não da sua conservação*. Essa classificação em nada interessa para os FS na conservação de dados: os dados não são por eles conservados nessas categorias, antes apenas por categorias técnicas que lhes permitem depois, quando a tal instados por entidade competente, fornecer dados que se enquadram nas categorias de dados de base ou de tráfego, incluindo localização^[xviii].

Repare-se na técnica legislativa do artigo 4.º da Lei 32/2008 (nessa parte não alterado pela Lei 18/2024), em que obriga os FS a conservarem os *dados necessários para* encontrar ou identificar a fonte, o destino de uma comunicação, etc., não a conservarem dados de base, dados de tráfego ou dados de localização. Aliás, nas diferentes categorias de dados previstas nos n.ºs 2 a 6 (“necessários para...”) há dados que se integram nos dados de base.

1.4.

Na alteração que através da Lei 18/2024 fez ao artigo 6.º da Lei 32/2008, o legislador confundiu os dois planos[xix], utilizando, para a criação de dois distintos regimes de *conservação* (n.ºs 1 e 2), as categorias que apenas deviam relevar para o *acesso*. A conjugação dos artigos 4.º e 6.º, n.ºs 1 e 2, da Lei 32/2008 suscita assim várias questões que serão abordadas *infra* (III.1.), para além de criar evidentes dificuldades aos FS.

1.5.

Como já referido, a 18.08.2026 será aplicável o Regulamento (UE) 2023/1543, que estabelece as regras segundo as quais uma autoridade de um Estado-Membro pode, num processo penal, emitir uma *Ordem Europeia de Produção* (OEP) ou uma *Ordem Europeia de Conservação* (OEC) e, assim, ordenar a um prestador de serviços que ofereça serviços na União e que esteja estabelecido noutro Estado-Membro ou, caso não esteja estabelecido, que esteja representado por um representante legal noutro Estado-Membro, que produza ou que conserve provas electrónicas, independentemente da localização dos dados – cf. artigos 1.º, n.º 1, e 34.º, n.º 2.

Apesar de a tradução oficial em língua portuguesa utilizar o verbo “conservar”, não se trata, na verdade, de *conservação* de dados, antes de *preservação*, ou seja, de *não destruição*[xx]/[xxi]. A versão original em língua inglesa usa antes a expressão “*European Preservation Order*”; para o que na nossa língua e lei consiste em “conservar”, usa antes o termo “*retention*”. Ou seja, “*preservation*” = preservação; “*retention*” = conservação.

Está expresso no n.º 2 do artigo 6.º do regulamento que a finalidade da *European Preservation Order* é impedir a remoção, o apagamento ou a alteração dos dados que já se encontram conservados, tendo em vista a emissão de um pedido subsequente para a produção desses dados através de auxílio judiciário mútuo, de uma decisão europeia de investigação (DEI) ou de uma ordem europeia de produção.

Cf. ainda, nesse sentido, na versão original, o Considerando 19, onde de forma indubitável se lê:

«This Regulation should regulate the gathering of data stored by a service provider at the time of receipt of a European Production Order or a European Preservation Order only. It

should not lay down a general data retention obligation for service providers and it should not have the effect of resulting in any general and indiscriminate retention of data. This Regulation also should not authorise the interception of data or the obtention of data that are stored after the receipt of a European Production Order or a European Preservation Order.» [\[xxii\]](#).

À “data retention” (“retenção de dados”) chamam a Lei 32/2008 e a Lei 58/2019 “conservação de dados”.

Este diploma *não permite, pois, a intercepção ou conservação de dados* (isto é, o registo de dados que viessem a ser produzidos após a recepção da OEP), antes apenas a sua *produção* (transmissão à entidade emissora da OEP de dados já conservados pelos FS, para que aquela os possa utilizar probatoriamente) ou a sua *preservação* (não destruição de dados já conservados no momento da recepção da ordem).

São conceitos de direito distintos que não deveriam ter sido confundidos na tradução oficial para português. É grave tal erro básico de tradução, num acto normativo com esta importância; é grave que a PPL 83/XVII o continue; graves serão certamente as consequências na aplicação destes diplomas.

As referidas provas electrónicas a produzir ou preservar consistem em dados de assinantes, dados de tráfego ou dados de conteúdo, conservados em formato electrónico, por um prestador de serviços ou em seu nome, *no momento da receção* de um certificado de ordem europeia de produção (COEP) ou de um certificado de ordem europeia de conservação (COEC) – artigo 3.º, n.º 8. Sublinho novamente, como expresso neste preceito, que *os dados têm de já estar conservados no momento da recepção da ordem*.

A classificação de *metadados* aí utilizada é distinta da nacional [\[xxiii\]](#). Como disposto no artigo 3.º, n.ºs 9, 10 e 11, para efeitos do presente regulamento, entende-se por:

«9) «Dados de assinantes», dados na posse de um prestador de serviços relacionados com a adesão aos seus serviços, relativos:

- a) À identidade de um assinante ou cliente, tais como o nome fornecido, a data de nascimento, o endereço postal ou geográfico, os dados de faturação e pagamento, o número de telefone ou o endereço de correio eletrónico;
- b) Ao tipo de serviço e respetiva duração, incluindo dados técnicos e dados que identifiquem medidas técnicas associadas ou interfaces fornecidas ao assinante ou cliente ou por ele utilizadas no momento do registo inicial ou da ativação, e dados relacionados com a validação da utilização do serviço, com exceção de palavras-passe ou outros meios de identificação utilizados em vez de uma palavra-passe que sejam fornecidos por um utilizador, ou criados a pedido do mesmo;

10) «Dados solicitados com o único objetivo de identificar o utilizador», os endereços IP e, se necessário, as portas de origem e o carimbo temporal pertinentes, nomeadamente a data e a hora, ou os equivalentes técnicos desses identificadores e informações conexas, quando solicitados pelas autoridades responsáveis pela aplicação da lei ou pelas autoridades judiciais com o único objetivo de identificar o utilizador numa investigação criminal específica;

11) «Dados de tráfego», dados relacionados com a prestação de um serviço por um prestador de serviços que servem para fornecer contexto ou informações adicionais sobre esse serviço e que são gerados ou tratados por um sistema de informação do prestador de serviços, tais como o remetente e o destinatário de uma mensagem ou de outro tipo de interação, sobre a localização do dispositivo, a data, a hora, a duração, o tamanho, a via, o formato, o protocolo utilizado e o tipo de compressão, e outros *metadados* das comunicações eletrónicas e dados, com exceção dos dados de assinantes, relacionados com o início e o fim da sessão de acesso de um utilizador a um serviço, tais como a data e a hora da utilização, o início (“log-in”) e o fim (“log-off”) da ligação ao serviço;»

Como veremos *infra* em IV.5., esta classificação impor-se-á necessariamente a nível interno^[xxiv], ou seja, quando a ordem de produção ou de preservação é feita em processo nacional, por autoridade nacional e dirigida a FS nacional (a que não se aplica directamente o regulamento).

2. Meio de prova, meio de obtenção de prova e conservação de (possível) meio de prova

2.1.

A leitura de alguns acórdãos proferidos por tribunais superiores evidencia que nos mesmos, nas decisões recorridas ou ainda nas posições assumidas pelos recorrentes/respondentes, não raras vezes há indevida leitura do Ac. TC 268/2022, que é resultado de confusão entre o que, nesta matéria, é meio de prova, meio de obtenção de prova e conservação de (possível) meio de prova.

Como é sabido, os meios de prova permitem por si o convencimento (das entidades competentes para a decisão) sobre os factos (a realidade do facto probando); os meios de obtenção de prova não o permitem, antes são apenas forma de obter os meios de prova que o permitem^[xxv].

Os metadados de telecomunicações são, em si, meio de prova; em concreto, prova documental (em formato tangível ou em formato digital). Recorde-se que, nos termos previstos no n.º 1 do artigo 164.º, se entende como documento «a declaração, sinal ou notação corporizada em escrito ou qualquer outro meio técnico, nos termos da lei penal». A lei penal em causa é o artigo 255.º, alínea a), do CP, que define documento como «a declaração corporizada em escrito, ou registada em disco, fita gravada ou qualquer outro meio técnico, inteligível para a generalidade das pessoas ou para um certo círculo de pessoas, que, permitindo reconhecer o emitente, é idónea para provar facto

juridicamente relevante, quer tal destino lhe seja dado no momento da sua emissão, quer posteriormente; e bem assim o sinal materialmente feito, dado ou posto numa coisa ou animal para provar facto juridicamente relevante e que permite reconhecer à generalidade das pessoas ou a um certo círculo de pessoas o seu destino e a prova que dele resulta».

Esses *metadados* podem estar inscritos numa factura detalhada que seja enviada por correio físico ou electrónico para o domicílio ou do seu titular^[xxvii]; podem ser registados através de intercepção das comunicações telefónicas^[xxviii] ou de dados informáticos; alguns podem ser encontrados nos sistemas informáticos utilizados nas comunicações; podem estar conservados pelos FS.

Questão diferente é a da sua forma de obtenção para o processo, para que possam ser utilizados como meio de prova. Podem ser *juntos* (artigo 164.º, n.º 1, do CPP), mas, quando corpóreos, são objectos susceptíveis de servir a prova e por isso podem ser *apreendidos* (artigo 178.º, n.º 1, do CPP), apreensão que é um meio de obtenção de prova. Para a apreensão pode ser necessário utilizar outros meios de obtenção de prova, como a *revista* e a *busca* – artigos 174.º a 177.º do CPP. Se forem documentos informáticos, prevê a LCC que a sua obtenção se faça através da *injunção/concessão de acesso a dados* (artigo 14.º, que se analisará em IV.3) e/ou *pesquisa e apreensão* (artigos 15.º, 16.º e 17.º).

Questão ainda diferente é a do regime de conservação dos *metadados* na posse dos FS, que permita o seu posterior acesso no processo. Aí estamos perante *conservação de (possível) meio de prova*^[xxviii].

2.2.

A admissibilidade dos metadados como prova documental enquanto tal não foi objecto de qualquer juízo de inconstitucionalidade do TC^[xxix]; não foi essa a “porta fechada” por esse tribunal, usando a expressão utilizada nos Acs. TRP de 07.12.2022, P. 5011/22.2JAPRT-A.P1 (Pedro Vaz Pato), e TRL 16.03.2026, P. 23/26.0GCALM-A.L1-9 (Rosa Maria Cardoso Saraiva). Não há qualquer desconformidade constitucional na utilização dos *metadados* como meio de prova no processo penal. O que foi apreciado pelo TC foi apenas o regime de conservação desses dados previsto na Lei 32/2008: o *meio de conservação de (um possível) meio de prova*.

Nenhum dos fundamentos invocados pelo TC (local de conservação dos dados, universalidade da conservação e notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal) *é sequer matéria de processo penal*: não respeita, v. g., à definição do catálogo de crimes em que é utilizável o meio de prova, ao catálogo de visados e ao critério de necessidade probatória (os três aspectos decorrência do princípio da proporcionalidade definido no artigo 18.º, n.º 2, da CRP), à reserva de juiz (decorrência do artigo 32.º, n.º 4, da CRP) e à necessidade de fundamentação.

O meio de prova (mesmo na forma mais ofensiva: dados de tráfego/localização) não tem qualquer problema de desconformidade constitucional: só pode ser acedido e utilizado com autorização de juiz, quando for indispensável para a prova de crime grave (de catálogo) e se respeitar a suspeito, arguido, intermediário ou vítima (com consentimento efectivo ou presumido). Considerar que a utilização destes dados, em si, viola a Constituição, deve conduzir então a que, por maioria de razão, todas as intercepções telefónicas e de dados informáticos o sejam também, pois estas, para além de permitirem o registo e utilização desses mesmos dados, fazem-no ainda relativamente ao conteúdo. Alguém o defende? Certamente que não o TC, que sempre que foi chamado a apreciá-lo, quer em fiscalização abstracta (cf. o Ac. 7/87), quer em concreta (cf., p. ex., os Acs. 300/05, 4/06, 378/08, 381/15 e 476/15), nunca encontrou nisso qualquer violação da Constituição.

A norma respeitante ao limite temporal (artigo 6.º) declarada inconstitucional pelo Ac. 268/2022 respeitava (apenas) à conservação dos dados, não define(ia), pois, qualquer limite temporal para a sua utilizabilidade probatória [que, aliás, nunca poderá ser legalmente fixada – os dados podem estar noutro local (impressos, na posse dos intervenientes nas comunicações, etc.), incluindo até noutro processo]. O mesmo sucedeu com a norma do artigo 2.º do Decreto n.º 91/XV da Assembleia da República, na parte em que alterava o artigo 4.º quando conjugado com o artigo 6.º da Lei 32/2008 (âmbito subjectivo e período da conservação), sobre a qual o TC no Ac. 800/2023 se pronunciou pela inconstitucionalidade.

É, pois, totalmente desprovido de fundamento o argumento de que o Ac. TC 268/2022 impede a utilização dos metadados para a prova de quaisquer crimes, sejam eles os “crimes graves” definidos pela Lei 32/2008, sejam os previstos no n.º 1 do artigo 187.º do CPP que não se incluam nessa definição de “crime grave”, utilizando os dados conservados ao abrigo da Lei 41/2004.

3. Metadados: conservação, preservação e intercepção

3.1.

É proibida a escuta, a instalação de dispositivos de escuta, o armazenamento ou outros meios de intercepção ou vigilância de comunicações e dos respectivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, com excepção dos casos previstos na lei – artigo 4.º, n.º 2, da Lei 41/2004.

Um dos casos de excepção previstos na lei é o que respeita aos dados de tráfego – artigo 6.º dessa lei. No n.º 1 deste artigo determina-se que, sem prejuízo do disposto nos números seguintes, os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas empresas que oferecem redes e ou serviços de comunicações electrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação. Os n.ºs 2 e 3 *permitem (mas não obrigam)* o tratamento de dados de tráfego necessários à facturação dos assinantes e ao pagamento de interligações (exemplificando alguns tipos de dados) até final do

período durante o qual a factura pode ser legalmente contestada ou o pagamento reclamado, que é hoje de seis meses (artigos 10.º, n.º 1, e 1.º, n.º 2, alínea d), da Lei 23/96).

Outra excepção era a prevista, aí como obrigatória, nos artigos 4.º e 6.º da Lei 32/2008, declarados inconstitucionais com força obrigatória geral pelo Ac. TC 268/2022.

Ou seja, quando a lei excepcionalmente o permite, os *metadados* são guardados, são *conservados*, são *retidos*, não são eliminados, fugindo ao regime regra. É disso que se deve falar quando se fala da *conservação* ou *retenção* [\[xxx\]](#) de *metadados*.

3.2.

Com esta *conservação* não se confunde a *preservação*, também chamada de *preservação expedita* (*quick-freeze*), prevista no artigo 12.º da LCC. Esta é uma medida cautelar similar às previstas no artigo 249.º do CPP que *visa* (e apenas isso permite) *impedir a destruição* de dados informáticos específicos armazenados num sistema informático, quando exista receio de que possam perder-se, alterar-se ou deixar de estar disponíveis. Aplica-se a qualquer tipo de dados informáticos, incluindo, pois, os dados de tráfego e de localização [\[xxxi\]](#).

Esta medida não consente a obtenção dos dados, apenas impede a sua destruição, permitindo que, depois, em devido tempo, se diligencie pela sua obtenção através das várias vias legalmente admissíveis (aspecto de que tratarei *infra* em V.).

Como é óbvio, *para que possa ser aplicada esta medida é necessário que os dados ainda existam*; concretamente quanto aos dados de tráfego e de localização, que ainda não tenham sido eliminados, o que, como vimos, é o que deve acontecer, excepto quando a lei o *permite* [v. g., os casos previstos nos artigos 4.º, n.º 3, da Lei 41/2004 (quando realizadas no âmbito de práticas comerciais lícitas, para o efeito de prova de uma transacção comercial nem de qualquer outra comunicação feita no âmbito de uma relação contratual, desde que o titular dos dados tenha sido disso informado e dado o seu consentimento), e 6.º, n.º 2, da mesma lei (tratamento de dados de tráfego necessários à facturação dos assinantes e ao pagamento de interligações)] ou *obriga* (era o caso dos artigos 4.º e 6.º da Lei 32/2008 na sua versão original, declarados inconstitucionais com força obrigatória geral pelo Ac. TC 268/2022, e dos mesmos artigos da mesma lei após a alteração introduzida pela Lei 18/2024), sempre por períodos legalmente fixados. Se os dados de tráfego não forem previamente conservados, não há preservação que lhes valha: só se pode preservar aquilo que ainda existe, que ainda não foi eliminado [\[xxxi\]](#). Se já tiverem sido eliminados, não há como recuperá-los, não há como preservá-los.

A Lei 32/2008 refere-se à preservação no artigo 7.º, n.º 1, alíneas e) e f), e depois no artigo 11.º, sempre a propósito da destruição de dados. Do artigo 7.º, n.º 1, alínea e), parece inferir-se que a preservação tem de ser ordenada por juiz. Porém, essa lei não tem qualquer regime de preservação.

Esse regime está apenas no artigo 12.º da LCC, que atribui a competência à “autoridade judiciária competente”. Estes preceitos do artigo 7.º vêm da redacção original. Como o artigo 11.º, n.º 2, da LCC estabelece que «as disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho», afigura-se-me que deve interpretar-se o artigo 12.º no sentido de, quando se trata de dados de tráfego e dados de localização, a autoridade judiciária competente para ordenar ou autorizar a preservação, ou para validar aquela ordenada por órgão de polícia criminal em situação de urgência, é apenas o juiz.

Note-se que a jurisprudência do TJUE apenas exige que a ordem de preservação seja de autoridade competente e sujeita a fiscalização jurisdicional efectiva^[xxxiii].

3.3.

A preservação expedita também não é uma forma de proceder a intercepção e gravação de dados de tráfego e de localização. A única via legal de o fazer é através do regime das intercepções das comunicações: tratando-se de dados respeitantes às comunicações feitas pelo telefone, o regime previsto nos artigos 187.º e 188.º do CPP; tratando-se de comunicações por meio técnico diferente do telefone que constituam transmissão de dados informáticos, o regime do artigo 18.º da LCC^[xxxiv].

Em primeiro lugar, recorde-se que o *artigo 12.º da LCC não constitui fundamento para a obtenção de quaisquer dados*: apenas impede que sejam eliminados ou alterados. Depois, note-se que está expresso na letra do seu n.º 1 que a medida se aplica a dados *armazenados*, ou seja, a dados de comunicações pretéritas. Só esses estão armazenados quando é proferida a ordem de preservação; os respeitantes a comunicações futuras – e só essas podem ser objecto de intercepção e gravação – ainda não existem. Finalmente, se assim fosse subverter-se-iam os regimes de admissibilidade das intercepções previstos nos artigos 187.º e 188.º do CPP e no artigo 18.º da LCC (catálogo de crimes, catálogo de visados, critério qualificado de necessidade probatória, controlo judicial periódico da medida), podendo ser aplicada em qualquer tipo de crime [cf. artigo 11.º, n.º 1, alínea c), da LCC], por decisão do MP ou até de OPC.

3.4.

Não se deixe o intérprete incauto iludir pela epígrafe do artigo 13.º da LCC («Revelação expedita de dados de tráfego»): não se prevê aí revelação de dados de tráfego, apenas obrigação (*ope legis*) para o FS a quem tenha sido ordenada a preservação de dados de indicar a quem ordenou a preservação que há outros FS através dos quais aquela comunicação tenha sido efectuada, para assim permitir que também a esses seja dada ordem de preservação de dados.

3.5.

O acesso a metadados conservados não é uma interceptação de dados^[xxxv]. Seja o fundamento de acesso o artigo 189.º, n.º 2, do CPP, o artigo 9.º da Lei 32/2008 ou o artigo 14.º da LCC (hipóteses que analisarei em IV.), nunca se trata de uma interceptação (a dados em transmissão), mas sim de acesso a dados de comunicações pretéritas (dados já armazenados). A interceptação, seja ela de comunicações telefónicas, de transmissão de dados informáticos ou ainda por outro meios técnicos, podendo incluir os respectivos *metadados*, é sempre para comunicações que estão a ocorrer, para dados que estão em transmissão, ou seja, em tempo real, e, por isso, necessariamente posteriores ao despacho que as autoriza/ordena.

III. Conservação

Há agora que analisar os diferentes possíveis fundamentos normativos para a conservação de *metadados* de comunicações electrónicas.

1. Lei 32/2008

1.1.

Na sua redacção original, o artigo 6.º da Lei 32/2008, sob a epígrafe “Período de conservação”, limitava-se ao seguinte preceito: «As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação».

Declarado inconstitucional com força obrigatória geral pelo Ac. TC 268/2022, foi depois alterado pela Lei 18/2024, que do mesmo apenas manteve parte da epígrafe (que passou a ser “Período e regras de conservação”), criando, em sete novos números, dois regimes distintos de conservação de dados, sempre obrigatórios para os FS: (i) um para dados “não de tráfego ou localização”, que resulta directamente da lei (n.º 1); (ii) outro para dados de tráfego e de localização, ordenado pelo STJ – n.ºs 2, 3, 4, 5 e 7.

1.2.

O primeiro regime obriga os FS conservar, pelo período de um ano a contar da data da conclusão da comunicação, os seguintes dados: a) Os dados relativos à identificação civil dos assinantes ou utilizadores de serviços de comunicações publicamente disponíveis ou de uma rede

pública de comunicações; b) Os demais dados de base; c) Os endereços de protocolo IP atribuídos à fonte de uma ligação.

É uma conservação cuja obrigatoriedade *resulta directamente da lei* (sem necessidade de qualquer acto de qualquer entidade a determiná-lo) e é *universal* (abrange todos os assinantes ou utilizadores e todas as comunicações realizadas por eles através dos FS).

Os dados incluídos na *alínea a)* (identificação civil dos assinantes ou utilizadores de serviços de comunicações publicamente disponíveis ou de uma rede pública de comunicações) são, por regra, conservados pelos FS durante toda a vigência do contrato e pelo menos seis meses depois do seu termo, por força da eventual necessidade de os usar como prova em litígios de facturação ou outros (cf. caps. III.2. e III.3., *infra*), ou mesmo para cumprimento de obrigações fiscais[xxxvii]. Não respeitam a quaisquer concretas comunicações, existindo independentemente delas, pelo que a obrigação de conservação pelo período de um ano a contar da data da conclusão da comunicação só terá efeito útil se o contrato terminar antes de decorridos seis meses após a última comunicação em que participa o assinante ou utilizador.

É problemática a referência na *alínea b)* a “demais dados de base”. Na verdade, a definição do que sejam dados de base, tendo a origem referida em II.1.3., nunca teve qualquer consagração legal[xxxviii]. Por outro lado, como visto no mesmo local, os FS não conservam os dados usando as categorias “base/tráfego/localização”, o que os deixa em dificuldade para cumprimento da obrigação que este artigo 6.º, n.º 1, lhes quer impor. Não obstante, e porque são dados que não respeitam a qualquer concreta comunicação, creio que neste grupo se podem incluir aqueles tipos de dados referidos no n.º 4 do artigo 14.º da LCC[xxxix]: o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso; os dados respeitantes à facturação e ao pagamento (p. ex., modo de pagamento definido, conta bancária autorizada para débito directo), disponíveis com base num contrato ou acordo de serviços; qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

A *alínea c)* refere-se apenas aos «endereços de protocolo IP atribuídos à fonte de uma ligação»[xl]. Tais dados são essenciais para determinar qual a origem de qualquer ligação na Internet. Podem, no entanto, ser insuficientes para essa finalidade. Pode ser necessário conhecer os respectivos portos de origem ou seu equivalente técnico e os códigos de identificação atribuídos ao utilizador para efeitos de acesso à Internet (estes últimos indispensáveis quando os FS utilizam a tecnologia NAT[xli] para permitir que múltiplos utilizadores usem o mesmo IP, ou quando vários utilizadores estão ligados a um mesmo *router*)[xlii].

Note-se que, com o rigor técnico que o preceito em análise não tem, o artigo 4.º, n.º 2, na sua alínea b), determina que os dados necessários para encontrar e identificar a fonte de uma comunicação são, no que diz respeito ao acesso à Internet, ao correio electrónico através da Internet

e às comunicações telefónicas através da Internet: *i)* Os códigos de identificação atribuídos ao utilizador; *ii)* O código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública; *iii)* O nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone estavam atribuídos no momento da comunicação. Vão, pois, muito além do mero endereço IP.

Por outro lado, na definição de “dados solicitados com o único objectivo de identificar o utilizador” que consta do Regulamento (UE) 2023/1543 estão incluídos os endereços IP e, se necessário, as portas de origem e o carimbo temporal pertinentes, nomeadamente a data e a hora, ou os equivalentes técnicos desses identificadores e informações conexas, quando solicitados pelas autoridades responsáveis pela aplicação da lei ou pelas autoridades judiciais com o único objectivo de identificar o utilizador numa investigação criminal específica.

Deste modo, creio que, quer por conjugação com o disposto no artigo 4.º, n.º 2, alínea b), quer por aplicação directa do Regulamento (a partir de 18.08.2026), na previsão da alínea c) devem incluir-se, para além do endereço IP, as portas de origem e o carimbo temporal pertinentes, nomeadamente a data e a hora (e fuso horário), os códigos de identificação do utilizador ou os equivalentes técnicos desses identificadores, designadamente o *MAC Address*, e informações conexas.

1.3.

Nos n.ºs 2, 3, 4, 5 e 7, o artigo 6.º prevê agora a *conservação, por decisão do STJ, de dados de tráfego e de localização*.

1.3.1.

O primeiro comentário vai para os *tipos de dados em causa*.

Como vimos em II.1.2., a Lei 32/2008 remete para a Lei 41/2004 a definição de dados de tráfego: quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma. Esta definição é de grande amplitude, abrangendo todos e quaisquer dados tratados para efeitos de envio de uma comunicação. Abrange, pois, quer o endereço IP, quer as portas de origem, os códigos de identificação do utilizador ou os equivalentes técnicos desses identificadores, designadamente o *MAC Address*, e informações conexas, pois todos eles são tratados (por serem necessários) ao envio de uma comunicação. Estando tais dados incluídos na previsão do artigo 6.º, n.º 1, alínea c), como

exposto, é forçoso concluir que o conceito de “dados de tráfego” que consta do n.º 2 do mesmo artigo tem de ser reduzido em simetria: incluídos na previsão do n.º 1, excluídos da previsão do n.º 2.

Quanto aos dados de localização, apenas cabe referir que nesta previsão se incluem apenas as situações em que a localização do equipamento é determinada *pela comunicação* (p. ex., telefones móveis, por referência à antena/célula a que estão ligados), *não quando isso resulta do próprio contrato* (v. g., o local onde o equipamento de comunicação foi instalado: o serviço de televisão, o telefone fixo, o *router* da internet, etc.).

1.3.2.

É *competente* para autorizar a conservação destes dados uma formação das secções criminais do STJ, constituída pelos presidentes das secções (que são duas) e por um juiz designado pelo Conselho Superior da Magistratura (CSM), de entre os mais antigos destas secções. Não havendo alteração na presidência das secções nem na designação do CSM, são, pois, sempre os mesmos três conselheiros a integrar este colectivo[\[xlii\]](#).

1.3.3.

O que está em causa nestes preceitos é *conservação* de dados; *não é preservação* de dados já conservados, *nem interceptação* de dados[\[xliii\]](#), *nem transmissão* (acesso e utilizabilidade probatória) de dados já conservados[\[xliv\]](#). A Lei 32/2008 não tem regime de *preservação* (que está no artigo 12.º da LCC, que abrange os dados aqui em causa e não foi alterada pela Lei 18/2024)[\[xlv\]](#), nem de *interceptação* (que se encontram apenas nos artigos 187.º e 188.º do CPP e no artigo 18.º da LCC, não alterados pela Lei 18/2024); tem normas sobre a transmissão dos dados, mas constam apenas do artigo 9.º.

Quer na letra desse artigo, quer na dos artigos 47.º, n.º 4, e 54.º, n.º 4, da LOSJ (igualmente alterados pela Lei 18/2024 e que respeitam à competência do STJ), está expresso que se trata de *conservação*. Devemos presumir que o legislador soube exprimir o seu pensamento em termos adequados – artigo 9.º, n.º 3, do Código Civil.

Tal redacção foi a encontrada no parlamento para superar a pronúncia de inconstitucionalidade feita no Ac. TC 800/2023 sobre o n.º 2 do artigo 6.º do Decreto n.º 91/XV da AR, que previa a conservação universal *ope legis* pelo período de três meses a contar da data da conclusão da comunicação, considerando-se esse período prorrogado até seis meses, salvo se o seu titular se tivesse oposto perante os FS à prorrogação dessa conservação, já descrita em I.2.8 a I.2.10.

O parlamento seguiu as “sugestões” do TJUE e do TC[\[xlvi\]](#), que viam na *conservação dirigida ou selectiva* uma forma de obviar à violação da CDFUE e da CRP, respectivamente. Concretamente,

seguir o tribunal do Luxemburgo no Acórdão de 05.04.2022 (C-140/20 – *Caso Commissioner of An Garda Síochána*)^[xlvi], onde este afirma (§ 101):

«[...] o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a medidas legislativas que preveem, a título preventivo, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização. Em contrapartida, o referido artigo 15.º, n.º 1, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública,

- [1] uma *conservação seletiva* dos *dados de tráfego* e dos *dados de localização* que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;
- [2] uma *conservação generalizada e indiferenciada dos endereços IP* atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;
- [3] uma *conservação generalizada e indiferenciada de dados relativos à identidade civil* dos utilizadores de meios de comunicações eletrónicas; e
- [4] uma imposição aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, do dever de procederem, por um determinado período, à *conservação rápida* dos *dados de tráfego* e dos *dados de localização* de que esses prestadores de serviços dispõem;

desde que essas medidas assegurem, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e que as pessoas em causa disponham de garantias efetivas contra os riscos de abuso.» (realces e numeração meus).

Ora, estas quatro hipóteses correspondem, respectivamente: a quarta, à preservação (*quick-freeze*)^[xlvii]; a terceira, à previsão da alínea a) do n.º 1 do artigo 6.º; a segunda, à previsão da alínea c) do n.º 1 do artigo 6.º; a primeira, à previsão do n.º 2 do artigo 6.º, que agora se analisa. Ou seja, esta última *não se trata de preservação, mas sim de conservação seletiva* dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado.

Assim sendo, *este é um procedimento autónomo, que ocorre fora de qualquer concreto processo*^[xlix], embora a informação que fundamente a autorização possa ter sido recolhida num ou vários processos determinados, mas também pelos serviços de informação ou possa resultar da análise de dados sobre criminalidade, entre outras fontes.

Como referido no citado acórdão:

«78) Os Estados-Membros têm assim, nomeadamente, a faculdade de adotar medidas de conservação contra pessoas que, a título dessa identificação, sejam objeto de um inquérito ou de outras medidas de vigilância atuais ou de inscrição no registo criminal nacional que mencione uma condenação anterior por atos de criminalidade grave que possam implicar um risco elevado de reincidência. Ora, quando essa identificação se baseia em elementos objetivos e não discriminatórios, definidos pelo direito nacional, a conservação seletiva dirigida a pessoas assim identificadas é justificada.

79) Por outro lado, uma medida de conservação seletiva dos dados de tráfego e dos dados de localização pode, segundo a escolha do legislador nacional e no estrito respeito do princípio da proporcionalidade, assentar igualmente num critério geográfico quando as autoridades nacionais competentes considerem, com base em elementos objetivos e não discriminatórios, que existe, numa ou em várias zonas geográficas, uma situação caracterizada por um risco elevado de preparação ou de prática de atos de criminalidade grave. Essas zonas podem ser, nomeadamente, locais caracterizados por um elevado número de atos de criminalidade grave, locais particularmente expostos à prática de atos de criminalidade grave, tais como locais ou infraestruturas frequentados regularmente por um número muito grande de pessoas, ou ainda locais estratégicos, como aeroportos, estações ou zonas de portagens (v., neste sentido, Acórdão de 6 de outubro de 2020, *La Quadrature du Net e o.*, C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 150 e jurisprudência referida).

80) Importa sublinhar que, segundo esta jurisprudência, as autoridades nacionais competentes podem adotar, relativamente às zonas referidas no número anterior, uma medida de conservação seletiva baseada num critério geográfico, como, nomeadamente, a taxa média de criminalidade numa zona geográfica, sem disporem necessariamente de indícios concretos relativos à preparação ou à prática, nas zonas em causa, de atos de criminalidade grave. Na medida em que uma conservação seletiva baseada nesse critério é suscetível de afetar, em função das infrações penais graves visadas e da situação específica dos respetivos Estados-Membros, simultaneamente locais caracterizados por um elevado número de atos de criminalidade grave e locais particularmente expostos à prática de tais atos, também não é, em princípio, suscetível de dar lugar a discriminações, uma vez que o critério relativo à taxa média de criminalidade grave não apresenta, por si só, nenhuma ligação com elementos potencialmente discriminatórios.

81) Além disso, e sobretudo, uma medida de conservação seletiva dirigida a locais ou infraestruturas regularmente frequentados por um número muito elevado de pessoas ou a locais estratégicos, como aeroportos, estações, portos marítimos ou zonas de portagens, permite às autoridades competentes recolher dados de tráfego e, nomeadamente, dados de localização de todas as pessoas que utilizam, num determinado momento, um meio de comunicação eletrónica num desses locais. Assim, essa medida de conservação seletiva é suscetível de permitir às referidas autoridades obter, através do acesso aos dados assim conservados, informações sobre a presença dessas pessoas nos locais ou nas zonas geográficas visados por essa medida, bem como sobre as suas deslocações entre ou no interior destes e daí retirar, para efeitos da luta contra a criminalidade grave, conclusões sobre a sua presença e a sua atividade nesses locais ou zonas geográficas num dado momento durante o período de conservação.

82) Importa ainda salientar que as zonas geográficas visadas por essa conservação seletiva podem e, se for caso disso, devem ser alteradas em função da evolução das condições que justificaram a sua seleção, permitindo assim, nomeadamente, reagir às evoluções da luta contra a criminalidade grave. Com efeito, o Tribunal de Justiça já declarou que a duração das medidas de conservação seletiva descritas nos n.os 76 a 81 do presente acórdão não pode ultrapassar a estritamente necessária à luz do objetivo prosseguido e das circunstâncias que as justificam, sem prejuízo de uma eventual renovação devido ao facto de continuar a ser necessário proceder a essa conservação (Acórdão de 6 de outubro de 2020, *La Quadrature du Net e o.*, C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 151).

83) No que respeita à possibilidade de prever critérios distintivos diferentes de um critério pessoal ou geográfico para aplicar uma conservação seletiva dos dados de tráfego e dos dados de localização, não se pode excluir que outros critérios, objetivos e não discriminatórios, possam entrar em linha de conta para garantir que o âmbito de uma conservação seletiva se limite ao estritamente necessário e estabelecer uma ligação, pelo menos indireta, entre os atos de criminalidade grave e as pessoas cujos dados são conservados. Não obstante, uma vez que o artigo 15.º, n.º 1, da Diretiva 2002/58 visa medidas legislativas dos Estados-Membros, é a estes últimos e não ao Tribunal de Justiça que incumbe identificar esses critérios, entendendo-se que não pode ser reinstituída por este meio uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização.»

A “formação especial” do STJ nunca exerce, pois, as funções de juiz de instrução em processo. Havendo conservação, a (eventual) posterior transmissão dos dados (acesso e utilização probatória) a quaisquer processos será feita nos termos definidos pelo artigo 9.º, cabendo a decisão ao respectivo juiz de instrução do processo.

Não criou aqui o legislador um novo regime de preservação (não eliminação) de dados já conservados, que, se não fosse esta previsão, teriam de ser os conservados ao abrigo da Lei 41/2004^[ii]. O regime de preservação já existia na nossa lei (artigo 12.º da LCC) e não foi alterado pela Lei 18/2004, sendo da competência do MP ou do juiz de instrução, consoante o tipo de dados, ou mesmo de órgão de polícia criminal em caso de urgência^[iii]. Seria totalmente desprovido de razão de ser que o legislador, que pretendia ajustar a lei interna às exigências do TJUE, tivesse querido derrogar um regime já existente e conforme à jurisprudência do TJUE, retirando essa competência ao MP e ao juiz de instrução, atribuindo-a a uma formação especial do mais alto tribunal judicial, assim criando um incidente processual completamente anómalo e susceptível de subverter a hierarquia dos tribunais, pois, seguindo esse entendimento, permite que, após deferimento pelo STJ do requerimento do MP, por considerar os dados necessários para a investigação e repressão do crime, pode depois o juiz de instrução, no mesmo processo, rejeitar o pedido do MP de acesso aos mesmos, por serem desnecessários à prova.

Também não se trata de interceptação, cujos regimes já existiam na nossa lei (artigos 187.º e 188.º do CPP e 18.º da LCC) e não foram alterados pela Lei 18/2004, e que, sob pena de inconstitucionalidade, sempre obrigariam aos posteriores procedimentos periódicos de controlo (artigo 188.º do CPP)^[iii], não previstos no artigo 6.º em análise.

1.3.4.

Dos n.ºs 2 e 3 do artigo 6.º resulta claro que o *STJ não actua oficiosamente, antes a requerimento*: autoriza, não ordena. Esse artigo não declara de forma expressa quem tem legitimidade para tal requerimento. Porém, do n.º 4 (no segmento «o Ministério Público comunica de imediato às entidades referidas no n.º 1 do artigo 4.º a submissão do pedido») infere-se que é *apenas o MP*. Tal é efectivamente a única possibilidade que tem sentido e coerência sistemática, pois, tratando-se de conservação de (possíveis) meios de prova, sendo o MP o titular da acção penal e quem dirige o inquérito, ocorrendo tal fora de qualquer concreto processo [não podendo haver, por isso, sequer assistente ou arguido interessados no uso desses (possíveis) meios de prova], apenas o MP o poderia fazer.

Sendo um procedimento autónomo que corre termos no STJ, e sendo o MP representado nesse supremo tribunal pelo Procurador-Geral da República (PGR)^[iiii], apenas a este – e, se for essa a sua decisão, aos procuradores-gerais adjuntos aí colocados que o coadjuvam ou substituem^[liv] – cabe o exercício desta competência.

Saber como se processa a recolha e tratamento de informação que sustenta e instrua a decisão de requerer esta conservação é algo que terá de ser determinado pelo PGR^[lv].

1.3.5.

Determina o n.º 3 do artigo 6.º que «[o] pedido de autorização judicial para conservação de dados de tráfego e de localização tem carácter urgente e deve ser decidido no prazo máximo de 72 horas». O que tem urgência é o procedimento que se inicia com o pedido (em rigor, um requerimento), não propriamente este, que se esgota quando apresentado, nem a recolha de informação que a ele conduz, que deve ser feita nos termos determinados pelo PGR. Deve ser decidido em 72 horas pela formação do STJ, prazo que tem natureza meramente ordenadora: o seu incumprimento não tem, só por si, qualquer consequência sobre o requerimento ou para o procedimento^[lvi].

Sendo urgente, corre em férias judiciais, mas, não estando em causa assegurar a liberdade de pessoas, não ao fim-de-semana – artigo 103.º, n.ºs 1 e 2, do CPP^[lvii].

Correndo em férias judiciais, e sendo inquestionável que os juízes conselheiros têm direito ao gozo de férias pessoais e que estas devem ser gozadas preferencialmente nos períodos de férias judiciais, tal serviço deve integrar o de turno em férias judiciais (garantindo-se a existência de um colectivo de três juízes) – artigo 36.º, n.º 1, da LOSJ, e artigo 54.º do DL 49/2014. Não creio necessário prever, para esse período, qualquer especial regime de substituição, pois o regime dos turnos serve precisamente para atribuir competência a quem, fora desse período, a não tem. Fora de férias judiciais, havendo eventual impedimento pontual de qualquer um dos juízes (p. ex., por doença), deverá o mesmo ser substituído nos termos gerais.

1.3.6.

O n.º 4 dispõe que «[d]e forma a salvaguardar a utilidade do pedido de autorização judicial para conservação de dados de tráfego e de localização, o Ministério Público comunica de imediato às entidades referidas no n.º 1 do artigo 4.º a submissão do pedido, não podendo os dados ser objeto de eliminação até à decisão final sobre a respetiva conservação».

Aqui se preceitua que, quando formula o pedido, o MP deve sempre logo comunicá-lo também aos FS que venham a ser os destinatários da obrigação de conservação (o que depende do seu âmbito territorial e/ou subjectivo). Apesar da letra da lei, creio que só o *deverá fazer se existir efectiva necessidade*, pois o requerimento pode ser feito com antecedência em relação à data pretendida para início da conservação^[lviii].

A comunicação aos FS não deve ser feita com cópia do requerimento, que necessariamente terá fundamentação de facto que não deve ser do conhecimento destes.

Logo que recebem essa comunicação, e se o requerimento do Ministério Público for para conservação imediata, os FS devem logo passar a conservar, em base própria, os dados referidos no

pedido do MP; se o requerimento do MP for apenas para data determinada posterior, só a partir desta deverão passar a fazê-lo (se for cumprido o prazo máximo de 72 horas para decisão, esta chegará aos FS antes da data pretendida pelo MP).

Se o requerimento do MP for deferido, os FS continuam a conservar os dados pelo período que for indicado na decisão; se for indeferido, devem proceder à sua destruição.

1.3.7.

O artigo 6.º nada diz sobre o *âmbito da conservação*. No entanto, bem compreendendo a sua razão de ser, *supra* exposta, é forçoso concluir que terá o âmbito que os seus concretos fundamentos de facto exigirem, como até exemplificado pelo TJUE. Poderá, pois, ser para *parte do território* (critério territorial)^[lix], ou para *algumas pessoas* / “*categorias de pessoas*”^[lx] (critério subjectivo), ou com uma mistura (variável) de ambos os critérios.

Não é de excluir a possibilidade de a conservação ser *universal* (todo o território, todas as comunicações de todos os assinantes/utilizadores), desde que existam excepcionais fundamentos para tal^[lxi].

1.3.8.

O artigo 6.º não define qualquer período máximo, limitando-se a estatuir que «[a] fixação e a prorrogação do prazo de conservação referida[s] nos números anteriores devem limitar-se ao estritamente necessário para a prossecução da finalidade prevista no n.º 1 do artigo 3.º, devendo cessar logo que se confirme a desnecessidade da sua conservação» (n.º 5), o que o princípio constitucional da proporcionalidade sempre imporia (cf. artigo 18.º, n.º 2, da CRP). Daqui resulta que a decisão deve fixar um período de conservação e que este período pode vir a ser prorrogado. A lei não estabelece limites ao número de prorrogações: o que importa sempre é que para tal exista fundamento.

Quanto a prazos, há assim que distinguir duas realidades: (i) o *período* durante o qual os FS vão estar a conservar os dados das comunicações que forem ocorrendo (p. ex., de 1 a 31 de Agosto de 2026); e (ii) o *prazo*, após o termo de cada concreta comunicação, em que os FS vão manter cada um dos respectivos dados que conservaram (p. ex., um ano).

Quanto ao primeiro, será o estritamente necessário face às concretas necessidades que fundamentam a conservação. Embora não existam limites máximos abstractos, a própria natureza excepcional desta conservação selectiva leva a que seja difícil imaginar situações que fundamentem, logo no momento da decisão, uma conservação por períodos longos. Até porque, havendo

possibilidade de prorrogação, se se mantiverem as circunstâncias de facto que fundamentaram a decisão inicial de conservação^[lxii], pode sempre o STJ, a requerimento do MP, autorizá-la.

Ainda que dentro do período fixado, a conservação deverá cessar logo que se confirme a desnecessidade da sua manutenção – parte final do n.º 3. Tal poderá suceder a requerimento do MP – sempre sujeito a deveres de objectividade e respeito pela lei^[lxiii] –, ou mesmo oficiosamente pelo tribunal (se o facto for do conhecimento público^[lxiv]).

Quanto ao segundo prazo (de manutenção dos dados conservados), é defensável considerar que será sempre durante um ano, por ser o prazo previsto no n.º 1 e o n.º 2 parecer pressupor a aplicação desse prazo também aos dados de tráfego e de localização. Ainda que assim não se considere, e se entenda que o prazo é variável e deve ser definido pelo STJ, não creio que possa ser superior a um ano^[lxv]. Se há esse limite máximo para os dados menos susceptíveis de violar a privacidade, previstos no n.º 1, *a fortiori* o mesmo deve acontecer para os mais susceptíveis de o fazer (dados de tráfego e de localização).

Como o próprio artigo, no n.º 2, ressalva a possibilidade de conservação pelas entidades referidas no n.º 1 do artigo 4.º nos termos definidos contratualmente com o cliente para efeitos emergentes das respectivas relações jurídicas comerciais ou por força de disposição legal especial, onde se inclui a Lei 41/2004, e que, ao abrigo desta, a conservação de dados de tráfego e de localização pode ir até aos seis meses^[lxvi], esta conservação do n.º 2 do artigo 6.º só terá verdadeiramente efeito útil se for por período superior a seis meses. De qualquer forma, por razões de segurança jurídica, a decisão de autorização deverá sempre definir com precisão qual o prazo de conservação.

Quanto a este prazo de manutenção dos dados, não creio que possa haver prorrogação. Existindo, em qualquer processo, a necessidade de os manter mais tempo conservados, o que há a fazer é utilizar o regime da preservação, previsto no artigo 12.º da LCC^[lxvii]. Não creio igualmente que possa haver destruição antecipada, pois nunca será possível saber se, até ao final do prazo, os mesmos vão ou não ser necessários em inquérito por crime grave (que pode nem estar ainda aberto por não ter ainda havido notícia do crime).

1.3.9.

O requerimento do MP, para além de devidamente fundamentado de facto e de direito, deverá, pelo que se expôs, conter um pedido que com precisão indique: os dados que pretende conservar (de tráfego e/ou localização); a indicação da zona geográfica onde vão ocorrer as comunicações cujos dados se pretende conservar e/ou identificação das pessoas intervenientes nas comunicações a quem respeitam os dados a conservar^[lxviii]; o período de conservação (data de início e data de fim); o prazo de manutenção dos dados de cada comunicação após o seu termo; os FS que devem ficar obrigados à conservação.

1.3.10.

A lei não prevê a possibilidade de qualquer contraditório prévio pelos FS: ao requerimento do MP seguir-se-á a decisão do STJ. Só assim poderá haver decisão no prazo de 72 horas após a entrada do requerimento.

Tal não significa que, depois de recebido o requerimento, não possa o STJ notificar o MP para clarificar algum aspecto, juntar algum documento em falta ou clarificar algum aspecto do seu pedido.

1.3.11.

O n.º 3 prescreve que a conservação apenas pode ser fundada na *necessidade* para a finalidade prevista no n.º 1 do artigo 3.º, que é exclusivamente a investigação, detecção e repressão de crimes graves por parte das autoridades competentes. Não exige, pois, qualquer necessidade probatória qualificada, como as previstas no artigo 179.º, n.º 1, alínea c) (grande interesse para a descoberta da verdade ou para a prova) ou no artigo 187.º, n.º 1, ambos do CPP (indispensabilidade para a descoberta da verdade), o que bem se compreende, pois, contrariamente a estes institutos, trata-se de mera conservação de (possível) meio de prova e não de meio de obtenção de prova.

1.3.12.

Poderá o STJ, ao determinar esta conservação selectiva, desde logo limitar a posterior utilizabilidade probatória dos dados, restringindo-a a algum(ns) tipo(s) de crime(s) grave(s)? P. ex., constituindo o fundamento da conservação o perigo de actos terroristas aquando da realização de importante evento político, poderá o STJ desde logo decidir que os dados que vierem a ser conservados apenas poderão ser utilizados para a prova de crimes previstos na Lei 52/2003?

Não creio que tal seja admissível. Desde logo, a finalidade da conservação resulta da própria lei (artigo 3.º, n.º 1: crimes graves, sem excepção), não cabendo ao tribunal substituir-se ao legislador. Por outro lado, quando é determinada a conservação não é possível conhecer, com a menor precisão, para a prova de que crimes poderá vir a ser necessária a utilização dos dados que vierem a ser conservados. Finalmente, o que releva é que, no momento da *transmissão*, estejam preenchidos os requisitos previstos nos n.ºs 1 a 4 do artigo 9.º, cabendo essa decisão ao juiz de instrução do caso, não ao STJ. É neste momento, e apenas neste, que opera o critério da proporcionalidade, fazendo-se a ponderação entre a utilização dos dados e o tipo de crime em causa, que passa pelo enquadramento do crime em causa no conceito de “crime grave” e, ainda, pelo critério de necessidade probatória previsto no n.º 1 do artigo 9.º.

1.3.13.

Nada dizendo a Lei 32/2008 em contrário, afigura-se recorrível a decisão de indeferimento (total ou parcial) do STJ, por aplicação do princípio consagrado no artigo 399.º do CPP. A competência para conhecer do recurso será do pleno das secções criminais – artigo 11.º, n.º 3, alínea b), do CPP (por analogia, já que não se trata de decisão das secções)[\[lxix\]](#). A legitimidade para recorrer será apenas do MP. Sendo de deferimento, o MP não terá interesse em agir. Os FS, não tendo a defender qualquer direito seu afectado pela decisão (cf. artigo 401.º, n.º 1, alínea d), do CPP), não têm legitimidade para responder ao recurso do MP, nem para recorrer das decisões de deferimento.

2. Lei 41/2004

2.1.

A Lei 41/2004 transpõe para a ordem jurídica nacional a Directiva 2002/58/CE, do Parlamento Europeu e do Conselho, sendo o primeiro diploma a definir um regime específico sobre o tratamento de dados pessoais no contexto da prestação de serviços de comunicações electrónicas, especificando e complementando as disposições da Lei 67/98, que permitia aos FS a conservação de *metadados* em determinadas situações. Também pela primeira vez, aí se previa a possibilidade de utilização probatória em processo judicial desses dados. Com ligeiras alterações introduzidas pelas Leis 46/2012 e 16/2022, mantém-se em vigor.

Esta lei, por um lado, proíbe de forma expressa o armazenamento de comunicações e dos respectivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, devendo estes dados ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação; mas, por outro, *permite (mas não obriga) aos FS que tratem (o que inclui a conservação) aqueles necessários à facturação dos assinantes e ao pagamento de interligações até final do período durante o qual a factura pode ser legalmente contestada ou o pagamento reclamado, que é hoje de seis meses após a prestação do serviço* (artigos 10.º, n.º 1, e 1.º, n.º 2, alínea d), da Lei 23/96) – cf. seus artigos 4.º, n.º 2, e 6.º, n.ºs 2 e 3.

A LCE consagra, entre os direitos dos utilizadores finais, o de receber facturas mensais não detalhadas sem encargos ou, mediante pedido, facturas detalhadas, nos termos do artigo 122.º – artigo 113.º, n.º 1, alínea g), desse diploma[\[lxx\]](#). O artigo 122.º, por sua vez, preceitua que os serviços de comunicações electrónicas acessíveis ao público, com excepção dos serviços de comunicações interpessoais independentes de números e dos serviços de transmissão utilizados para a prestação de serviços máquina a máquina, são facturados mensalmente, devendo as facturas, para além do mais, a discriminação dos serviços prestados e dos preços correspondentes [n.º 1, alínea a)]; o utilizador final pode optar por uma *factura mensal detalhada*, a qual deve traduzir com o maior

pormenor possível os serviços prestados, sem prejuízo do legalmente estabelecido em matéria de tratamento de dados pessoais e protecção da privacidade no sector das comunicações electrónicas (n.º 3); nas facturas detalhadas não são identificadas as chamadas facultadas a título gratuito, incluindo as chamadas para serviços de assistência (n.º 5), de onde se infere, *a contrario*, que são identificadas as chamadas não gratuitas. Deste modo, pelo menos até à emissão da factura mensal correspondente a cada concreta comunicação, os FS estão obrigados a conservar os respectivos dados.

O n.º 4 do artigo 4.º da Lei 41/2004 preceitua que «[a]s empresas que oferecem serviços de comunicações eletrónicas só podem tratar os dados referidos no n.º 1 se o assinante ou utilizador a quem os dados digam respeito tiver dado o seu consentimento prévio e expresso, que pode ser retirado a qualquer momento, e apenas na medida do necessário e pelo tempo necessário à comercialização de serviços de comunicações eletrónicas ou à prestação de serviços de valor acrescentado». Contrariamente ao afirmado no Ac. 800/2023^[lxxi] (mas não no voto de vencido do Cons. JC Loureiro), *este consentimento não é necessário para tratamento dos dados para efeitos de facturação e pagamentos de interligação, antes apenas para a conservação dos dados para efeitos de comercialização dos serviços de comunicações electrónicas ou para o fornecimento de serviços de valor acrescentado*, o que bem se compreende, pois sem essa conservação não poderia haver facturação, logo os FS não poderiam prestar o serviço a quem não consentisse. Esta interpretação resulta clara quando se atenta no artigo 6.º, n.ºs 2 e 3, da Directiva 2002/58, que a Lei 41/2004 transpôs. O n.º 2 do artigo 6.º, que prevê o tratamento dos dados de tráfego necessários para efeitos de facturação dos assinantes e de pagamento de interligações, não exige consentimento; só o n.º 3 o exige, quando o tratamento é para efeitos de (i) comercialização dos serviços de comunicações electrónicas ou para o (ii) fornecimento de serviços de valor acrescentado. O mesmo está expresso no considerando 26 da directiva^[lxxii].

2.2.

Quanto aos *dados de localização*^[lxxiii], dispõe o n.º 1 do artigo 7.º:

«Nos casos em que sejam processados dados de localização, para além dos dados de tráfego, relativos a assinantes ou utilizadores das redes públicas de comunicações ou de serviços de comunicações eletrónicas acessíveis ao público, o tratamento destes dados é permitido apenas se os mesmos forem tornados anónimos».

Aparentemente, estes dados só podem ser conservados se forem tornados anónimos, ou seja, se não permitirem identificar o utilizador (assim lhes retirando qualquer interesse probatório). Creio, diferentemente, que *esta norma não afasta a possibilidade de os FS conservarem esses dados quando os mesmos sejam necessários à facturação e ao pagamento* (pense-se, p. ex., nas comunicações feitas no estrangeiro, sujeitas a pagamentos adicionais por “roaming”, cujo valor pode divergir de país para

país, em que é imprescindível conhecer a posição geográfica do equipamento terminal do utilizador). Sendo imprescindíveis à facturação, tais dados de localização são ainda dados de tráfego, incluídos na definição deles feita no artigo 2.º, n.º 1, alínea d): «quaisquer *dados tratados* para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou *para efeitos da faturação da mesma*» (realces meus).

Por outro lado, o n.º 2 do referido artigo 7.º preceitua que «[é] permitido o registo, o tratamento e a disponibilização de dados de localização, nomeadamente da informação sobre a localização do chamador, às organizações com competência legal para receber ou tratar comunicações de emergência, para efeitos de resposta a essas comunicações». Do n.º 3 do artigo 10.º resulta que não se trata de mera permissão, antes de *verdadeira obrigação* de registo e tratamento dos dados de localização de um assinante ou utilizador, nomeadamente a informação sobre a localização do chamador, por forma a disponibilizar esses dados às organizações com competência legal para receber ou tratar comunicações de emergência, para efeitos de resposta a essas comunicações, obrigação cujo incumprimento constitui contra-ordenação [cf. artigo 14.º, n.º 2, alínea d)]. Esta obrigação é igualmente imposta pelo artigo 67.º, n.º 2, alínea b), da LCE.

A Lei 41/2004 não define, de forma expressa, qualquer prazo de conservação. Prescrevendo que o registo e o tratamento são para efeitos de resposta a essas comunicações, infere-se que os dados serão conservados durante períodos muito curtos. Através do Regulamento 989/2024^[lxxiv], a ANACOM regulamentou a disponibilização da informação sobre a localização do chamador ao Ponto de Atendimento de Segurança Pública, mas não definiu aí qual o prazo máximo de conservação.

2.3.

Podendo então os FS conservar esses dados por período de até seis meses após o fim de cada comunicação (o que por regra acontece), podem ou não ser obtidos e utilizados para efeitos de prova em processo penal^[lxxv]?

Até à Lei 32/2008, não existia na lei portuguesa qualquer outro regime de conservação de dados de tráfego e de localização que não a Lei 41/2004. Até à revisão CPP operada pela Lei 48/2007, não previa sequer o CPP de forma expressa a possibilidade de acesso e utilização probatória desses dados. Não obstante, eles eram acedidos e utilizados^[lxxvi].

Questão que inicialmente se colocou foi a respeitante à definição da entidade competente para ordenar/autorizar aos FS que os entregassem no processo. Foi nesse contexto que foram emitidos os Pareceres do CCPGR 16/94 e 21/2000, que, com a jurisprudência que se foi consolidando, concluíam que a obtenção dos dados de tráfego dependia da decisão judicial, mas não já a obtenção dos dados de base. O fundamento para a sua obtenção (acesso e utilização probatória) resultava da conjugação do previsto nos artigos 187.º, 190.º^[lxxvii] e 269.º, n.º 1, alínea c), do CPP

para as escutas telefónicas, aplicável por extensão (para as condições de admissibilidade), mesmo não havendo regime legal expresso sobre a conservação dos dados^[lxxviii].

A conformidade constitucional dessa interpretação normativa, na ausência de previsão legal expressa, foi levada ao TC, tendo este concluído, no Ac. 486/09, que, estando o acesso à facturação detalhada e localização celular compreendidos no real conteúdo das técnicas de ingerência nas telecomunicações expressamente previstas pelo legislador no artigo 187.º do CPP, não existia desrespeito ao princípio da legalidade consagrado no artigo 34.º, n.º 4, da CRP. Permitindo a lei o mais (o acesso aos dados de conteúdo), permitia o menos (o acesso aos dados de tráfego e aos dados de localização). Pode ler-se na sua fundamentação:

«[...] a interceptação e gravação das conversações ou comunicações telefónicas incorpora necessariamente uma “facturação detalhada” dessas comunicações, que é levada a cabo pelo órgão de polícia criminal interveniente e que se materializa no auto de gravação a juntar ao processo, o qual contém, relativamente o aparelho de telefone escutado, além de outros dados, os números de telefone chamados, a data da chamada, a hora de início e a duração de cada chamada, isto é os elementos de tráfego cobertos pelo sigilo das telecomunicações constantes da facturação detalhada.

[...] as referidas interceptações das comunicações telefónicas são sempre necessária e tecnicamente precedidas da localização celular do equipamento móvel em causa, sem a qual não pode haver estabelecimento e transmissão das comunicações.

Daí que seja possível concluir, com recurso a um simples raciocínio lógico, que o artigo 187.º, n.º 1, do C.P.P./87, ao permitir a interceptação e gravação das conversações ou comunicações telefónicas, permite também, inevitavelmente, o acesso a todos os dados de tráfego inerentes à concretização dessa técnica de ingerência nas telecomunicações, onde se incluem os dados da facturação detalhada cobertos pelo sigilo das telecomunicações e a localização celular.

E, sendo esses dados de tráfego apenas uma parte dos dados facultados pela realização de “escutas telefónicas”, nada obstará, e até imporá a exigência que as técnicas de intromissão nas comunicações telefónicas se limitem à medida necessária para alcançar o objectivo de investigação criminal visado, que o acesso a esses dados de tráfego seja efectuado, dispensando a realização duma “escuta telefónica”, quando esta não se revele necessária aos fins da investigação.»

A utilização no processo penal dos dados conservados pelos FS ao abrigo da Lei 41/2004 era, pois, válida. A Lei 32/2008 nada alterou neste aspecto, como veremos.

Pouco depois do Ac. TC 268/2022, ainda em 2022, os Acs. TRP de 10.07.2022 (José António Rodrigues da Cunha), TRC de 12.10.2022 (Maria Alexandra Guiné), TRC de 12.10.2022 (Paulo Guerra) e TRP de 07.12.2022 (Pedro Vaz Pato) apreciaram expressamente essa questão e, ainda que nem sempre pelos mesmos fundamentos, responderam-lhe negativamente. O primeiro apenas porque considerou inaplicável o artigo 189.º, n.º 2 (e com isso não havendo qualquer norma-fundamento para obtenção), os demais porque, para além disso, consideraram que a aplicação da Lei 41/2004 se limita à protecção contratual, no contexto das relações estabelecidas entre as empresas fornecedoras de serviços de comunicações electrónicas e os seus clientes, não sendo lícito recorrer a ela para efeitos de investigação criminal. No último ainda se refere que não se pode aplicar o regime da Lei 41/2004 se dele resulta a mesma falta de garantias, no plano da investigação criminal, que levou à declaração de inconstitucionalidade da Lei 32/2008, pois, de outro modo, estaríamos a “deixar entrar pela janela” aquilo a que o Ac. TC 268/2022 fechou a porta. Este acórdão foi seguido pelo TRE no Ac. de 28.02.2023, P. 661/17.1TELSB.E1 (Ana Bacelar).

Mais recentemente, o TRL, nos Acs. de 24.04.2025, P. 335/24.7PILRS-B.L1-9, e de 19.03.2026, P. 23/26.0GCALM-A.L1-9, ambos relatados por Rosa Maria Cardoso Saraiva, citando os acórdãos inéditos do mesmo tribunal de 20.06.2024, P. 18/24.8JBLSB-A.L1-9 (Amélia Carolina Teixeira), e de 06.03.2025, P. 103/24.6JBLSB-A.L1 (Ana Marisa Arnêdo), decidiu que os dados de tráfego guardados pelos operadores de comunicação nos termos consentidos pela Lei 41/2004 não podem, como tal, conhecer utilização probatória em sede de tramitação processual penal por a finalidade da sua conservação ser distinta.

Em sentido contrário, embora nem sempre com fundamentos em tudo coincidentes, foi decidido nos Acs. TRL 26.01.2023, P. 849/20.8PBCSC.L1-9 (Bráulio Martins), TRL 22.02.2023, P. 495/22.1JAFUN-A.L1-5 (Alda Tomé Casimiro), TRP 29.03.2023, P. 47/22.6PEPRT-Z.P1 (Maria Joana Grácio), TRC 19.02.2025, P. 285/22.1JGLSB.C1 (Maria Teresa Coimbra), TRL 23.01.2026, P. 760/25.6GEALM-B.L1-5 (PAULO BARRETO) e TRL 04.06.2024, P. 41/24.2JBLSB-A.L1-5 (Maria José Machado). Estes acórdãos encontram a norma de acesso no n.º 2 do artigo 189.º do CPP, com excepção do último, que o faz no artigo 9.º da Lei 32/2008 (e assim também Duarte Rodrigues Nunes^[lxxix]).

2.5

Ao utilizar tais dados conservados ao abrigo da Lei 41/2004 não se está a “ofender” o Ac. TC 268/2022^[lxxx], nem os Acs. do TJUE por ele invocados.

O TC não apreciou, nem directa, nem indirectamente, a conformidade constitucional de os FS poderem *conservar* os *metadados* como a Lei 41/2004 o permite. Não estava em causa a conservação para efeitos de facturação, apenas a feita com a *finalidade exclusiva* de utilização

probatória em processo penal. De igual forma, não apreciou o TC a questão da *admissibilidade de utilização* no processo penal dos dados conservados para efeitos de facturação.

De igual forma, os Acs do TJUE (Grande Secção), de 21.12.2016, C-203/15 e C-698/15) (*Tele2 Sverige AB e Secretary of State for the Home Department*), de 06.10.2020, 623/17 (*Privacy International*) e, da mesma data, C-511/18, C-512/18 e C-520/18 (*La Quadrature du Net* e outros) versaram apenas sobre a possibilidade de, ao abrigo do artigo 15.º, n.º 1, da Directiva 2002/58 (que foi transposta para Portugal através da Lei 41/2004), poderem os Estados *impor* aos FS a conservação generalizada dos dados de tráfego/localização para *fins de salvaguardar a segurança nacional* (ou seja, a segurança do Estado), a defesa, a segurança pública, e a *prevenção, a investigação, a detecção e a repressão de infracções penais* ou a utilização não autorizada do sistema de comunicações electrónicas.

Ou seja, nesses acórdãos *nunca foi objecto de censura a admissibilidade de conservação dos dados para fins de facturação, nem a admissibilidade de posterior utilização desses dados para prova em processo penal.*

Antes pelo contrário, posteriormente, no Ac. de 30.04.2024 (C-470/21 – *La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs* e outros), proferido pelo Tribunal Pleno, sublinhe-se, foi expressamente admitida a validade, dizendo:

«98. Em contrapartida, *tal objetivo de luta contra as infracções penais em geral permite justificar que seja dado acesso aos dados de tráfego e de localização que foram armazenados e, consequentemente, conservados na medida e pelo período necessário à comercialização dos serviços, à faturação e à prestação de serviços de valor acrescentado, como autorizado pelo artigo 6.º da Directiva 2002/58 (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.ºs 108 e 167).*» (realces meus).

Efectivamente, já no Ac. de 06.10.2020 (*La Quadrature du Net* e outros), o tribunal, no ponto 167, afirmou que

«[...] os Estados-Membros têm a possibilidade de prever na sua legislação que um acesso a dados de tráfego e a dados de localização pode, no respeito dessas mesmas condições materiais e processuais, ocorrer para efeitos de luta contra a criminalidade grave ou de salvaguarda da segurança nacional quando os referidos dados são conservados por um fornecedor em conformidade com os artigos 5.º, 6.º e 9.º ou ainda com o artigo 15.º, n.º 1, da Directiva 2002/58».

Ora, como já referido, o artigo 6.º desta directiva é precisamente aquele que prevê a possibilidade de conservação para efeitos de facturação e comerciais.

No mesmo sentido, nos Acs. de 05.04.2022 (C-140/20 - *Caso Commissioner of An Garda Síochána*), de 22.09.2022 (C-793/19 e C-794/19 - *Caso SpaceNet e Telekom Deutschland*) e de 07.09.2023 (C-162/22 - *Caso Lietivus Respublikos generalinė prokuratūra*), quando o TJUE afirma que o referido artigo 15.º, n.º 1, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da CDFUE, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, para além do mais, uma imposição aos prestadores de serviços de comunicações electrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efectiva, do dever de procederem, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem, está precisamente a referir-se aos dados que os prestadores de serviço já conservaram sem decisão judicial, ou seja, aqueles que conservaram para efeitos de facturação e comerciais. Esta “conservação” rápida de dados que já estão conservados, sendo na verdade uma ordem de não eliminação, chama-se, na lei nacional, preservação, como vimos [\[lxxxii\]](#). O TJUE pressupõe, desta forma, que os dados conservados pelos FS para efeitos de facturação e comerciais e que por esta via serão preservados podem ser usados como prova contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública. Ou seja, o tribunal (i) admite a utilização desses dados com meio de prova em processo penal (por crimes graves) e (ii) que possa haver necessidade de conservar esses dados para além do prazo em que os FS os conservam – logo, se ainda estiverem nesse período de conservação, não será necessária qualquer conservação adicional (preservação).

2.6.

Objecta o Ac. TRP de 07.12.2022 (Pedro Vaz Pato) que não se pode aplicar o regime da Lei 41/2004 se dele resulta a mesma falta de garantias, no plano da investigação criminal, que levou à declaração de inconstitucionalidade da Lei 32/2008, pois, de outro modo, estaríamos a “deixar entrar pela janela” aquilo a que o Ac. TC 268/2022 “fechou a porta”. Acrescenta que «essa falta de garantias que levou à declaração de inconstitucionalidade das referidas normas da Lei n. 32/2008 não diz respeito apenas ao prazo de conservação dos dados de tráfego, pelo que não seria suprida essa inconstitucionalidade tão só pela redução a seis meses desse prazo (o que resultaria da aplicação da referida Lei n.º 41/2008). Diz respeito à ausência de notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros».

É abusivo colocar no Ac. TC 268/2022 qualquer juízo concreto sobre a adequação do prazo de seis meses para a conservação dos dados. Não só o TC não apreciou tal aspecto, como nunca o poderia fazer para um prazo (previsto na Lei 41/2004) que tem outra finalidade: possibilitar a

facturação e o pagamento. Sendo isso possível no prazo de seis meses após a comunicação, não poderá deixar de ser esse o prazo mínimo de conservação.

Por outro lado, cabe dizer que se o tribunal judicial (qualquer que seja) considerar que as normas da Lei 41/2004 que permitem a conservação de dados de tráfego/localização (nos termos expostos) são inconstitucionais, deve com esse fundamento recusar expressamente a sua aplicação, sendo assim obrigatório o recurso pelo MP, permitindo que o TC venha a apreciar tal juízo – artigos 70.º, n.º 1, alínea a), e 73.º, n.º 1, alínea a), e n.º 3, da Lei 22/82. O que ainda nenhum fez.

O fundamento “não se prever a notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal” foi utilizado pelo TC apenas quanto ao artigo 9.º da Lei 32/2008, que, recorde-se, respeitava ao *acesso* a esses dados (não à *conservação*). Ora, a Lei 41/2004 não tem norma de acesso (hoje apenas no artigo 189.º, n.º 2, do CPP, ou, para alguns, no novo artigo 9.º da Lei 32/2008), mas tão só de conservação. Logo, carece de qualquer fundamento a “transposição” para a Lei 41/2004 dessa carência que o TC dizia existir na versão original da Lei 32/2008. Se há esse vício ele então está no CPP. Mas mesmo assim tal não lhe pode ser apontado, pois o regime das regras relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, detecção, investigação ou repressão de infracções penais ou de execução de sanções penais, que naturalmente inclui os direitos de acesso dos titulares dos dados, consta hoje da Lei 59/2019 (cf. artigos 13.º a 19.º). *Não é, pois, matéria que caiba ao CPP.*

Os fundamentos para o juízo de inconstitucionalidade que recaíram sobre os artigos 4.º e 6.º da Lei 32/2008 foram “apenas” os de a lei não prescrever a obrigatoriedade de os dados serem conservados em território da UE, por um lado, e de impor a universalidade da conservação (todos os utilizadores e assinantes), por outro.

Ora, quanto a este último aspecto, atendendo à finalidade da conservação (permitir a facturação e pagamento), esta não poderá deixar de abranger todas as comunicações e serviços prestados pelo FS, sob pena de as não conservadas não poderem ser facturadas. Também este é argumento que não pode ser utilizado com a Lei 41/2004.

Resta a omissão de previsão legal obrigando à conservação dos dados em território da UE – verdadeiramente, uma inconstitucionalidade por omissão, sublinhe-se. A Lei 41/2004 não o diz expressamente, assim como não o fazia a Lei 32/2008. Nem o fazem a quase totalidade das leis que prevêm bases de dados informatizadas.

Porém, actualmente, essa é matéria que nem necessita estar regulada nesta lei (nem em qualquer lei sectorial), pois a questão da territorialidade e da transferência na e para fora da UE está agora definida nos artigos 44.º a 50.º do RGPD, sendo de realçar que, não se tratando de conservação de dados realizada para efeitos de prevenção, investigação, detecção e repressão de infracções penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de

ameaças à segurança pública, não se aplica a exclusão de aplicação do RGPD prevista no seu artigo 2.º, n.º 2, alínea d). Ou seja, o RGPD é efectivamente aplicável a estas bases de dados. Sendo o RGPD um Regulamento da UE, é obrigatório em todos os seus elementos e directamente aplicável em todos os Estados-Membros, vinculando todas as entidades, públicas e privadas— artigo 288.º do TFUE. A execução do RGPD cabe em Portugal à CNPD (artigos 3.º e 4.º, n.º 2, da LPDP), que até pode sancionar a transferência internacional de dados pessoais em violação do disposto nos artigos 44.º a 49.º do RGPD – artigo 37.º, n.º 1, alínea j), da LPDP.

Se a Lei 41/2004 tivesse, antes do RGPD, quaisquer disposições relativas ao local de conservação dos dados ou à sua transferência para fora do espaço da UE, teriam estas sido tacitamente revogadas ou derogadas, ou pelo menos obrigariam à sua interpretação em conformidade com o RGPD.

Não há, pois, qualquer omissão legislativa que, em consequência, seja óbice constitucional à conservação dos dados feita ao abrigo da Lei 41/2004, não podendo esse argumento ser utilizado para recusar o acesso a esses dados para prova em processo penal, designadamente com fundamento no artigo 189.º, n.º 2, do CPP, como veremos *infra*.

2.7.

Objecta-se ainda que a Lei 41/2004 não prevê de forma expressa a utilizabilidade no processo penal dos dados cuja conservação permite.

No n.º 7 do artigo 6.º dessa lei, dispõe-se que «[o] disposto nos números anteriores não prejudica o direito de os tribunais e as demais autoridades competentes obterem informações relativas aos dados de tráfego, nos termos da legislação aplicável, com vista à resolução de litígios, em especial daqueles relativos a interligações ou à faturação». Ou seja, *expressamente prevê a possibilidade de utilização dos dados para prova nos tribunais* (o que de modo algum significa que a conservação dos dados seja feita para esse fim).

Para os citados acórdãos TRC de 12.10.2022 (Paulo Guerra) e TRP de 07.12.2022 (Pedro Vaz Pato) isso apenas significa a possibilidade de utilização em acções cíveis respeitantes a litígios sobre a facturação. Em defesa desse entendimento apelam ao disposto no n.º 4 do artigo 1.º: «As exceções à aplicação da presente lei que se mostrem estritamente necessárias para a proteção de atividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infrações penais são definidas em legislação especial». Porém, esta norma significa apenas que podem existir outras excepções (aos limites de conservação definidos nesta lei) previstas em legislação especial (tendo como fundamento exclusivo a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infracções penais, e não, como estas, o interesse dos FS), e não que daí se retire qualquer limitação à utilização dos dados para a prova em processo penal. Como referido no Ac. TC 486/2009, «a Lei n.º 41/2004 *não prejudica a*

possibilidade de existência de legislação especial que restrinja a sua aplicação no que respeita à inviolabilidade das comunicações, nomeadamente para efeito de investigação e repressão de infracções penais (artigo 1.º, n.º 4)» (realce meu). Não significa, pois, que para efeitos de investigação e repressão de infracções penais o regime seja apenas o previsto noutra legislação.

Como *supra* referido, os *metadados* são prova documental/digital. No caso dos conservados ao abrigo da Lei 41/2004, são documentos que existem independentemente do processo penal – *não há qualquer especial meio que seja necessário prever para a sua obtenção*. Poderiam ser obtidos por busca, por pesquisa e apreensão de dados informáticos, por injunção (ordem), cabendo à lei determinar que meios podem ser utilizados, o que, quanto à injunção, está feito no artigo 189.º, n.º 2, do CPP^[bxxxii], como *infra* se verá.

Ainda que a Lei 41/2004 não previsse – como prevê – a possibilidade de utilização probatória desses dados em processo penal, os mesmos poderiam ser obtidos e utilizados, desde que não existisse qualquer crime na sua conservação. A norma-fundamento para tal está no CPP. Repare-se que, quanto às bem mais gravosas intercepções das comunicações, a Lei 41/2004 – que é a lei que visa a protecção da privacidade no sector das comunicações electrónicas – tem uma previsão bem mais escassa do que a que confere à utilização dos dados de tráfego conservados: limita-se a declarar a sua proibição, «com excepção dos casos previstos na lei». Alguém duvida que o artigo 187.º do CPP e o artigo 18.º da LCC são normas-fundamento suficientes para a utilização desse meio de obtenção de prova?

De qualquer forma, *não tem de haver expressa previsão para que todos os meios de prova possam ser utilizados no processo penal*. Recorde-se o elementar *princípio da legalidade e liberdade da prova* consagrado no artigo 125.º do CPP: são admissíveis as provas que não forem proibidas por lei. No caso, não são proibidas. Não é necessário que, em cada sector da sociedade, da vida social, política, económica, desportiva, etc., em que são gerados documentos (que, quase inevitavelmente, contêm dados pessoais^[bxxxiii]), exista lei que expressamente preveja a possibilidade de posterior utilização probatória dos mesmos em processo penal para que tal possa suceder. Se assim fosse, basicamente nenhuma prova documental seria admissível.

Consequentemente, não creio, sequer, que estejamos perante uma situação de “mudança ou alienação de fim”, hipótese que Duarte Rodrigues Nunes suscita para depois afastar^[bxxxiv]: após a aquisição processual do meio de prova, não há qualquer mudança no fim probatório a que se destina. O que se passa antes disso só tem relevância se nisso existir qualquer ilicitude criminal (que no caso não existe). De qualquer forma, o artigo 23.º, n.º 1, da Lei 58/2019 (LPDP – Lei de Protecção de Dados Pessoais), que é aplicável a estes dados, expressamente permite o tratamento de dados pessoais por entidades públicas para finalidades diferentes das determinadas pela recolha com vista a assegurar a prossecução do interesse público que de outra forma não possa ser acautelado, nos termos da alínea e) do n.º 1, do n.º 4 do artigo 6.º e da alínea g) do n.º 2 do artigo 9.º do RGPD. O n.º 4 do artigo 6.º remete para o a alínea d) do n.º 1 do artigo 23.º, onde está prevista precisamente a

«prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública».

Com especial relevo para esta questão, recordemos ainda o Ac. TC 213/2008, que não julgou inconstitucional a norma do artigo 125.º do CPP na interpretação segundo a qual é permitida a admissão e valoração de provas documentais relativas a listagens de passagens de um veículo automóvel nas portagens das auto-estradas, que foram registadas pelo sistema de identificador da «Via Verde», armazenadas numa base de dados informatizada e ulteriormente juntas ao processo criminal, sem o consentimento do arguido e por mera determinação do MP. Nesse caso, estava em causa a obtenção de provas documentais sobre factos susceptíveis de violar a privacidade de pessoas, armazenadas numa base de dados informatizada, e, apesar de não haver previsão legal expressa para a admissibilidade da sua utilização, o TC não só o julgou conforme à CRP, como assim considerou quanto à competência para o ordenar pertencer ao MP.

De grande relevância é ainda o Ac. TC 607/2003, respeitante à possibilidade de utilização probatória de um diário, algo que a lei não prevê expressamente. O TC apenas julgou inconstitucional a sua valoração como meio de prova *na ausência de uma ponderação*, efectuada à luz dos princípios da necessidade e da proporcionalidade, sobre o conteúdo, em concreto, desses diários, não, pois, por falta de previsão legal expressa. Ora, quanto aos dados de tráfego/localização, a ponderação à luz dos princípios da necessidade e da proporcionalidade está feita pelo legislador na redacção do artigo 189.º, n.º 2, do CPP e no artigo 9.º, n.ºs 1 a 4, da Lei 32/2008 (para quem o defenda que a norma de acesso a estes dados está nesta última lei), e igualmente se impõe ao aplicador por força directa do artigo 18.º, n.º 2, da CRP.

Estando no artigo 189.º, n.º 2, do CPP ou no artigo 9.º, n.ºs 1 a 4, da Lei 32/2008 o fundamento legal para a sua obtenção e utilização probatória, assim está cumprido a exigência de previsão legal para a restrição de direitos fundamentais, imposta pelo artigo 18.º, n.º 2, da CRP. De igual forma, assim se fica fora da proibição de prova prevista no artigo 126.º, n.º 3 do CPP: a intromissão nas telecomunicações (findas, sublinhe-se) é feita como previsto na lei.

2.8.

De grande relevo hermenêutico é hoje o facto de, com a redacção introduzida pela Lei 18/2024, o n.º 2 do artigo 6.º da Lei 32/2008 dispor que «[o]s dados de tráfego e de localização apenas podem ser objeto de conservação mediante autorização judicial fundada na sua necessidade para a finalidade prevista no n.º 1 do artigo 3.º, *sem prejuízo daqueles conservados pelas entidades referidas no n.º 1 do artigo 4.º nos termos definidos contratualmente com o cliente para efeitos emergentes das respetivas relações jurídicas comerciais ou por força de disposição legal especial.*» (realce meu). A expressa ressalva da admissibilidade de conservação para efeitos emergentes das relações jurídicas comerciais com o cliente ou por força de disposição legal especial, que o legislador – certamente

conhecendo a divisão doutrinal e jurisprudencial que existia quanto a esse aspecto – quis introduzir numa lei que regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes (artigo 1.º, n.º 1), *é clara manifestação de que foi sua intenção deixar claro que o regime previsto neste diploma não prejudica o ainda previsto na Lei 41/2004 e a admissibilidade de utilização para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes*^[xxxv]. Esse é o único sentido útil de tal ressalva, sendo certo que há que presumir que o legislador consagrou as soluções mais acertadas e soube exprimir o seu pensamento em termos adequados – artigo 9.º, n.º 3, do Código Civil.

2.9.

De tudo o que fica exposto, creio que fica clara a *admissibilidade legal de utilização probatória dos dados de tráfego/localização conservados pelos FS ao abrigo da Lei 41/2004*^[xxxvi].

O contrário é que seria absolutamente incompreensível: permitir aos FS a conservação e utilização dos dados de tráfego/localização para efeitos de facturação e não permitir a sua utilização em processo judicial para prova de crimes graves seria uma inadmissível perversão de princípios estruturantes do Estado de Direito. O Estado não pode renunciar ao seu dever de protecção dos direitos fundamentais – da vida, liberdade, e segurança das pessoas, *etc.* –, e para tanto, em medida proporcional, de prevenir e investigar o crime e de perseguir e sancionar quem o comete. Ao Estado também cabe garantir os direitos e liberdades fundamentais das vítimas, não apenas dos suspeitos ou arguidos^[xxxvii], não apenas dos sujeitos económicos.

3. Lei das Comunicações Electrónicas

Os FS não só podem, como na prática *estão obrigados a manter registos de alguns dos dados que respeitam ao contrato celebrado com os seus clientes, utilizadores finais, incluindo a sua identificação*. Vejamos.

A anterior Lei das Comunicações Electrónicas (aprovada pela Lei 5/2004) obrigava os FS a conservar qualquer suporte duradouro, incluindo gravação telefónica, relacionado com a celebração, alteração ou cessação do contrato de comunicações electrónicas durante todo o período de vigência acordado, inicial ou sucessivo, acrescido do correspondente prazo de prescrição e caducidade – artigos 48.º, n.º 7, e 47.º-A, n.º 5, alínea a).

Essa lei foi revogada e substituída pela Lei 16/2022, que aprovou a nova Lei das Comunicações Electrónicas. Apesar de não ter preceitos exactamente iguais aos referidos artigos 48.º, n.º 7, e 47.º-A,

n.º 5), alínea a), contém outros de onde resulta idêntica obrigação de conservação desses dados e documentos^[lxxxviii].

Do n.º 12 do artigo 120.º resulta que as empresas que oferecem redes e ou serviços de comunicações electrónicas só poderão opor-se à denúncia dos contratos por iniciativa dos assinantes, com fundamento na existência de um período de fidelização, ou exigirem quaisquer encargos por incumprimento de um período de fidelização, se tiverem prova de que o consumidor concordou com esses termos do contrato.

Sempre que um cliente autorize o pagamento de bens ou serviços de terceiros através da factura de comunicações, a empresa deve conservar a declaração de autorização durante todo o período de vigência do contrato, acrescido do prazo de prescrição do procedimento contra-ordenacional – artigo 125.º, n.º 3.

Obriga ainda o n.º 6 do artigo 136.º as empresas a conservar, em suporte duradouro adequado, durante o prazo de prescrição e caducidade das obrigações resultantes do contrato, qualquer suporte duradouro, incluindo gravação telefónica, relacionado com a denúncia do contrato por iniciativa do consumidor.

Para além destes, têm de manter registos sobre outros dados, sob pena de não conseguirem prestar o serviço contratado: p. ex., número de acesso e dados através dos quais tem acesso ao serviço (número de telefone, endereço IP, números identificadores dos dispositivos do cliente) e dados de facturação (modo de pagamento definido, conta bancária autorizada para débito directo, etc.). Sem esses dados os FS não poderiam sequer exercer a sua actividade.

Veremos *infra* que o artigo 14.º, n.ºs 1 e 4, da LCC constitui o fundamento normativo para a obtenção e utilização probatórias desses dados.

IV. Acesso e Utilização Probatória

Passo agora a analisar os diferentes possíveis fundamentos normativos para o acesso a utilização probatória penal de *metadados* de comunicações electrónicas conservados.

1. Artigo 9.º da Lei 32/2008

1.1.

O artigo 9.º original da Lei 32/2008 foi declarado inconstitucional com força obrigatória geral pelo Ac. TC 268/2022 na parte em que não previa uma notificação ao visado – deixou então de poder ser fundamento normativo para acesso e utilização de *metadados*.

No Decreto n.º 91/XV da AR, já constava a alteração ao artigo 9.º, com inserção dos n.ºs 7 e 8 com um novo regime de notificação ao visado; em sede de fiscalização preventiva, o TC pronunciou-se pela sua não inconstitucionalidade – Ac. 800/2023^[lxxxix]. A Lei 18/2024 introduziu no artigo 9.º tais números com a mesma exacta redacção. Assim superada a inconstitucionalidade encontrada pelo TC, não se adivinha fundamento para quaisquer outras.

1.2.

O artigo 9.º da Lei 32/2008 é assim hoje fundamento normativo para o acesso (transmissão) e utilização probatória dos dados constantes das bases que, em cumprimento desta lei (directamente ou por decisão do STJ), os FS devem conservar. Note-se: apenas para os dados conservados pelos FS ao abrigo desta lei, não para quaisquer outros que conservem com qualquer outro fundamento jurídico, designadamente aqueles analisados no capítulo anterior (principalmente, a Lei 41/2004, cuja norma de acesso está no n.º 2 do artigo 189.º do CPP)^[xc]: isso resulta expresso da letra do n.º 1, que começa por «[a] transmissão dos *dados referentes às categorias previstas no artigo 4.º [...]*» (destaque meu). São, pois, apenas estes dados conservados e não quaisquer (eventuais) outros.

1.3.

O artigo contém um *regime único de acesso e utilização probatória*: aplica-se a todos os diferentes tipos de dados, previstos nos n.ºs 1 e 2 do artigo 6.º, sendo a competência para autorizar a sua transmissão sempre de juiz.

Tendo o artigo 6.º passado a referir-se de forma expressa a dados de identificação do subscritor e ao endereço IP fonte da comunicação, deveria o legislador ter acompanhado aquela que era já jurisprudência nacional pacífica^[xci], incluindo do TC^[xcii], e também do TJUE^[xciii], e em coerência com o disposto no artigo 14.º, n.º 4, da LCC^[xciv], atribuindo nesses casos a competência ao MP, e não sempre, como fez, ao juiz^[xcv].

1.4.

A transmissão dos dados só é admissível se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão de crimes graves – n.º 1 do artigo 9.º

O critério de necessidade probatória é, pois, o mais elevado da nossa lei processual penal, idêntico ao exigido para utilização de interceptações de conteúdo – artigo 187.º, n.º 1, do CPP e artigo

18.º, n.º 2, da LCC. Não há qualquer justificação para tal equiparação, pois a agressão a direitos fundamentais é muito superior com o conhecimento do conteúdo das comunicações do que com os *metadados* a elas respeitantes. Por outro lado, há incoerência com o previsto no n.º 2 do artigo 189.º do CPP e no artigo 14.º da LCC, que se bastam com a mera necessidade probatória (sempre sem prejuízo de obediência a critérios de proporcionalidade que resultam directamente do artigo 18.º, n.º 2, da CRP).

1.5.

Igualmente injustificada é a restrição de transmissão de todos os tipos de dados à investigação, detecção e repressão de apenas “crimes graves”, como definidos no artigo 2.º, n.º 1, alínea g). Tal apenas deveria acontecer com os dados de tráfego e de localização, com maior susceptibilidade de agressão a direitos fundamentais, e não também com os dados previstos no n.º 1 do artigo 6.º, que deveriam poder ser utilizados em todos os tipos de crime (pelo menos em abstracto), em conformidade até com a já referida jurisprudência do TJUE [\[xcvii\]](#).

1.6.

O n.º 3 do artigo 9.º exige ainda que os dados a transmitir sejam relativos a (a) suspeito ou arguido; (b) pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou (c) vítima de crime, mediante o respectivo consentimento, efectivo ou presumido. Segue, pois, catálogo de “visados” idêntico ao previsto para as escutas telefónicas (n.º 4 do artigo 187.º do CPP).

1.7.

Da necessidade de requerimento do MP expressa no n.º 2 e da menção a “juiz de instrução” no n.º 1 parece resultar que os dados apenas podem ser transmitidos a processo que se encontre na fase de inquérito.

Porém, do regime da notificação ao titular dos dados (n.ºs 7 e 8) parece resultar, *a contrario*, que pode ocorrer também noutras fases do processo. Repare-se que o n.º 7 estabelece a regra geral (notificação ao titular dos dados no prazo máximo de 10 dias a contar do despacho que autoriza a transmissão) e o n.º 8 prevê a excepção quando a transmissão for em inquérito (caso em que o MP pode requerer ao juiz que proteja a notificação). Ou seja, se o legislador estabelece um regime especial para a fase de inquérito é porque há um regime geral para outras fases do processo.

Na verdade, não há nenhum fundamento para restringir a transmissão de dados à fase de inquérito. A necessidade probatória (até para defesa dos arguidos) pode ser a mesma em qualquer fase do processo e o grau de ofensa a direitos fundamentais não depende da fase do processo. O único obstáculo que pode existir é o do prazo de conservação (um ano para os dados do n.º 1 do artigo 6.º; o que for definido pelo STJ para os dados do n.º 2): mas, se, em instrução ou mesmo julgamento, os dados pretendidos ainda se mantiverem conservados, nada impede que sejam utilizados para prova [\[xcvii\]](#).

1.8.

Como já referido, para superar a inconstitucionalidade invocada pelo TC, foi inserido neste artigo a obrigatoriedade de notificação ao titular dos dados – n.ºs 7 e 8.

O n.º 7 prescreve que, sem prejuízo do disposto no número seguinte, o despacho que autoriza a transmissão dos dados referentes às categorias previstas no n.º 1 do artigo 4.º é notificado ao titular dos dados no prazo máximo de 10 dias a contar da sua prolação; o n.º 8 estabelece uma exceção, preceituando que se, em inquérito, o MP considerar que a notificação referida no número anterior comporta risco de pôr em causa a investigação, dificultar a descoberta da verdade ou criar perigo para a vida, para a integridade física ou psíquica ou para a liberdade dos participantes processuais, das vítimas do crime ou de outras pessoas devidamente identificadas, pode solicitar ao juiz de instrução criminal que proteja a notificação, a qual é realizada logo que a razão do protelamento deixar de existir ou, o mais tardar, no prazo máximo de 10 dias a contar da data em que for proferido despacho de encerramento desta fase processual.

Daqui resulta que a notificação deve ser ordenada pelo juiz que autoriza a transmissão, logo aquando do despacho, e que, por regra, deve ser executada no prazo de 10 dias; excepcionalmente, e apenas no inquérito, a requerimento do MP, pode o juiz determinar que isso seja feito apenas quando a razão do protelamento deixar de existir ou, o mais tardar, após o encerramento do inquérito.

A notificação só deve ser ordenada e realizada *se e quando* o titular dos dados estiver devidamente identificado (o que muitas vezes não acontece). Essa notificação segue as regras gerais das notificações previstas no CPP e deve ser feita pela secção judicial. A contagem do prazo processa-se igualmente nos termos definidos no CPP.

O incumprimento constitui mera irregularidade (artigo 118.º, n.º 2, do CPP): não há tipificação como nulidade e não há proibição de prova, pois, quanto à notificação, não há qualquer vício na intromissão na vida privada / telecomunicações (tal como não há quando falta a validação da apreensão ocorrida durante busca domiciliária, p. ex.).

1.9.

O artigo 9.º não prevê quaisquer *prazos máximos de resposta por parte dos FS*. Mas devia.

1.10.

O n.º 3 do artigo 7.º prescreve que «[a] transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se *mediante comunicação eletrónica*, nos termos das *condições técnicas e de segurança* fixadas em *portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações*, que devem observar um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados», o que é repetido no n.º 10.

Tal portaria era a Portaria 469/2009, que, sem que se perceba o motivo (que não se encontra expresso em qualquer documento do processo legislativo acessível na respectiva página *online* do parlamento), foi revogada pela Lei 16/2022, que aprovou a Lei das Comunicações Electrónicas, já referida. Até ao momento, não foi publicada outra portaria. Acompanhando a citada Nota Prática 26 do Gabinete do Cibercrime da PGR, afigura-se-me que, por força do n.º 3 do artigo 146.º do Código do Procedimento Administrativo, devem considerar-se em vigor as normas de tal portaria revogada de que depende a produção de efeitos da Lei 32/2008 (e daí que, acompanhando quer essa Nota Prática, quer a jurisprudência superior publicada, quer até a posição tacitamente assumida pela Assembleia da República aquando do processo legislativo que conduziu à Lei 18/2024, não veja motivo para questionar a produção de efeitos da Lei 32/2008 neste momento).

De qualquer forma, estas não são normas de processo penal e, por isso, o seu eventual incumprimento não constitui qualquer vício, nem afecta a utilizabilidade probatória desses meios de prova – cf. artigo 118.º, n.º 1, do CPP.

1.11.

O Regulamento (UE) 2023/1543 não se aplica quando, em processo nacional, se pretendem obter dados conservados por FS estabelecido ou representado em Portugal (artigo 1.º, n.º 1), mas, não obstante, terá várias implicações para muitos dos aspectos previstos no artigo 9.º ora analisados, que analisarei em IV.5.

2. Artigo 189.º, n.º 2, do CPP

2.1.

Após a revisão do CPP operada pela Lei 48/2007, e até à entrada em vigor da Lei 32/2008, o único fundamento normativo para a obtenção de dados de tráfego/localização estava no n.º 2 do artigo 189.º do CPP.

Não obstante ser então pacífico na jurisprudência a admissibilidade da junção aos autos desses dados, com reserva de competência do juiz^[xcviii], aquando da grande revisão do CPP em 2007 o legislador entendeu – bem – dever deixá-lo expresso na letra desse diploma. Assim veio a suceder com a introdução do n.º 2 do artigo 189.º Esse preceito teve origem no anteprojecto da Unidade de Missão para a Reforma Penal (UMRP)^[xcix], em cuja Exposição de Motivos se pode ler: «Exige-se também, de forma expressa, que haja despacho do juiz para *obter e juntar* aos autos dados sobre a localização celular ou o tráfego de comunicações, restringindo-se tal meio de prova aos crimes e pessoas referidos no âmbito do regime das escutas (artigo 189.º)» (realces meus). Quer o preceito, quer esse parágrafo viriam a constar da PPL 109/X. O n.º 2 do artigo 189.º aprovado é o que consta desta proposta. Nunca foi, pois, intenção do legislador aplicar tal regime à obtenção desses dados por via da *intercepção*: esta não se confunde com a mera *obtenção e junção* (de dados conservados) ^[c]. Aliás, a possibilidade de realização de intercepções por decisão de “não juiz” seria certamente questão que nem se colocaria à UMRP.

Efectivamente, *o n.º 2 do artigo 189.º nunca disse respeito (nem agora o faz, como veremos) a intercepções, ou seja, à intercepção e gravação desses dados em tempo real*. A extensão do regime de intercepção das comunicações telefónicas às comunicações feitas por outros meios técnicos era feita apenas pelo n.º 1 desse artigo, que o dizia expressamente: «O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à *intercepção das comunicações* entre presentes» (realces meus). Daí que, contrariamente ao n.º 2, expressamente determinasse a aplicabilidade do disposto no artigo 188.º, que é onde estão definidos os procedimentos da execução e controlo das intercepções.

O n.º 2, pelo seu lado, para além de não prever a aplicabilidade do disposto no artigo 188.º – o que sempre seria indispensável caso se tratasse de intercepções, que é onde estão definidos os procedimentos da execução e controlo destas –, não prevê qualquer limitação à fase de inquérito para o acesso a esses dados, o que, mais uma vez, teria de fazer, à semelhança do que então foi inserido no n.º 1 do artigo 187.º para as escutas, se se tratasse de intercepção (devido à óbvia ineficácia de medida dessa natureza quando o processo não está em segredo de justiça). Como ficou expresso na letra do preceito, a aplicação do disposto no artigo 187.º é apenas para o catálogo de crimes (n.º 1 – âmbito objectivo) e para o catálogo de visados (n.º 4 – âmbito subjectivo). Não houve neste aspecto qualquer lacuna ou incongruência por parte do legislador, pois nunca foi sua intenção que este preceito se aplicasse à intercepção deste tipo de dados. A norma-fundamento para a intercepção de dados de tráfego/localização respeitantes às comunicações telefónicas continuou

apenas no artigo 187.º (com os procedimentos definidos no artigo 188.º): essa permite a interceptação do conteúdo e dos dados de tráfego/localização ou só dos dados de tráfego/localização.

Deste modo, no período entre a Lei 48/2007 e a Lei 32/2008, o fundamento para o acesso e utilização dos dados de tráfego/localização estava apenas no artigo 189.º, n.º 2, do CPP, e o fundamento para a sua conservação, apenas na Lei 41/2004.

2.2.

A Lei 32/2008 manteve inalterado o n.º 2 do artigo 189.º do CPP. A questão que então se colocou foi se aquela lei, com o seu artigo 9.º, tinha ou não revogado ou derogado tacitamente o n.º 2 do artigo 189.º, havendo várias posições assumidas, todas com argumentos válidos.

É inquestionável que a Lei 32/2008 modificou o campo de aplicação do n.º 2 do artigo 189.º do CPP: a matéria que era regulada neste número, directamente e por remissão para os n.ºs 1 e 4 do artigo 187.º (que tipo de crimes admitiam esse meio de prova, a que pessoas poderiam respeitar, qual a entidade competente para ordenar a sua produção^[cii]), passou a estar regulada pelo artigo 9.º da Lei 32/2008. Sendo posterior a norma deste artigo e regulando a mesma exacta matéria, revogou/derrogou tacitamente a anterior^{[cii]/[ciii]}.

Saber se ocorreu uma revogação (total) ou apenas uma derrogação (parcial) foi questão nunca totalmente resolvida. Sempre defendi que o artigo 189.º, n.º 2, do CPP continuou a ser o fundamento normativo para obtenção de dados de tráfego/localização para os crimes previstos no artigo 187.º, n.º 1, do CPP, que não se integravam na definição de “crimes graves” prevista na alínea g) do n.º 1 do artigo 2.º da Lei 32/2008^{[civ]/[cv]}. Mera derrogação, pois. Note-se que o TJUE sempre considerou que a definição de infracção grave, não tendo a União legislado sobre a matéria, é da competência dos Estados-Membros^[cvi]. O legislador português pode, pois, legislar no sentido de admitir a utilização probatória dos *metadados* não só para o catálogo inserido na alínea g) do n.º 1 do artigo 2.º da Lei 32/2008, como para o catálogo do n.º 1 do artigo 187.º do CPP, crimes para que permite até medidas mais gravosas, como a interceptação de conteúdo.

Sendo total ou parcial, certo é que, nos termos prescritos no n.º 1 do artigo 282.º da CRP, com a declaração de inconstitucionalidade com força obrigatória geral da norma do artigo 9.º da Lei 32/2008 pelo Ac. TC 268/2022, *a norma do n.º 2 do artigo 189.º foi ripristinada na sua plenitude*, por força do disposto no n.º 1 do artigo 282.º da CRP ^{[cvii]/[cviii]}.

Deste modo, *após o Ac. TC 268/2022, e antes da Lei 18/2024, o artigo 189.º, n.º 2, do CPP constituiu (o único) fundamento normativo para obtenção de dados de tráfego/localização.*

2.3.

Com a redacção dada pela Lei 18/2024 ao artigo 9.º, já analisado, a Lei 32/2008 voltou a restringir o campo de aplicação do n.º 2 do artigo 189.º: este é norma de acesso/utilização apenas aos dados conservados em bases que não as previstas na Lei 32/2008, designadamente as previstas na Lei 41/2004.

O legislador de 2024, não podendo desconhecer a polémica existente sobre a possibilidade de o artigo 189.º, n.º 2, ser norma de acesso, manteve este preceito inalterado. Não pode – afigura-se-me claro – atribuir-se ao legislador qualquer intenção de incumbir tal função apenas ao artigo 9.º da Lei 32/2008.

2.4.

Deste modo, o n.º 2 do artigo 189.º do CPP é norma de acesso e utilização probatória de *metadados* conservados ao abrigo da Lei 41/2004^[cix].

3. Artigo 14.º da LCC

3.1.

Após o surgimento da LCC em 2009, houve quem entendesse que este diploma tinha passado a ser o fundamento normativo convocável para a obtenção de dados de tráfego/localização celular. Nesse sentido, Duarte Rodrigues Nunes, para quem o artigo 9.º original da Lei 32/2008 foi tacitamente revogado pelos artigos 12.º e ss. da LCC^[cx], sendo o artigo 18.º o fundamento normativo para a sua obtenção^[cxii]. Cf. ainda Paulo Dá Mesquita^[cxiii] e vários acórdãos do TRE [p. ex., o de 20.01.2015, P. 648/14.6GCFAR-A.E1 (João Gomes de Sousa)]^[cxiiii], concordando com essa revogação (pelo menos parcial), mas para quem o fundamento passou a estar no artigo 14.º desta lei.

Não creio que seja essa a mais fundada interpretação a fazer.

A LCC não contém qualquer norma que seja fundamento para a conservação de metadados. Contém, o que não é pouco, um *verdadeiro regime geral de prova digital*, sendo as disposições processuais previstas nos seus artigos 12.º a 17.º aplicáveis, em abstracto, a processos relativos a qualquer tipo de crime. Efectivamente, por força do disposto no n.º 1 do artigo 11.º, aplicam-se elas a processos relativos a crimes (a) previstos nessa lei, (b) cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico. Ora, se quase todos (mas nem todos) os tipos de crimes podem ser cometidos por meio de um sistema informático, em todos pode ser necessário recolher prova em suporte electrónico. Estas disposições aplicam-se a todos os processos que necessitem de dados informáticos para a prova: estando essa prova, por definição, em formato digital^[cxv], pode ser obtida através das disposições processuais dos artigos 12.º a 17.º da LCC. Carecem, pois, de fundamento quaisquer posições que pretendam

delimitar os campos de aplicação recíprocos da Lei 32/2008 e da LCC com base nos tipos de crime a que se aplica esta última ou com base nos aparelhos usados nas comunicações (telefónicos, na Lei 32/2008; sistemas informáticos, na LCC^[cxvi]).

3.2.

O artigo 14.º da LCC prevê a possibilidade de emissão de ordem pela autoridade judiciária competente a quem tenha disponibilidade ou controlo de dados informáticos, específicos e determinados, armazenados num determinado sistema informático, incluindo os FS, que os comunique ao processo ou que permita o acesso aos mesmos. Porém, essa lei nada alterou quanto ao regime de acesso aos dados de tráfego e de localização^[cxvii], e não é por força do disposto no n.º 2 do artigo 11.º («As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho»). É o próprio artigo 14.º que expressamente determina essa inaplicabilidade. Vejamos.

Prescreve o n.º 1 do artigo 14.º da LCC que:

«Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência».

O n.º 4 adita que:

«O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo *qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo*, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar:

- a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;
- b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou
- c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.» (realces meus).

Este n.º 4 contém, pois, um *regime especial para a injunção (ordem) dirigida aos fornecedores de serviços*, que, como definido no artigo 2.º, alínea d), são «qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores».

Ora, resulta claro do corpo deste n.º 4 que os *dados relativos aos clientes ou assinantes não podem incluir dados relativos ao tráfego*^[cxvii] ou ao conteúdo. Pode induzir em erro o disposto nas alíneas b) (quando se refere aos «dados respeitantes à facturação») e c) deste artigo (quando se refere a «qualquer outra informação sobre a localização do equipamento de comunicação»), levando à conclusão de que dados de facturação são a facturação detalhada, incluída nos dados de tráfego, e que a informação sobre a localização do equipamento de comunicação respeita à localização dos equipamentos móveis em cada momento durante cada comunicação.

Essa é conclusão que se nos afigura infundada. Desde logo, porque isso contraria o exposto no corpo do n.º 4 («qualquer informação diferente dos dados relativos ao tráfego»), que essas alíneas apenas se destinam a concretizar. Depois, porque em cada uma delas, na parte final, está exposto que esses dados têm de estar «disponíveis com base num contrato ou acordo de serviços», e isso apenas sucede quando os dados de facturação *não respeitam às concretas comunicações* (que número ligou a que número, de que local em território nacional ou estrangeiro, durante quanto tempo, que volume de dados foram transmitidos, etc.^[cxviii]), mas sim a outro tipo de dados, como o tipo de contrato, o valor do serviço prestado (p. ex., o valor global do serviço contratado, incluindo o número de canais de televisão, o telefone “fixo”, o números de telefones “móveis”, o número de minutos/sms/volume de dados incluídos, etc.), os tipos de meios de pagamento contratados (pré ou pós-pagamento, por débito directo ou por referências bancárias, etc.) e o local onde o equipamento de comunicação foi instalado (o serviço de televisão, o telefone fixo, o *router* da internet, etc.). Finalmente, não poderemos esquecer a origem destas normas: a CCiber, em concreto o seu artigo 18.º. Nele se determina que:

«1 – Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para conferir poder às suas autoridades competentes para ordenarem:

a) [...]; e

b) A um prestador de serviços que preste os seus serviços no território da Parte que disponibilize os dados dos assinantes relacionados com esses serviços que estejam na sua posse ou sob o seu controlo.

2 — [...].

3 — Para efeitos do presente artigo, entende-se por «dados relativos aos assinantes» quaisquer informações que um prestador de serviços possua sobre os assinantes dos seus

serviços, sob a forma de dados informáticos ou sob qualquer outra forma, distintas dos dados de tráfego ou de conteúdo e que permitam determinar:

- a) O tipo de serviço de comunicação utilizado, as medidas técnicas adoptadas a esse respeito e a duração do serviço;
- b) A identidade, o endereço postal ou geográfico e o número de telefone do assinante e qualquer outro número de acesso, os dados referentes à facturação e ao pagamento, disponíveis com base num contrato ou num acordo de serviços;
- c) Qualquer outra informação sobre a localização do equipamento de comunicação disponível com base num contrato ou num acordo de prestação de serviços.»

Para bem compreendermos estas normas da CCiber, é sempre essencial a leitura do seu Relatório Explicativo. Ora, no § 178 precisa-se, com clareza, também pelos exemplos invocados, o que está em causa:

«No decorrer de uma investigação criminal, a informação relativa ao subscritor poderá revelar-se necessária, basicamente, em duas situações que passamos a descrever: a primeira, quando há que identificar quais os serviços, e as medidas técnicas a eles associadas, que foram utilizados ou estão a ser utilizados por um subscritor, tal como o *tipo de serviço telefónico utilizado* (por ex.: móvel), o *tipo de outros serviços conexos utilizados* (por ex.: reencaminhamento de chamadas, voice-mail, etc.). o *número de telefone ou outro endereço técnico* (por ex.: endereço de e-mail). A segunda, nos casos em que é conhecido um endereço técnico, a informação relativa ao subscritor é necessária como forma de ajudar a identificar a pessoa visada. Outras informações relativas ao subscritor, tal como *informação comercial sobre facturação e registos de pagamento do subscritor*, poderão igualmente ser de alguma utilidade no contexto de investigações criminais, nomeadamente quando o crime que está a ser alvo de investigação envolve uma situação de fraude informática ou outras infracções de natureza económica» (destaques meus).

E no § 180, com especial relevo para a compreensão do que seja a “localização” de que se fala, pode ainda ler-se:

«A informação relativa ao subscritor não se limita à informação directamente relacionada com a utilização do serviço de comunicação. Designa igualmente toda e qualquer informação, *exceptuando os dados de tráfego ou de conteúdo*, através da qual poderá ser determinada a identidade do utilizador, o *seu endereço postal ou geográfico*, o número de telefone ou outro número de acesso, bem como informação sobre facturação e pagamentos, a qual é disponibilizada com base no acordo ou contrato de prestação de serviços firmado entre o subscritor e o fornecedor de serviços. Refere-se ainda a toda e qualquer informação, *exceptuando os dados de tráfego ou de conteúdo*, relativamente ao *local onde se encontra instalado o equipamento de comunicação* e que é disponibilizada com base no acordo ou

contrato de serviços celebrado. Esta última informação poderá ser relevante, em termos práticos, *apenas nos casos em que não se trate de equipamento portátil [...]*» (destaques meus).

É ainda relevante referir que a PPL 289/X, que esteve na origem na LCC, incluía um artigo (o 13.º) que dispunha: «A transmissão de dados conservados ao abrigo da Lei n.º 32/2008, de 17 de Julho, pode ser ordenada nos termos, condições e circunstâncias previstos nesse diploma»^[cxix]. Esse artigo não veio a constar da LCC, sinal claro de que o legislador quis afastar desta lei a obtenção desses dados.

3.3.

Creio, pois, ser inquestionável que o *artigo 14.º não é fundamento normativo convocável para a obtenção de dados de tráfego e de dados de localização celular conservados*. Nem antes, nem depois do Ac. TC 268/2022.

São, pois, de afastar os argumentos nesse sentido utilizados nos citados Acs. TRC de 12.10.2022 (Paulo Guerra) e TRP de 07.12.2022 (Pedro Vaz Pato), com consequências ao nível da apreciação da reprimendação do artigo 189.º, n.º 2, do CPP, já analisado.

O *artigo 14.º da LCC é apenas fundamento para a obtenção dos dados de subscritor e de acesso elencados nas diferentes alíneas do n.º 4, incluindo o IP*, dados esses conservados com fundamento distinto da Lei 32/2008, designadamente a Lei 41/2004^[cxx] e a LCE.

Tais dados são admissíveis para a prova em relação a todos os crimes que se incluam na previsão do artigo 11.º, n.º 1, dessa lei, sem qualquer limitação de âmbito subjectivo, sendo no inquérito o MP a autoridade judiciária competente para ordenar a injunção aí prevista.

Fazendo clara distinção entre diferentes níveis de ingerência em direitos fundamentais, o TJUE admite o acesso a dados de identificação de pessoas para prova de crimes que não se enquadrem no conceito de “crime grave”. No Ac. (Grande Secção) de 02.10.2018 (C-207/16), o TJEU declarou:

«O artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que o *acesso das autoridades públicas aos dados com vista à identificação dos titulares dos cartões SIM ativados num telemóvel roubado, tais como o apelido, o nome próprio e, sendo caso disso, o endereço desses titulares, constitui uma ingerência nos direitos fundamentais destes últimos*,

consagrados nesses artigos da Carta, que não apresenta uma gravidade tal que esse acesso deva ser limitado, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, à luta contra a criminalidade grave.» (realce meu).

4. Artigo 18.º da LCC?

Como *supra* exposto, Duarte Rodrigues Nunes defendia, antes da Lei 18/2024, que o artigo 9.º da Lei 32/2008 fora tacitamente revogado pelos artigos 12.º e ss. da LCC, sendo o artigo 18.º desta lei o fundamento normativo para a obtenção de dados de tráfego [\[cxxi\]](#)/[\[cxxii\]](#).

Assentava tal posição no facto de o artigo 14.º não permitir a aplicação da injunção para apresentação ou concessão de acesso a esse tipo de dados (o que merece a minha concordância, como acabei de expor) [\[cxxiii\]](#) e pela definição de interceptação que (ainda) consta do artigo 2.º, alínea e), dessa lei: «o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros». Embora o Autor não o afirme expressamente, parece que entende que é ainda interceptação a captação (ou seja a apreensão) de dados armazenados num sistema informático. Não creio que fosse essa a melhor interpretação a fazer, por várias razões.

Em primeiro lugar, a fonte única desta definição é a Lei 109/91 (lei da criminalidade informática), revogada e substituída pela LCC, que no seu artigo 2.º, alínea f), definia “intercepção” da mesma exacta forma. A definição em causa interessava apenas ao artigo 8.º, que dispunha sobre o crime de interceptação ilegítima: «Quem, sem para tanto estar autorizado, e através de meios técnicos, interceptar comunicações que se processam no interior de um sistema ou rede informáticos, a eles destinadas ou deles provenientes, será punido com pena de prisão até três anos ou com pena de multa». Ou seja, não tinha a definição em causa qualquer relevo ou aplicação no âmbito do direito processual, até porque esta lei não continha qualquer regime de interceptação e gravação de dados informáticos em transmissão. Deste modo, no âmbito da actual LCC, *o seu relevo é igualmente apenas para o crime de interceptação ilegítima*, previsto no artigo 7.º, não para o regime processual previsto no artigo 18.º.

Quanto ao regime do artigo 18.º, foi intenção declarada do legislador da LCC adaptar o regime de intercepções de comunicações previsto no CPP [\[cxxiv\]](#); de modo algum criar um novo conceito de, através da interceptação, se aceder a dados armazenados.

Em segundo lugar, note-se que dos n.ºs 2 e 4 do artigo 18.º resulta claro que o que está em causa é a interceptação e gravação de dados que estão *em transmissão*, não se aplicando a dados armazenados. Interceptar é o acto de aceder e conhecer o conteúdo da comunicação; gravar é o de registar para posterior utilização probatória o conteúdo e *metadados* dessa comunicação que está a ser transmitida. O legislador da LCC seguiu os termos que o CPP desde sempre utilizou no n.º 1 do artigo 187.º: interceptar e gravar.

Em terceiro lugar, os procedimentos previstos no artigo 188.º, aplicáveis por força do disposto no n.º 4 do artigo 18.º da LCC, apenas se justificam por estar em causa interceptação de dados que estão em transmissão. De forma significativa, nesse número o legislador não determina a aplicação do disposto no n.º 2 do artigo 189.º do CPP, aquele (único) que, como *supra* exposto, se aplica à obtenção de dados de tráfego/localização armazenados.

Finalmente, em quarto lugar, se fosse como defendido por este Autor, todas as apreensões de dados informáticos constituiriam interceptações, ficando sem qualquer sentido os específicos regimes de apreensão definidos nos artigos 15.º, 16.º e 17.º da LCC.

Pelo exposto, o artigo 18.º da LCC não constitui nem nunca constituiu fundamento para a obtenção de dados de tráfego/localização conservados[\[cxxv\]](#).

5. Regulamento (UE) 2023/1543

5.1.

A 18.08.2026 iniciar-se-á a aplicação do Regulamento (UE) 2023/1543, que estabelece as regras segundo as quais uma autoridade de um Estado-Membro pode, num processo penal, emitir uma Ordem Europeia de Produção (*European Production Order*) ou uma Ordem Europeia de Conservação (*European Preservation Order*) e, assim, ordenar a um prestador de serviços que ofereça serviços na União e que esteja estabelecido noutro Estado-Membro ou, caso não esteja estabelecido, que esteja representado por um representante legal noutro Estado-Membro, que produza ou que conserve[\[cxxvi\]](#) provas electrónicas, independentemente da localização dos dados[\[cxxvii\]](#).

O regulamento não se aplica quando a ordem não atravessa fronteiras, ou seja, quando a autoridade emissora da ordem e o FS seu destinatário se encontram no mesmo Estado-Membro. Por isso, quando, em processo nacional, se pretender obter dados conservados por FS estabelecido ou representado em Portugal continuará aplicável a lei nacional.

No entanto, importa não esquecer que, tratando-se de regulamento da UE, é obrigatório em todos os seus elementos e directamente aplicável em todos os Estados-Membros, vinculando todas as entidades, públicas e privadas – artigo 288.º do TFUE. Por isso, e como veremos de seguida, sendo imperativo o regime que prevê para a obtenção e preservação transnacional destes meios de prova, o mesmo deverá igualmente aplicar-se internamente, sob pena de absoluta incoerência do sistema.

É o que passo a demonstrar, analisando os seus aspectos mais importantes[\[cxxviii\]](#), em confronto com a lei nacional: (i) âmbito material de aplicação das *European Production Orders* e das *European Preservation Orders*; (ii) condições de emissão de uma ordem de produção; (iii) condições de

emissão de uma ordem de preservação; (iv) a competência para emitir esses dois tipos de ordens; (v) prazos para cumprimento das ordens.

5.2.

Quanto ao *âmbito material de aplicação das ordens*, o n.º 2 do artigo 2.º do regulamento prescreve que

«[a]s ordens europeias de produção e as ordens europeias de conservação só podem ser emitidas no âmbito e para efeitos de processos penais, e para execução de uma pena ou medida de segurança privativas de liberdade com uma duração mínima de quatro meses, na sequência de processos penais, imposta por uma decisão que não tenha sido proferida na ausência da pessoa condenada, nos casos em que essa pessoa condenada tenha fugido à justiça. Tais ordens também podem ser emitidas no âmbito de processos relacionados com infracções penais pelas quais uma pessoa coletiva possa ser responsabilizada ou punida no Estado de emissão».

Permite, pois, a sua *utilização também para efeitos de assegurar a execução de uma pena ou medida de segurança privativas de liberdade com uma duração mínima de quatro meses, nos casos em que essa pessoa condenada tenha fugido à justiça*. Não se trata de utilização das ordens no processo que tenha como objecto a investigação/punição de crimes de evasão [\[cxxix\]](#), antes para localização e captura do fugitivo (no processo da condenação ou da execução da pena por cumprir). Nem a Lei 32/2008 nem a LCC o permitem. Deveria, pois, alterar-se a lei interna, sob pena de ficarmos com o absurdo regime de, se o fugitivo se encontrar em Portugal, não poderem ser utilizados estes dados para o localizar, mas tal já ser admissível se passar fronteira para qualquer Estado-Membro.

5.3.

Relacionado com o âmbito material de aplicação das ordens estão, nas condições de emissão de uma ordem de produção, os *tipos de crime* – n.ºs 3 e 4 do artigo 5.º.

A ordem de produção para obter *dados de assinantes* ou *dados solicitados com o único objectivo de identificar o utilizador* pode ser emitida *para todas as infracções penais* e para efeitos de execução de uma pena ou medida de segurança privativas de liberdade (nos termos *supra* indicados) – n.º 3 do artigo 5.º. No direito interno, a LCC também o permite, pelo menos em abstracto, para todos os tipos de crime (por força do n.º 2 do seu artigo 11.º), mas a Lei 32/2008 só o admite para “crimes graves”.

Quanto a ordens de produção para obter dados de tráfego (n.º 4 do artigo 5.º), podem ser emitidas: a) Para infracções penais puníveis no Estado de emissão com uma pena privativa de

liberdade de duração máxima não inferior a três anos; ou b) Para as infracções seguintes, se forem cometidas, total ou parcialmente, através de um sistema de informação: i) as infracções referidas nos artigos 3.º a 8.º da Directiva (UE) 2019/713, ii) as infracções referidas nos artigos 3.º a 7.º da Directiva 2011/93/UE, iii) as infracções referidas nos artigos 3.º a 8.º da Directiva 2013/40/UE; c) Para as infracções penais referidas nos artigos 3.º a 12.º e 14.º da Directiva (UE) 2017/541. Este catálogo de crimes é muito mais amplo que o de “crimes graves” previsto na Lei 32/2008.

Deveria, pois, uniformizar-se o regime interno em conformidade com o regulamento, sob pena de dados que se enquadram no n.º 1 ou no n.º 2 do artigo 6.º desta lei, se estiverem conservados por FS nacionais, não poderem ser utilizados em Portugal para prova de alguns tipos de crime, mas depois poderem ser entregues a autoridades estrangeiras para prova dos mesmos exactos tipos de ilícito; se estiverem conservados por FS noutros Estados-Membros, já poderão ser utilizados para prova em processos nacionais, por aplicação directa do regulamento. Absurdo, claro, em prejuízo da eficácia do nosso sistema processual penal e dos bens jurídicos que cada tipo de crime protege.

5.4.

Quanto às *condições de emissão de uma ordem de preservação*, o n.º 3 do artigo 6.º prescreve que pode ser emitida para todas as infracções penais, se pudesse ter sido emitida nas mesmas condições num processo nacional semelhante. O artigo 12.º da LCC admite, em abstracto, por força do n.º 2 do artigo 11.º da mesma lei, a preservação no âmbito de processo quanto a qualquer tipo de crime. Nenhuma diferença há então entre os dois regimes.

5.5.

Evidente diferença há no que respeita à competência para emitir as ordens de produção [\[cxxx\]](#).

O regulamento (nos n.ºs 1 e 2 do artigo 4.º), em conformidade com a jurisprudência do TJUE já citada, estabelece um regime distinto consoante os tipos de dados em causa:

i. Quanto a *dados de assinantes* ou *dados solicitados com o único objectivo de identificar o utilizador*, a ordem pode ser emitida por:

a. Um juiz, um tribunal, um juiz de instrução ou um magistrado do MP competente no processo em causa; ou

b. Qualquer outra autoridade competente, tal como definida pelo Estado de emissão, e que, no processo em causa, intervenha enquanto autoridade de investigação num processo penal com competência para ordenar a recolha de elementos de prova de acordo com a lei nacional; num tal caso, a ordem deve ser validada, após a análise da

sua conformidade com as condições de emissão de uma ordem europeia de produção ao abrigo do presente regulamento, por um juiz, um tribunal, um juiz de instrução ou um magistrado do MP do Estado de emissão.

ii. Quanto a *dados de tráfego*, a ordem pode ser emitida por:

- a. Um juiz, um tribunal ou um juiz de instrução que seja competente no processo em causa; ou
- b. Qualquer outra autoridade competente, tal como definida pelo Estado de emissão, e que, no processo em causa, intervenha enquanto autoridade de investigação num processo penal com competência para ordenar a recolha de elementos de prova de acordo com a lei nacional; num tal caso, a ordem deve ser validada, após a análise da sua conformidade com as condições de emissão de uma ordem europeia de produção ao abrigo do presente regulamento, por um juiz, um tribunal ou um juiz de instrução do Estado de emissão.

Em síntese, quanto ao primeiro grupo de dados (“não de tráfego”), a ordem de produção pode ser emitida por juiz, tribunal, juiz de instrução ou magistrado do MP que sejam competentes no processo em causa; quanto aos dados de tráfego, do elenco das entidades competentes são retirados os magistrados do MP [\[cxxxii\]](#).

Note-se que, neste ponto, *nada fica por definir pelos Estados-Membros. A atribuição de competência resulta de forma directa e completa do regulamento*. A menção a “competência no processo em causa” respeita ao concreto processo, a quem no concreto processo é competente (material, funcional e territorialmente competente), não devendo ser interpretada no sentido de “tipo de classe profissional que o direito interno defina como competente”. Daí que seja usada a mesma fórmula quando está e quando não está incluído o MP. Isto resulta claro do Considerando 36, onde se lê:

«Quando é emitida uma ordem europeia de produção ou uma ordem europeia de conservação, deverá estar sempre envolvida uma autoridade judicial no processo de emissão ou no processo de validação da mesma. Tendo em conta a natureza mais sensível dos dados de tráfego, com exceção dos dados solicitados com o único objetivo de identificar o utilizador tal como definido no presente regulamento, e dos dados de conteúdo, a emissão ou a validação de uma ordem europeia de produção para a obtenção dessas categorias de dados exigirá o seu reexame por um juiz. Uma vez que os dados de assinantes e os dados solicitados com o único objetivo de identificar o utilizador tal como definido no presente regulamento são menos sensíveis, uma ordem europeia de produção para a obtenção de tais dados também pode ser emitida ou validada por magistrados do Ministério Público competentes. Em conformidade com o direito a um processo equitativo, tal como protegido pela Carta e pela Convenção para a Proteção dos Direitos do Homem e das Liberdades

Fundamentais, os magistrados do Ministério Público devem exercer as suas responsabilidades de forma objetiva, tomando as suas decisões em relação à emissão ou validação de uma ordem europeia de produção ou de uma ordem europeia de conservação exclusivamente com base nos elementos factuais dos autos e tendo em conta todos os elementos de prova incriminatórios e exculpatórios».

É diferente quanto à possível competência de outras autoridades que, no processo em causa, intervenham enquanto autoridade de investigação num processo penal com competência para ordenar a recolha de elementos de prova de acordo com a lei nacional [as alíneas b) dos n.ºs 1 e 2 em análise]. Aí, sim, é deixado à definição do Estado de emissão: «Qualquer outra autoridade competente, *tal como definida pelo Estado de emissão* [...]». Em Portugal, poderiam, em abstracto, ser as autoridades de polícia criminal.

O que, neste ponto consta da PPL 83/XVII (artigo 26.º-B da LCC proposto) é *contrário* ao regulamento no que respeita às autoridades judiciais e *incoerente* com o direito interno no que respeita às autoridades de investigação e o regime de preservação. No n.º 1 proposto prescreve-se que «[é] competente para emitir, validar e transmitir uma ordem europeia de produção ou uma ordem europeia de conservação de prova eletrónica a autoridade judicial nacional com competência para a direção do processo na fase em que este se encontra»; acrescenta o n.º 2 que «[o] disposto no n.º 1 não prejudica as competências do juiz de instrução para autorizar ou ordenar a prática de atos na fase de inquérito, nos termos da lei». Ou seja, por um lado afasta totalmente a possibilidade de as autoridades de investigação (não judiciais) emitirem ordens de produção ou de preservação, e, por outro, mantém a reserva de juiz de instrução para autorizar ou ordenar a prática de actos na fase de inquérito, que diz já prevista na lei.

Ora, quanto a este último aspecto, se não há dúvidas quanto aos *dados de tráfego*, em que há sempre reserva de juiz, quer por força do artigo 9.º da Lei 32/2008, quer do artigo 189.º, n.º 2, do CPP (e nisso conformidade com o definido no regulamento), elas surgem quanto aos dados de *dados de assinantes* e aos *dados solicitados com o único objectivo de identificar o utilizador*, pois, no âmbito da Lei 32/2008, também há reserva de juiz, mas o mesmo não sucede no âmbito do artigo 14.º, n.º 4, da LCC (face a dados conservados ao abrigo da Lei 41/2004 ou da LCE), em que o MP é competente.

Deste modo, para além de chocar frontalmente com o regulamento, retirando ao MP competência que este lhe atribui – choque de que sempre sairá a perder, face ao valor supra-legal do regulamento UE –, não oferece critério que possa operar, pois essa diferente competência consoante o diferente regime de conservação de dados não se aplica para dados conservados noutros Estados-Membros.

A PPL é ainda incoerente no que respeita às autoridades de investigação, pois o n.º 2 do artigo 12.º da LCC permite que a preservação seja também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judicial competente ou quando haja urgência ou perigo na

demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do CPP.

Pelo exposto, também neste aspecto deveria o artigo 9.º da Lei 32/2008 ser alterado, atribuindo competência ao MP para ordenar a transmissão dos tipos de dados aí previstos, sob pena de existir uma diferença injustificada e absurda, em que, se o processo for nacional, os FS só transmitirão os dados se a ordem for de juiz, mas se for de outro Estado-Membro o fazerem por ordem do MP ou até de autoridades de investigação (sujeitas a validação do MP ou de juiz).

De igual modo, também a classificação de dados feita nos n.ºs 1 e 2 do artigo 6.º da Lei 32/2008, sendo distinta daquela utilizada pelo regulamento para divisão de competências entre as autoridades de emissão das ordens, terá de ser substituída por esta.

5.6.

O artigo 26.º-C da LCC proposto na PPL 83/XVII, estabelece, no seu n.º 1, que

«[é] competente para e assegurar a execução de uma ordem europeia de produção ou de conservação de prova eletrónica a autoridade nacional com competência para executar a mesma medida de investigação em território nacional, de acordo com o disposto na lei processual penal, nas leis de organização do sistema judiciário e no Estatuto do Ministério Público».

Por princípio, não é competência dessas autoridades “assegurar a execução” de qualquer dos tipos de ordens. As Ordens Europeias de Produção e as Ordens Europeias de Preservação devem ser dirigidas directamente ao estabelecimento designado ou ao representante legal designado pelo prestador de serviços em causa – artigo 7.º, n.º 1, do regulamento. Porém, quando se trate de uma Ordem Europeia de Produção para obter dados de tráfego, com excepção dos dados solicitados exclusivamente para identificar o utilizador (como definidos no artigo 3.º, n.º 10), ou para obter dados de conteúdo^[cxxxii], a autoridade emissora, ao mesmo tempo que transmite o COEP ao FS destinatário, tem de notificar a autoridade de execução^[cxxxiii], transmitindo também o COEP a essa autoridade – artigo 8.º, n.º 1. Para quê? Não para que esta “autoridade de execução” assegure a execução, antes para que, no prazo peremptório de 10 dias, possa recusar a sua execução, nos termos e com os fundamentos definidos no artigo 12.º. Se o não fizer nesse prazo, ou se, antes de o mesmo terminar, confirmar à autoridade emissora e ao destinatário que não vai invocar qualquer motivo de recusa, deve o FS transmitir os dados directamente à autoridade emissora – artigo 10.º, n.º 2.

As autoridades de execução só assumem a execução da COEP ou da COEC se o FS destinatário das mesmas não der cumprimento ao COEP no prazo previsto ou não der cumprimento a um COEC

sem indicar motivos aceites pela autoridade emissora e, se aplicável, sempre que a autoridade de execução não invocar nenhum dos motivos de recusa previstos no artigo 12.º – artigo 16.º, n.º 1.

O critério proposto na PPL («a autoridade nacional com competência para executar a mesma medida de investigação em território nacional») afigura-se altamente problemático quanto às ordens de produção que respeitem a dados de assinantes e a dados solicitados com o único objectivo de identificar o utilizador, pois, como vimos já, temos diferentes entidades competentes consoante o regime de conservação dos dados: se for o da Lei 32/2008, é o juiz (artigo 9.º, n.º 1, dessa lei); se for o da Lei 41/2004, é no inquérito o MP (artigo 14.º, n.º 4, da LCC). A autoridade emissora não saberá, pois, a quem remeter a COEP. Melhor seria que, utilizando os critérios que constam do artigo 4.º do regulamento, a lei estabelecesse de forma clara que, quanto aos COEP, a autoridade de execução seria, tratando-se de dados de tráfego e de localização, o juiz de instrução, e, tratando-se de dados de assinantes e de dados solicitados com o único objectivo de identificar o utilizador, o MP; tratando-se de COEC, sempre o MP, pois o artigo 12.º da LCC atribui-lhe tal competência no inquérito.

5.7.

O regulamento não faz qualquer restrição com base na fase do processo (daí que admita a emissão da ordem por juiz, tribunal, juiz de instrução ou, quando não se trate de dados de tráfego, magistrado do MP): as ordens de produção ou de preservação são admissíveis em qualquer fase do processo, incluindo na execução da pena, para localizar o condenado fugitivo. Este aspecto reforça a posição que assumi em IV.1.7.

5.8.

O regulamento fixa prazos máximos para cumprimento pelos FS das ordens de produção e de preservação recebidas, sob pena de serem sancionados pecuniariamente – artigos 10.º, 11.º e 15.º.

Quanto às ordens de produção, por regra (a que pode haver algumas condicionantes no caso de dados de tráfego), o destinatário deve transmitir os dados solicitados o mais tardar no prazo de 10 dias após a recepção do COEP – artigo 10.º, n.º 2. Em casos de ameaça iminente à vida, integridade física ou segurança de uma pessoa, ou a infra-estruturas críticas, os dados devem ser transmitidos o mais tardar no prazo de 8 horas – artigo 10.º, n.º 4.

Quanto às ordens de preservação, deve o destinatário, sem demora indevida, preservar os dados solicitados – artigo 11.º, n.º 1.

Deveria a lei portuguesa prever iguais prazos, pois não há motivo para que os FS nacionais fiquem obrigados ao seu cumprimento quando a ordem provém de autoridade de outro Estado-Membro, mas não quando tem origem em juiz ou procurador nacional. A PPL 83/XVII propõe a

criação de um regime sancionatório de natureza contra-ordenacional para o incumprimento desses prazos, mas é omissa quanto à generalização dos prazos às ordens internas.

5.9.

Por tudo o que fica exposto, a lei nacional deveria ser alterada em conformidade com o regime definido pelo Regulamento (UE) 2023/1543. A PPL 83/XVII – erradamente, afigura-se-me – não segue tal caminho. Em alguns casos, deverá aplicar-se directamente o regulamento; no mais, ou faremos uma interpretação actualista da lei em conformidade com o regulamento ou teremos de viver no absurdo.

V. Síntese conclusiva

O percurso legislativo dos *metadados* de comunicações electrónicas em Portugal revela uma articulação complexa entre regimes, exigindo que o intérprete conjugue normas de conservação e de acesso que nem sempre comunicam de forma fluída e coerente. A Lei 18/2024 não só não resolveu muitos dos problemas que existiam, como lhes acrescentou outros.

Temos hoje vários regimes jurídicos de conservação de *metadados* que podem ser utilizados como prova em processo penal (a Lei 32/2008, a Lei 41/2044 e a LCE), bem como vários regimes jurídicos de acesso e utilização probatória (o artigo 9.º da Lei 32/2008, o artigo 189.º, n.º 2, do CPP e o artigo 14.º, n.º 4, da LCC). Apesar de várias incoerências quando se confrontam tais regimes, é possível fazer – como fica feita – interpretação dos mesmos em conformidade com a jurisprudência do TJUE e do TC.

Assim, nesta data – ignorando por ora completamente o Regulamento (UE) 2023/1543 –, a aplicação conjugada desses diferentes regimes de conservação e de utilização probatória é sintetizada no quadro que se segue:

TIPOS DE DADOS	CONSERVAÇÃO		ACESSO / UTILIZAÇÃO			
	Fundamento	Prazo	Âmbito Objectivo	Âmbito Subjectivo	Competência Acesso	Fundamento Acesso
IDENTIFICAÇÃO CLIENTE	Art. 6/2 L41/2004 - LCE	Sem prazo pré- definido	Todos os crimes (Art. 11/1 LCC)	Qualquer pessoa	MP (inquérito) Juiz (após inquérito)	Art. 14/4/b LCC
	Art. 6/1 L32/2008	1 ano	Crimes graves	Catálogo Art. 9/3 L32/2008	Juiz	Art. 9/2 L32/2008
DADOS IDENTIFICAÇÃO UTILIZADOR (IP/N.º de contacto contratado, MAC, portos)	Art. 6/2 L41/2004 + Art. 10 L23/96	6 meses	Todos os crimes (Art. 11/1 LCC)	Qualquer pessoa	MP (inquérito) Juiz (após inquérito)	Art. 14/4/b LCC
	Art. 6/1 L32/2008	1 ano	Crimes graves	Catálogo Art. 9/3 L32/2008	Juiz	Art. 9/1 L32/2008
Tráfego (só dados essenciais à facturação)	Art. 6/2 L41/2004 + Art. 10 L23/96	6 meses	Catálogo Art. 187/1 CPP	Catálogo Art. 187/4 CPP	Juiz	Art. 189/2 CPP
Localização (só dados conexos a tráfego essenciais à facturação)	Art. 6/2 L41/2004 + Art. 10 L23/96	6 meses	Catálogo Art. 187/1 CPP	Catálogo Art. 187/4 CPP	Juiz	Art. 189/2 CPP
Tráfego e Localização STJ	Art. 6/2 L32/2008	O fixado pelo STJ	Crimes graves	Catálogo Art. 9/3 L32/2008	Juiz	Art. 9/2 L32/2008

A adaptação do direito interno ao Regulamento (UE) 2023/1543 seria óptima oportunidade para resolver boa parte dos problemas normativos existentes. Face ao que consta da PPL 83/XVII, nesta data pendente na AR, é provável que a oportunidade seja desperdiçada. Mais grave: acrescentar-se-ão novos graves problemas aos muitos que ainda subsistem – Portugal arrisca-se a viver o absurdo de tratar de forma desigual ordens de produção de dados nacionais e estrangeiras, prejudicando a eficácia da justiça penal.

Ainda não será desta que o regime se endireita.

(*) O Sumário Executivo foi redigido com recurso ao www.chatgpt.com.

(**) O Resumo foi redigido com recurso ao www.chatgpt.com.

[i] Sobre a sua definição, cf., *infra*, II.1.1.

[ii] Incomensuravelmente menos do que aqueles hoje existentes, com a total “electronização” das comunicações.

[iii] Cf. o DL 355/87, que definia o regime de fixação das tarifas e dos preços dos serviços prestados pelos operadores das comunicações de uso público.

[iv] Cf. VERDELHO, Pedro. Técnica no novo C.P.P.: Exames, perícias e prova digital, *Revista do Centro de Estudos Judiciários*. 2008, n.º 9, p. 166.

[v] Sobre esses problemas, cf. PINHO, Carlos. Os problemas interpretativos resultantes da Lei n.º 32/2008 2008, de 17 de Julho (Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações). *Revista do Ministério Público*. 2012, n.º 129, pp. 63-93. Alguns deles serão abordados *infra*.

[vi] Acessível, como todos os demais acórdãos desse tribunal citados, em <http://www.tribunalconstitucional.pt/tc/acordaos/>.

[vii] Acessível, como os demais acórdãos deste tribunal citados, em <https://curia.europa.eu/juris/>.

[viii] O TC não chegou a apreciar se o prazo de um ano era ou não excessivo.

[ix] Na data em que o presente texto é encerrado (15.06.2026), está pendente na AR a Proposta de Lei (PPL) n.º 83/XVIII/3.^a, que «transpõe a Diretiva (UE) 2023/1544, e estabelece o regime sancionatório aplicável às infrações das normas constantes da referida Diretiva e do Regulamento

(UE) 2023/1543, relativo às ordens europeias de produção e de conservação para efeitos de prova eletrónica e de execução de penas privativas de liberdade na sequência de processos penais».

[x] Sendo regulamento da UE, é obrigatório em todos os seus elementos e directamente aplicável em todos os Estados-Membros, vinculando todas as entidades, públicas e privadas— artigo 288.º do TFUE.

[xi] Por exemplo, para aceder à internet e utilizar uma qualquer rede social (v. g., o *Facebook*), uma pessoa pode necessitar de contratar um serviço de telecomunicações (com a *MEO*, a *NOS*, a *Vodafone*, etc.), gerando dados de identificação do subscritor (dados de base); quando estabelece um concreto acesso, gerará dados de acesso (v. g., o IP que lhe foi atribuído), que se devem incluir nos dados de base; durante esse acesso, haverá transmissão de dados informáticos (dados de conteúdo, durante a comunicação). Ora, o volume de dados transmitido é um dado de tráfego, que o FS necessitará conhecer para efeitos de facturação. Já os dados respeitantes à interacção com o *Facebook* (v. g., o que aí publicou, comentou, etc.) não são dados que o FS conheça ou possa conservar: apenas o *Facebook* – um OSP global – os possui. Os *metadados* de que agora tratamos – objecto, para além do mais, da Lei 32/2008 e do Ac. TC 268/2022 que sobre ela recaiu – não respeitam aos dados na posse dos OSP: não é esse o regime jurídico da sua conservação [em que não há qualquer obrigatoriedade de conservação, antes apenas limites a tal, resultantes do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho – Regulamento Geral de Protecção de Dados (RGPD)].

[xii] Acessíveis em <https://www.ministeriopublico.pt/pareceres-pgr>.

[xiii] Elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respectivo serviço: identificação do utilizador, morada, número de acesso e dados através dos quais o utilizador tem acesso ao serviço [estes elementos são fornecidos ao explorador do serviço para efeitos do estabelecimento do acordo (do contrato) de ligação à respectiva rede ou atribuídos por este àquele (o número de acesso)]. São dados que existem independentemente de qualquer comunicação.

[xiv] Direcção, destino, trajecto e duração da comunicação, bem como a localização dos aparelhos em comunicação.

[xv] Conteúdo da comunicação: som, imagem, texto, etc.

[xvi] O Regulamento (UE) 2023/1543, porém, também se aplica aos dados de conteúdo

[xvii] Cf., p. ex., o Ac. TC 241/2002, em que se discutia a sua admissibilidade em processo laboral.

[xviii] P. ex., saber qual a identidade (nome, morada, etc.) do utilizador de um número de telefone que telefonou para um indivíduo ameaçando matá-lo é ter acesso a dados de base. Porém, para que

possam fornecer tais informações, os FS têm de guardar dados sobre as telecomunicações que são dados de tráfego. Estes dados de tráfego, porém, não são fornecidos ao processo.

[xix] O mesmo sucedeu com o TC, nos Acs. 268/2022 e 800/2023.

[xx] Sobre a diferença, cf. *infra* II.3.

[xxi] A PPL 83/XVIII enferma do mesmo “pecado”.

[xxii] Na tradução oficial portuguesa: «O presente regulamento apenas deverá regulamentar a recolha de dados conservados por um prestador de serviços no momento da receção de uma ordem europeia de produção ou de uma ordem europeia de conservação. O presente regulamento não poderá estabelecer uma obrigação geral de retenção de dados para os prestadores de serviços e não poderá resultar numa retenção generalizada e indiscriminada de dados. O presente regulamento também não poderá autorizar a interceção de dados ou a obtenção de dados conservados após a receção de uma ordem europeia de produção ou de uma ordem europeia de conservação.»

[xxiii] Como é distinta a divisão de competência entre juiz e MP para ordenar a sua produção – cf., *infra*, IV.5.

[xxiv] Em sentido oposto a esta afirmação (que, não obstante, mantenho), a PPL 83/XVIII – que foi conhecida a 01.06.2026 e que baixou à comissão sem votação a 11.06.2026 – não segue esta classificação. Limita-se, no artigo 3.º, alínea i), a definir as “provas electrónicas como dados de assinantes, dados de tráfego ou dados de conteúdo, conservados em formato electrónico», não definindo em que consistem estas três categorias. Mais grave: omite por completo os “dados solicitados com o único objetivo de identificar o utilizador”. Como o Governo não pode deixar de saber qual o valor normativo de um regulamento UE, e como os formulários de Certificados de Ordem Europeia de Produção (COEC) e de Ordem Europeia de Conservação (COEC) são os anexos ao regulamento e não são alteráveis, tratar-se-á apenas de péssima técnica legislativa, que, se vier a ganhar forma de lei, causará enormes (e desnecessárias) dificuldades aos aplicadores e até aos FS, como é fácil de antever.

[xxv] Sobre a distinção, cf. p. ex. SILVA, Germano Marques da. *Curso de Processo Penal*, vol. II. Lisboa: Editorial Verbo, 1993, ISBN 972-22-1592-2, pp. 163-164. Como refere este Autor, em alguns casos, o próprio meio de obtenção de prova acaba por ser um meio de prova, como sucede com as revistas e buscas se nelas não forem recolhidos elementos indiciadores da responsabilidade dos suspeitos/arguidos. Por outro lado, acrescento, os autos que devem ser elaborados dessas diligências de prova realizadas no decurso do inquérito (artigos 109.º a 101.º e 275.º, n.º 1, do CPP) constituem prova documental dos termos em que se desenrolaram.

[xxvi] Algo a que todos têm direito gratuitamente – artigo 122.º, n.ºs 2 e 3, da Lei das Comunicações Electrónicas.

[xxvii] Como sucedeu em vários dos processos em que, logo após o Ac. TC 268/2022, foram interpostos recursos de revisão buscando nele seu fundamento [p. ex., Acs. de 06.09.2022, P. 618/16.0SMPRT-B.S1 (Ernesto Vaz Pereira), 06.09.2022, P. 4243/17.0T9PRT-K.S1 (Teresa Almeida), 08.11.2022, P. 107/13.4P6PRT-D.S1 (Conceição Gomes), 10.11.2022, P. 35/15.9PESTB-Z.S2 (Maria do Carmo Silva Dias), 10.11.2022, P. 120/17.2TELSB-B.S1 (Cid Geraldo) e de 30.11.2022, P. 71/11.4JABRG-G.S1 (Paulo Ferreira da Cunha)]. Equivocaram-se os requerentes, pois a obtenção de dados de tráfego/localização através das intercepções telefónicas não foi objecto de apreciação pelo TC e nenhuma desconformidade constitucional lhe pode ser apontada.

[xxviii] Duarte Rodrigues Nunes refere-se-lhes como «medida de prevenção criminal que se integra na chamada investigação proactiva, (que é essencial para responder às novas formas de criminalidade, em que uma investigação meramente reativa, i. e., apenas a partir da obtenção da notícia do crime, é manifestamente ineficaz), sendo que a investigação proativa inicia-se num momento prévio à prática do crime ou ao conhecimento da sua prática pelas autoridades e visa, entre outras finalidades, obter uma *notitia criminis*, obter informações que facilitem a investigação de crimes que venham a ser cometidos (como sucede no caso da conservação de *metadados* ou da imposição de deveres de colaboração/reporte ao abrigo da Lei n.º 83/2017, de 18 de agosto) ou relativas ao modo de funcionamento de certas formas de criminalidade (as chamadas informações de *intelligence*) ou evitar o cometimento de crimes já planeados ou minimizar os seus efeitos para as vítimas» – cf. NUNES, Duarte Rodrigues. Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de *metadados* conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?. *Revista do Ministério Público*, 2022, n.º 170, p. 37. Assim sucede noutros aspectos da vida social, como a aquisição de armas de fogo e suas munições, que, mesmo para quem tem para tal licença legal, de tudo deve ficar registo (cf. artigos 31.º, 35.º, n.º 3, 51.º e 75.º da Lei 5/2006), ou no âmbito do mercado dos valores mobiliários (cf. os inúmeros tipos de registo previstos no Código do Mercado dos Valores Mobiliários).

[xxix] Assim, Ac. STJ 03.11.2022, P. 19/20.5JBLSB.L1.S1 (António Gama): «O que declarou o acórdão do Tribunal Constitucional n.º 268/2022 [...] foi a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º, da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º, da mesma lei, por violação do disposto nos números 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição. Não declarou «nula a prova recolhida (...) com o recurso aos *metadados* fornecidos pelas operadoras» nem a «nulidade da análise aos *metadados*» nem disse que toda e qualquer recolha e conservação dados e independentemente do período de conservação constitui prova proibida».

[xxx] Na sua versão em língua inglesa, a Directiva 2002/58/CE usa o termo “retention”; na versão em francês, o termo “conservation”.

[xxxi] A inclusão dos dados de tráfego está expressa na letra do n.º 1 desse artigo.

[xxxii] Aspecto incompreendido e por isso erradamente invocado no requerimento da Provedora de Justiça que esteve na origem do Ac. TC 268/2022. No seu artigo 66.º, afirma-se que «já existem na ordem jurídica medidas menos restritivas do que aquelas de que vimos falando – a conservação generalizada e indiferenciada durante todo um ano de todos os «*metadados*» respeitantes a todos os cidadãos – e que se mostram também elas adequadas à prossecução da finalidade que o n.º 1 do artigo 3.º da Lei n.º 32/2008 enuncia. É o que se verifica com o regime de preservação de dados (*quickfreeze*), tal como previsto e regulado pelo artigo 12.º da Lei n.º 109/2009 [...]». O *quick-freeze* de modo algum é uma alternativa à conservação de *metadados*, antes a pressupõe. Se não houve primeiro *conservação*, não é depois possível a *preservação*.

[xxxiii] Nos Acs. de 05.04.2022 (C-140/20 - Caso *Commissioner of An Garda Síochána*), de 22.09.2022 (C-793/19 e C-794/19 – Caso *SpaceNet e Telekom Deutschland*) e de 07.09.2023 (C-162/22 – Caso *Lietivus Respublikos generalinė prokuratūra*), o TJUE afirma que o artigo 15.º, n.º 1, da Directiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da CDFUE, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, para além do mais, a uma imposição aos prestadores de serviços de comunicações electrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efectiva, do dever de procederem, por um determinado período, à conservação rápida (*quick freeze*) dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem.

No primeiro dos acórdãos indicados, pode ler-se no ponto 88 que «[o] Tribunal de Justiça precisou que uma medida de conservação desta natureza não deve ser limitada aos dados das pessoas identificadas previamente como apresentando uma ameaça para a segurança pública ou para a segurança nacional do Estado-Membro em causa ou das pessoas concretamente suspeitas de terem praticado um ato de criminalidade grave ou uma ofensa à segurança nacional. Com efeito, segundo o Tribunal de Justiça, embora deva respeitar o quadro instituído pelo artigo 15.º, n.º 1, da Directiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, e tendo em conta as considerações que figuram no n.º 55 do presente acórdão, tal medida pode, se for essa a escolha do legislador e respeitando os limites do estritamente necessário, ser alargada aos dados de tráfego e aos dados de localização relativos a pessoas diferentes das que são suspeitas de ter planeado ou cometido uma infração grave ou uma ofensa à segurança nacional, desde que tais dados possam, com base em elementos objetivos e não discriminatórios, contribuir para o esclarecimento dessa infração ou dessa ofensa à segurança nacional, tais como os dados da vítima desta e do seu meio social ou profissional (Acórdão de 6 de outubro de 2020, *La Quadrature du Net e o.*, C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 165)».

[xxxiv] Artigo 18.º que, sendo posterior, de forma tácita derogou parcialmente o n.º 1 do artigo 189.º do CPP, que, após a revisão introduzida pela Lei 48/2007, determina que «[o] disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas

de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceptação das comunicações entre presentes». Ora, a interceptação e gravação das conversações ou comunicações transmitidas por “correio electrónico ou outras formas de transmissão de dados por via telemática” está agora integralmente prevista no artigo 18.º da LCC (veja-se o n.º 2 deste artigo, que refere expressamente a «intercepção e o registo de transmissões de dados informáticos»). Neste sentido, MESQUITA, Paulo Dá, Prolegómeno sobre prova electrónica e interceptação de comunicações no direito processual penal português – o Código e a Lei do Cibercrime. In MESQUITA, Paulo Dá. Processo Penal, Prova e Sistema Judiciário. Coimbra: Coimbra Editora, 2010, p. 102 e ss.

O artigo 189.º, n.º 1, continua a ser aplicável à interceptação e gravação das conversações ou comunicações transmitidas por meio técnico que não seja o telefone (a que se aplica directamente o disposto nos artigos 187.º e 188.º do CPP) ou o “correio electrónico ou outras formas de transmissão de dados por via telemática” (a que se aplica o disposto no artigo 18.º da LCC): são elas as comunicações por ondas de rádio de muito baixa frequência (que não estejam alocadas a serviços de comunicações móveis), como p. ex., as feitas através de *walkie-talkies*, Serviço Rádio Pessoal – Banda do Cidadão, radioamadores, *morse*, etc. Nestes casos, porém, como não há uma entidade que seja a fornecedora do serviço, não há quem possa proceder à conservação dos dados de tráfego e ou de localização; não há, pois, registos desses dados.

[xxxv] Incorrectas, pois, as afirmações feitas nesse sentido nos Acs. TRC de 12.10.2022 (Maria Alexandre Guiné) e TRC de 12.10.2022 (Paulo Guerra).

[xxxvi] Recorde-se que os documentos fiscalmente relevantes (designadamente facturas e facturas-recibo) e outros registos devem ser guardados pelas empresas durante um período mínimo de 10 anos (prazo que se inicia no final do ano civil a que os documentos dizem respeito) – cf. n.º 1 do artigo 52.º do Código do IVA, n.º 1 do artigo 125.º do Código do IRC e n.º 1 do artigo 19.º do DL 28/2019.

[xxxvii] Alertando para tal facto, cf. *Nota Prática do Gabinete do Cibercrime da Procuradoria-Geral da República* n.º 26/2024, pp. 10-12. [Em linha]. Disponível em https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/2024.05.10_nota_pratica_26_pedidos_de_dados_a_operadores_2.pdf. [Visualizado, como todos os recursos *online* citados, em: 14.06.2026].

[xxxviii] Cf., *infra*, IV.3.

[xxxix] Como IP significa *Internet Protocol*, “protocolo *Internet Protocol*” é pleonástico; melhor seria dizer apenas “endereço de IP”.

[xl] Cf. http://www.tcpipguide.com/free/t_IPNetworkAddressTranslationNATProtocol.htm.

[xli] Aí se inclui o endereço *MAC (Media Access Control)*: um identificador único de 6 pares de caracteres alfanuméricos (0-F) separados por dois pontos ou travessões, em que os primeiros 6 caracteres identificam o fabricante, enquanto os 6 últimos são exclusivos do aparelho; é atribuído fisicamente à placa de rede do dispositivo (como *Wi-Fi* ou *Ethernet*) pelo fabricante, permitindo a identificação do aparelho numa rede local, de modo a que os equipamentos de rede (*switchs/routers*) lhe entreguem todos os dados que lhe são destinados. Assim, p. ex., o conhecimento do IP poderá permitir identificar o titular de um contrato de serviço de Internet instalado numa habitação, mas, para saber qual computador, utilizando a rede *Wi-Fi* dessa habitação, fez o acesso em causa, será necessário conhecer o *MAC adress*. Os FS não conhecem quem é o titular do MAC, pelo que para tal é necessário ter acesso físico às máquinas suspeitas. Através de um dos muitos serviços “Mac adress lookup” disponíveis *online* (p. ex., <https://maclookup.app/> e <https://macvendors.com/>) é possível, com os primeiros 6 caracteres do endereço, saber apenas quem é o fabricante do componente e algumas poucas características técnicas que, no entanto, não permitem identificar o utilizador.

[xlii] Cf., *infra*, III.1.3.5., as excepções a esta regra por força de férias e impedimentos.

[xliii] Sobre a distinção entre conservação, preservação e intercepção, cf., *supra*, II.3.

[xliv] Neste sentido, MILHEIRO, Tiago Caiado. A competência da Formação do Supremo Tribunal de Justiça nos termos da Lei n.º 32/2008, de 17 de julho (“Lei dos Metadados”) e as normas processuais de acesso a dados conservados de tráfego e de localização. *Julgar Digital*. 2025. [Em linha]. Disponível em: <https://julgar.pt/a-competencia-da-formacao-do-supremo-tribunal-de-justica-nos-termos-da-lei-n-o-322008-de-17-de-julho-lei-dos-metadados-e-as-normas-processuais-de-acesso-a-dados-conservados-de/>, pp. 6-7.

[xlv] Cf. o *supra* exposto em II.3.2.

[xlvi] Que cita e acompanha o TJUE – cf. §§ 9, 13 e 38 do Ac. 800/2023.

[xlvii] Também nos §§ 164 a 167 do Acórdão de 06.10.2020, *La Quadrature du Net* e o. (C-511/18, C-512/18 e C-520/18), e no Acórdão de 22.09.2022, *SpaceNet* e *Telekom Deutschland* (C-793/19 e C-794/19).

[xlviii] Note-se a menção a “dados de que esses prestadores de serviços dispõem”, ou seja, a dados já conservados, dados de comunicações pretéritas.

[xlix] Assim também MILHEIRO, Tiago Caiado, A competência..., cit., p. 8, e Artigo 189.º. In: António Gama et al. Comentário Judiciário do Código de Processo Penal. Coimbra: Almedina. 2026, p. 918.

[l] Cf., *infra*, III.2. A conservação terá sempre de ser apenas para futuro; se os dados já se encontram conservados/retidos, podem apenas ser preservados. Não há conservação após ou sobre conservação; antes apenas preservação após conservação. Muito menos pode haver conservação

sobre dados que, estando já conservados, foram preservados para não serem destruídos no final do período máximo de conservação (ou seja, cronologicamente: conservação >> preservação >> conservação). Sobre a conservação decidida pelo STJ ser necessariamente apenas para futuro, cf. Ac. TRL de 23.01.2026, P. 760/25.6GEALM-B.L1-5.

[li] Cf. *supra*, III.3.2.

[lii] Cf., p. ex., Acs. TC 407/97 e 379/2004.

[liii] Cf. artigo 8.º, n.º 1, alínea a), do Estatuto do Ministério Público (EMP).

[liv] Cf. artigo 20.º, n.º 2, do EMP.

[lv] Cf. artigo 19.º, n.º 2, alínea b), do EMP.

[lvi] Naturalmente que, se, por hipótese académica, o requerimento não for apreciado antes de decorrido o período de conservação pretendido pelo MP, o mesmo pode tornar-se supervenientemente inútil.

[lvii] Diploma que, face à natureza da matéria em causa, creio aplicável subsidiariamente – artigo 3.º do CPP.

[lviii] Pense-se no exemplo de grande evento político, religioso ou desportivo com data de início determinada: nada impede o MP de, pretendendo o início da conservação apenas uma semana antes do seu início, apresentar o requerimento duas ou três semanas antes dessa data.

[lix] P. ex., com risco acrescido (aeroportos, *etc.*) ou por apresentarem já criminalidade grave acima da média. Sendo para área territorial delimitada, serão destinatários da obrigação de conservação todos os FS que nela operarem.

[lx] O TJUE acentua sempre a necessidade de a conservação ser fundada em elementos objectivos e não discriminatórios. Porém, na prática, uma decisão que permitisse a conservação dos dados de tráfego/localização apenas a determinados grupos de pessoas estaria em grave risco de ofender a Constituição nos seus princípios da igualdade (artigo 13.º, n.º 1) e presunção de inocência (artigo 32.º, n.º 2), bem a proibição de discriminação nos tratamentos dos dados pessoais (artigo 35.º, n.º 3), para além de que não teria qualquer eficácia; a limitação da conservação a determinadas áreas geográficas poderá não ser inconstitucional, mas a sua eficácia será igualmente reduzida. Na prática, a conservação nunca poderá ser autorizada para grupos (p. ex., os membros do grupo criminoso X) ou categorias de pessoas (p. ex., todos os já condenados por crimes de terrorismo): a decisão terá sempre de individualizar cada concreta pessoa assim visada, não podendo isso sei deixado à execução dos FS.

[lxi] Pense-se, p. ex., em uma vaga de ataques terroristas, um pouco por todo o território, que se vai mantendo ao longo de semanas: justificaria, creio, a conservação universal enquanto se mantivesse

esse fundamento.

[lxii] Imagine-se que há uma vaga de furtos a caixas ATM, com explosivos, durante a noite, em diversos pontos do Algarve. Tal poderia fundamentar a conservação de dados de tráfego e de localização durante um mês em todos os concelhos do Algarve, para todos os FS nessa zona. Se, estando perto do fim esse período, se mantivessem os crimes, haveria fundamento para prorrogar essa conservação durante mais algum tempo.

[lxiii] Cf. artigo 3.º, n.º 2, do EMP.

[lxiv] P. ex., o cancelamento do importante evento político que fundamentava a conservação.

[lxv] Assim, MILHEIRO, Tiago Caiado, Artigo 189.º, cit., p. 923.

[lxvi] Sobre este ponto, cf., *infra*, III.2.

[lxvii] Cf. II.3.2.

[lxviii] Note-se que, se a conservação visar pessoas determinadas, não bastará identificá-las: será sempre necessário identificar outros dados, como o(s) número(s) de telefone, ou números de cartão SIM, ou IMEI, ou endereço(s) IP (se definidos contratualmente) ou número do contrato que incluía vários aparelhos de comunicação. Note-se ainda que, como sucede nas intercepções telefónicas, ficarão conservados dados de todas as muitas pessoas que comunicarem com os visados (mas só os dados dessas comunicações).

[lxix] Assim MILHEIRO, Tiago Caiado. Artigo 189.º, cit., p. 920.

[lxx] O direito a receber facturas não detalhadas também está consagrado no artigo 8.º, n.º 1, da Lei 41/2004.

[lxxi] E também por MILHEIRO, Tiago Caiado, Artigo 189.º, cit., pp. 909 e 912.

[lxxii] Que dispõe:

«Os dados relativos aos assinantes tratados em redes de comunicações electrónicas para estabelecer ligações e para transmitir informações contêm informações sobre a vida privada das pessoas singulares e incidem no direito ao sigilo da sua correspondência ou incidem nos legítimos interesses das pessoas colectivas. Esses dados apenas podem ser armazenados na medida do necessário para a prestação do serviço, *para efeitos de facturação e de pagamentos de interligação*, e por um período limitado. *Qualquer outro tratamento desses dados que o prestador de serviços de comunicações electrónicas publicamente disponíveis possa querer efectuar para a comercialização dos seus próprios serviços de comunicações electrónicas, ou para a prestação de serviços de valor acrescentado, só é permitido se o assinante tiver dado o seu acordo, com base nas informações exactas e completas que o*

prestador de serviços de comunicações electrónicas publicamente disponíveis lhe tiver comunicado relativamente aos tipos de tratamento posterior que pretenda efectuar e sobre o direito do assinante de não dar ou retirar o seu consentimento a esse tratamento [...].» (realces meus).

[[lxxiii](#)] Definidos no artigo 2.º, n.º 1, alínea e), como «quaisquer dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público».

[[lxxiv](#)] Publicado no D.R. n.º 166 (Série II - Parte E), de 28.08.2024.

[[lxxv](#)] Sendo positiva a resposta, *infra* em IV. se verá qual a norma de acesso.

[[lxxvi](#)] Cf., p. ex., Ac. TRG 10.01.2005, P. 2013/04-1 (Francisco Marcolino), Ac. TRC 17.05.2006, P. 1265/06 (Orlando Gonçalves), Ac. TRC 15.11.2006, P. 915/06.2TAAVR-A.C1 (Jorge Dias) e Ac. TRE 26.06.2007, P. 843/07-1 (Guilhermina de Freitas). Todos os acórdãos dos tribunais judiciais indicados encontram-se acessíveis em <http://www.dgsi.pt/>.

[[lxxvii](#)] O artigo 190.º dispunha então, sob a epígrafe «extensão»: «O disposto nos artigos 187.º, 188.º e 189.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, bem como à interceptação das comunicações entre presentes». Com a revisão de 2007, esta norma passou para o n.º 1 do artigo 189.º.

[[lxxviii](#)] Cf., p. ex., Ac. TRL 10.12.2003, P. 8673/2003-3 (Maria Isabel Duarte) e Ac. TRL 23.06.2004, P. 5845/2004-3 (Clemente Lima).

[[lxxix](#)] A conservação e utilização probatória de metadados após a Lei n.º 18/2024, de 5 de fevereiro. *Privacy and Data Protection Magazine*. 2025, n.º 8, p. 82.

[[lxxx](#)] Neste sentido, FIDALGO, Sónia, Conservação de Metadados – O Acórdão n.º 268/2022. *Revista Portuguesa de Direito Constitucional*. 2023, n.º 3, pp. 53 ss.

[[lxxxi](#)] Cf., *supra*, II.3.

[[lxxxii](#)] Cujos requisitos (âmbito objectivo, âmbito subjectivo, competência de juiz) se aplicam mesmo que o meio de obtenção de prova seja a busca (nas instalações dos FS).

[[lxxxiii](#)] Todas as informações relativas a uma pessoa singular identificada ou identificável – artigo 3.º, n.º 1, alínea c), da Lei 59/2019.

[[lxxxiv](#)] Impedirá o Acórdão..., cit., pp. 50-51.

[lxxxv] No mesmo sentido, MILHEIRO, Tiago Caiado, Artigo 189.º, cit., p. 917, e NUNES, Duarte Rodrigues, A conservação..., cit., p. 82.

[lxxxvi] Essa é também a conclusão de NUNES, Duarte Rodrigues, *ob. cit.*, pp. 47-53, e de MILHEIRO, Tiago Caiado, Artigo 189.º, cit., pp. 908-913, embora por argumentos nem sempre coincidentes.

[lxxxvii] Sobre o direito à protecção do Estado contra a vitimização primária ou repetida é de grande relevância a jurisprudência do Tribunal Europeu dos Direitos Humanos (TEDH), particularmente, por estar em causa telecomunicações e sua protecção, o Acórdão K.U. c. Finlândia (Queixa n.º 2872/02), de 02.12.2008, onde, na fundamentação da sua decisão, o TEDH referiu que «[...] a previsão de um crime tem efeito dissuasor limitado se não existir meio de identificar o agente e chamá-lo à justiça» (§46) e que «[...] pese embora a liberdade de expressão e a confidencialidade das telecomunicações sejam considerações relevantes (primárias) e os utilizadores de telecomunicações e de serviços de internet devam ter garantias de que a sua própria privacidade e liberdade de expressão será respeitada, *tais garantias não são absolutas e devem por vezes ceder em face de outros imperativos legítimos, tais como a prevenção de crimes e a protecção dos direitos e liberdades dos outros* [tarefa esta de concordância prática que cabe ao legislador assegurar]» (§49, *italico meu*). Tal jurisprudência foi reafirmada recentemente no Acórdão *Helme c. Estónia* de 07.10.2025 (Queixa n.º 3023/22), onde igualmente se questionava a admissibilidade de interferência nas telecomunicações.

[lxxxviii] A obrigação de conservação de documentos respeitantes ao contrato pode resultar ainda de normativos da ANACOM (que é a autoridade reguladora nacional). P. ex., no âmbito da portabilidade de números, «[o] PR [Prestador Recetor] deve conservar os documentos relativos às portabilidades, por um período mínimo de 5 anos, a contar da data da respetiva apresentação» – cf. artigo 11.º, n.º 12, do Regulamento Relativo à Portabilidade de Números (Regulamento 38/2025, publicado no D.R. n.º 6 (Série II - Parte E), de 09.01.2025).

[lxxxix] Cf., *supra*, I.2.8 e I.2.9.

[xc] Neste sentido, MILHEIRO, Tiago Caiado. A competência..., cit., p. 4.

[xci] P. ex., entre os mais recentes, Acs. STJ de 23.01.2025, P. 5/18.5GAAMT-E.S1 (Albertina Pereira), TRP de 24.05.2023, P. 747/20.5JGLSB.P1 (Pedro M. Menezes), TRE de 28.03.2023, P. 663/22.6JGLSB-A.E1 (Artur Vargues) e TRL de 04.11.2025, P. 927/25.7JGLSB-A.L1-5 (Paulo Barreto).

[xcii] Cf., p. ex. os Acs. 420/2017 e 268/2022 (§ 17.1), que enquadram os endereços IP junto dos dados de base.

[xciii] No Ac. de 30.04.2024 (*La Quadrature du Net II* – C-470/21), o tribunal considerou que

«[...] tendo em conta este princípio da proporcionalidade, há que considerar que a exigência de um controlo prévio por um órgão jurisdicional ou por uma entidade administrativa independente se impõe quando, no contexto de uma regulamentação nacional que prevê o

acesso de uma autoridade pública a dados pessoais, esse acesso comporta o risco de uma ingerência grave nos direitos fundamentais da pessoa em causa no sentido de que poderia permitir a essa autoridade pública tirar conclusões precisas sobre a vida privada dessa pessoa e, se for caso disso, estabelecer o seu perfil pormenorizado. Inversamente, esta exigência de um controlo prévio não é aplicável quando a ingerência nos direitos fundamentais em causa, pelo acesso de uma autoridade pública a dados pessoais, não possa ser qualificada de grave. É esse o caso do acesso a dados relativos à identidade civil dos utilizadores dos meios de comunicações eletrónicas com o único objetivo de identificar o utilizador em causa e sem que esses dados possam ser associados a informações relativas às comunicações efetuadas, uma vez que, segundo a jurisprudência do Tribunal de Justiça, a ingerência que comporta tal tratamento dos referidos dados não pode, em princípio, ser qualificada de grave (v., neste sentido, Acórdão de 6 de outubro de 2020, *La Quadrature du Net* e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.^{os} 157 e 158)»;

decidiu em consequência que

«[...] o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º e do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que não se opõe a uma regulamentação nacional que autoriza a autoridade pública responsável pela proteção dos direitos de autor e dos direitos conexos contra as violações desses direitos cometidas na Internet a aceder aos dados, conservados pelos prestadores de serviços de comunicações eletrónicas acessíveis ao público, relativos à identidade civil correspondente a endereços IP recolhidos previamente por organismos de titulares de direitos, para que essa autoridade possa identificar os titulares desses endereços, utilizados para atividades suscetíveis de constituir tais violações, e possa tomar, se for caso disso, medidas a seu respeito» (com respeito por garantias que indica).

No Ac. de 02.03.2021 (*Prokuratuur* - C-746/18), o que foi decidido foi:

«O artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que atribui competência ao Ministério Público, cuja missão é dirigir a instrução do processo penal e exercer, sendo caso disso, a ação pública num processo posterior, para autorizar o acesso de uma autoridade pública aos dados de tráfego e aos dados de localização para fins de instrução penal.».

Apenas respeita a dados de tráfego e dados de localização, portanto.

[xciv] Cf., *infra*, IV.3.2.

[xcv] Defendendo que a competência deve ser do MP, cf. também FIDALGO, Sónia, ob. cit., pp. 53-55.

[xcvi] Entre muitas outras consequências graves desta injustificada restrição, para a investigação da generalidade de crimes cometidos *online* não é possível, através da aplicação desta lei, obter os endereços IP atribuídos à fonte de uma ligação. Sem isso, é em regra impossível identificar o autor do crime. O que nos pode valer é o artigo 14.º da LCC (cf., *infra*, IV.3), desde que os FS conservem esses dados ao abrigo da Lei 41/2004, o que de modo algum é garantido (cf., *supra*, III.2).

[xcvii] Admitindo a sua utilização também na instrução e julgamento, MILHEIRO, Tiago Caiado. Artigo 189.º, cit. pp. 926-927 (mas defendendo que a norma de acesso é o n.º 2 do artigo 189.º do CPP, aspecto de que discordo).

[xcviii] Cf. *supra* III.2.

[xcix] Sobre esta norma, cf. a Acta n.º 20, p. 6.

[c] Cf. Pedro Verdelho, ob. cit., pp. 162-163.

[ci] Dois outros aspectos eram omissos da letra da lei: o critério da necessidade probatória, que assim tinha de respeitar “apenas” a proporcionalidade imposta pelo artigo 18.º, n.º 2, da CRP, e a fase do processo em que era admissível a sua obtenção, que assim eram todas (desde que, naturalmente, os dados estivessem ainda conservados).

[cii] Assim, CORREIA, João Conde, Prova digital: as leis que temos e a lei que devíamos ter. *Revista do Ministério Público*. 2014, n.º 139, p. 36.

[ciii] A revogação de uma lei (ou norma) pode resultar de declaração expressa, da incompatibilidade entre as novas disposições e as regras precedentes ou da circunstância de a nova lei (ou norma) regular toda a matéria da lei (ou norma) anterior – cf. artigo 7.º, n.º 2, do Código Civil. A revogação pode ser expressa ou tácita, total (ab-rogação) ou parcial (derrogação). A revogação é expressa «quando consta de declaração feita na lei posterior» e tácita «quando resulta da incompatibilidade entre as disposições novas e as antigas, ou ainda quando a nova lei regula toda a matéria da lei anterior – substituição global» – cf. MACHADO, J. Baptista, *Introdução ao Direito e ao Discurso Legitimador*, Coimbra: Almedina, 1990, ISBN 9789724004716, pp. 165-166.

[civ] Nesse sentido, cf. Acs. STJ 02.02.2023, P. 7035/20.5T9LSB.L1.S1 (Maria do Carmo Dias), de 08.11.2022, P. 107/13.4P6PRT-D.S1 (Conceição Gomes), de 21.06.2023, P. 1229/19.3TELSB-A.S1 (Ernesto Vaz Pereira) e de 21.02.2024, P. 966/14.3JAPRT-C.S1 (Lopes da Mota).

[cv] Para além disso, creio que *sempre foi esse o único fundamento para a obtenção desses dados no estrangeiro*. O artigo 9.º da Lei 32/2008 apenas se aplica ao acesso aos dados a que referem os seus artigos 3.º e 4.º, ou seja, aos dados conservados pelos FS nacionais, únicos a quem se aplica essa lei. Do n.º 6 resulta claro que apenas a esses respeita, pois apenas essas entidades devem elaborar registos da extracção dos dados transmitidos às autoridades competentes e enviá-los trimestralmente à CNPD, nunca entidades estrangeiras. O próprio Ac. TC 268/2022 assume

tacitamente esse entendimento, pois os fundamentos da inconstitucionalidade que aponta (não prever a obrigação de notificação ao interessado) não podem exigir-se por lei portuguesa a FS que esteja em qualquer outro Estado.

[cvi] Cf. Ac. de 30.04.2024, C-178/22 (Caso *Procura della Repubblica presso il Tribunale de Bolsano*):

«45. [...] no que respeita à definição do conceito de «infração grave», resulta da jurisprudência que, na medida em que a União não tenha legislado na matéria, a legislação penal e as regras de processo penal são da competência dos Estados-Membros. Todavia, estes devem exercer essa competência no respeito do direito da União (v., neste sentido, Acórdão de 26 de fevereiro de 2019, *Rimšēvičs e BCE/Letónia*, C-202/18 e C-238/18, EU:C:2019:139, n.º 57 e jurisprudência referida). A este respeito, há que observar que a definição de infrações penais, circunstâncias atenuantes e agravantes e sanções reflete tanto as realidades sociais como os costumes jurídicos que variam não só entre os Estados-Membros mas também no tempo. Ora, estas realidades e costumes têm uma certa importância para determinar as infrações consideradas de carácter grave.

46. Por conseguinte, tendo em conta a repartição de competências entre a União e os Estados-Membros nos termos do TFUE e as diferenças importantes que existem entre os sistemas jurídicos dos Estados-Membros no domínio penal, há que considerar que incumbe aos Estados-Membros definir as «infrações graves» para efeitos da aplicação do artigo 15.º, n.º 1, da Diretiva 2002/58.»

[cvii] Merecem, pois, censura os Acs. TRC de 12.10.2022 (Maria Alexandre Guiné) e TRC de 12.10.2022 (Paulo Guerra).

[cviii] Sobre o n.º 1 do artigo 282.º da CRP, escrevem CANOTILHO, Gomes & MOREIRA, Vital, *Constituição da República Portuguesa Anotada*. 4.ª ed. Coimbra: Coimbra Editora. 2014, ISBN: 9789723222869, pp. 975-976): «A declaração de inconstitucionalidade (ou de ilegalidade) tem efeito repristinatório (nº 1, *in fine*), determinando a reentrada em vigor de normas eventualmente revogadas pela norma declarada inconstitucional (ou ilegal). Trata-se de um efeito directo da inconstitucionalidade (ou da ilegalidade), pois, sendo a norma inválida desde a origem, é inválida desde logo a revogação de normas anteriores que ela tenha efectuado.». Justificando este efeito, escreve MEDEIROS, Rui. Artigo 282.º. In *Constituição da República Anotada*, vol. III, 2.ª ed., MIRANDA, Jorge & MEDEIROS, Rui (org.). Lisboa: Universidade Católica Editora. 2020, ISBN 9789725407318, p. 726): «Se a norma revogatória é inválida desde a origem e como tal vem a ser declarada, ela não possui nenhuma capacidade de modificação da ordem jurídica e não pode revogar validamente a norma precedente sobre a mesma matéria. [...] Por outro lado, a solução adotada evita o vazio legislativo e, nessa medida, previne diferenças de tratamento de casos análogos e a criação de um estado de incerteza gravemente lesivo para os particulares.». Para este efeito, é irrelevante que a revogação seja expressa ou tácita: «[n]os casos em que a revogação, expressa ou tácita, do regime

anterior seja efetuada pela norma declarada inconstitucional, é incontestável o efeito repristinatório da declaração de inconstitucionalidade» – Ac. TC 319/2018.

[cix] Neste sentido, MILHEIRO, Tiago Caiado, *A competência...*, cit., p. 9 ss.; também, embora antes da Lei 18/2004, FIDALGO, Sónia, ob. cit., pp. 55-56002E

[cx] NUNES, Duarte Rodrigues. *Os meios de obtenção de prova previstos na Lei do Cibercrime*. 1.^a ed. Coimbra: Gestlegal, 2018, ISBN: 978-989-54076-4-4, pp. 25-32.

[cxi] *Ibidem*, pp. 60 e 155.

[cxii] Ob. cit., pp. 113-114.

[cxiii] Nesse acórdão é feita uma apreciação de todo o regime que resulta da conjugação do CPP, da Lei 32/2008 e da LCC que agora não cabe comentar. De qualquer forma, não posso deixar de assinalar que, contrariamente ao aí defendido, o artigo 4.º da Lei 32/2008 respeita a todas as comunicações electrónicas, abrangendo, pois, quer as telefónicas, quer as de dados informáticos (vd. as diferentes categorias de dados a conservar aí referidas, que mencionam expressamente, p. ex., o acesso à Internet e ao correio electrónico através da Internet). Note-se ainda que a LCC não contém qualquer norma que seja fundamento para a conservação de quaisquer *metadados* (e recorde novamente que não é isso que permite o seu artigo 12.º). Daí que, se não fosse a Lei 32/2008 o fundamento para conservação de dados das comunicações que consistem em transmissão de dados informáticos, não existiria outro (não levando por ora em consideração a Lei 41/2004).

[cxiv] Prova digital é aquela informação gerada, guardada ou transmitida em formato binário que possa ser valorada em processo judicial.

[cxv] Nesse sentido, MILHEIRO, Tiago Caiado, Artigo 189.º, cit., p. 925. Note-se que os dados de tráfego e de localização previstos na Lei 32/2008 são dados informáticos, registados em suporte electrónico e transmitidos electronicamente – artigos 7.º, n.º 3, e 10.º dessa lei.

[cxvi] Apenas quanto aos dados de base.

[cxvii] Estes estão definidos no artigo 2.º, alínea c), como os «dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente».

[cxviii] Estes dados não resultam do contrato, mas sim das concretas comunicações.

[cxix] Explicando essa intenção, pode ler-se na respectiva Exposição de Motivos: «A realização de intercepções de comunicações electrónicas e, sobretudo, a obtenção de dados de tráfego, são ferramentas processuais essenciais em processo-crime em que se investiguem crimes cometidos por via das redes de comunicações, tendo essa preocupação ficado espelhada no diploma que obriga

os operadores de comunicações a guardarem os dados de tráfego dos seus clientes, tendo em vista a sua eventual necessidade em investigação criminal – Lei n.º 32/2008, de 17 de Julho, que regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas. *Importa assim superar o actual regime, de modo a fornecer ao sistema processual penal normas que permitam a obtenção de dados de tráfego e a realização de intercepções de comunicações em investigações de crimes praticados no ambiente virtual. É o que se pretende fazer por via da lei que agora se propõe.*» (realces meus).

[cxx] Em sentido concordante, antes da Lei 18/2024, FIDALGO, Sónia, ob. cit., próprio. 53-33.

[cxxi] *Os meios de obtenção de prova...*, cit., pp. 60 e 155.

[cxxii] Actualmente, considera que o novo artigo 9.º da Lei 32/2008 constitui *lex posterior* face às normas da LCC, e, por isso, quando se tratar da utilização de *metadados* que tenham sido alvo de conservação, aplica-se o actual artigo 9.º da Lei 32/2008, por força do princípio *lex posterior derogat legi priori* – *A conservação e utilização probatória de metadados...*, cit., p. 84.

[cxxiii] Argumento que pressupõe que a LCC teria de ter tal regime, o que, face à assinalada diferença entra a proposta de lei e a lei aprovada, fica por demonstrar.

[cxxiv] Cf. a PPL 289/X, que esteve na origem da LCC: «Do mesmo modo, foi adaptado para este diploma o regime de intercepção de comunicações, previsto no Código de Processo Penal para as comunicações telefónicas. Na verdade, o Código prevê já uma extensão do regime das intercepções telefónicas a outras comunicações, por exemplo electrónicas. Todavia, essa extensão não resolve o problema da investigação de crimes informáticos ou relacionados com a informática, porque o âmbito de aplicação deste regime, por via da extensão, é o mesmo das intercepções telefónicas. Ora, torna-se necessário abranger os crimes informáticos em geral, bem como aqueles cometidos por via de computadores, assim se motivando a criação de norma especial. Esta norma adopta em geral as regras do Código de Processo Penal, que é adaptado em função da especificidade dos crimes a que, por via desta nova lei, é aplicável.»

[cxxv] No mesmo sentido, FIDALGO, Sónia, ob. cit., p. 55.

[cxxvi] Verdadeiramente, trata-se de *preservação* e não de *conservação*, como exposto em II.1.5. Não querendo contribuir para a reprodução do equívoco, vou utilizar preferencialmente a designação original em inglês: *European Preservation Order*.

[cxxvii] Cf. artigo 1.º, n.º 1, e 34.º, n.º 2.

[cxxviii] E não tudo, que sairia fora do objecto do presente texto.

[cxxix] Crimes que podem nem ter ocorrido, fugindo o condenado antes do início do cumprimento de pena.

[cxxx] Não quanto às ordens de preservação, pois o n.º 3 do artigo 4.º preceitua que podem ser emitidas por: a) Um juiz, um tribunal, um juiz de instrução ou um magistrado do MP competente no processo em causa; ou b) Qualquer outra autoridade competente, tal como definida pelo Estado de emissão, e que, no processo em causa, intervenha enquanto autoridade de investigação num processo penal com competência para ordenar a recolha de elementos de prova de acordo com a lei nacional; num tal caso, a ordem deve ser validada, após a análise da sua conformidade com as condições de emissão de uma ordem europeia de conservação ao abrigo do presente regulamento, por um juiz, um tribunal, um juiz de instrução ou um magistrado do MP do Estado de emissão. Esse é o regime que consta já do artigo 12.º da LCC.

[cxxxi] Assim: WALH, Thomas. *E-evidence Regulation and Directive Published*. [Em linha]. Disponível em: URL <https://eucrim.eu/news/e-evidence-regulation-and-directive-published/?>; ERBEŽNIK, Anže. A new EU system on cross-border gathering of e-evidence – analysis and open questions. *Dignitas*, n.º 98(2023), pp. 47-72. [Em linha]. Disponível em URL: <http://revije.nova.uni.si/index.php/dignitas/article/view/327/292>; SILVA, Thales & DUARTE, Evandro. E-evidence regulation 1544/2023 in the european union: a paradigm shift from judicial to “direct” cooperation. *Observatório de la Economía Latinoamericana*. N.º 23. e10987. [Em linha]. Disponível em: URL <https://ojs.observatoriolatinoamericano.com/ojs/index.php/olel/article/view/10987>. SACHOULIDOU, Athina. Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of ‘judicial’ cooperation. [Em linha]. Disponível em: URL <https://journals.sagepub.com/doi/epub/10.1177/20322844241258649>.

[cxxxii] Matéria fora do objecto deste texto, que respeita apenas aos *metadados*.

[cxxxiii] O regulamento define “autoridade de execução” como a autoridade competente do Estado de execução que, em conformidade com o direito nacional desse Estado, tem competência para receber uma ordem europeia de produção e um COEP ou uma ordem europeia de conservação e um COEC transmitidos pela autoridade emissora para comunicação ou para execução em conformidade com o presente regulamento – artigo 1.º, n.º 17.

Luís Lemos Triunfante: Juiz de Direito | Licenciado em Direito e Mestre em Estudos Europeus pela Escola de Direito do Porto e Instituto de Estudos Políticos da Universidade Católica Portuguesa | Ex-Vogal Tesoureiro da Associação Sindical dos Juízes Portugueses | Ex-Perito Nacional Destacado no Gabinete Português da Eurojust | Membro da Coletânea de Jurisprudência da Casa do Juiz

Sumário Executivo: 1) A prova digital tornou-se um elemento central do processo judicial contemporâneo, exigindo novos critérios quanto à sua autenticidade, integridade e fiabilidade. 2) A jurisprudência do TJUE estabelece um modelo restritivo em matéria penal, proibindo a recolha e conservação indiscriminada de dados e impondo os princípios da necessidade, proporcionalidade e proteção dos direitos fundamentais. 3) Os acórdãos Digital Rights, Tele2, Prokuratuur e SpaceNet consolidam exigências essenciais: ligação à criminalidade grave, controlo prévio independente e relevância da legalidade da obtenção da prova para a sua admissibilidade. 4) Em Portugal, esta jurisprudência levou à reconfiguração do regime legal e jurisprudencial, com reforço do controlo judicial e da exigência de conformidade constitucional na obtenção da prova digital. 5) No domínio civil e comercial, prevalece um modelo mais permissivo, baseado na equivalência funcional entre meios digitais e tradicionais e na livre apreciação da prova. 6) A prova digital é, assim, tratada de forma dual: restringida no processo penal para proteger direitos fundamentais e admitida no processo civil, mas sujeita a controlo técnico crescente. 7) O artigo contém a sugestão de tabela comparativa com a jurisprudência do TJUE (Prova Digital), um quadro comparativo: prova digital (TJUE vs. Portugal) e um quadro sistémico integrado da prova digital entre a jurisprudência do TJUE e a nacional em matéria penal e civil.

Resumo: O artigo analisa o papel da prova digital na jurisprudência europeia e portuguesa, evidenciando a sua centralidade no processo judicial contemporâneo e a necessidade de adaptação dos modelos tradicionais de prova. No domínio penal, a jurisprudência do TJUE assume um papel determinante, impondo limites rigorosos à utilização de dados digitais, sobretudo quanto à sua recolha, conservação e acesso. A admissibilidade da prova depende da sua ligação à criminalidade grave, do respeito pelos princípios da necessidade e proporcionalidade e da existência de controlo prévio por autoridade independente, sendo ainda relevante a legalidade da sua obtenção. Estas exigências tiveram impacto direto no direito português, conduzindo a uma maior exigência na validação da prova digital e ao reforço das garantias processuais, incluindo a possibilidade de exclusão de prova obtida de forma ilícita. Em contraste, no domínio civil e comercial, a prova digital é

amplamente admitida, com base no princípio da equivalência funcional entre suportes digitais e tradicionais. O seu valor probatório depende sobretudo da verificação da autenticidade, integridade e fiabilidade técnica dos dados. Conclui-se que a prova digital se insere num modelo dual: restritivo e constitucionalizado no processo penal, e funcional e tecnicamente escrutinado no processo civil, refletindo o equilíbrio entre eficácia probatória e proteção dos direitos fundamentais.

Palavras-Chave: Prova digital; Dados de comunicações eletrónicas; Metadados; TJUE; Jurisprudência europeia; Processo Penal; Processo Civil; Admissibilidade da prova; Direitos fundamentais; Proporcionalidade; Necessidade; Controlo judicial; Criminalidade grave; Conservação de dados; Legalidade da prova; Exclusão da prova ilícita; Equivalência funcional; Suporte duradouro; Fiabilidade técnica; Autenticidade; Integridade; Livre apreciação da prova; eIDAS; Prova eletrónica; Jurisprudência portuguesa; Constitucionalização da prova digital; Dualismo probatório.

Índice: I. Introdução; II.1 - Matéria penal; Tabela Comparativa - Jurisprudência do TJUE (Prova Digital); Impacto da jurisprudência do TJUE no ordenamento jurídico e na jurisprudência portuguesa; II.2 - Matéria civil; III. Conclusão geral; Quadro comparativo: prova digital (TJUE vs. Portugal); Quadro comparativo: prova digital (TJUE vs. Portugal); Quadro sistémico integrado da prova digital entre a jurisprudência do TJUE e a nacional em matéria penal e civil.

I. Introdução

A prova digital representa atualmente um dos domínios mais sensíveis e complexos do processo judicial contemporâneo, resultante da crescente digitalização das comunicações, da ubiquidade dos dispositivos eletrónicos e da expansão das infraestruturas digitais. Esta transformação implica uma revisitação profunda das categorias clássicas do direito probatório, designadamente no que respeita à autenticidade, integridade, fiabilidade e valoração da prova. A especificidade técnica da prova digital, marcada pela sua volatilidade e facilidade de manipulação, exige a construção de novos critérios dogmáticos capazes de assegurar a sua credibilidade.

Após o artigo *"O Direito penal em ação: dos alicerces à cobertura - jurisprudência do Tribunal Constitucional em matéria de prova digital"*, de Mariana Coimbra Piçarra, que saiu na Revista Julgar *"A Justiça no Mundo Virtual, Digitalização, IA & Prova digital"*, págs. 163 e ss.,^[i] nesta segunda edição da mesma revista, também com a temática da IA e da prova digital, considere relevante prosseguir num levantamento e análise da jurisprudência europeia e nacional mais relevantes na matéria penal e civil, com indicação da bibliografia mais relevante^[iii].

II. 1 - Matéria penal

O Tribunal de Justiça da União Europeia (TJUE) desenvolveu uma linha jurisprudencial estruturante em matéria de prova digital, assumindo uma verdadeira função de conformação constitucional no espaço europeu.

1 - Acórdão do TJUE (Grande Secção) de 8 de abril de 2014 (Digital Rights Ireland/C-293/12 e C-594/12)

O primeiro acórdão relevante para esta área é o acórdão do TJUE (Grande Secção) de 8 de abril de 2014 (Digital Rights Ireland), proferido nos processos apensos C-293/12 e C-594/12^[iii], o qual constitui um marco fundamental na compreensão jurídica da prova digital, sobretudo no que respeita à utilização de dados de comunicações eletrónicas como instrumento probatório em processos penais. O TJUE parte do reconhecimento de que os chamados metadados — isto é, dados de tráfego e de localização — assumem um elevado valor probatório, uma vez que permitem identificar a origem e o destino das comunicações, a sua duração, frequência e localização, possibilitando traçar perfis detalhados dos comportamentos individuais. Na verdade, considerados no seu conjunto, estes dados são suscetíveis de revelar com grande precisão aspetos essenciais da vida privada, como hábitos quotidianos, deslocações, relações sociais e padrões de interação.

Neste sentido, o TJUE admite que a conservação desses dados pode constituir um instrumento útil e até adequado à investigação, deteção e repressão de criminalidade grave, incluindo o terrorismo, reconhecendo assim a sua relevância no plano da prova digital. A utilização de tais dados confere às autoridades meios adicionais de investigação e reforça a capacidade de reconstrução factual, sendo, por isso, um elemento central na prova indireta em ambiente digital. Contudo, esta utilidade não é suficiente para legitimar qualquer regime de recolha e conservação. O problema central identificado no acórdão reside na forma indiscriminada e generalizada como a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho de 15 de março de 2006, relativa à conservação de dados gerados e ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Diretiva 2002/58/CE^[iv] impunha a conservação desses dados. A diretiva abrangia a totalidade dos utilizadores de serviços de comunicações eletrónicas, independentemente de qualquer suspeita de envolvimento em atividades criminosas, criando assim uma base massiva de dados potencialmente utilizáveis como prova. Esta lógica preventiva e universal contraria princípios fundamentais do direito probatório, nomeadamente o princípio da necessidade e da pertinência da prova, uma vez que não existe uma ligação concreta entre os dados recolhidos e factos específicos em investigação.

Acresce que o regime não previa critérios objetivos que delimitassem o acesso das autoridades a esses dados, nem exigia um controlo prévio por uma autoridade judicial ou entidade independente. A ausência de um mecanismo de supervisão efetiva fragiliza a legitimidade da prova

digital obtida, pois elimina um elemento essencial de garantia dos direitos fundamentais e de controlo da proporcionalidade. Sem esse controlo, a utilização dos dados pode tornar-se arbitrária e desprovida de enquadramento jurídico rigoroso.

Outro aspeto crítico prende-se com a indeterminação das finalidades de acesso e utilização dos dados. A diretiva remetia genericamente para “infrações graves”, sem densificar o conceito nem estabelecer critérios uniformes, o que abria espaço a interpretações amplas e a uma utilização extensiva da prova digital para além do estritamente necessário. Esta indeterminação compromete a segurança jurídica e afeta diretamente a validade da prova obtida nesse contexto.

O TJUE também sublinha deficiências relevantes ao nível das garantias técnicas e organizativas de proteção dos dados. A diretiva não assegurava um nível suficientemente elevado de segurança, nem previa mecanismos rigorosos de controlo da integridade, conservação e destruição dos dados. Estas falhas têm implicações diretas no domínio da prova digital, na medida em que colocam em causa a fiabilidade dos dados, a sua autenticidade e a cadeia de custódia, elementos essenciais para a sua admissibilidade e valor probatório.

Perante este quadro, o TJUE aplica de forma exigente o princípio da proporcionalidade, concluindo que a ingerência nos direitos fundamentais — nomeadamente o direito à vida privada e à proteção de dados pessoais — é de grande amplitude e gravidade e não se encontra devidamente limitada ao estritamente necessário. Assim, embora reconheça a importância da prova digital baseada em metadados, o acórdão afirma que a sua recolha e utilização só são admissíveis quando sujeitas a critérios rigorosos de necessidade, adequação e proporcionalidade, bem como a garantias efetivas de controlo e proteção.

Em conclusão, o acórdão estabelece um equilíbrio claro: a prova digital é um instrumento legítimo e valioso no combate à criminalidade, mas a sua obtenção não pode assentar em mecanismos de vigilância generalizada e indiscriminada. A legitimidade da prova digital depende, assim, de um enquadramento normativo que assegure a sua vinculação a finalidades concretas, o controlo por autoridades independentes e o respeito por elevados padrões de proteção de dados.

2 - Acórdão do TJUE (Grande Secção) de 21 de dezembro de 2016 (Tele2 Sverige e Watson/C 203/15)

O segundo acórdão relevante nesta área é o acórdão do TJUE (Grande Secção) de 21 de dezembro de 2016 (Tele2 Sverige e Watson (C 203/15)[\[v\]](#), o qual aprofunda e densifica significativamente a jurisprudência iniciada no caso Digital Rights Ireland, assumindo particular relevância no domínio da prova digital, sobretudo quanto à admissibilidade, limites e condições de utilização de dados de tráfego e localização como meios probatórios em processo penal.

O TJUE parte da constatação de que os dados de comunicações eletrónicas — embora não incluam o conteúdo das comunicações — constituem um instrumento de prova digital extremamente poderoso. Estes dados permitem identificar a origem, o destino, a duração, a frequência e o contexto das comunicações, bem como localizar os utilizadores, possibilitando a reconstrução detalhada das suas interações e comportamentos. Considerados globalmente, são suscetíveis de revelar aspetos altamente sensíveis da vida privada, permitindo traçar perfis individuais com um grau de precisão comparável ao acesso ao próprio conteúdo das comunicações.

Neste sentido, o TJUE reconhece novamente a utilidade destes dados para efeitos de investigação criminal, designadamente no combate à criminalidade grave e ao terrorismo. A prova digital baseada em metadados é, assim, admitida como um instrumento legítimo e relevante no processo penal. Contudo, o acórdão centra-se na necessidade de compatibilizar essa utilidade com a tutela dos direitos fundamentais, em especial o direito à vida privada, à proteção dos dados pessoais e à liberdade de expressão.

O ponto decisivo do acórdão reside na afirmação categórica de que uma obrigação de conservação generalizada e indiferenciada de todos os dados de tráfego e de localização é incompatível com o direito da União. O TJUE considera que tal regime gera uma ingerência particularmente grave nos direitos fundamentais, uma vez que abrange a totalidade da população, independentemente de qualquer suspeita ou ligação a atividades criminosas, e permite uma vigilância potencialmente contínua da vida dos cidadãos. Do ponto de vista da prova digital, isto equivale à criação de um sistema de recolha preventiva e massiva de meios probatórios, indiscriminadamente dirigidos a toda a população, o que contraria os princípios estruturantes da atividade probatória.

Em particular, o acórdão sublinha que a recolha de prova digital deve estar sujeita ao princípio da estrita necessidade. A conservação de dados só é admissível quando limitada ao que é estritamente necessário para atingir objetivos legítimos, como a luta contra a criminalidade grave, não podendo justificar-se com base em finalidades genéricas ou amplas. Assim, a prova digital não pode ser obtida por via de mecanismos de recolha universal, mas sim através de medidas seletivas e dirigidas.

O acórdão introduz, neste ponto, um critério fundamental: a distinção entre conservação generalizada (inadmissível) e conservação seletiva (potencialmente admissível). A conservação de dados pode ser permitida apenas se for orientada por critérios objetivos que estabeleçam uma ligação entre os dados recolhidos e o objetivo de combate à criminalidade grave. Essa limitação pode basear-se, por exemplo, em categorias de pessoas, zonas geográficas ou períodos temporais associados a riscos concretos. Assim, no plano da prova digital, impõe-se que a recolha seja circunscrita e orientada por relevância probatória, rejeitando-se a lógica de acumulação indiscriminada de informação.

Outro contributo essencial do acórdão reside na densificação das garantias relativas ao acesso aos dados. O TJUE afirma que o acesso das autoridades aos dados conservados constitui uma ingerência autónoma e adicional, que deve obedecer a requisitos rigorosos. Em particular, estabelece que: i) o acesso deve restringir-se à luta contra a criminalidade grave; ii) deve basear-se em critérios objetivos que limitem o universo de pessoas afetadas; iii) deve estar sujeito a controlo prévio por uma autoridade judicial ou administrativa independente.

Estas exigências são fundamentais do ponto de vista da prova digital, pois asseguram que a sua obtenção seja conforme ao direito e, consequentemente, admissível em juízo. A ausência de tais garantias comprometeria não só a legalidade da prova, mas também a sua credibilidade e legitimidade.

O TJUE refere ainda a necessidade de garantir elevados padrões de proteção, segurança e integridade dos dados. A prova digital depende da fiabilidade técnica dos dados, pelo que o regime jurídico deve assegurar medidas robustas contra acesso ilícito, manipulação ou uso abusivo. Nesse sentido, o acórdão exige que os dados sejam protegidos por garantias técnicas adequadas, sujeitos a controlo por uma autoridade independente e, em regra, conservados no território da União, assegurando um nível elevado de proteção. Estes requisitos refletem preocupações típicas da prova digital, como a integridade dos dados e a preservação da cadeia de custódia.

Por fim, o acórdão reforça a ideia de que a exceção à confidencialidade das comunicações não se pode transformar em regra. O regime de conservação de dados deve manter-se como uma derrogação limitada, sob pena de esvaziar o núcleo essencial do direito à privacidade. Assim, o TJUE estabelece um paradigma claro: a prova digital é admissível e relevante, mas a sua obtenção deve respeitar um quadro restritivo, baseado em necessidade, proporcionalidade e controlo institucional.

Em síntese, o acórdão Tele2 Sverige e Watson consolida um modelo exigente de prova digital no espaço europeu: admite a utilização de metadados como meio probatório de grande valor, mas rejeita a sua recolha indiscriminada e impõe um conjunto rigoroso de condições quanto à sua produção, acesso e conservação. Dessa forma, afirma-se um equilíbrio entre eficácia da investigação criminal e proteção dos direitos fundamentais, determinante para a validade e legitimidade da prova digital.

3 - Acórdão do TJUE (Grande Secção) de 2 de março de 2021 (Prokuratuur/C-746/18)

O terceiro acórdão relevante nesta área é o acórdão do TJUE (Grande Secção) de 2 de março de 2021 – (Prokuratuur) C-746/18^[vi], o qual representa um desenvolvimento decisivo da jurisprudência europeia sobre dados de comunicações eletrónicas, abordando de forma direta a questão da admissibilidade da prova digital em processo penal e clarificando as condições em que dados de tráfego e localização podem ser utilizados como elementos probatórios.

O ponto de partida do TJUE reside no reconhecimento de que os dados de comunicações eletrónicas — como os dados de tráfego e de localização — possuem um valor probatório particularmente elevado. Estes dados permitem não apenas identificar a origem e o destino de comunicações, mas também determinar o momento, a duração, a frequência e o contexto dessas interações, bem como reconstruir deslocações e padrões de comportamento. Assim, considerados no seu conjunto, possibilitam retirar conclusões muito precisas, ou mesmo extremamente detalhadas, sobre a vida privada dos indivíduos, incluindo hábitos quotidianos, relações sociais e movimentos geográficos.

Deste modo, a prova digital baseada nestes dados assume uma relevância central na investigação criminal moderna. No entanto, precisamente por essa capacidade intrusiva, o TJUE sublinha que a sua utilização está sujeita a um controlo jurídico particularmente rigoroso, centrado na proteção dos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (2000/C 364/01) [\[viii\]](#).

Um dos contributos fundamentais do acórdão consiste na reafirmação de que o acesso a dados de tráfego e de localização constitui, em si mesmo, uma ingerência grave nesses direitos fundamentais. O TJUE esclarece que essa gravidade não depende da quantidade de dados acedidos nem da duração do período em causa. Mesmo um acesso limitado, quer temporalmente quer quantitativamente, pode permitir inferências precisas sobre a vida privada, razão pela qual deve ser qualificado como ingerência grave. Esta afirmação tem implicações diretas no domínio da prova digital, pois impede que a admissibilidade da prova se baseie na ideia de que um acesso “reduzido” seria automaticamente legítimo.

Consequentemente, o acórdão estabelece um critério rigoroso quanto às finalidades que podem justificar o acesso a este tipo de prova digital. A regra é clara: apenas a luta contra a criminalidade grave ou a prevenção de ameaças graves à segurança pública pode legitimar o acesso a dados suscetíveis de revelar aspetos detalhados da vida privada. Afasta-se, assim, qualquer possibilidade de utilização desses dados como prova em investigações relativas à criminalidade em geral, independentemente da extensão ou intensidade do acesso. Este entendimento reforça a ideia de que a prova digital não pode ser utilizada de forma indiscriminada, devendo estar funcionalmente ligada a finalidades de especial gravidade.

O acórdão introduz ainda uma distinção relevante entre diferentes categorias de dados. O TJUE admite que determinados dados mais limitados — como dados de identificação simples — podem implicar uma ingerência menos intensa e, por isso, ser utilizados para fins mais amplos. Contudo, quando estão em causa dados de tráfego e localização, capazes de revelar o conteúdo relacional e comportamental da vida dos indivíduos, o nível de proteção exigido é substancialmente mais elevado. Esta diferenciação é essencial para a construção de uma teoria da prova digital, na medida em que associa o regime de admissibilidade à natureza e ao potencial revelador do dado.

Outro aspeto central do acórdão prende-se com as condições de acesso aos dados. O TJUE reafirma que esse acesso deve ser limitado ao estritamente necessário e baseado em critérios objetivos que estabeleçam uma ligação entre os dados solicitados e o objetivo da investigação. A prova digital não pode resultar de um acesso geral ou indiferenciado, mas deve ser direcionada a situações concretas, envolvendo, em princípio, pessoas suspeitas de infrações graves. Este requisito reforça a exigência de pertinência e necessidade da prova no processo penal.

Particular relevância assume a exigência de controlo prévio por uma autoridade independente. O TJUE clarifica que esse controlo constitui uma garantia essencial da legalidade da prova digital, destinando-se a assegurar o equilíbrio entre as necessidades da investigação e a proteção dos direitos fundamentais. No entanto, vai mais longe ao afirmar que o Ministério Público não pode ser considerado uma entidade independente para este efeito, pelo facto de participar no processo penal como parte interessada e dirigir a investigação.

Esta conclusão tem enorme impacto no plano probatório: significa que a prova digital obtida com base em autorização do Ministério Público, sem validação por um órgão jurisdicional ou entidade verdadeiramente independente, pode estar ferida de ilegalidade. Consequentemente, a sua admissibilidade em juízo fica comprometida.

O acórdão aborda também diretamente a questão da utilização processual da prova digital obtida em violação do direito da União. O TJUE reconhece que a definição das regras de admissibilidade compete, em princípio, ao direito nacional, no quadro da autonomia processual. Todavia, impõe limites através dos princípios da equivalência e da efetividade. Em particular, afirma que o juiz nacional deve afastar elementos de prova quando a sua utilização comprometa o direito a um processo equitativo, designadamente quando o arguido não tenha podido contestar eficazmente os dados ou quando estes possam influenciar decisivamente a apreciação dos factos.

Deste modo, o acórdão estabelece uma ligação direta entre a legalidade da obtenção da prova digital e a sua admissibilidade em julgamento. A prova obtida através de conservação ou acesso ilícitos pode ter de ser excluída, sobretudo se a sua utilização comprometer garantias processuais fundamentais.

Em síntese, o acórdão Prokuratuur consolida um modelo exigente de prova digital no direito da União. Por um lado, reconhece o elevado valor probatório dos dados de comunicações eletrónicas; por outro, impõe limites rigorosos à sua obtenção e utilização. Estes limites traduzem-se na exigência de ligação a criminalidade grave, na necessidade de critérios objetivos de acesso, no controlo prévio por autoridade independente e na possibilidade de exclusão da prova obtida ilegalmente. Assim, o TJUE reafirma que a eficácia da investigação criminal não pode ser prosseguida à custa de uma erosão estrutural dos direitos fundamentais, estabelecendo um equilíbrio claro entre a função probatória dos dados digitais e as garantias essenciais do processo penal.

A evolução recente da jurisprudência do TJUE em matéria de dados de comunicações eletrónicas revela uma progressiva densificação do regime jurídico da prova digital, especialmente a partir do acórdão Prokuratuur (2021), consolidando um modelo cada vez mais exigente quanto à sua obtenção e utilização. Com efeito, após esse acórdão, o TJUE continuou a desenvolver de forma consistente critérios materiais e processuais que condicionam a admissibilidade da prova baseada em metadados, sendo particularmente relevantes os acórdãos La Quadrature du Net (acórdão do TJUE (Grande Secção) de 6 de outubro de 2020 - (C-511/18, C-512/18 e C-520/18)[\[viii\]](#) e SpaceNet/Telekom Deutschland (acórdão do TJUE (Grande Secção) de 20 de setembro de 2022 (C-793/19 e C-794/19)[\[ix\]](#)).

Desde logo, no acórdão La Quadrature du Net, o TJUE introduz uma inflexão qualitativa na sua jurisprudência, ao admitir, de forma excecional, a possibilidade de conservação generalizada e indiferenciada de dados, mas apenas em contextos de segurança nacional, designadamente perante ameaças graves como o terrorismo. Fora desses cenários, mantém-se a proibição de conservação indiscriminada, reafirmando a orientação estabelecida em Digital Rights Ireland (2014) e Tele2 Sverige e Watson (2016). O contributo essencial deste acórdão, do ponto de vista da prova digital, reside na ideia de que a validade da prova não depende apenas do momento do acesso aos dados, mas antes de todo o regime jurídico de conservação e tratamento. Isto significa que a prova digital passa a ser avaliada “a montante”: se o sistema de conservação for incompatível com o direito da União, os dados obtidos podem ficar comprometidos enquanto meio probatório.

Esta lógica é aprofundada no acórdão de 20 de setembro de 2022, SpaceNet/Telekom Deutschland, que reafirma de forma categórica a proibição geral da conservação indiscriminada de dados de tráfego e localização. Contudo, o TJUE admite exceções muito delimitadas, nomeadamente a conservação seletiva e dirigida ou, em certos casos específicos, a conservação de categorias de dados menos intrusivas, como os endereços IP ou dados de identidade civil dos utilizadores. Esta distinção introduz um elemento estrutural novo na teoria da prova digital: uma diferenciação entre tipos de dados em função da sua capacidade intrusiva. Assim, dados que permitem traçar perfis detalhados da vida privada ficam sujeitos a um regime restrito, associado à criminalidade grave, enquanto dados menos sensíveis podem ser utilizados com maior flexibilidade. Este raciocínio conduz à emergência de uma verdadeira “graduação probatória” dos dados digitais, que influencia diretamente a admissibilidade, o valor probatório e o controlo de proporcionalidade da sua utilização.

Paralelamente, o TJUE tem reiterado, em decisões posteriores inseridas na linha Tele2-Prokuratuur, três princípios estruturantes. Em primeiro lugar, a centralidade da gravidade da ingerência: sempre que os dados em causa permitam reconstruir ou perfilar a vida privada dos indivíduos, está-se perante uma ingerência grave nos direitos fundamentais, o que implica que a sua utilização só possa ser justificada no âmbito da luta contra a criminalidade grave. Em segundo lugar, a exigência de controlo prévio por uma autoridade independente — preferencialmente judicial — sendo excluída a possibilidade de esse controlo ser exercido pelo Ministério Público, enquanto parte

no processo penal. Em último lugar, a afirmação de uma ligação estreita entre a legalidade da obtenção da prova digital e a sua admissibilidade em juízo: dados obtidos em violação do direito da União devem, em princípio, ser excluídos ou, pelo menos, sujeitos a rigorosa ponderação à luz dos princípios da equivalência e da efetividade.

A análise conjunta destes acórdãos permite identificar uma evolução clara do TJUE, que passa de uma posição inicial centrada na utilidade funcional da prova digital para uma abordagem de contenção estrutural da sua obtenção. O critério decisivo deixa de ser a quantidade de dados recolhidos e passa a ser a sua capacidade de gerar inferências sobre a vida privada — o chamado “efeito de profiling”. Esta mudança conduz a uma verdadeira constitucionalização da prova digital, na medida em que a sua admissibilidade passa a depender da conformidade com os direitos fundamentais, do respeito pelo princípio da proporcionalidade e da existência de um controlo judicial efetivo.

Por fim, a jurisprudência recente evidencia também uma diferenciação tipológica entre categorias de dados, afastando a ideia de uma prova digital homogénea. Enquanto os dados de tráfego e de localização são considerados altamente intrusivos e, por isso, sujeitos a um regime particularmente restritivo, os dados de identificação simples admitem um tratamento mais flexível. Esta distinção tem implicações diretas na prática probatória, influenciando o modo como os tribunais avaliam a legalidade, a pertinência e o valor dos diferentes meios de prova digital.

Em síntese, a jurisprudência mais recente do TJUE, culminando nos acórdãos Prokuratuur e SpaceNet, reforça a ideia de que a prova digital baseada em metadados é simultaneamente um instrumento de elevada eficácia investigatória e uma fonte potencial de grave ingerência nos direitos fundamentais. Por essa razão, a sua admissibilidade depende cada vez mais da legalidade do regime de recolha e conservação, consagrando-se um modelo exigente que procura equilibrar a eficácia da investigação penal com a proteção da vida privada e dos dados pessoais.

Segue sugestão de tabela comparativa com a jurisprudência do TJUE:

Tabela Comparativa – Jurisprudência do TJUE (Prova Digital)

Elemento	Digital Rights (2014)	Tele2 Sverige (2016)	Prokuratuur (2021)	SpaceNet / Telekom (2022)
Objeto principal	Validade da Diretiva 2006/24 (<i>data retention</i>)	Compatibilidade de regimes nacionais de conservação e acesso	Acesso a dados e admissibilidade como prova em processo penal	Regimes nacionais de conservação de dados (Alemanha)
Posição geral	Invalidação da diretiva por violação de direitos fundamentais	Proibição da conservação generalizada indiscriminada	Reforço das condições de acesso e impacto na prova	Consolidação e refinamento do regime restritivo
Conservação generalizada	Não admissível (violação da proporcionalidade)	Expressamente proibida	Admitida apenas se previamente lícita (regra reafirmada)	Reafirma proibição geral
Exceções à conservação	Não desenvolvidas	Apenas conservação seletiva possível	Mantém lógica de seletividade	Admite exceções muito limitadas (IP, identidade, segurança nacional)
Distinção entre tipos de dados	Não explícita	Residual	Implícita (dados que revelam vida privada)	Forte distinção (dados intrusivos vs. dados simples)
Critério central	Proporcionalidade	Necessidade + proporcionalidade	Gravidade da ingerência	Graduação da intrusividade
Acesso aos dados	Pouco densificado	Deve ser limitado e controlado	Só para criminalidade grave	Mantém exigência rigorosa
Finalidade (uso probatório)	Não diretamente tratado	Apenas criminalidade grave	Criminalidade grave (regra clara)	Reforça e estabiliza
Gravidade da ingerência	Elevada (caráter global da conservação)	Muito grave (vigilância massiva)	Sempre grave, independentemente da duração	Confirma gravidade estrutural
Controlo prévio	Não detalhado	Controlo judicial ou independente obrigatório	Reforça (MP não é independente)	Mantém exigência

Papel do Ministério Público	Não abordado	Não central	Não é autoridade independente	Mantém exclusão
Ligação prova-legalidade	Implícita	Emergente	Forte ligação (ilegalidade → inadmissibilidade possível)	Consolidação
Impacto direto na prova digital	Fundacional	Estruturante	Decisivo (admissibilidade)	

Síntese:

A análise evolutiva da jurisprudência do TJUE em matéria de prova digital, especialmente no que respeita aos dados de comunicações eletrónicas, revela uma trajetória clara de progressiva densificação e restrição do seu regime jurídico. O ponto de partida situa-se no acórdão Digital Rights Ireland (2014), onde o TJUE, ao declarar inválida a Diretiva 2006/24, reconhece simultaneamente o elevado potencial probatório dos metadados e a necessidade de os submeter a um controlo rigoroso à luz do princípio da proporcionalidade. Nesta fase, a preocupação centra-se essencialmente na validade das medidas legislativas que impõem a conservação de dados, sendo ainda incipiente a articulação direta com a admissibilidade processual da prova digital.

Essa articulação começa a ganhar forma no acórdão Tele2 Sverige e Watson (2016), no qual o TJUE procede a uma verdadeira sistematização dos limites à conservação e ao acesso aos dados. Aqui, afirma-se com clareza a proibição da conservação generalizada e indiscriminada, introduzindo-se simultaneamente critérios estruturantes que marcam a evolução subsequente: a necessidade de limitar o acesso aos dados à luta contra a criminalidade grave, a exigência de controlo prévio por uma autoridade independente e a imposição de critérios objetivos que assegurem a ligação entre os dados e a investigação. Neste momento, o enfoque desloca-se da mera validade normativa para a definição de um quadro jurídico de obtenção da prova digital.

O acórdão Prokuratuur (2021) representa um ponto de viragem decisivo, ao estabelecer uma ligação direta e explícita entre a legalidade da obtenção dos dados e a sua admissibilidade enquanto meio de prova em processo penal. O TJUE afirma que o acesso a dados de tráfego e de localização constitui, em regra, uma ingerência grave nos direitos fundamentais, independentemente da quantidade de dados ou da duração do acesso, exigindo por isso a sua limitação à criminalidade grave. Paralelamente, reforça a exigência de controlo prévio por uma autoridade verdadeiramente independente, excluindo expressamente o Ministério Público dessa função, dada a sua posição de parte no processo. Nesta fase, a prova digital deixa de ser apenas uma questão de investigação para assumir pleno relevo processual, sendo avaliada à luz das garantias de um processo equitativo.

Por sua vez, o acórdão SpaceNet/Telekom Deutschland (2022) consolida e refina esta evolução, introduzindo um elemento adicional de diferenciação: a distinção entre categorias de dados em função do seu grau de intrusividade. O Tribunal estabelece uma verdadeira tipologia da prova digital, distinguindo entre dados altamente intrusivos — como os dados de tráfego e localização — e dados menos sensíveis — como os dados de identificação civil ou, em certos casos, os endereços IP. Esta diferenciação permite uma maior flexibilidade no tratamento dos dados menos intrusivos, ao mesmo tempo que reforça a proteção dos dados suscetíveis de revelar o perfil completo da vida privada dos indivíduos. Surge, assim, uma lógica de graduação probatória, que influencia diretamente a admissibilidade, o valor e o controlo de proporcionalidade da prova digital.

Desta evolução resulta uma transformação profunda do regime jurídico aplicável à prova digital. Se, numa fase inicial, o enfoque estava na utilidade funcional dos dados enquanto instrumento de investigação, a jurisprudência mais recente evidencia uma clara tendência para a limitação estrutural da sua obtenção e utilização. O critério decisivo deixa de ser a quantidade de dados recolhidos e passa a ser a sua capacidade de reconstruir a vida privada — o chamado efeito de “profiling”. Consequentemente, a admissibilidade da prova digital passa a depender de um conjunto de requisitos cumulativos: a legalidade do regime de conservação, o respeito pelos princípios da necessidade e da proporcionalidade, a existência de controlo prévio por uma autoridade independente e a sua utilização em contextos de especial gravidade.

Em conclusão, a jurisprudência recente do TJUE revela a consolidação de um modelo altamente exigente de prova digital, no qual a eficácia da investigação criminal é equilibrada com uma tutela reforçada dos direitos fundamentais. A prova baseada em metadados é reconhecida como um instrumento de elevada utilidade probatória, mas a sua admissibilidade está cada vez mais condicionada pela conformidade com o direito da União. Este processo traduz uma verdadeira constitucionalização da prova digital, em que a validade dos meios probatórios depende não apenas da sua relevância para a descoberta da verdade, mas também das condições jurídicas da sua obtenção e das garantias processuais que asseguram a sua utilização legítima [\[x\]](#).

Impacto da jurisprudência do TJUE no ordenamento jurídico e na jurisprudência portuguesa:

A jurisprudência do TJUE em matéria de dados de comunicações eletrónicas — desde Digital Rights Ireland (2014) até SpaceNet/Telekom Deutschland (2022), passando por Tele2 Sverige (2016) e Prokuratuur (2021) — teve um impacto profundo e progressivo no ordenamento jurídico português, tanto ao nível legislativo como jurisprudencial, determinando uma reconfiguração relevante do regime da prova digital.

Desde logo, o impacto mais visível ocorreu no plano normativo, em particular quanto à Lei n.º 32/2008, de 17 de julho (regime de conservação de dados de comunicações eletrónicas) [\[xi\]](#), que

constituía a transposição da Diretiva 2006/24/CE. À semelhança do que aconteceu noutros estados-membros, esta lei previa um regime de conservação generalizada e indiferenciada de dados de tráfego e localização. A jurisprudência do TJUE — especialmente em Digital Rights e, de forma reforçada, em Tele2 — veio colocar em causa a compatibilidade desse regime com o direito da União, ao afirmar a proibição de conservação indiscriminada e a necessidade de critérios seletivos e proporcionais.

Este desenvolvimento teve uma repercussão direta no sistema constitucional português, culminando no acórdão do Tribunal Constitucional n.º 268/2022^[xii], que declarou a inconstitucionalidade de várias normas da Lei n.º 32/2008. O Tribunal Constitucional, seguindo de perto a jurisprudência do TJUE, considerou que a conservação generalizada de dados violava os direitos fundamentais à reserva da vida privada e à autodeterminação informativa. Trata-se de um exemplo paradigmático de “diálogo judicial europeu”, em que o direito da União, tal como interpretado pelo TJUE, funciona como parâmetro relevante para a interpretação constitucional interna.

Do ponto de vista normativo, também existem novidades, através da transposição da Diretiva (UE) 2023/1544, para o acesso, conservação e obtenção de provas eletrónicas em processos penais ^[xiii]

No plano jurisprudencial, o impacto faz-se sentir de forma particularmente intensa na jurisprudência penal portuguesa. Após os acórdãos Tele2 e Prokuratuur, os tribunais portugueses passaram a enfrentar com maior acuidade a questão da admissibilidade da prova digital obtida através de dados de telecomunicações. A partir destes acórdãos, tornou-se claro que não basta que a prova seja relevante para os factos; é necessário que tenha sido obtida em conformidade com um regime legal compatível com o direito da União.

Neste contexto, a jurisprudência portuguesa começou a evidenciar três tendências claras.

Em primeiro lugar, observa-se uma crescente atenção à legalidade da origem da prova digital. Os tribunais passaram a questionar se os dados utilizados em processo penal foram conservados e acedidos de acordo com os critérios estabelecidos pelo TJUE, designadamente quanto à proibição da conservação indiscriminada e à exigência de ligação à criminalidade grave. Isto traduz uma mudança significativa: a prova digital já não é analisada apenas em termos de pertinência ou fiabilidade, mas também quanto à conformidade do seu regime de obtenção.

Em segundo lugar, ganha relevo a exigência de controlo prévio por autoridade independente, densificada no acórdão Prokuratuur. Embora o modelo processual penal português já preveja, em regra, a intervenção do juiz de instrução na autorização de meios de obtenção de prova, a jurisprudência europeia veio reforçar a necessidade de que esse controlo seja efetivo, prévio e independente. Por outro lado, a exclusão do Ministério Público como entidade apta a autorizar o

acesso a dados com forte potencial intrusivo teve impacto relevante na leitura das normas processuais nacionais, sobretudo na delimitação das competências do Ministério Público versus juiz.

Em último lugar, começa a afirmar-se, ainda que de forma gradual, uma maior sensibilidade para a eventual exclusão da prova digital obtida ilegalmente, em linha com o princípio da efetividade desenvolvido na jurisprudência do TJUE. Ainda que o ordenamento português não consagre automaticamente uma regra de exclusão da prova ilícita baseada em direito da União, os tribunais têm em conta, cada vez com maior intensidade, se a utilização desses dados compromete o direito a um processo equitativo, nomeadamente quando a prova digital tem um peso determinante na formação da convicção do tribunal.

Por outro lado, a jurisprudência europeia mais recente, designadamente o acórdão SpaceNet, começa também a influenciar o modo como os tribunais portugueses encaram a natureza dos diferentes tipos de dados. A distinção entre dados altamente intrusivos (como tráfego e localização) e dados menos sensíveis (como dados de identificação) contribui para uma abordagem mais diferenciada da prova digital, permitindo maior flexibilidade em relação a certos tipos de informação, mas mantendo um nível elevado de exigência para dados com maior potencial de invasão da vida privada.

Do ponto de vista sistemático, esta evolução tem conduzido a uma verdadeira reconfiguração da teoria da prova digital no direito português. A prova baseada em metadados deixou de ser analisada como um mero instrumento técnico de investigação para passar a ser enquadrada numa lógica constitucional e europeia de proteção de direitos fundamentais. A admissibilidade da prova depende agora de um conjunto de requisitos que transcendem o direito processual penal interno, incluindo a conformidade com o direito da União, a proporcionalidade da ingerência e a existência de garantias institucionais adequadas.

Em conclusão, a jurisprudência do TJUE teve um impacto profundo no ordenamento jurídico português, promovendo uma revisão crítica do regime de conservação e acesso a dados, influenciando decisivamente a jurisprudência constitucional e reorientando a prática dos tribunais penais. Este impacto traduz-se numa crescente exigência de legalidade, proporcionalidade e controlo na obtenção da prova digital, consolidando um modelo em que a eficácia da investigação penal deve coexistir com uma forte tutela dos direitos fundamentais.

A jurisprudência portuguesa recente — do STJ e dos Tribunais da Relação — evidencia de forma clara o impacto profundo da evolução do direito da UE em matéria de prova digital, especialmente no que respeita à utilização de dados de comunicações eletrónicas como meio probatório. Essa influência é particularmente visível em acórdãos proferidos após a consolidação da jurisprudência do TJUE (Digital Rights, Tele2, Prokuratuur e, mais recentemente, SpaceNet), refletindo uma progressiva reconfiguração das categorias tradicionais do processo penal.

No âmbito do STJ, não se identifica propriamente um acórdão isolado com carácter fundacional, mas sim uma linha jurisprudencial consolidada. Assim, a título meramente exemplificativo, assume particular relevância o acórdão do STJ de 30 de setembro de 2020 (Proc. n.º 158/17.8JAFUN.L1.S1, Rel. Manuel Braz), no qual se reconhece que os dados de telecomunicações constituem um meio probatório particularmente relevante, embora deva ser assegurado o respeito pelas exigências legais e constitucionais quanto à sua obtenção. Neste aresto, afirma-se expressamente que «os dados de comunicações [...] são suscetíveis de constituir relevante meio de prova, desde que obtidos no respeito pelas exigências legais e constitucionais» [\[xiv\]](#).

Posteriormente, o acórdão do STJ de 16 de março de 2022 (Proc. n.º 105/20.7JELSB.L1.S1, Rel. Nuno Gonçalves) vem aprofundar esta orientação, já sob influência direta da jurisprudência do TJUE e do acórdão do Tribunal Constitucional n.º 268/2022. O Tribunal sublinha a necessidade de um controlo judicial efetivo sempre que esteja em causa a recolha de prova envolvendo ingerências relevantes na esfera da vida privada, afirmando que «a obtenção e utilização de prova carece de controlo jurisdicional quando esteja em causa ingerência em direitos fundamentais» [\[xv\]](#).

No plano das Relações, o impacto da jurisprudência europeia e constitucional surge com maior intensidade. O acórdão da Relação de Lisboa de 5 de julho de 2022 (Proc. n.º 184/20.3JELSB.L1-5, Rel. Jorge Gonçalves) [\[xvi\]](#) constitui um exemplo paradigmático, ao analisar a admissibilidade da prova obtida ao abrigo da Lei n.º 32/2008 após a sua declaração de inconstitucionalidade. Neste contexto, o tribunal afirma que a utilização de dados conservados em regime incompatível com os direitos fundamentais não pode ser aceite sem uma ponderação rigorosa da sua validade.

No mesmo sentido, o acórdão da Relação do Porto de 22 de junho de 2022 (Proc. n.º 478/19.0JAPRT.P1, Rel. Henrique Araújo) [\[xvii\]](#) reconhece que a ilegalidade na obtenção dos dados pode contaminar a validade da prova, aproximando-se da lógica desenvolvida pelo TJUE no acórdão Prokuratuur, ao estabelecer uma ligação entre a legalidade da obtenção e a admissibilidade probatória.

Por sua vez, o acórdão da Relação de Guimarães de 13 de fevereiro de 2023 (Proc. n.º 122/21.0GBVNF.G1, Rel. Sérgio Silva) [\[xviii\]](#) aborda diretamente a questão da exclusão da prova digital obtida de forma irregular, enfatizando a necessidade de salvaguarda do direito a um processo equitativo e a importância do contraditório.

Já o acórdão da Relação de Coimbra de 14 de dezembro de 2022 (Proc. n.º 91/21.0GBCLD.C1, Rel. Vasques Osório) [\[xix\]](#) reflete uma abordagem particularmente estruturada, analisando a admissibilidade da prova digital à luz dos princípios da proporcionalidade e da legalidade da obtenção, numa lógica claramente influenciada pelo direito da União.

Em termos globais, estes acórdãos demonstram que a jurisprudência portuguesa evoluiu significativamente, passando de uma abordagem centrada na utilidade e fiabilidade da prova digital para uma perspetiva mais exigente, que integra a legalidade do regime de conservação e acesso, o

respeito pelos direitos fundamentais e a necessidade de controlo judicial efetivo. Observa-se ainda alguma divergência quanto à consequência da ilegalidade — sobretudo entre exclusão automática ou ponderação —, mas existe um ponto comum inequívoco: a prova digital deixou de ser um meio neutro de investigação para passar a ser um instrumento juridicamente condicionado, cuja validade depende cada vez mais do cumprimento dos *standards* europeus definidos pelo TJUE^[xx].

II.2 – Matéria civil

No domínio civil e comercial, a jurisprudência relativa à prova digital desenvolveu-se de forma distinta da verificada no plano penal, assumindo uma orientação mais funcional e centrada na equivalência entre meios eletrónicos e tradicionais, embora progressivamente densificada quanto aos critérios de fiabilidade, integridade e controlo. Este desenvolvimento resulta, por um lado, da jurisprudência do TJUE e, por outro, da concretização realizada pelos tribunais portugueses, designadamente pelo STJ e pelos Tribunais da Relação.

No plano do direito da União, um dos primeiros acórdãos relevantes é o acórdão *Content Services* (C-49/11, de 5 de julho de 2012^[xxi]), no qual o TJUE analisa a forma de prestação de informação em contratos celebrados à distância. O TJUE afirmou que a simples disponibilização de informação num *website* não é suficiente para cumprir os requisitos legais, sendo necessário que essa informação seja fornecida em suporte que permita a sua conservação e reprodução futura. Este acórdão introduz, assim, critérios fundamentais para a prova digital em matéria civil: a exigência de durabilidade, acessibilidade e possibilidade de reprodução, que funcionam como garantias mínimas da fiabilidade do suporte eletrónico.

Essa linha é desenvolvida no acórdão *BAWAG* (C-375/15, de 25 de janeiro de 2017^[xxii]), no qual o TJUE reconhece a validade da comunicação eletrónica através de plataformas digitais (como caixas de correio bancárias online), desde que o consumidor possa aceder facilmente à informação e esta seja armazenada de modo duradouro. Neste contexto, o TJUE consolida a noção de “suporte duradouro”, essencial para a validade e para o valor probatório da comunicação digital, reconhecendo implicitamente que os registos eletrónicos podem servir como meios de prova desde que assegurem a conservação estável da informação.

Paralelamente, a jurisprudência do TJUE relativa ao Regulamento eIDAS (Regulamento n.º 910/2014) tem desempenhado um papel estruturante, ao consagrar o princípio da equivalência funcional entre documentos digitais e documentos em suporte papel. Ainda que não exista um único acórdão estruturante, o entendimento consolidado é o de que as assinaturas eletrónicas qualificadas têm o mesmo valor jurídico que assinaturas manuscritas, sendo inadmissível uma discriminação baseada no suporte digital. Este princípio projeta-se diretamente na prova civil, reforçando a admissibilidade e o valor probatório dos documentos eletrónicos.

No ordenamento português, estes princípios têm sido progressivamente concretizados e densificados pela jurisprudência, com especial enfoque na admissibilidade e valoração de emails, documentos eletrónicos e registos informáticos.

No domínio civil e comercial, a evolução da prova digital apresenta características distintas, traduzindo-se numa lógica predominantemente funcional e tecnicamente orientada.

No âmbito do Supremo Tribunal de Justiça, destaca-se o acórdão de 5 de junho de 2018 (Proc. n.º 182/15.8T8BRG.G1.S1, Rel. Abrantes Geraldês)[\[xxiii\]](#), no qual se reconhece que o email constitui um documento particular, podendo assumir valor probatório relevante, sujeito, contudo, à eventual impugnação da sua autenticidade.

Por sua vez, o acórdão do STJ de 27 de outubro de 2020 (Proc. n.º 2198/17.5T8VNG.P1.S1, Rel. Ilídio Sacarrão Martins)[\[xxiv\]](#) afirma a aplicabilidade do princípio da livre apreciação da prova, sublinhando que os documentos eletrónicos devem ser avaliados quanto à sua credibilidade, autenticidade e coerência.

No mesmo sentido, o acórdão do STJ de 17 de junho de 2021 (Proc. n.º 1786/18.0T8BRG.G1.S1, Rel. José Rainho)[\[xxv\]](#) reconhece a validade dos contratos eletrónicos e admite os registos informáticos como meio de prova da formação da vontade negocial.

Ao nível das Relações, o acórdão da Relação de Lisboa de 21 de fevereiro de 2019 (Proc. n.º 969/17.0T8LSB.L1-1, Rel. Pedro Martins)[\[xxvi\]](#) confirma a relevância dos emails como meio de prova da formação de acordos e negociações comerciais.

Por seu turno, o acórdão da Relação do Porto de 28 de janeiro de 2020 (Proc. n.º 196/19.0T8PRT.P1, Rel. Rui Moreira)[\[xxvii\]](#) sublinha que os registos informáticos só assumem valor probatório pleno se estiverem garantidas a sua fiabilidade técnica e integridade.

Finalmente, o acórdão da Relação de Coimbra de 13 de julho de 2021 (Proc. n.º 254/19.0T8VIS.C1, Rel. Manuel Capelo)[\[xxviii\]](#) destaca a necessidade de perícia informática em casos em que a prova digital apresente complexidade técnica, enquanto o acórdão da Relação de Guimarães de 24 de fevereiro de 2022 (Proc. n.º 378/20.8T8VRL.G1, Rel. Jorge Teixeira)[\[xxix\]](#) enfatiza a importância do controlo da autenticidade e da prevenção da manipulação dos dados digitais.

Em matéria de prova digital, com doutrina e destaques jurisprudenciais, destacaria ainda as seguintes obras[\[xxx\]](#).

Em síntese conclusiva, a evolução conjugada da jurisprudência do TJUE e dos tribunais portugueses revela a consolidação de um modelo de prova digital em matéria civil e comercial assente em três ideias fundamentais. Em primeiro lugar, afirma-se o princípio da equivalência funcional, segundo o qual os meios digitais têm o mesmo valor jurídico que os meios tradicionais, desde que respeitem determinados requisitos. Em segundo lugar, reforça-se a exigência de

fiabilidade técnica, traduzida nos critérios de durabilidade, acessibilidade e integridade da informação. Em último lugar, consolida-se o modelo da livre apreciação da prova digital, em que o julgador avalia casuisticamente a autenticidade e a credibilidade dos meios eletrónicos, podendo recorrer a instrumentos técnicos de validação.

Diferentemente do domínio penal — onde a prova digital é fortemente condicionada por exigências de legalidade e restrição —, no plano civil e comercial predomina uma lógica de aceitação e valoração, ainda que sujeita a um escrutínio técnico crescente. O resultado é um sistema probatório híbrido, em que a digitalização das relações jurídicas é plenamente reconhecida, mas exige uma adaptação contínua dos critérios tradicionais de prova às especificidades tecnológicas.

A evolução mais recente da jurisprudência em matéria civil e comercial sobre prova digital — sobretudo no período posterior a 2020 — revela uma transformação progressiva, ainda que menos visível do que no domínio penal, mas não menos relevante do ponto de vista sistemático. Trata-se de uma evolução marcada não tanto por grandes acórdãos estruturantes do TJUE, mas antes por uma consolidação de princípios e por uma crescente densificação da sua aplicação prática na jurisprudência nacional.

No plano do direito da União, o desenvolvimento mais recente não se traduz na emergência de um novo *leading case* semelhante aos acórdãos *Tele2* ou *Prokuratuur*, mas sim num reforço consistente de linhas jurisprudenciais já estabelecidas. Em particular, a noção de “suporte duradouro”, construída a partir dos acórdãos *Content Services* e *BAWAG*, continua a assumir um papel central. O TJUE tem afirmado, de forma reiterada, que a relevância jurídica de uma comunicação digital depende da sua capacidade de ser armazenada de forma estável, de não poder ser alterada unilateralmente e de permanecer acessível ao destinatário. Estes requisitos funcionam como critérios técnicos mínimos de admissibilidade da prova digital, traduzindo uma preocupação com a integridade e a permanência da informação.

Paralelamente, o desenvolvimento do quadro normativo europeu, sobretudo através do Regulamento eIDAS, contribuiu para consolidar o princípio da equivalência funcional entre meios digitais e tradicionais. A ideia de que documentos eletrónicos, assinaturas digitais e selos eletrónicos não podem ser discriminados face aos seus equivalentes em papel tornou-se um verdadeiro princípio estruturante. Mais do que uma mera equiparação formal, esta equivalência implica que a prova digital seja plenamente admissível no processo civil, desde que cumpra requisitos de fiabilidade técnica. Assim, a discussão desloca-se progressivamente da admissibilidade para a análise da qualidade e credibilidade da prova.

Um outro vetor relevante da evolução recente conecta-se com a expansão do comércio eletrónico e das plataformas digitais. Ainda que o TJUE não tenha proferido decisões diretamente centradas na prova digital, a sua jurisprudência nestes domínios tem reconhecido implicitamente a validade de elementos como *logs* informáticos, históricos de transações e comunicações eletrónicas enquanto suporte factual das relações jurídicas digitais. Este reconhecimento reforça a ideia de que

a realidade probatória no comércio contemporâneo é essencialmente digital, exigindo uma adaptação dos modelos tradicionais.

No que respeita ao ordenamento jurídico português, a evolução recente é mais visível e concretizada. Os tribunais, em especial o Supremo Tribunal de Justiça e os Tribunais da Relação, têm vindo a aprofundar a análise da prova digital, não tanto ao nível da sua admissibilidade — que é amplamente aceite —, mas sobretudo quanto ao seu valor probatório. Observa-se uma clara transição de um modelo de aceitação quase automática, baseado na analogia com a prova documental tradicional, para um modelo de validação técnica exigente.

Em primeiro lugar, a jurisprudência mais recente evidencia uma crescente exigência de verificação da autenticidade dos meios digitais. Os tribunais passaram a valorizar de forma mais intensa a origem da prova — quem a produziu, em que contexto, e com que garantias de fiabilidade —, reconhecendo que a facilidade de manipulação de dados digitais exige uma abordagem mais cautelosa. A autenticidade deixa de ser presumida para se tornar objeto de análise concreta.

Em segundo lugar, assume crescente relevância a questão da integridade e da rastreabilidade da informação. Elementos como *logs* de sistemas, registos informáticos ou comunicações eletrónicas só são valorizados na medida em que seja possível assegurar que não foram alterados e que existe um rasto verificável da sua produção e conservação. Este aspeto aproxima a jurisprudência portuguesa das exigências técnicas desenvolvidas no contexto europeu, ainda que adaptadas ao princípio da livre apreciação da prova.

Em último lugar, verifica-se uma valorização crescente da prova pericial em matéria digital. A complexidade técnica dos sistemas informáticos leva os tribunais a recorrer mais frequentemente a perícias especializadas, designadamente para verificar a autenticidade de emails, a integridade de ficheiros ou o funcionamento de sistemas informáticos. Esta tendência evidencia a emergência de uma dimensão técnico-científica da prova digital, que ultrapassa os modelos tradicionais de apreciação judicial.

Além disso, a jurisprudência recente sugere, ainda que de forma implícita, uma diferenciação entre tipos de prova digital. Certos meios — como documentos assinados digitalmente com certificação qualificada — tendem a beneficiar de maior credibilidade, enquanto outros — como emails simples ou capturas de ecrã — são tratados com maior cautela e frequentemente exigem confirmação adicional. Esta diferenciação aproxima-se da lógica europeia de graduação da intrusividade ou fiabilidade dos dados, ainda que adaptada ao contexto civil.

Em termos evolutivos, pode afirmar-se que o sistema passou de uma fase inicial de mera aceitação formal da prova digital para uma fase de maturidade caracterizada pelo seu escrutínio técnico. Se, anteriormente, a principal preocupação era a de admitir os meios digitais como prova, hoje a questão central reside na sua validação e na determinação do seu valor probatório concreto.

Em conclusão, a fase mais recente da evolução revela um modelo equilibrado e sofisticado. A prova digital é hoje plenamente aceite no direito civil e comercial, refletindo a transformação digital da sociedade e da economia. No entanto, essa aceitação é acompanhada por um aumento significativo das exigências de controlo, assente em critérios como autenticidade, integridade, durabilidade e acessibilidade. Diferentemente do que sucede no domínio penal — onde a prova digital é fortemente condicionada por exigências de legalidade e proteção de direitos fundamentais —, no campo civil predomina uma lógica de abertura e valoração, mas com uma crescente tecnicização. O resultado é um sistema probatório dinâmico, que procura conciliar a flexibilidade necessária à realidade digital com a segurança jurídica indispensável à decisão judicial.

A evolução global da prova digital revela, assim, uma dualidade estrutural:

No domínio penal, predomina um modelo restritivo, constitucionalizado e orientado para a proteção dos direitos fundamentais, em que a prova digital é admissível apenas sob condições rigorosas de legalidade e controlo.

No domínio civil e comercial, prevalece um modelo permissivo, baseado na equivalência funcional e na livre apreciação da prova, mas progressivamente tecnicizado.

Esta diferenciação resulta da distinta natureza dos interesses em presença: enquanto no processo penal está em causa o exercício do poder punitivo do Estado, justificando um controlo reforçado, no processo civil prevalece a autonomia das partes e a necessidade de adaptar o sistema probatório à realidade digital das relações jurídicas.

III. Conclusão geral

A prova digital ocupa hoje um lugar central nos sistemas jurídicos europeu e português, mas sob regimes diferenciados. No domínio penal, afirma-se um paradigma de limitação estrutural, em que a admissibilidade depende da conformidade com direitos fundamentais e com o direito da União. No domínio civil, consolida-se um paradigma de aceitação funcional, em que a prova digital é plenamente admissível, desde que respeite critérios técnicos de fiabilidade [\[xxxi\]](#).

Em termos sintéticos, a evolução pode ser traduzida na seguinte fórmula:

No processo penal, a prova digital é restringida para proteger; no processo civil, é admitida, mas tecnicamente escrutinada. Este duplo modelo revela a adaptação do direito à transformação digital, procurando conciliar a eficácia dos meios tecnológicos com a salvaguarda dos valores fundamentais do sistema jurídico e dos direitos fundamentais.

Segue proposta de quadro comparativo sobre a prova digital entre o TJUE e Portugal:

Quadro comparativo: prova digital (TJUE vs. Portugal)

Tema	TJUE (União Europeia)	Portugal
Fundamento jurídico	Carta dos Direitos Fundamentais da UE (arts. 7.º e 8.º – vida privada e proteção de dados)	Constituição da República Portuguesa (arts. 26.º, 34.º e 35.º – vida privada, comunicações e dados)
Natureza dos dados digitais	Dados pessoais e metadados (IP, localização, tráfego) altamente intrusivos e protegidos	Emails, dados informáticos e comunicações equiparados a correspondência ou documentos
Retenção de dados	Proibição de retenção generalizada e indiscriminada (Digital Rights Ireland; Tele2)	Restrições reforçadas após jurisprudência do Tribunal Constitucional
Acesso aos dados pelas autoridades	Exige finalidade legítima (p. ex., criminalidade grave) + controlo judicial/independente	Necessidade de autorização judicial (Lei do Cibercrime e CPP)
Controle jurisdicional	Deve existir controlo prévio ou por entidade independente	Juiz de instrução assume controlo direto e material da prova
Valoração da prova digital	Afetada pela legalidade da obtenção (violação pode comprometer utilização)	Apreensão válida não basta — juiz deve avaliar conteúdo e relevância
Decisões automatizadas / IA	Intervenção humana deve ser efetiva e significativa (caso OQ v. Land Hessen)	Ainda sem jurisprudência estruturada equivalente, mas aplicam-se princípios constitucionais

Segue proposta de quadro sistémico integrado da prova digital entre a jurisprudência do TJUE e a nacional em matéria penal e civil:

1. MATRIZ GERAL

Dimensão	Penal (TJUE)	Penal (Portugal)	Civil/Comercial (TJUE)	Civil/Comercial (Portugal)
Função da prova digital	Instrumento de investigação altamente intrusivo	Meio probatório relevante, mas condicionado	Meio normal de documentação das relações jurídicas	Meio probatório central nas relações económicas
Posição de princípio	Restritiva	Restritiva (influência europeia)	Permissiva	Permissiva
Critério central	Proteção de direitos fundamentais	Legalidade e constitucionalidade	Equivalência funcional	Livre apreciação + fiabilidade
Natureza da ingerência	Sempre grave (dados telecomunicações)	Grave (segundo TJUE)	Não qualificada como ingerência grave	Sem qualificação constitucional forte

2. OBTENÇÃO DA PROVA DIGITAL

Critério	Penal (TJUE)	Penal (Portugal)	Civil/Comercial (TJUE)	Civil/Comercial (Portugal)
Legalidade da recolha	Essencial (condição de admissibilidade)	Central (após TC 268/2022)	Pouco problematizada	Relevante, mas não estruturante
Conservação de dados	Proibida se generalizada (Digital Rights, Tele2, SpaceNet)	Lei 32/2008 limitada/inconstitucional	Admitida sem restrições estruturais	Aceite
Finalidade	Criminalidade grave	Criminalidade grave	Relações jurídicas privadas	Relações jurídicas privadas
Seleção dos dados	Deve ser dirigida	Tendência crescente	Não exigida	Não exigida

3. CONTROLO E GARANTIAS

Critério	Penal (TJUE)	Penal (Portugal)	Civil/Comercial (TJUE)	Civil/Comercial (Portugal)
Controlo prévio	Obrigatório (juiz ou entidade independente)	Juiz de instrução	Não exigido	Não exigido
Ministério Público	Não independente (Prokuratuur)	Não substitui juiz	Sem relevância	Sem relevância
Crítérios legais claros	Obrigatórios	Reforçados	Não estruturantes	Não estruturantes

4. ADMISSIBILIDADE DA PROVA

Critério	Penal (TJUE)	Penal (Portugal)	Civil/Comercial (TJUE)	Civil/Comercial (Portugal)
Ligação obtenção-admissibilidade	Direta (Prokuratuur)	Crescente	Fraca	Fraca
Prova ilícita	Pode exigir exclusão	Divergência (exclusão vs ponderação)	Não central	Avaliada casuisticamente
Crítério principal	Processo equitativo	Constituição + UE	Validade funcional	Livre apreciação

5. VALORAÇÃO DA PROVA DIGITAL

Crítério	Penal	Civil/Comercial
Modelo geral	Restritivo	Livre apreciação
Peso probatório	Muito elevado, mas condicionado	Variável
Fator decisivo	Legalidade da obtenção	Fiabilidade técnica
Análise judicial	Jurídico-constitucional	Técnico-probatória

6. DIFERENCIAÇÃO DOS DADOS DIGITAIS

Tipo de dados	Penal (TJUE + Portugal)	Civil/Comercial (Portugal)
Dados de tráfego/localização	Altamente protegidos	Pouco relevantes
Dados de identificação	Regime mais flexível	Normalmente aceites
Emails simples	Contexto probatório frágil	Documento sujeito a apreciação
Assinaturas digitais qualificadas	Forte valor	Muito forte valor
Logs informáticos	Relevantes, mas condicionados	Valorizados se fráveis

7. EVOLUÇÃO GERAL

Fase	Penal	Civil/Comercial
Inicial	Aceitação funcional	Aceitação documental
Intermédia	Limitação (Tele2)	Equiparação digital
Atual	Restrição estrutural + constitucionalização	Tecnicização e validação

Bibliografia:

LEMONS TRIUNFANTE, Luís, *Manual de Cooperação Judiciária Internacional em Matéria penal*, 2.^a Edição, Almedina 2026

JUSZCZAK, Adam e SASON, Elisa, *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice An Introduction to the New EU Package on E-evidence*, disponível em <https://eucrim.eu/media/articles/pdf/eucrim-article-2023-014.pdf>.

FRANSSEN, Vanessa e TOSZA, Stanislaw, *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2025

BIASIOTTI, Maria Angela, BONNICI, Jeanne Pia Mifsud, CANNATACI, TURCHI, Fabrizio *Handling and Exchanging Electronic Evidence Across Europe*, Springer, 2018

FLANDER, Benjamin e ERBERZNIK, Anže, *TOOLKIT FOR HANDLING AND ADMISSIBILITY OF ELECTRONIC EVIDENCE Empowering Legal Practitioners to Critically Review E-Evidence from the Procedural Rights Perspective*, Koper, 2024, disponível em [https://www.researchgate.net/profile/Anze-](https://www.researchgate.net/profile/Anze-Erberznik/publication/382952245_Toolkit_for_Handling_and_Admissibility_of_Electronic_Evidence_Empowering_Legal_Practitioners_to_Critically_Review_E-Evidence_from_the_Procedural_Rights_Perspective/links/66da31ed64f7bf7b199976af/Toolkit-for-Handling-and-Admissibility-of-Electronic-Evidence-Empowering-Legal-Practitioners-to-Critically-Review-E-Evidence-from-the-Procedural-Rights-Perspective.pdf)

[Erberznik/publication/382952245_Toolkit_for_Handling_and_Admissibility_of_Electronic_Evidence_Empowering_Legal_Practitioners_to_Critically_Review_E-Evidence_from_the_Procedural_Rights_Perspective/links/66da31ed64f7bf7b199976af/Toolkit-for-Handling-and-Admissibility-of-Electronic-Evidence-Empowering-Legal-Practitioners-to-Critically-Review-E-Evidence-from-the-Procedural-Rights-Perspective.pdf](https://www.researchgate.net/profile/Anze-Erberznik/publication/382952245_Toolkit_for_Handling_and_Admissibility_of_Electronic_Evidence_Empowering_Legal_Practitioners_to_Critically_Review_E-Evidence_from_the_Procedural_Rights_Perspective/links/66da31ed64f7bf7b199976af/Toolkit-for-Handling-and-Admissibility-of-Electronic-Evidence-Empowering-Legal-Practitioners-to-Critically-Review-E-Evidence-from-the-Procedural-Rights-Perspective.pdf)

DIAS MEIRELES, Ana Isa, *Prova Digital no Processo Judicial - A Blockchain e Outros Caminhos para os Tribunais* - Almedina 2023,

MATOS BRANDÃO, Diogo de, *A prova digital no processo civil, repensar o Sistema*, Nova Causa, braga, 2020; SILVA PEREIRA, Fernando, *Prova Eletrónica em Processo Civil*, Almedina, março 2026,

SIMÃO, Rui, *Ativos digitais no Direito Civil*, Almedina 2026,

PINTO MONTEIRO, António Pedro, *Garantias processuais e prova digital*, disponível em <https://portal.oa.pt/media/144059/antonio-pedro-pinto-monteiro.pdf>

SOUSA E SILVA, Nuno, *Lições de Direito Digital*, Almedina 2026

[i] O artigo visou apresentar uma seleção de acórdãos recentes do Tribunal Constitucional (2021 e 2024), proferidos em sede de fiscalização abstrata e fiscalização concreta da constitucionalidade, sobre aspetos relevantes suscitados pelo regime da prova digital. A autora refere ainda que a seleção coligida pretende auxiliar os tribunais de primeira instância na apreciação de questões jurídico-constitucionais em matéria de prova digital no inquérito.

[ii] O artigo não tem a ambição de proceder a um levantamento exaustivo de toda a jurisprudência existente até à data, mas sim servir como guião de consulta e navegação na jurisprudência europeia e nacional mais relevantes, em matérias penal e civil, com sugestões de quadros comparativos e de análise.

[iii] Aborda as matérias de «Comunicações eletrónicas — Diretiva 2006/24/CE — Serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações — Conservação de dados gerados ou tratados no contexto da oferta desses serviços — Validade — artigos 7.º, 8.º e 11.º da Carta dos Direitos Fundamentais da União Europeia», disponível em [/https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0293](https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0293)

[iv] Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32006L0024>

[v] Aborda as matérias de: “«Reenvio prejudicial — Comunicações eletrónicas — Tratamento de dados pessoais — Confidencialidade das comunicações eletrónicas — Proteção — Diretiva 2002/58/CE — artigos 5.º, 6.º e 9.º bem como artigo 15.º, n.º 1 — Carta dos Direitos Fundamentais da União Europeia — artigos 7.º, 8.º e 11.º bem como artigo 52.º, n.º 1 — Legislação nacional — Prestadores de serviços de comunicações eletrónicas — Obrigação que incide sobre a conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização — Autoridades nacionais — Acesso aos dados — Inexistência de um controlo prévio por parte de um órgão jurisdicional ou uma autoridade administrativa independente — Compatibilidade com o direito da União», disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62015CJ0203>

[vi] Aborda as matéria de: “«Reenvio prejudicial — Tratamento de dados pessoais no setor das comunicações eletrónicas — Diretiva 2002/58/CE — Prestadores de serviços de comunicações eletrónicas — Confidencialidade das comunicações — Limitações — artigo 15.º, n.º 1 — artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia — Legislação que prevê a conservação generalizada e indiferenciada dos dados relativos ao tráfego e dos dados de localização pelos prestadores de serviços de comunicações eletrónicas — Acesso das autoridades nacionais aos dados conservados para efeitos de inquéritos — Luta contra a criminalidade em geral — Autorização dada pelo Ministério Público — Utilização dos dados no âmbito do processo penal enquanto elementos de prova — Admissibilidade», disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62018CJ0746>

[vii] Disponível em https://www.europarl.europa.eu/charter/pdf/text_pt.pdf

[viii] Aborda as matérias: «Reenvio prejudicial — Tratamento de dados pessoais no setor das comunicações eletrónicas — Prestadores de serviços de comunicações eletrónicas — Prestadores de serviços de armazenamento e fornecedores de acesso à Internet — Conservação generalizada e indiferenciada de dados de tráfego e de dados de localização — Análise automatizada de dados — Acesso em tempo real aos dados — Salvaguarda da segurança nacional e luta contra o terrorismo — Luta contra a criminalidade — o Diretiva 2002/58/CE — Âmbito de aplicação — artigo 1.º, n.º 3 e artigo 3.º — Confidencialidade das comunicações eletrónicas — Proteção — artigo 5.º e artigo 15.º, n.º1 — Diretiva 2000/31/CE — Âmbito de aplicação — Carta dos Direitos Fundamentais da União Europeia — artigos 4.º, 6.º, 8.º e 11.º e artigo 52.º, n.º 1 — artigo 4.º, n.º 2, TUE» , disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62018CJ0511>

[ix] Aborda as matérias: «Reenvio prejudicial — Tratamento de dados pessoais no setor das comunicações eletrónicas — Confidencialidade das comunicações — Prestadores de serviços de comunicações eletrónicas — Conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização — Diretiva 2002/58/CE — artigo 15.º, n.º1 — artigos 6.º, 7.º, 8.º, 11.º 1 — Carta dos Direitos Fundamentais da União e artigo 52.º Nos processos apensos C-793/19 e C-794/19, , n.º 1

— artigo 4.º , n.º 2, TUE», disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62019CJ0793>

[x] Para maior desenvolvimento sobre a prova digital na União Europeia ver LEMOS TRIUNFANTE, Luís, *Manual de Cooperação Judiciária Internacional em Matéria penal*, 2.ª Edição, Almedina 2026, em concreto Capítulo I 3.6 Estratégia europeia para a justiça eletrónica 2024-2028, págs. 67 e ss. Capítulo III 12.15. Prova eletrónica – acesso transfronteiriço a meios de prova eletrónicos, págs. 426 e ss. Capítulo IV 2. O novo paradigma da obtenção da prova digital na UE, págs. 537 a 547, e indicação da respetiva bibliografia, e JUSZCZAK, Adam e SASON, Elisa, *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice An Introduction to the New EU Package on E-evidence*, disponível em <https://eucrim.eu/media/articles/pdf/eucrim-article-2023-014.pdf>. Sobre a utilização da prova digital nas investigações criminais, FRANSSEN, Vanessa e TOSZA, Stanislaw, *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2025, e sobre as bases europeias, BIASIOTTI, Maria Angela, BONNICI, Jeanne Pia Mifsud, CANNATACI, TURCHI, Fabrizio *Handling and Exchanging Electronic Evidence Across Europe*, Springer, 2018 e sobre a admissibilidade da prova eletrónica, FLANDER, Benjamin e ERBERZNIK, Anže, *TOOLKIT FOR HANDLING AND ADMISSIBILITY OF ELECTRONIC EVIDENCE Empowering Legal Practitioners to Critically Review E-Evidence from the Procedural Rights Perspective*, Koper, 2024, disponível em https://www.researchgate.net/profile/Anze-Erberznik/publication/382952245_Toolkit_for_Handling_and_Admisibility_of_Electronic_Evidence_Empowering_Legal_Practitioners_to_Critically_Review_E-Evidence_from_the_Procedural_Rights_Perspective/links/66da31ed64f7bf7b199976af/Toolkit-for-Handling-and-Admissibility-of-Electronic-Evidence-Empowering-Legal-Practitioners-to-Critically-Review-E-Evidence-from-the-Procedural-Rights-Perspective.pdf

[xi] Já com três alterações decorrentes das Leis n.º 79/2021 de 24.11, 18/2024, de 05.02 e 18/2024, de 05.02, disponível em https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1264&tabela=leis

[xii] Disponível em <https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html>

[xiii] Muito recentemente em comunicado do Conselho de Ministros de 21.05.2026 o Governo anunciou: 11. *Aprovou uma Proposta de Lei que cria um enquadramento jurídico, através da transposição da Diretiva (UE) 2023/1544, para o acesso, conservação e obtenção de provas eletrónicas em processos penais. O diploma reforça a capacidade do Estado para combater a cibercriminalidade e reduzir a impunidade no espaço digital. Concretamente, é prevista a obrigação de os prestadores de serviços digitais que operam na UE designarem um estabelecimento ou representante legal para responder a ordens judiciais, a definição de procedimentos rápidos para conservar e entregar dados eletrónicos, a atribuição de competências neste domínio à ANACOM e ao Ministério Público e a criação de um regime sancionatório com coimas elevadas e sanções acessórias em caso de incumprimentos*; disponível em <https://portugal.gov.pt/gc25/governo/comunicados-do->

[xiv] STJ, Ac. de 30.09.2020, Proc. n.º 158/17.8JAFUN.L1.S1, Rel. Manuel Braz.

[xv] STJ, Ac. de 16.03.2022, Proc. n.º 105/20.7JELSB.L1.S1, Rel. Nuno Gonçalves

[xvi] TRL, Ac. de 05.07.2022, Proc. n.º 184/20.3JELSB.L1-5, Rel. Jorge Gonçalves.

[xvii] TRP, Ac. de 22.06.2022, Proc. n.º 478/19.0JAPRT.P1, Rel. Henrique Araújo.

[xviii] TRG, Ac. de 13.02.2023, Proc. n.º 122/21.0GBVNF.G1, Rel. Sérgio Silva.

[xix] TRC, Ac. de 14.12.2022, Proc. n.º 91/21.0GBCLD.C1, Rel. Vasques Osório.

[xx] Nesta área, ver extensas nota prática de jurisprudência sobre prova digital n.º 16/2020, de 19 de março de 2020 cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_16_jurisprudencia_prova_digital_2.pdf e jurisprudência temática de Direito Processual Penal n.º 110 – janeiro 2022 – prova digital [/https://carlospintodeabreu.com/wp-content/uploads/2023/01/prova-digital-jurisprudencia.pdf](https://carlospintodeabreu.com/wp-content/uploads/2023/01/prova-digital-jurisprudencia.pdf)

[xxi] Aborda as matérias de: «Reenvio prejudicial — Diretiva 97/7/CE — Proteção dos consumidores — Contratos à distância — Informação do consumidor — Informações fornecidas ou recebidas — Suporte durável — Conceito — Hiperligação no sítio Internet do fornecedor — Direito de rescisão», disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62011CJ0049>

[xxii] Aborda as matérias de: «Reenvio prejudicial — Diretiva 2007/64/CE — Serviços de pagamento no mercado interno — Contratos-quadro — Informação geral prévia — Dever de fornecer essa informação em papel ou noutro suporte duradouro — Informações transmitidas através de uma caixa de correio eletrónico integrada num sítio Internet de banca em linha», disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62015CJ0375>

[xxiii] STJ, Ac. de 05.06.2018, Proc. n.º 182/15.8T8BRG.G1.S1, Rel. Abrantes Geraldês.

[xxiv] STJ, Ac. de 27.10.2020, Proc. n.º 2198/17.5T8VNG.P1.S1, Rel. Ilídio Sacarrão Martins.

[xxv] STJ, Ac. de 17.06.2021, Proc. n.º 1786/18.0T8BRG.G1.S1, Rel. José Rainho.

[xxvi] TRL, Ac. de 21.02.2019, Proc. n.º 969/17.0T8LSB.L1-1, Rel. Pedro Martins.

[xxvii] TRP, Ac. de 28.01.2020, Proc. n.º 196/19.0T8PRT.P1, Rel. Rui Moreira.

[xxviii] TRC, Ac. de 13.07.2021, Proc. n.º 254/19.0T8VIS.C1, Rel. Manuel Capelo.

[xxix] TRG, Ac. de 24.02.2022, Proc. n.º 378/20.8T8VRL.G1, Rel. Jorge Teixeira

[xxx] DIAS MEIRELES, Ana Isa - *Prova Digital no Processo Judicial - A Blockchain e Outros Caminhos para os Tribunais* - Almedina 2023, que aborda a desmaterialização, com a evolução - constante - ao nível do digital, nos situamos numa esfera desprotegida. As provas e os meios de prova confundem-se, unem-se e surgem, muitas vezes, associadas ao digital: quer no momento da sua criação, quer no momento do seu armazenamento, quer no momento efetivo da sua produção perante um julgador, em concreto o potencial da *blockchain* na realidade probatória; MATOS BRANDÃO, Diogo de, *A prova digital no processo civil, repensar o Sistema*, Nova Causa, braga, 2020; SILVA PEREIRA, Fernando, *Prova Eletrónica em Processo Civil*, Almedina, março 2026, obra que trata de modo abrangente o tema da prova eletrónica em processo civil, distinguindo os tipos de documentos eletrónicos e a respetiva eficácia probatória, as espécies e a força probatória das cópias, e ocupando-se do problema da admissibilidade, do modo de produção e da respetiva impugnação. É tratado extensamente o problema da prova por cibernavegação (navegação na internet), distinguindo-se os casos em que a atividade de navegação, realizada pelo juiz, constitui um mero auxiliar na prática ou na valoração de outras provas, daqueles em que o objeto da prova diz respeito ao conteúdo de uma página web (inspeção de um lugar virtual), daqueles ainda em que a atividade de navegação na internet se destina a obter informações, utilizadas pelo juiz na fundamentação da decisão. A obra está em diálogo permanente com a jurisprudência. A obra está dividida em Parte I - Noção de documento eletrónico, tipos de assinaturas eletrónicas e cópias, Parte II - Eficácia probatória dos documentos eletrónicos, Parte III - Admissibilidade, modalidades de produção, valoração e impugnação da prova eletrónica e - Jurisprudência nacional citada ao longo de toda a obra e em concreto nas págs. 163 e 164 - índice de jurisprudência. Nesta sede e num domínio do direito cada vez mais relevante, ainda a obra SIMÃO, Rui, *Ativos digitais no Direito Civil*, Almedina 2026, a qual se debruça sobre o desafio dos ativos digitais no Direito Civil, repensando as categorias clássicas à luz da realidade tecnológica. Entre criptomoedas, contas digitais, dados e outros bens imateriais, coloca-se uma questão central: como identificar, apreender, transmitir e proteger aquilo que já não se vê?. Sobre as garantias processuais e prova digital, destacaria PINTO MONTEIRO, António Pedro, *Garantias processuais e prova digital*, com 1. Introdução 2. Conceito de prova digital. 3. enquadramento normativo da prova digital (ou a falta dele). 4. Fragilidades, problemas e desafios da prova digital: a importância das garantias processuais. 5. Possíveis formas de superação das fragilidades da prova digital: a *blockchain*. 6. Conclusão, disponível em <https://portal.oa.pt/media/144059/antonio-pedro-pinto-monteiro.pdf>

[xxxi] Num âmbito mais vasto do direito digital, ver SOUSA E SILVA, Nuno, *Lições de Direito Digital*, Almedina 2026, obra que explora, de forma abrangente e acessível, os complexos desafios jurídicos suscitados pela utilização disseminada de tecnologias da informação. Da tutela dos programas de computador e bases de dados à regulação da inteligência artificial, abrangendo os contratos informáticos, o comércio eletrónico, a governação da Internet, os direitos fundamentais no ciberespaço, a proteção de dados e a responsabilidade de plataformas. O autor disponibilizou recentemente índice de jurisprudência e bibliografia da obra, muito vasta, disponível em

https://nss.pt/images/_Data/Publicacoes-Monografias/Nuno_Sousa_e_Silva_-_Lic%CC%A7o%CC%83es_de_Direito_Digital_Bibliografia.pdf.

Tiago Brandão de Pinho: Juiz de Direito (*)

Sumário Executivo ():** (1) A crescente digitalização da sociedade tornou a prova digital uma realidade corrente na jurisdição administrativa e fiscal, exigindo uma adaptação da prática judiciária às novas formas de produção e conservação da informação. (2) A prova digital não impõe um novo regime jurídico da prova. Os institutos probatórios tradicionais permanecem aplicáveis, exigindo apenas cuidados acrescidos na verificação da autenticidade e da integridade dos elementos digitais. (3) Os documentos eletrónicos possuem plena admissibilidade probatória, sendo determinante confirmar a sua autoria, autenticidade e integridade, preferencialmente através da consulta da fonte original. (4) AO caso do comprovativo de pagamento adulterado demonstra que a validação junto do sistema de origem permite detetar manipulações que não são visíveis no próprio documento. (5) A simples entrega de um suporte digital não basta. Os documentos têm de ser incorporados no processo eletrónico para assegurar o contraditório e a preservação da prova. (6) A imagem de um ecrã prova apenas o conteúdo nele exibido, não constituindo, por si só, prova da veracidade dos factos representados. (7) As imagens georreferenciadas podem servir para reconstruir a realidade passada, desde que sejam devidamente contextualizadas e conjugadas com outros meios de prova. (8) A perícia é adequada quando sejam necessários conhecimentos técnicos especializados; a inspeção judicial permite ao juiz verificar diretamente a informação existente nos sistemas eletrónicos. (9) A inquirição de testemunhas por meios eletrónicos é compatível com as garantias processuais, desde que sejam asseguradas a autenticidade do depoimento e o contraditório.

Resumo (*):** O texto analisa o crescente papel da prova digital na jurisdição administrativa e fiscal, através da apresentação de casos concretos decididos no Tribunal Administrativo e Fiscal de Loulé. O autor sustenta que a evolução tecnológica não tornou necessário criar um novo direito probatório, uma vez que os meios de prova digitais podem ser enquadrados nos institutos clássicos da prova documental, das reproduções mecânicas, da perícia, da inspeção judicial e da prova testemunhal. O verdadeiro desafio reside em assegurar a autenticidade, a integridade e a preservação da informação digital. Após definir os conceitos de prova digital e de facto digital, o estudo demonstra como os documentos eletrónicos, os screenshots, as imagens do Google Street View, os ortofotomapas, os sistemas informáticos e as videoconferências podem assumir relevância probatória. Em todos os casos analisados, a fiabilidade da prova depende da possibilidade de confirmar a sua origem, confrontar a informação com a fonte original e garantir que os elementos digitais não sofreram manipulações. A análise jurisprudencial evidencia que a utilização da prova digital exige uma

apreciação crítica por parte do julgador. O caso do comprovativo de pagamento adulterado ilustra a importância da verificação junto do sistema oficial; os casos relativos ao Street View e aos ortofotomapas demonstram o potencial das imagens digitais para reconstituir factos passados; e os exemplos respeitantes aos screenshots revelam que estes apenas comprovam o conteúdo exibido no ecrã, não necessariamente a realidade do facto representado. O autor conclui que a transformação digital alterou sobretudo o suporte da prova, mas não os princípios fundamentais do direito probatório. Os tribunais continuam a aplicar as regras tradicionais de apreciação da prova, adaptando-as às especificidades dos meios digitais, num contexto em que a validação técnica e a preservação da autenticidade assumem importância decisiva para a descoberta da verdade e para a realização da justiça.

Palavras-Chave (****): Prova digital; Documento eletrónico; Valoração da prova; Jurisdição administrativa e fiscal; Reproduções mecânicas; Inspeção judicial; Perícia informática; Autenticidade da prova.

Índice: (1) Da Justiça na Era da Informação em que vivemos...; (2) A prova digital; (2.1) Noção de meio de prova digital; (2.2) Noção de facto digital; (3) A prova através de documento eletrónico; (3.1) A pescada, antes de ser, já o era: o comprovativo de pagamento «digipulado»; (3.2) Um detalhe que não faz diferença ou abertura da caixa de Pandora?: o modo de junção de documentos eletrónicos aos autos; (4) A prova através de reproduções mecânicas; (4.1) *Screenshots*: as aparências iludem?: o valor probatório de imagem que reproduz um ecrã; (4.2) *Street View*: uma cápsula do tempo?: o valor probatório de fotografias que reproduzem vias rodoviárias; (4.3) Ortofotomapas: ver para crer, medir para saber?: o valor probatório de mapas que reproduzem o território; (5) A prova através de perícia a facto eletrónico; (5.1) Bebida do dia: chá do sumiço: o mistério das linhas desaparecidas em *software* de faturação; (6) A prova por inspeção judicial a facto eletrónico; (6.1) Declaração escondida com rabo de fora?: a impugnação da autenticidade da declaração Modelo 3 de IRS; (7) A prova testemunhal através de videoconferência eletrónica; (7.1) As testemunhas à distância de um clique. *Online*, mas sem rede?: inquirições no TAF, na comarca do vizinho e na casa da testemunha; (8) ... à Justiça na Era da Inteligência que se anuncia.

1. Da Justiça na Era da Informação em que vivemos...

Primeiro, a mecânica substituiu a produção manual. Depois, o aço substituiu o ferro; o telégrafo, com o código morse e os seus dois sinais (um curto e outro comprido), substituiu os mensageiros; e a eletricidade substituiu o óleo e o gás.

Mais tarde, o transistor permitiu controlar a passagem da eletricidade com o fecho ou a abertura do circuito, funcionando como um interruptor. Quando o interruptor está ligado e, portanto, o circuito elétrico se encontra fechado, a passagem de eletricidade é representada pelo número 1; quando o interruptor está desligado e, assim, o circuito aberto, a ausência de eletricidade é representada pelo número 0.

Esta é a base do código binário, semelhante ao código morse: uns e zeros, lidos com a passagem ou a ausência de eletricidade, operam como a emissão de sinais longos e curtos. O sinal dos dígitos binários (sinal digital) é, assim, sincopado, ao contrário do que acontece nos meios analógicos, em que o sinal é contínuo, ficando armazenado nos sulcos do vinil, na fita da cassete ou na folha de papel, perdendo qualidade sempre que é copiado.

Cada dígito corresponde a um bit - acrónimo de bi(nary digi)t; cada conjunto de 8 bits corresponde a um byte (um *pedaço*, do inglês *bite*, que, para evitar a confusão com bit, viu o i ser trocado por um y).

A medida do *pedaço* de código binário corresponde a um carater. Enquanto no código morse os caracteres têm diferentes tamanhos, sendo as letras mais comuns mais curtas para facilitar a comunicação através do som ou da luz, no código binário cada carater é identificado por 8 bits, o que corresponde a um byte.

O acrónimo «TAF» corresponde, assim, a 3 bytes, ou 24 bits: 01010100 significa «T» em código binário; 01000001 é o «A»; e 01000110 o «F». Uma fotografia digital de qualidade elevada pode ser composta por cerca de um milhão de bytes (um megabyte); um episódio de uma série pode ocupar mil milhões de bytes (um gigabyte); uma biblioteca de ficheiros pode ocupar um servidor com um bilião de bytes (um terabyte).

Os bits podem ser copiados sem perder qualidade, pois um 0 será sempre um 0, e um 1 será sempre um 1, independentemente do modo como são registados ou do suporte em que é feito o seu armazenamento.

Os transístores não são ligados individualmente a fios de cobre nem soldados de forma manual: são colocados em placas de silício, os *chips*, que funcionam como circuitos integrados (pois contêm também as pistas onde a eletricidade circula e outros elementos que controlam e direcionam o fluxo de eletricidade) e que, num computador portátil ou num *smartphone* atual, podem conter entre 15 a 25 mil milhões de transístores. Estes chips são a base da indústria que permitiu, entre outras, a criação da internet, dos telemóveis e da televisão por satélite, tecnologias que, através de um número de quebras de eletricidade curtíssimas, representadas por 0 e por 1, que, para um humano, são praticamente impossíveis de quantificar, substituíram, tornaram quase obsoletos ou transformaram o serviço dos correios, as enciclopédias, os mapas rodoviários que habitavam os porta-luvas dos automóveis, os estúdios de fotografia ou o comércio local. É a terceira revolução industrial. É a Era da Informação.[\[1\]](#)

Omnipresente na rotina diária de cada um de nós, encontramos-na nas relações entre as empresas tecnológicas e os utilizadores das tecnologias (muitas vezes gratuitas, pois uma conta no *TikTok*, no *Instagram* ou no *Facebook* pode ser criada sem qualquer pagamento, embora todos saibamos que “*não há almoços grátis*”); entre as plataformas de comércio eletrónico (como a *Amazon*) ou o *website* do barbeiro da esquina que permite, com poucos cliques de rato, fazer a gestão da agenda e do serviço diretamente com os seus clientes; entre vizinhos, pais e colegas de equipa (nos grupos do *WhatsApp* ou do *Telegram*); e, naturalmente, nas relações entre o Estado e os cidadãos.

A desmaterialização do procedimento e do processo administrativo e tributário está não só na letra das leis de processo e na Portaria n.º 350-A/2025/1, de 9 de outubro, mas também no *eTribunal* - que agrega o *Citius*, o *Magistratus* (o *SITAF* encontra-se descontinuado desde o final do ano passado) e o *MPCodex*, permitindo a troca de informações entre Advogados e Representantes, Oficiais de Justiça, Juizes e Magistrados do Ministério Público -, e, bem assim, nos serviços da Administração Pública.

Com efeito, as obrigações de pagamento dos cidadãos não se esgotam nas tesourarias dos serviços e cumprem-se, muitas vezes, através da SIBS - Sociedade Interbancária de Serviços que gere a rede Multibanco e a aplicação MB Way. As obrigações declarativas dos contribuintes são realizadas (ou resultam de declarações já pré-preenchidas) e apresentadas no Portal das Finanças. Os serviços municipais de urbanismo recorrem a imagens georreferenciadas ou colhem as suas próprias imagens através de câmaras eletrónicas. A maior parte dos procedimentos tem tramitação eletrónica, nomeadamente os que tendem à celebração de contratos. E mesmo quando não têm, como o processo judicial é, ele próprio, eletrónico (cfr. os artigos 24.º, n.º 1, do Código de Processo nos Tribunais Administrativos, e 97.º, n.º 4, do Código de Procedimento e de Processo Tributário), os meios de prova, mesmo se analógicos, têm, por regra, de ser transformados em ficheiro eletrónico para poderem ser juntos ao processo (formato .pdf quando se trate de documento escrito; .mp4 quando se trate de documento vídeo; .png ou .jpeg quando seja exclusivamente uma imagem; .mp3 ou .ogg quando se trate de documento áudio - cfr. o artigo 7.º da Portaria 350-A/2025/1).

Naturalmente, depois de o digital nos revolucionar o quotidiano, chegou, como era expectável, aos Tribunais, local onde se compõem os litígios que por vezes o próprio digital potencia. A prova digital, apesar de recente, tem vindo a conquistar nos Tribunais o espaço que a Vida lhe reserva. E são vários os tópicos que têm animado a discussão na doutrina, que vão desde a definição de prova digital à necessidade, ou não, de princípios e garantias específicas.[\[iii\]](#)

Neste texto, mais do que entrar nessas discussões, iremos apresentar alguns exemplos reais em que Juizes do Tribunal Administrativo e Fiscal de Loulé lidaram com prova digital no âmbito da sua atividade probatória (na fixação de meios de prova digitais, na produção de prova digital e na valoração da prova sobre facto digital), destacando as dificuldades que sentiram e as soluções que encontraram.[\[iii\]](#)

Nestes casos, o Tribunal indicou, interpretou e aplicou os institutos legais existentes: o digital não obrigou à aplicação de um direito probatório novo. Os meios de prova digitais reconduzem-se aos institutos gerais (do documento particular, da reprodução mecânica, da perícia, da inspeção, da prova testemunhal...), embora por vezes com ligeiras adaptações. Em todos eles, com a prova digital o que mudou não foi o regime aplicável, mas o suporte em que o facto se encontrava e o cuidado com que se aferiu da sua autenticidade (a autoria) e da sua integridade (ausência de manipulação).

Três preocupações vão surgindo ao longo da exposição: a de que, quando o original é digital, a *autenticidade* e a *integridade* da cópia se afere no confronto com a fonte; a de que a imagem de um ecrã prova o ecrã, e não necessariamente o facto que o ecrã exhibe; e a de que a prova digital, *incorpórea* e *volátil* por natureza, tem de ser fixada num suporte estável para sobreviver no processo.

Os casos estão organizados por meio de prova e são precedidos de breves nótulas sobre o regime jurídico de cada um. Cada um traz consigo uma pequena história e um título. Veremos um comprovativo de pagamento a que faltava a data, querendo comprovar o que ainda não tinha acontecido (capítulo 3.1), e uma *pen* que se julgava bastante para entregar um processo instrutor (3.2). Veremos depois o que prova, e o que não prova, a imagem de um ecrã sobre informação relativa a um serviço prestado pelos CTT, que mostrava o que o sistema dizia, mas não o que sucedera (4.1); as panorâmicas do *Street View*, que serviram de cápsula do tempo a um acidente de viação (4.2); e os ortofotomapas que, datados, desmentiram uma preexistência inventada (4.3). Seguir-se-á o “chá do sumiço” - a perícia que apurou se as linhas desaparecidas num programa de faturação eram defeito ou manipulação (5.1), e a declaração Modelo 3 que o Tribunal foi consultar à fonte, em inspeção feita no próprio gabinete (6.1). Por fim, as testemunhas à distância de um clique, *online* mas sem rede, e a lição que delas se tirou (7.1). E em todos eles hão de reaparecer algumas daquelas preocupações supra enunciadas.

2. A prova digital

2.1. Noção de meio de prova digital

Nos termos do artigo 341.º do Código Civil, “*As provas têm por função a demonstração da realidade dos factos*”.

A prova serve, assim, para revelar o que “*os factos são em si mesmo*”, sendo certo que “*a realidade é sempre percebida numa visão parcelar, distinta de pessoa para pessoa e, por isso, dela apenas se pode ter determinada verdade, que [é] aquela que o julgador assimilou e que, obviamente, não é absoluta no sentido de excluir qualquer espécie de humano error*”.[\[iv\]](#)

A prova funciona como uma «máquina do tempo» e/ou de «teletransporte» que, apesar de ter por finalidade a *demonstração da realidade*, se basta com o *conhecimento da verdade* de acordo

com a convicção do Juiz, no caso de prova sujeita à livre apreciação, ou com a vontade da lei, no caso de prova tarifada.

Esta imagem há de acompanhar-nos. Em alguns casos, a máquina recua no tempo, com as imagens panorâmicas do *Street View* ou os ortofotomapas que trazem ao presente o estado de um lugar num ano já ido. Noutros, encurta o espaço: a inspeção a facto eletrónico não leva o Juiz ao servidor distante, antes traz o servidor ao Tribunal, e a videoconferência aproxima a testemunha que está a milhares de quilómetros. Nesta viagem pelo tempo e/ou pelo espaço, o que se procura é tornar presente, perante o julgador, um facto que não o está.

Por outro lado, se *“a prova em juízo de um facto reclamasse a certeza absoluta da verificação do facto, a actividade jurisdicional saldar-se-ia por uma constante e intolerável denegação de justiça. A prova tem, por isso mesmo, atenta a inelutável precariedade dos meios de conhecimento da realidade (especialmente dos factos pretéritos e dos factos do foro interno de cada pessoa), de contentar-se com certo grau de probabilidade do facto: a probabilidade bastante, em face das circunstâncias concretas da espécie, para convencer o julgador (que conhece as realidades do Mundo e as regras de experiência que nele se colhem) da verificação ou realidade do facto”*.[\[v\]](#)

E o que importa é, essencialmente, o meio como é demonstrada a realidade do facto, isto é, o meio através do qual o Juiz toma conhecimento da verdade.

Quando a prova é produzida com a exibição de informação que se encontra representada ou transmitida através do código binário, a prova diz-se digital porque a sua apreciação pressupõe a descodificação eletrónica dos 0 e dos 1 que a compõem, com a consequente apresentação da informação no ecrã e/ou nos altifalantes. Esta é a noção que iremos utilizar no presente texto.[\[vi\]](#)

Nesta noção de prova digital cabem, então, vários meios de prova. Pode ser digital a prova documental, se o documento for gerado por um dispositivo eletrónico. Como pode ser digital a prova testemunhal, se a inquirição for realizada por videoconferência em que câmaras e microfones convertem a imagem e a voz em sinais elétricos. Também pode ser digital a prova pericial ou a prova por inspeção, se o objeto da perícia ou da inspeção for um ficheiro informático e a produção da prova exigir o acesso a uma infraestrutura eletrónica.

A diferença entre prova digital e prova eletrónica é, essencialmente, de perspetiva: a expressão “prova digital” dá ênfase ao modo como a informação é transmitida, ou seja, à transformação dos sinais elétricos em código binário; já a expressão “prova eletrónica” dá relevo à tecnologia que suporta a informação, isto é, ao facto de esta depender de componentes físicos e elétricos (chips, ecrãs, baterias...). Tudo o que é digital é, por natureza, eletrónico, pois a codificação em dígitos binários é trabalhada e descodificada em sistemas computacionais. No entanto, nem tudo o que é eletrónico é digital: por exemplo, as gravações das inquirições de testemunhas mais antigas, em cassetes e CD, dependem de impulsos eletromagnéticos e de corrente elétrica, mas a informação é guardada numa onda contínua, e não em código binário.

Diferente do *meio de prova*, o instrumento de que o Juiz se serve para firmar a sua convicção sobre a verificação ou a não verificação do facto, é o *objeto da prova*, entendida como o facto a demonstrar.

Concretizaremos, de seguida, a diferença, de modo a identificarmos a existência de factos digitais.

2.2. Noção de facto digital

Também o facto pode ser digital, se a ocorrência da vida real ou de qualquer mudança ocorrida no mundo exterior, ou ainda se o estado, a qualidade ou a situação real da coisa respeitar a realidades que são compostas, ou representadas, através do código binário.

A obrigação de faturação através de programas informáticos gera ficheiros eletrónicos, como, por exemplo, faturas digitais que substituem integralmente as faturas em papel. Se, por exemplo, para efeito de dedução do IVA, se discutir se foram, ou não, cumpridos os requisitos de preenchimento de uma fatura eletrónica, estaremos perante um facto digital.

O mesmo se diga sobre a comunicação entre duas partes contratantes, através de mensagens de correio eletrónico, se tiver de ser apreciado o teor das suas declarações. Do mesmo modo, o registo audiovisual da tomada de declarações em suporte digital num procedimento disciplinar é um facto eletrónico.

3. A prova através de documento eletrónico

O Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014, vulgarmente designado por Regulamento eIDAS (*Electronic Identification, Authentication and Trust Services*), “Tendo em vista assegurar o correto funcionamento do mercado interno e alcançar um nível adequado de segurança dos meios de identificação eletrónica e dos serviços de confiança”, veio, além do mais, instituir “um quadro legal para as assinaturas eletrónicas” e para os documentos eletrónicos.

Nos termos do seu artigo 3.º, alínea 35), documento eletrónico é “qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual”, sendo que - artigo 46.º - “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”.

Deste modo, o documento eletrónico é um documento para os efeitos do artigo 362.º do Código Civil (“diz-se documento qualquer objecto elaborado pelo homem com o fim de reproduzir ou

representar uma pessoa, coisa ou facto”), apenas com a particularidade de ter um suporte capaz de armazenar código binário. Assim, textos, anotações, desenhos, fotografias, registos áudio ou plantas não perdem a natureza de documento por se encontrarem codificados em ficheiros .pdf, .png, .jpg, .mp3 ou outro, nem podem deixar de ser admitidos como meio de prova no contencioso administrativo e tributário por se encontrarem armazenados em formato eletrónico.

Este Regulamento foi executado pelo Decreto-Lei n.º 12/2021, de 9 de fevereiro, que veio *regular a validade, eficácia e valor probatório dos documentos eletrónicos, bem como o reconhecimento e aceitação, na ordem jurídica portuguesa, dos meios de identificação eletrónica de pessoas singulares e coletivas.*[\[vii\]](#)

Por força do seu artigo 3.º, n.º 1, *“O documento eletrónico satisfaz o requisito legal de forma escrita quando o seu conteúdo seja suscetível de representação como forma escrita”,* sendo que - n.º 2 -, *a aposição de uma assinatura eletrónica qualificada equivale à assinatura autógrafa dos documentos com forma escrita em suporte de papel,* o que lhe atribui - n.º 5 - a força probatória de documento particular assinado.

Se a assinatura não for qualificada, o valor do documento eletrónico fica sujeito à livre apreciação do Juiz - n.º 10.

Nos termos do n.º 11 do mesmo artigo 3.º, no caso de o documento autêntico ser copiado para um suporte que não permita a verificação e validação das assinaturas eletrónicas, como no caso de impressão de um ficheiro .pdf assinado, *a cópia tem a força probatória das cópias fotográficas, prevista no n.º 2 do artigo 387.º do Código Civil.*

Por outro lado, se um ato ou contrato for digitalizado, a cópia digitalizada tem a *“força probatória do original, salvo se a pessoa a quem forem apresentadas requerer a exibição desse original”* - artigo 5.º-A.

O regime probatório do documento eletrónico acompanha, então, o instituto geral da prova documental. E assim, no que respeita aos documentos particulares:

- Tal como o documento analógico deve ser assinado - cfr. o artigo 373.º, n.º 1, do Código Civil -, também ao documento particular eletrónico deve ser aposta assinatura eletrónica qualificada[\[viii\]](#);

- Se o documento particular eletrónico não estiver assinado, a falta deste requisito legal faz com que a sua força probatória seja apreciada livremente pelo Juiz, uma vez que não é possível determinar a sua autoria;

- Uma vez que não se trata de documento autêntico, a autoria do documento particular eletrónico não se impõe por si: *a letra e/ou a assinatura de um documento particular consideram-se verdadeiras, quando reconhecidas, expressa ou tacitamente, ou não impugnadas pela parte*

contra quem o documento é apresentado - artigo 374.º, n.º 1, primeira parte, do Código Civil. Estabelecida a autoria, o documento *“faz prova plena quanto às declarações atribuídas ao seu autor, sem prejuízo da arguição e prova da falsidade do documento”*, mas apenas *“na medida em que sejam contrárias aos seus interesses”* - artigo 376.º, n.ºs 1 e 2, do mesmo compêndio legal.

- Impugnada a veracidade da letra ou da assinatura, inverte-se o ónus da prova, passando a incumbir à parte que apresentou o documento a prova da sua veracidade - artigo 374.º, n.º 2 -, sendo o seu valor probatório apreciado, a final, na decisão da matéria de facto, em função da prova produzida no incidente. Além desta impugnação da veracidade do documento particular eletrónico, a lei admite também a arguição da sua falsidade - cfr. o artigo 375.º, n.º 2, do Código Civil -, o que poderá suceder no caso de a parte alegar, por exemplo, que a aposição da assinatura eletrónica avançada foi feita por alguém que usurpou as suas credenciais de assinatura;

- Finalmente, as reproduções de documentos particulares eletrónicos seguirão o regime das reproduções mecânicas, como se detalhará no capítulo seguinte.

Verifica-se, assim, que as questões que de algum modo separam o documento eletrónico do documento analógico são, essencialmente, questões tecnológicas, não jurídicas.

Apesar do seu suporte diferente, são as mesmas as preocupações relativas à determinação da *autenticidade* (a autoria a quem as declarações serão imputadas) e da *integridade* (a ausência de adulteração do teor). A maior dificuldade é causada por o documento eletrónico ser, por um lado, *incorpóreo*, uma sequência de 0 e de 1, que pode ser armazenada em diferentes suportes (uma *pen*, um CD, um servidor na nuvem...), e, por outro, *volátil*, na medida em que a sua cópia/adulteração não perde qualidade (um 1 é sempre um 1; um 0 é sempre um 0), podendo o seu desaparecimento (mais uma vez de meros 0 e 1) não deixar rasto.

A estas duas preocupações junta-se uma terceira, processual e não tecnológica, mas que o digital agudiza: a do contraditório. Para que a prova possa ser contraditada, tem de estar verdadeiramente no processo - incorporada, acessível e estável -, e não dependente de um suporte ou de um sistema a que só uma das partes acede. Veremos esta exigência decidir o modo de junção dos documentos (capítulo 3.2) e pesar na valoração de um depoimento prestado à distância, longe do controlo do tribunal (capítulo 7.1).

Face às preditas dificuldades, na prova digital torna-se mais difícil distinguir o «gato» da «lebre».

A tarefa pode ser levada a bom porto, mas a determinação da genuinidade do documento eletrónico fica dependente da leitura e interpretação de metadados (informações técnicas estruturadas sobre o documento eletrónico, como a data, o local e as características do *smartphone* que tirou a fotografia digital, ou a data da última alteração e o tamanho de um ficheiro de texto), ou de registos de identificação de quem acedeu ao suporte eletrónico para fazer a cópia ou o *download* do ficheiro.

São estas fragilidades, e os modos de as superar, que os casos que ora apresentamos ilustram.

3.1. A pescada, antes de ser, já o era: o comprovativo do pagamento da taxa de justiça «digipulado»

O caso: na área administrativa do Tribunal Administrativo e Fiscal de Loulé foi apresentada, em 26 de junho de 2025, uma Petição Inicial de *"Impugnação Judicial"*, contra o Ministério da Justiça, que correu termos sob o n.º 349/25.0BELLE, em que se pedia *"a extinção da responsabilidade disciplinar"* do Autor e, *consequentemente, a extinção do processo disciplinar*, bem como *"declarados cessados os efeitos da pena disciplinar aplicada ao impugnante"*. O processo foi autuado na 13.ª Espécie – Outros Processos, e concluso ao Juiz titular *"por dúvidas na sua distribuição"*, que determinou a sua distribuição na 1.ª Espécie – Ação Administrativa. A correção à distribuição foi efetuada e o Réu citado. Como a Petição Inicial não foi acompanhada do comprovativo do pagamento da taxa de justiça, nem de documento relativo à concessão, ou ao pedido, de apoio judiciário, a secretaria notificou a Mandatária do Autor, em 11 de julho de 2025, para juntar o comprovativo em falta, sem sucesso. Em setembro, o processo foi concluso ao Juiz *"com informação a V. Exa. que não se mostra junto o [comprovativo do] prévio pagamento da taxa de justiça devida pela propositura da presente ação, sendo que os Documentos Únicos de Cobrança (DUC) juntos a fls. 10 e 11 do SITAF e indicados no formulário de apresentação da peça processual petição inicial (...), encontram-se sem cobrança. Notificada a Ilustre Mandatária do Autor a 11/07/2025, conforme consta a fls. 24 do SITAF, não foi junto qualquer pagamento da taxa de justiça devida"*. Consequentemente, foi proferido despacho que findou o processo *"atenta a falta de comprovação do pagamento da taxa de justiça ou do benefício de apoio judiciário, na modalidade de dispensa de pagamento da taxa de justiça"*.

O processo poderia ter terminado aqui.

No entanto, em 17 de setembro de 2025, foi apresentado requerimento no qual a Mandatária afirmou que *"O Autor efectuou o pagamento de taxa de justiça e multa e juntou os DUCs com a P.I."*. Para o demonstrar, juntou como *"Comprovativo de pagamento"* os documentos únicos de cobrança, um relativo à taxa de justiça e outro à multa, e dois documentos bancários intitulados *"Detalhe Pagamento"*, rematados pela menção *"Documento Processado por Computador"*, aparentemente gerados pelo serviço de *homebanking* do BPI, e que tinha as informações habituais relativas à *"Operação"*, à *"Descrição"*, ao *"Número"*, ao *"Tipo Pagamento"*, à *"Referência"*, ao *"Montante"* e à *"Situação"*. Tinha muita informação, mas não tinha tudo: entre a linha *"Número"* e a linha *"Tipo Pagamento"*, onde normalmente se encontra a linha *"Data Pagamento"*, estava um espaço em branco.

A questão a decidir e o facto a apurar: confrontado com o Requerimento, o Juiz considerou que o requerimento deixava nos autos uma questão nova, de natureza instrumental: era fidedigno o

comprovativo do pagamento da taxa de justiça? Os factos a apurar eram duplamente digitais. Por um lado, o pagamento das taxas de justiça através de DUC fica registado no Sistema das Custas Judiciais, gerido pelo Instituto de Gestão Financeira e Equipamentos da Justiça, I.P. (IGFEJ), pelo que o “original” do facto - a operação de pagamento e a respetiva data - só existia codificada em código binário naquele sistema de informação. Por outro, o próprio comprovativo era um documento eletrónico, gerado por uma aplicação bancária e transferido ou impresso e digitalizado para junção aos autos, isto é, uma reprodução cujo regime é o que se descreveu na introdução deste capítulo: faz prova plena dos factos que representa se a sua exatidão não for posta em causa. E havia razões para a pôr em causa: nos comprovativos de operações bancárias, a data não costuma faltar.

A fixação do meio de prova: o Juiz não ordenou perícia, nem inspeção. No mesmo despacho em que se pronunciou sobre o requerimento, *atendendo aos documentos juntos com o requerimento*, foi ordenada a remessa, *por email, ao IGFEJ, das cópias dos DUC, “a fim de se apurar a sua fidedignidade e a aparente contradição entre o seu teor e a informação constante”* dos autos, no sentido de o DUC relativo à taxa de justiça se *apresentar sem cobrança* no dia 11 de julho de 2025. Em vez de discutir diretamente a exatidão da reprodução do ficheiro .pdf que continha a digitalização dos DUC e dos comprovativos dos pagamentos, o Tribunal requisitou a informação (o facto digital) à entidade que administra o registo informático onde os pagamentos das taxas de justiça são lançados e conciliados (cfr. o artigo 436.º, n.º 1, do CPC), num movimento idêntico ao que se verá no capítulo 6.1 (para aferir a autenticidade e a genuinidade de uma declaração modelo 3 de IRS): quando o original é digital, a genuinidade da cópia afere-se pelo confronto com a fonte.

A produção da prova: a resposta do IGFEJ chegou, também por correio eletrónico, em 6 de outubro de 2025, e informava que o pré-pagamento n.º 702080097001058, relativo à taxa de justiça do processo, no montante de € 306,00, tendo por depositante o Autor, apresentava como “*data de pagamento*” o dia 17 de setembro de 2025 (o dia em que o requerimento fora apresentado, posterior à decisão que findou o processo) e como “*data de registo*” o dia 22 do mesmo mês.

A valoração da prova: face à informação prestada, o Juiz concluiu que o pagamento que o requerimento afirmava ter sido feito por ocasião da apresentação da petição inicial, em 26 de junho de 2025, só foi realizado em 17 de setembro do mesmo ano, precisamente o dia da apresentação do requerimento, duas semanas depois de o processo ter sido findo e quase três meses depois da propositura da ação. O comprovativo queria mesmo ser como a pescada que antes de ser apanhada pelo pescador (pescada), já era pescada (peixe).

Decisão do incidente: o Juiz considerou que “*Não é usual nos comprovativos de pagamento por via bancária a omissão da data da operação. Pelo contrário: esse elemento é muito importante, precisamente para comprovar quando foi efetuado o pagamento, com todas as implicações probatórias que isso pode originar*”, e salientou a “*ambiguidade da afirmação de que o Autor «efectuou o pagamento da taxa de justiça e multa e juntou os DUC com a p.i.», sem indicação da data*”. A omissão, conjugada com a informação do IGFEJ e com a ambiguidade da afirmação de que

os DUC tinham sido juntos com a petição inicial, levou o Juiz *“a concluir que o documento junto com o requerimento de 17.09.2025 foi manipulado, ou adulterado, com a supressão da data da realização do pagamento, tendo em vista obter um benefício ilegítimo, qual seja a admissão da petição inicial”*. Não surpreende, assim, que o processo tenha sido batizado pelo seu titular como o processo do *“comprovativo digipulado”*, tendo sido determinada a extração de certidão, entre outros documentos, do requerimento de 17 de setembro e da informação prestada pelo IGFEJ, e ordenada a sua remessa ao Ministério Público, *“por indícios da prática de crime de falsificação de documentos e prestação de falsas declarações (artigos 256.º e 348.º-A do Código Penal)”*.

Trânsito: não foi interposto recurso.

Comentário: este caso ilustra, em simultâneo, a fragilidade do documento eletrónico assinalada na introdução deste capítulo e o modo de a superar. A adulteração de um ficheiro .pdf não exige conhecimentos técnicos relevantes e pode não deixar, à vista desarmada, qualquer rasto: suprimir a linha com a data é coisa que um editor de documentos ou de imagens faz sem esforço. Mas a mesma desmaterialização que facilita a manipulação da cópia guarda a verdade na fonte: a operação de pagamento ficou registada, com data, montante e estado, num sistema de informação, e bastou uma mensagem de correio eletrónico, sem encargos nem demoras, para que a contradição se tornasse evidente para o Juiz. Curiosamente, o alarme não foi despoletado por um radar tecnológico: foi uma regra de experiência comum (os comprovativos bancários têm data) que levou o julgador a desconfiar do documento. Na prova documental digital, como se vê, a livre apreciação continua a começar nos sentidos e na experiência de quem julga; o que muda é a fonte onde se vai verificar o facto.

3.2. Um detalhe que não faz diferença ou a abertura da caixa de Pandora?: o modo de junção de documentos eletrónicos aos autos

O caso: no Tribunal Administrativo e Fiscal de Loulé correu termos, sob o n.º 458/21.4BELLE, uma ação de contencioso pré-contratual em que a Autora pretendia obter a anulação da decisão de adjudicação de uma empreitada a uma Contrainteressada. A estória que aqui vamos contar não está relacionada com a decisão da matéria de facto e de direito que ocorreu no palco principal, mas com alguns detalhes de bastidores relativos ao modo como os documentos que compunham o processo administrativo entraram no teatro das operações. A peça tem três atos.

Primeiro Ato: a entrega da pen. Em 7 de outubro de 2021, a Secretária do Tribunal lavrou cota a consignar que foi recebida *“uma pen com o processo instrutor, que contém inúmeros documentos, que resulta num número muito avultado de fotocópias, já que os documentos excedem a capacidade para serem introduzidos automaticamente no SITAF. Como ainda falta a digitalização de inúmeros documentos da referida pen [remeto-a] à secção, para o processo ser conclusivo à Mmª Juiz titular do processo”*. A entidade demandada tinha cumprido, ou julgava ter cumprido, a obrigação de proceder

ao envio do processo administrativo que o artigo 84.º, n.º 1, do Código de Processo nos Tribunais Administrativos lhe impunha, entregando ao Tribunal um suporte físico de armazenamento de dados (*pen*) onde os ficheiros se encontravam gravados. A secretaria, confrontada com um objeto que não conseguia verter para dentro do processo eletrónico, através da impressão dos ficheiros e posterior digitalização, apresentou a questão a quem a poderia resolver.

A decisão: o suporte não é o documento. Por despacho de 12 de outubro de 2021, a Juíza começou por traçar o quadro normativo do modo de junção: por força do artigo 24.º, n.ºs 1 e 2, do CPTA, os atos processuais que devam ser praticados por escrito pelas partes são apresentados em juízo por via eletrónica, nos termos definidos pela Portaria n.º 380/2017, de 19 de dezembro (Portaria SITAF),[\[ix\]](#) cujo artigo 3.º determinava que a apresentação de peças processuais, documentos e processo instrutor deveria ser efetuada através do sistema informático de suporte à atividade dos tribunais administrativos e fiscais (SITAF); e o artigo 10.º da mesma Portaria apenas admitia a apresentação de documentos (que não fossem documentos vídeo ou áudio) pelos meios previstos nas alíneas a) a c) do n.º 5 do artigo 24.º do CPTA (entrega na secretaria judicial, remessa pelo correio ou envio através de telecópia), quando a dimensão dos documentos excedesse o limite que ali se fixava (à data, 20 MB). Concluiu ser, *“por isso, inadmissível a apresentação do processo instrutor através da entrega de um dispositivo de armazenamento de dados (pen drive) onde os documentos que o integram se encontram gravados (por não estarem em causa documentos vídeo ou áudio)”*, sublinhando que *“os documentos que integram o processo administrativo carecem de ser incorporados ou apensados ao processo, para que nele possam valer como prova documental, não cabendo ao tribunal proceder à extracção dos respectivos ficheiros a partir do suporte de gravação enviado”*. E determinou que a entidade demandada apresentasse o processo administrativo *através do sistema informático de apoio à atividade dos tribunais, mediante o menor número possível de requerimentos, ou, em alternativa, em suporte físico, pelos meios previstos nas alíneas a) a c) do n.º 5 do artigo 24.º do CPTA* (no pressuposto de que o processo administrativo poderia ser considerado, para efeitos do então n.º 5 do artigo 10.º da Portaria SITAF, um “documento” que, por si só, desrespeitava o limite previsto no n.º 1).

Trânsito: não foi interposto recurso.

Comentário: a decisão assenta na distinção, central neste capítulo, entre o documento eletrónico e o seu suporte. O documento eletrónico é uma sequência de dígitos binários codificados, que tanto pode estar gravada numa *pen*, como num CD, como num servidor na nuvem: a *pen* é o envelope, não a carta. Juntar aos autos o suporte não é juntar os documentos, porque o que vale como prova documental (o que as partes podem consultar e contraditar, o que o juiz pode examinar e citar) é o que está incorporado no processo eletrónico, não o que está gravado num objeto que repousa numa prateleira da secretaria ou do arquivo. E a extração dos ficheiros a partir do suporte digital não é tarefa do tribunal: quem apresenta documentos tem o ónus de os apresentar em condições de serem juntos. Os (parcos) recursos humanos do Tribunal não devem estar alocados ao

cumprimento de uma obrigação da parte, quando, ainda por cima, tal intermediação pode contaminar a prova.

Segundo Ato: o regresso ao papel. Em 19 de novembro de 2021, a Ré veio *“remeter os documentos referentes ao processo administrativo em suporte de papel”*, juntando o *“Processo administrativo em 6 volumes”*. Num processo com natureza eletrónica, o cumprimento da lei acabou por fazer-se... em papel, uma válvula de escape analógica do sistema que garante, a quem apresenta, a certificação da entrega e, ao Tribunal, a incorporação controlada dos documentos no processo.

Terceiro Ato: os ficheiros individuais. No despacho saneador, de 4 de janeiro de 2022, depois de dispensar a realização da audiência prévia, conhecer das exceções dilatórias, fixar o valor da causa, identificar o objeto do litígio e enunciar os temas da prova, o Tribunal voltou ao assunto, agora por sua iniciativa: *“Por se prefigurar necessário para uma adequada instrução dos autos (com eventual exibição a perito ou testemunhas) e fundamentação da decisão a proferir”*, foi ordenada a notificação da entidade demandada *para juntar aos autos, por via eletrónica, em ficheiros individuais*, as peças nucleares do procedimento que enumerou, correspondentes aos documentos com especial relevo para o exame e a decisão da causa, por forma a integrarem o processo eletrónico. O processo administrativo já estava nos autos – em seis volumes de papel – e a obrigação de envio estava cumprida, mas a Juíza, ao invés de ordenar a digitalização de todos os documentos que o integravam, o que originaria uma infundável quantidade de ficheiros cuja extensão não permitiria um adequado exame dos mesmos (cfr. artigo 12.º, n.º 2, da Portaria SITAF), optou por outra forma de preparar a produção de prova e agilizar a comunicação com peritos e testemunhas, tendo entendido que a junção em ficheiros individuais servia de forma processualmente adequada a instrução.

Trânsito: a Autora interpôs recurso contra a sentença, mas sem colocar em xeque o modo de junção dos documentos aos autos. Ainda assim, deixa-se a ligação para o acórdão que negou provimento ao recurso: <https://dgsl.pt/acordaos/fd531984cc7fc3d0>.

Comentário: um detalhe que não faz diferença ou a abertura da caixa de Pandora? À primeira vista, a resposta é a primeira: nenhum dos três atos influenciou a decisão e todas as questões se resolveram com despachos singelos, sem incidentes, sem nulidades e sem outro custo para as partes que não fosse o tempo. Mas foi precisamente porque o Tribunal tratou o detalhe com rigor que a caixa não chegou a abrir-se. Se a *pen* tivesse sido aceite, ou os autos passariam a conter prova documental não incorporada, dependente de um objeto físico e da sua leitura por equipamento alheio ao processo, subtraída ao exame imediato das partes e da Juíza; ou os funcionários teriam sido assoberbados com a tarefa de introduzir os ficheiros no processo, com a possibilidade de surgirem erros, como o esquecimento do *upload* de um ficheiro, o apagar involuntário de outro, ou a troca por outro ficheiro que se encontrasse já armazenado no computador onde a operação fosse feita. E no caso, poupou-se-lhes o trabalho de digitalizar integralmente o processo administrativo, com todos os documentos que o compunham, muitos deles sem relevância alguma para o exame da causa e a decisão a proferir. O modo de junção é a porta por onde o documento eletrónico – incorpóreo, volátil

e dependente do suporte e do formato, como se viu na introdução deste capítulo – entra no mundo do processo. Bem fechada a porta, o modo de junção é mesmo um detalhe que não faz diferença; mal fechada, é por ela que saem os males da caixa de Pandora.

Vista a entrada do documento eletrónico no processo, falta saber o que provam as suas reproduções - as fotografias, as imagens e os mapas que captam o próprio mundo. Será tudo farinha do mesmo saco? É o objeto do capítulo seguinte.

4. A prova através de reproduções mecânicas

Nos termos do artigo 368.º do Código Civil, as reproduções fotográficas ou cinematográficas, os registos fonográficos e, em geral, quaisquer outras reproduções mecânicas de factos ou de coisas fazem prova plena dos factos e das coisas que representam, se a parte contra quem são apresentadas não impugnar a sua exatidão. É um regime de prova plena condicionada: vale enquanto a exatidão não for posta em causa; impugnada esta, o valor da reprodução passa a depender de prova que a confirme.

O *screenshot*, a fotografia panorâmica de rua e o ortofotomapa partilham esta natureza: são reproduções mecânicas de factos ou de coisas, apenas com a particularidade de o registo ser codificado em dígitos binários. Mas, sob a aparência comum, escondem-se diferenças que os casos seguintes - um tríptico relativo a fotos, imagens e mapas digitais - hão de revelar. No primeiro caso, relativo à força probatória de um *screenshot*, conclui-se que é diferente reproduzir uma coisa de reproduzir um registo sobre a coisa: a imagem de um ecrã prova o que o ecrã mostra, não necessariamente o facto que o ecrã afirma. Nos demais, um relativo às fotografias panorâmicas e outro a ortofotomapas, aprecia-se o modo de captação, o grau de precisão e momento temporal das imagens que as transforma em verdadeira «máquina do tempo».

4.1 Screenshots: as aparências iludem?: o valor probatório de imagem que reproduz o ecrã

O caso: no processo n.º 164/11.8BELLE, uma cidadã residente no Reino Unido deduziu Oposição a um processo de execução fiscal instaurado no Serviço de Finanças de Loulé 1 para cobrança de € 53.161,19, relativos a IRS do ano de 2005. Citada em 24 de dezembro de 2010, alegou, além do mais, que apenas nessa véspera de Natal tomou conhecimento da existência da dívida, pelo que a liquidação não lhe foi notificada antes de 31 de dezembro de 2009, data em que terminara o prazo de caducidade do direito à liquidação. Na Contestação, a Fazenda Pública sustentou que a liquidação do imposto e a liquidação dos juros compensatórios foram remetidas em 24 de julho de 2009, através de cartas enviadas sob os registos n.ºs RY484446966PT e RY484739372PT, para a morada do representante fiscal da Oponente constante do cadastro, sendo ineficaz a mudança de domicílio enquanto não comunicada à Administração Tributária. Defendeu

que, por força da presunção do artigo 149.º, n.º 3, do CIRS, a Oponente se deveria considerar notificada em 31 de julho e em 3 de agosto de 2009, dentro do prazo de caducidade. E para prova da remessa, invocou o documento de fls. 110 dos autos: uma impressão do seu sistema informático, onde figuravam os números das liquidações, as datas de emissão das cartas e os respetivos números do registo postal.

A questão a decidir e o facto a apurar: nos termos dos artigos 268.º, n.º 3, da Constituição e 77.º, n.º 6, da LGT, a eficácia do ato tributário depende da sua notificação ao contribuinte, na forma prevista na lei. A questão de direito era, pois, a de saber se a liquidação se tornara eficaz antes de esgotado o prazo de caducidade. Em causa estava a prova da remessa das cartas registadas para o domicílio fiscal, facto conhecido de que a lei manda firmar, por presunção, o facto desconhecido da notificação. O facto a apurar era, então, singelo e rigorosamente analógico: a entrega aos CTT, em 24 de julho de 2009, de duas cartas registadas, com determinados números, endereçadas ao Sujeito Passivo para determinada morada. Mas a prova oferecida para o demonstrar era digital: a imagem impressa de um ecrã.

A produção da prova: para os atos preparatórios da liquidação (as notificações para entrega da declaração em falta, para o exercício do direito de audição sobre o projeto de relatório e do relatório final da inspeção), a Fazenda Pública juntou à Contestação os ofícios e os respetivos registos postais, alguns com aviso de receção. Para o ato decisivo, o envio das liquidações, ofereceu apenas a impressão de um *screenshot*. Nenhum talão de aceitação, nenhuma certidão dos CTT: a remessa das cartas registadas tinha, a seu favor, apenas a impressão da imagem do ecrã do sistema informático da parte que a alegava.

A valoração da prova: o Tribunal julgou não provado que as liquidações tivessem sido remetidas, em 24 de julho de 2009, através das cartas registadas identificadas na Contestação. Na fundamentação da decisão da matéria de facto, ficou consignado que o documento apresentado era *“mera impressão do seu sistema informático”* e que *tal impressão apenas criava “a convicção de que foi inserido naquele sistema a informação relativa às liquidações e a elementos conexos com o serviço de registo dos CTT, mas não que nas datas aí insertas se verificaram os eventos descritos, designadamente que a liquidação foi enviada sob registo sem aviso”,* sendo tais dados *“totalmente omissos quanto ao destinatário e respectiva morada”*. E, convocando jurisprudência corrente, citou-se o acórdão do Tribunal Central Administrativo Norte de 12 de abril de 2013, processo n.º 01727/07: *“tais prints não podem deixar de ser considerados como documentos internos elaborados pela própria Administração, para efeitos internos, não oponíveis [à Oponente]. Na verdade, os ditos prints não provam a remessa da liquidação em causa para o domicílio [da Oponente], nem o seu recebimento, sendo ainda de realçar que nada nos garante que os prints juntos estejam em conformidade com os elementos com base nos quais foram, alegadamente, elaborados, esses sim, com valor probatório”*. Não tendo sido dada como provada a remessa, não operou a presunção do artigo 149.º, n.º 3, do Código do IRS, pelo que a Administração não cumpriu o ónus que sobre si

recaía de demonstrar a eficácia da liquidação antes do termo do prazo de caducidade, ocorrido em 31 de dezembro de 2009.

Decisão: a Oposição foi julgada procedente por não se ter provado que as cartas tinham sido recebidas pelo contribuinte antes de completado o prazo de caducidade do direito à liquidação.

Trânsito: não foi interposto recurso.

Comentário: o que prova, então, a imagem de um ecrã? A impressão junta pela Fazenda - e o mesmo vale para o *screenshot*, seu irmão nativo digital, captado sem passagem pelo papel - é uma reprodução mecânica, sujeita ao regime do artigo 368.º do Código Civil descrito na introdução deste capítulo: faz prova plena dos factos que representa, se a parte contrária não impugnar a sua exatidão. Simplesmente, o que a imagem de um ecrã representa é... o ecrã. Não impugnada, prova plenamente que, no momento da captura, o sistema exibia aquela informação; já não prova que a informação exibida corresponda à realidade. Entre a fotografia de uma coisa e a fotografia de um registo sobre a coisa vai a mesma distância que separa a testemunha presencial da testemunha que ouviu dizer: o sistema informático diz aquilo que lhe disseram.

O valor de convencimento da imagem de um ecrã depende da relação entre o sistema retratado e o facto a provar. Quando o facto vive dentro do sistema - o pagamento da taxa de justiça lançado no sistema do IGFEJ (capítulo 3.1), a declaração Modelo 3 submetida no Portal das Finanças (capítulo 6.1) -, o ecrã está colado à fonte, e a sua imagem, sobretudo se confrontada com o próprio sistema, pode sustentar a convicção do julgador. Quando o facto vive fora do sistema - a entrega física de duas cartas num balcão dos CTT -, o ecrã apenas mostra que alguém ali inscreveu que o facto ocorreu: a imagem prova a inscrição, não a ocorrência.

As aparências iludem? A imagem do ecrã não mentiu: apresentou, com fidelidade, aquilo que o ecrã mostrava. Quem se iludiu foi quem tomou o exibido pelo sucedido.

Por agora, a imagem não engana sobre si mesma: mostra com fidelidade o que representa, e o erro está apenas em quem a lê. Mas há de chegar o dia - e o capítulo 8 anuncia-o - em que a própria imagem poderá ser uma ilusão sem original, um *deepfake* integralmente gerado por inteligência artificial. Aí, já não bastará perguntar se a imagem foi adulterada, ou saber da sua falsidade material; será preciso perguntar se alguma vez o seu conteúdo correspondeu à realidade, ou saber da sua falsidade ideológica. Voltaremos ao tema, no final. Para já, continuamos com a imagem que se segue.

4.2. Street View: uma cápsula do tempo?: o valor probatório de fotografias que reproduzem vias rodoviárias

O caso: no Tribunal Administrativo e Fiscal de Loulé correu termos, sob o n.º 652/16.0BELLE, uma Ação Administrativa em que o Autor pedia a condenação de um Município a indemnizá-lo pelos

danos sofridos num acidente de viação ocorrido em 17 de julho de 2014, numa Estrada Municipal. Conduzindo um motociclo, o autor não parou no sinal vertical de STOP existente num entroncamento e embateu num automóvel que circulava em sentido contrário. Advogou que o acidente aconteceu devido à deficiente visibilidade do sinal de STOP, por este estar dobrado e em mau estado de conservação, e, conseqüentemente, devido à omissão dos deveres de sinalização e de vigilância da estrada que recaíam sobre o Município. O Município defendeu que existia, em 17 de julho de 2014, um sinal de pré-aviso de cedência de passagem (B1) por si lá colocado, tendo junto fotografias disponibilizadas pelo *Google Street View*. Chamada a intervir como interveniente acessória, por força do contrato de seguro, a Seguradora pugnou pela improcedência da Ação.

A audiência final teve lugar em 2 de maio de 2023, quase nove anos depois do embate.

A questão a decidir e o facto a apurar. O decurso do tempo era a principal dificuldade para a instrução do processo: como reconstituir, em 2023, o estado de um sinal de trânsito e a configuração de um entroncamento tal como existiam em julho de 2014? O sinal fora, entretanto, substituído; o local alterara-se; e o próprio Autor de nada se recordava, por ter sofrido um *“traumatismo craniano com amnésia para o episódio”*. Qual a melhor «máquina do tempo» (o meio de prova mais eficiente e eficaz) para trazer o passado ao processo?

No plano do mérito, discutia-se a responsabilidade civil extracontratual do município pelos danos resultantes da (alegada) omissão dos deveres de sinalização e vigilância, bem como a eventual concorrência de culpa do lesado. Mas, descendo ao plano dos factos, duas questões dependiam decisivamente da prova por imagem: a primeira, o estado em que o sinal de STOP se encontrava (dobrado, mas ainda assim visível?); a segunda, a (in)existência, à data do acidente, de um sinal de pré-aviso de cedência de passagem que o Município sustentava ter ali colocado. Para o demonstrar, porém, o Município juntara imagens do local, retiradas do *Google Street View*, mas sem menção da data em que haviam sido capturadas. Faltava uma imagem reportada a 2014. E essa imagem existia: nas panorâmicas históricas do *Google Street View*, recolhidas em maio de 2014, cerca de dois meses antes do acidente.

A fixação do meio de prova: no início da audiência de julgamento, o Município requereu a junção de três registos da sinalização existente no local, obtidos a partir dos resultados apresentados pela funcionalidade *Street View* do Google Maps. Tais registos correspondiam, então, à impressão em papel de *screenshots* de fotografias panorâmicas, a 360 graus, ao nível do solo, tiradas pela Google e/ou pelos utilizadores do Google Maps, que permitem visualizar, de forma imersiva, o aspeto dos locais que integram o mapa.

Ouvidas as partes, que não manifestaram qualquer oposição, a junção aos autos dos documentos foi admitida.

No entanto, o Tribunal foi mais longe e oficiosamente, com a concordância de todos os mandatários presentes, determinou o acesso ao Google Maps, através do computador e do ecrã da

sala de audiências, identificando nos autos os dois *URL* que apontavam para as imagens do local do acidente, em maio de 2014, a fim de serem exibidas durante a audiência.

Não foi, assim, determinada a realização de uma perícia, nem se pediram esclarecimentos à plataforma. Com o acordo das partes, criaram-se as condições para confrontar as testemunhas com uma reprodução fotográfica do local do acidente, disponibilizada por um terceiro e referenciada a uma data certa.

A produção da prova: a aplicação foi acedida ao vivo, durante a audiência. As imagens de maio de 2014 foram exibidas às testemunhas com conhecimento direto do local, não de forma estática, através das impressões juntas aos autos pelo Município, mas de forma dinâmica, através de cibernavegação, permitindo percorrer as estradas em que circularam os veículos que embateram. A navegação no *browser* do computador do Tribunal permitiu visualizar de forma unida, ainda que sincopada, de fotografia panorâmica em fotografia panorâmica, o percurso efetuado pelos veículos ao longo das estradas mapeadas, de forma semelhante à liberdade de movimento que os equipamentos de realidade virtual permitem.

O militar da GNR que elaborara a participação do acidente e a condutora do automóvel embatido confirmaram que aquilo que lhes foi mostrado no ecrã da sala de audiências correspondia à realidade que conheciam.

No final, a volatilidade da prova digital, manifestada na leitura contínua de código binário que transformou registos fotográficos panorâmicos numa espécie de vídeo, foi preservada no processo através de *screenshots* escolhidos pela Juíza, que foram anexados à ata da audiência de julgamento.

A valoração da prova: na fundamentação da decisão da matéria de facto, o Tribunal consignou que *teve em conta “as imagens do Google Maps datadas de Maio de 2014”,* que representavam a situação existente naquela data, utilizando os *screenshots* em três linhas fundamentadoras. Permitiram, em primeiro lugar, a perceção das características do local e da dinâmica do acidente, suprimindo a amnésia do autor e ancorando os depoimentos das testemunhas presenciais. Deram, depois, a conhecer o estado habitual do sinal - *“ligeiramente dobrado, mas ainda assim facilmente visível”* -, que o militar da GNR *“confirmou corresponder, aproximadamente, à situação com que se deparou no dia do acidente, ainda que pudesse estar um pouco mais dobrado”*. E foram, por fim, decisivos para afastar a tese do Município quanto à existência do sinal B1 (sinal de pré-aviso de cedência de passagem): como das imagens de maio de 2014 resultava que esse sinal ainda não existia, aparecendo apenas nas fotografias capturadas em 2018, o Tribunal presumiu que fora colocado já depois do acidente, julgando não provada a sua existência à data.

A consulta do Google *Street View* e os *screenshots* não foram, assim, tomados como retrato do instante do acidente, mas como elemento que, conjugado com a prova testemunhal, permitiram reconstituir o estado do local nas semanas que o antecederam.

Decisão: a ação foi julgada parcialmente procedente. O Tribunal teve por verificada a ilicitude, sob a forma de funcionamento anormal do serviço, por o Município não ter reparado o sinal danificado nem sinalizado de outro modo o perigo existente na via. Mas entendeu, num juízo de prognose póstuma, que o acidente se ficou a dever, em medida determinante, ao comportamento culposos do próprio autor, que circulava a velocidade superior a 50 km/h e não se apercebeu de um sinal que um condutor médio, atento e dentro daquele limite, poderia ter reconhecido. O Município foi, por isso, condenado a indemnizar o autor apenas em parte da quantia pedida, sendo absolvido do mais.

Trânsito: o Município recorreu para o Tribunal Central Administrativo Sul, com fundamento, além do mais, em erro na decisão da matéria de facto, uma vez que apesar de o Tribunal ter dado como provado que o sinal de STOP se encontrava, por vezes, danificado, sustentando que ficou demonstrado, através da prova testemunhal produzida, que o sinal se danificava por embates frequentes de camiões e que o Município atuava quando tinha conhecimento do defeito. O recurso encontra-se pendente.

Comentário: a mesma prova digital que sustentou a censura ao município - a deficiente sinalização do local -, sustentou igualmente a censura ao lesado: a configuração do entroncamento, tal como o *Street View* a revelou, tornava pouco crível que um condutor atento e dentro do limite de velocidade não conseguisse ver o automóvel à sua frente.

O caso anterior ilustrou uma situação em que a imagem de um ecrã (o *screenshot*) provava o conteúdo do ecrã, não o facto relevante para a decisão da causa. Aqui, a imagem é de outra natureza: não retrata um sistema que, por sua vez, descreve o facto, mas transmite, codificado em modo binário, o próprio local. É um meio de prova que, ao abrigo do predito artigo 368.º do Código Civil, faz prova plena do que representa se a exatidão não for impugnada, com a particularidade de a representação ter sido produzida por um terceiro alheio ao litígio (a plataforma, através de recursos próprios ou de contributos de utilizadores seus) e de vir acompanhada de uma referência temporal.

Justamente por isso, a sua valoração reclama três cautelas. A primeira respeita à natureza incorpórea e mediada da percepção: o Tribunal não inspeciona o local, vê uma representação do local, filtrada pelo ecrã e pela plataforma, o que recomenda o confronto da imagem com quem conhece a realidade retratada, como aqui sucedeu com as testemunhas presenciais. A segunda prende-se com a etiqueta temporal e a costura espacial das fotos: a data é uma informação a que o utilizador do Google tem acesso sem ser através do acesso direto aos metadados; a panorâmica do *Street View* resulta da costura automática de fotografias recolhidas por um veículo em circulação, mas a ligação entre fotos pode conter falhas. A terceira é a volatilidade: o Google atualiza as imagens e nada garante que o mesmo endereço devolva no momento da elaboração da sentença a mesma informação que apresentou durante a audiência – daí a relevância de incorporar no processo o *screenshot*, armazenando noutra suporta a informação que foi mostrada anteriormente.

4.3. Ortofotomapas: ver para crer, medir para saber?: o valor probatório de mapas que reproduzem o território

O caso: no processo n.º 934/13.2BELLE, o Ministério Público, agindo em defesa da legalidade urbanística e do ordenamento do território, impugnou os três atos que, num procedimento de obras, uma Câmara Municipal praticou a favor dos Contrainteresados: a aprovação do projeto de arquitetura, o deferimento do licenciamento e a concessão da autorização de utilização de uma moradia implantada em solo da Reserva Agrícola Nacional. O licenciamento assentou num pressuposto de facto: o de que a obra era de mera alteração e ampliação de uma construção preexistente, edificada em data anterior a 1951, de acordo com o registo predial, a matriz, um atestado da junta de freguesia e uma certidão da própria câmara. Sobre este alicerce documental foi construída toda a operação que, assim, não precisava do parecer da entidade regional da reserva agrícola e escapava à proibição de novas edificações fora dos espaços urbanos e urbanizáveis. O Ministério Público sustentou o oposto, que nenhuma construção ali preexistia e que a moradia foi construída de raiz, sem licença, em 2005 ou 2006, tendo junto imagens aéreas do terreno.

A questão a decidir e o facto a provar: tudo se resumia a uma questão de facto, a de saber se, no local onde veio a ser implantada a moradia, existia, ou não, uma edificação anterior àquele licenciamento e, existindo, desde quando. A dificuldade consistia em estar em causa a prova da (in)existência de uma construção em anos idos: isto é, a prova daquilo que o presente já não mostrava porque, entretanto, se alterou a situação que preexistia no local e foi construída a casa dos Contrainteresados.

A fixação do meio de prova: o estado do território em determinado ano pretérito é um facto consumado e irrepetível que não é passível de inspeção no presente. Só sobrevive enquanto registo e um registo idóneo a demonstrar o aspeto físico de um lugar, numa data certa, é a cobertura aérea. O Ministério Público tinha juntado imagens aéreas do terreno, mas o Tribunal solicitou a junção de ortofotomapas - reproduções de fotografias aéreas produzidas e arquivadas por entidades cartográficas oficiais, como a Direção-Geral do Território, o Instituto Geográfico Português ou o Instituto Geográfico do Exército, com georreferenciação, isto é, a inscrição da data e das coordenadas, permitindo localizar o território fotografado no espaço e no tempo - com a área do prédio delimitada e sinalizada, bem como outras fotografias aéreas que constavam de um inquérito-crime.

A produção da prova: cumprindo o despacho, o Ministério Público juntou aos autos as reproduções aerofotográficas com a indicação do exato local da edificação, certidão das mesmas com a delimitação da área do prédio e cópias certificadas das fotografias aéreas extraídas do inquérito. Reuniu-se, assim, uma série temporal de coberturas, relativas aos anos de 1972, de 1987, de 1995, de 1997, de 2002, de 2005 e de 2007, que funciona como uma verdadeira sequência cronológica do território. As imagens mais antigas eram fotografias de película (analógicas); as mais recentes, digitais. O que se verificou foi que em todas as imagens tiradas entre 1972 e 2005, no ponto

assinalado, não havia nenhuma construção. Só no ortofotomapa da Direção-Geral do Território relativo a 2007, já depois de emitido o alvará, são visíveis trabalhos de remodelação e o início das obras. As imagens, datadas, fixam o intervalo: a moradia nasceu entre a cobertura de agosto de 2005 e a deslocação ao local do fiscal municipal que a fotografou em julho de 2006. A força desta prova documental teve, ainda, outro efeito: um dos depoentes, confrontado com as imagens, admitiu ter sido ele a erguer a edificação *“possivelmente por volta de 2005”*.

A valoração: não tendo sido impugnada a exatidão das reproduções, operou em pleno o efeito do artigo 368.º do Código Civil: os ortofotomapas fizeram prova plena dos factos e das coisas que representavam, isto é, do estado do território em cada uma das datas. Daí ter o Tribunal afirmado, na fundamentação da decisão sobre a matéria de facto, *ter ficado “absolutamente convicto que, no local onde veio a ser implantada a moradia dos contra-interessados, não (pre)existia, até pelo menos ao ano de 2005, edificação alguma”*. A prova digital criou, então, no julgador, uma convicção mais forte que todos os elementos que sustentaram o procedimento, entre os quais a descrição predial, a inscrição matricial, a declaração modelo 1 do IMI, o «atestado» da junta e a «certidão» camarária, todos a afiançar uma preexistência anterior a 1951. Sucede que a força probatória do documento autêntico não cobre a verdade intrínseca dos factos que o funcionário não percecionou diretamente, mas que apenas recebeu por declaração de terceiro (artigo 371.º, n.º 1, do Código Civil).

Decisão: o Tribunal concluiu, então, que o prédio correspondente a um outro artigo matricial, inscrito em 1971 para um barracão de alfaias com 17,50m², fora *deslocalizado*, por via de declarações fiscais sucessivas, de modo a fazê-lo coincidir com o local onde a moradia veio a ser construída, viabilizando a escritura e o licenciamento sobre uma preexistência falsa. A consequência decisória seguiu-se sem esforço: provada a inexistência de edificação legalmente preexistente, concluiu-se pela existência de erro nos pressupostos da licença que violava, assim, o Plano Diretor Municipal e carecia do parecer da entidade regional da reserva agrícola nacional.

Trânsito: o Município interpôs recurso contra a sentença, mas apenas quanto à decisão de direito (não atribuição de efeitos aos atos declarados nulos). Ainda assim, deixa-se a ligação para o acórdão que negou provimento ao recurso: <https://dgsl.pt/acordaos/404632100085fc04>.

Comentário: Fotos, Imagens e Mapas não são, assim, todos farinha do mesmo saco. A panorâmica de rua, captada ao nível do solo e imersiva, a fotografia aérea, a imagem de satélite e o ortofotomapa partilham a mesma natureza digital e o mesmo regime das reproduções mecânicas, mas distinguem-se no modo de captação, na perspetiva e no grau de precisão que oferecem. O ortofotomapa, geometricamente corrigido e georreferenciado, admite medições rigorosas sobre a imagem; a panorâmica do *Street View* oferece imersão e reconhecimento do local, mas não escala métrica fiável. Cada género tem, por isso, a sua vocação probatória própria. Se na inspeção judicial de facto eletrónico, como se verá, é o sistema que se desloca ao gabinete do Juiz, e não o Juiz que vai ter com o objeto inspecionado, o recurso à prova documental por imagens permite uma

deslocação no tempo. Aliás, no caso, de nada teria servido ao Tribunal ter-se deslocado ao local, pois a questão era a de saber o que lá existia antes de ser construída a casa.

5. A prova através de perícia a facto eletrónico

Nos casos anteriores, o Tribunal leu por si as imagens, porque para as compreender bastavam os sentidos e a experiência comuns. Nem sempre é assim: quando o facto digital exige conhecimentos especiais que o julgador não possui, o caminho deve ser outro, o da perícia.

Dispõe o artigo 116.º, n.º 1, do Código de Procedimento e de Processo Tributário que *poderá haver prova pericial “sempre que o juiz entenda necessário o parecer de peritos especializados”, a qual – n.º 4 – “será regulada nos termos do Código do Processo Civil”*. Nos termos da primeira parte do artigo 388.º do Código Civil, *a prova pericial tem por fim a perceção ou apreciação de factos por meio de peritos, quando sejam necessários conhecimentos especiais que os julgadores não possuam*.

Pretendeu, assim, o legislador que o Juiz tivesse a possibilidade de se socorrer de um especialista para elaborar um parecer de natureza técnica relativo aos factos relevantes para a decisão da causa.

Apesar de este meio de prova ter sido pensado para superar a falta de *conhecimentos especiais* dos julgadores, o legislador determinou, ainda assim, que *“A força probatória das respostas dos peritos é fixada livremente pelo tribunal”* – artigo 389.º do Código Civil. Por este motivo se diz que *“O Juiz é o perito dos peritos”*, mas na prática, face a um relatório devidamente fundamentado, tirado por unanimidade no caso de a perícia ser colegial (no caso de as partes requererem ou o Juiz entender que a perícia reveste especial complexidade – artigo 478.º, n.º 1, do Código de Processo Civil), e na ausência de outra prova produzida, raramente as conclusões do relatório não serão suficientes para criar no Juiz a convicção sobre a (não) verificação do facto.

“A perícia, requerida por qualquer das partes ou determinada oficiosamente pelo juiz, é requisitada pelo tribunal a estabelecimento, laboratório ou serviço oficial apropriado ou, quando tal não seja possível ou conveniente, realizada por um único perito, nomeado pelo juiz de entre pessoas de reconhecida idoneidade e competência na matéria em causa” – artigo 467.º, n.º 1, do CPC.

Por força do artigo 475.º, n.º 1, do mesmo diploma, *“Ao requerer a perícia, a parte indica logo, sob pena de rejeição, o respetivo objeto, enunciando as questões de facto que pretende ver esclarecidas através da diligência”,* sendo que – artigo 476.º, n.º 2, primeira parte – *“Incumbe ao juiz, no despacho em que ordene a realização da diligência, determinar o respetivo objeto”*.

A perícia é, assim, um meio de prova adequado para apreciar factos que requeiram conhecimentos especiais, como a genuinidade de um documento, a falsidade de uma assinatura, a

análise de programação informática, a correção do tratamento contabilístico de determinada operação, a recuperação de dados informáticos apagados, ou a integridade de um ficheiro.

Se não forem necessários conhecimentos especiais para a apreciação do facto, então, em vez da perícia e da intervenção de um agente externo, o Juiz pode lançar mão da inspeção, como se verá de seguida.

Na perícia a facto eletrónico, o objeto pode ser um sistema, um ficheiro ou um código informático, pelo que o método de análise é relevante para garantir um resultado capaz de ajudar a criar a convicção do Juiz.

Impõe-se, desde logo, que a intervenção do(s) perito(s) não contamine o objeto da perícia, pois, como se disse já, o documento ou o facto digital pode ser copiado sem perda de qualidade, mas também se assinalou que as alterações aos *bits* podem ser extremamente difíceis de detetar.

Por outro lado, a própria preparação da perícia não está isenta de dificuldades, pois é o mesmo julgador que *não tem conhecimentos especiais* que terá de *determinar o seu objeto*, desde logo com a elaboração de quesitos (a enunciação das questões de facto que pretende ver esclarecidas) que têm de ser simultaneamente percetíveis pelo perito, suscetíveis de apreciação pericial e úteis para a decisão da causa.

5.1. Bebida do dia: chá do sumiço: o mistério das linhas desaparecidas em *software* de faturação

O caso: no processo n.º 185/12.3BELLE, os Impugnantes, que exploravam um restaurante, pediam a anulação das liquidações de IRS e de IVA dos anos de 2007 e 2008, emitidas na sequência de uma ação inspetiva que recorrera a métodos indiretos. Na origem das correções estava uma recolha efetuada pela equipa de auditoria informática da Direção de Finanças, que copiara para um CD não regravável o sistema informático de faturação dos Impugnantes, o programa X. Analisada a base de dados com uma aplicação de auditoria, a Inspeção concluiu que o ficheiro «Detalhe» - o único que permite a sumarização do IVA por taxas e que, por isso, serve de base aos fechos diários - apresentava incongruências na numeração das suas linhas: em 24.538 linhas ativas de processos (mesas) com anulações, foram identificadas 4.025 linhas em que o campo «Relation_Seq_Number» remetia para linhas de anulação com numeração igual ou superior à última linha existente - processos que referiam, por exemplo, a anulação de uma linha n.º 8 quando só tinham cinco linhas e deveriam ter, pelo menos, nove. A estas somavam-se anulações pouco verosímeis (refeições completas, com entradas, pratos principais, vinho e digestivos, integralmente canceladas, subsistindo apenas um café ou uma água) e falhas na numeração sequencial dos processos, com mesas inteiras desaparecidas. A Inspeção presumiu então a matéria coletável aplicando, mês a mês, a percentagem de pedidos ilicitamente eliminados ao total dos pedidos registados, multiplicada pelo preço médio por pedido. Os Impugnantes deduziram Impugnação Judicial, pedindo a anulação das liquidações, advogando que as anomalias eram consequência do funcionamento normal do

programa em face dos circunstancialismos habituais (clientes que pedem faturas individuais e obrigam a apagar parte do pedido para abrir nova mesa; o cliente que vê um amigo na outra ponta do restaurante e termina a refeição em conjunto, obrigando à junção das mesas no programa de faturação; produtos anulados por engano; clientes que mudam de ideias e alteram a encomenda...), e que *“qualquer apagamento de linhas deixa rasto”*.

A questão a decidir e o facto a provar: as questões de direito eram as de saber se estavam reunidos os pressupostos do recurso à avaliação indireta da matéria coletável e se houvera erro ou manifesto excesso na sua quantificação. Mas tudo gravitava em torno de uma hipótese nuclear, a dar como provada ou não provada: as incoerências encontradas na base de dados resultavam da utilização normal do programa pelo utilizador final, ou de manipulação? O facto a provar era, em rigor, o comportamento de um software: o que faz o programa X, nos seus ficheiros internos, quando se divide uma conta, se juntam duas mesas ou se anula um pedido por engano?

A fixação do meio de prova: os Impugnantes requereram a realização de uma perícia logo na Petição Inicial, indicando o seu perito, mas sem indicarem o objeto nem enunciarem as questões de facto a esclarecer. Convidados, por duas vezes, a completar o requerimento, limitaram-se a remeter para a parte II do articulado, que misturava matéria contabilística, informática e de direito. Coube então ao Tribunal, em substituição dos requerentes, formular os quesitos, o que obrigou o Juiz a traduzir casos comuns do quotidiano da restauração, alegados na Petição, em hipóteses tecnicamente testáveis do comportamento do programa informático de faturação. Foi, então, determinada uma perícia colegial para a contabilidade e uma perícia singular, a requisitar a estabelecimento oficial apropriado, para a informática. A primeira entidade contactada pelo Tribunal para realizar a perícia informática foi a Polícia Judiciária que concluiu que os quesitos apresentados, *“elevadamente específicos no que concerne a determinado software”, “apenas poder[iam] ser respondidos de forma tecnicamente inquestionável pela própria empresa desenvolvedora”,* e propôs que a perícia fosse realizada pela empresa que produziu e comercializava o programa X ou, em alternativa, a Microsoft. Os Impugnantes aceitaram a sugestão de ser a empresa a realizar a perícia, mas a Fazenda recusou-a, por entender que a empresa tinha interesse no resultado da diligência. Contactada a Microsoft, esta informou que não dispunha de técnicos disponíveis para realizar perícias. O Tribunal acabou por requisitar a diligência à Associação Portuguesa de Software, que anunciava no seu site a realização de exames periciais.

A produção da prova: a Fazenda juntou aos autos o CD com a cópia do sistema recolhida na inspeção, e o perito tentou montar com ele um ambiente de produção. Não teve, todavia, sucesso, por o CD conter apenas parte dos ficheiros do programa X e as bases de dados, faltando *“todos aqueles ficheiros necessários para tornar a aplicação exequível, em particular o seu sistema operativo, que no caso era uma distribuição de Linux”*. O perito alertou, ainda, que *“caso se tivesse optado por preservar a prova através da captura de uma imagem completa do sistema, ao invés de fazer apenas uma cópia do sistema de ficheiros disponível, este problema seria facilmente ultrapassado”*. Por se tratar de uma solução muito específica, só os técnicos da empresa produtora dispunham dos

elementos necessários para reproduzir com exatidão a versão instalada no restaurante, pelo que o perito propôs a conversão da diligência em perícia colegial. Ouvidas as partes, e agora sem oposição da Fazenda, o Tribunal oficiou a empresa responsável pelo programa X para identificar um técnico, tendo depois solicitado aos dois peritos que cooptassem o terceiro. A perícia foi realizada nas instalações da empresa produtora, onde os peritos recriaram *“um ambiente idêntico ao do utilizador final na sua versão de produção”*, usando a mesma versão do software, disponibilizada do repositório original, em conjunto com o backup constante do CD apreendido à ordem do processo. O ambiente em que a perícia foi realizada teve, todavia, duas diferenças em relação ao ambiente do restaurante: por um lado, não foi possível utilizar a licença original do restaurante, por falta de palavra-passe, o que foi suprido com a emissão de uma licença gerada exclusivamente para a perícia; por outro, também não foi replicado o endereço IP da rede do restaurante. De seguida, os peritos concretizaram, uma a uma, as hipóteses descritas nos quesitos e, no final, chegaram a uma pronúncia unânime: nem a divisão de contas, nem a junção de mesas criavam divergências entre produtos e valores; qualquer anulação ficava registada na respetiva linha de detalhes; a omissão de linhas e a referência a linhas inexistentes descritas no Relatório de Inspeção não se deviam à normal utilização do programa; e o programa não permitia ao utilizador apagar linhas de processos emitidos - tal só seria possível *“usando uma ferramenta de manipulação da base de dados externa ao [Programa X]”*, como um editor de texto ou uma folha de cálculo. Notificado o relatório, a Fazenda pediu ainda um esclarecimento sobre a quebra de sequência no ficheiro de cabeçalho, que os peritos prestaram conjuntamente, fechando a última porta: a quebra dever-se-ia a uma configuração que *“não se encontrava ativa no backup analisado”*, ou à adulteração dos dados por um utilizador.

A valoração da prova: as respostas dos peritos foram vertidas, quase literalmente, na fundamentação da decisão da matéria de facto. Consequentemente, os factos alegados pelos Impugnantes como explicação para as anomalias foram dados como não provados por confronto com as respostas constantes do relatório pericial. Por outro lado, foi dado como provado que as incoerências não resultavam do uso normal do programa e que o apagamento de linhas exigia ferramenta externa. Na fundamentação, o Tribunal sublinhou que a manipulação foi *“certificada, por unanimidade, por três peritos imparciais, um pertencente a uma associação de software independente e dois com ligações profissionais ao grupo empresarial responsável pela criação e desenvolvimento do programa”*.

Decisão: demonstrada a adulteração da base de dados - e, com ela, que os elementos de suporte à contabilidade não eram fidedignos -, ficou legitimado o recurso aos métodos indiretos; e, não tendo os Impugnantes provado a existência de erro ou de manifesto excesso do critério de quantificação, a Impugnação foi julgada improcedente, mantendo-se as liquidações de IRS e IVA de 2007 e 2008.

Trânsito: não foi interposto recurso.

Comentário: as principais dificuldades sentidas neste processo estiveram relacionadas com a elaboração dos quesitos, a escolha dos peritos e a criação das condições para a perícia ser realizada num ambiente controlado.

Aqui foram precisos três terceiros, com conhecimentos especiais, para dizer ao Tribunal o que o programa fazia. No caso seguinte, o facto digital era simples de ver: bastava abri-lo. E o que o Juiz pode ver por si não precisa de ouvir de outrem.

6. A prova por inspeção judicial a facto eletrónico

Nos termos do artigo 390.º do Código Civil, *“A prova por inspeção tem por fim a percepção direta de factos pelo tribunal”*. Trata-se, pois, de um dos melhores exemplos do princípio da imediação, na medida em que o Juiz não conhece o facto através do relato de terceiros (peritos, partes ou testemunhas), nem da sua representação documental, mas através dos seus próprios sentidos. Pelo que, naturalmente, *“O resultado da inspecção é livremente apreciado pelo tribunal”* - artigo 391.º do Código Civil -, que não tarifado pela lei.

Também a prova por apresentação da coisa, prevista no artigo 416.º do Código de Processo Civil, é uma prova real e direta. Aqui, no entanto, em vez de ser o Juiz a sair do Tribunal e a deslocar-se até ao local onde a coisa se encontra, esta, *se for móvel e não causar inconveniência, é posta à disposição do Tribunal* através da sua entrega na secretaria, onde a parte contrária a pode examinar e colher fotografia. A diferença, neste caso, entre a prova por inspeção e a prova por apresentação da coisa é, essencialmente, o local onde a prova é produzida.

A coisa a examinar pode, no entanto, ser um imóvel, ou uma coisa móvel que não pode ser apresentada na secretaria, como um barco, por exemplo. Neste circunstancialismo, o Juiz deve *“deslocar-se ao local da questão ou mandar proceder à reconstituição dos factos, quando a entender necessária”* - artigo 490.º, n.º 1, parte final, do CPC -, produzindo, então, a prova por inspeção.

Este meio de prova, além de não carecer de intermediação, é também mais rápido que a prova pericial, embora seja igualmente *lavrado um auto da diligência*, no qual se registam *“todos os elementos úteis para o exame e decisão da causa, podendo o juiz determinar que se tirem fotografias para serem juntas ao processo”* - artigo 493.º do CPC.

Além da sua finalidade principal, comum a todos os meios de prova - *“a demonstração da realidade dos factos”*, na terminologia do predito artigo 341.º do Código Civil -, a inspeção judicial pode, em alguns casos, ter uma função preliminar, tendo em vista a organização da instrução do processo. O Juiz pode, por exemplo, numa ação de responsabilidade intentada contra um município, inspecionar o local onde ocorreu um acidente para ficar com uma ideia mais clara da causa de pedir do Autor e perceber de forma mais precisa os factos por este alegados.

Ora, do exposto resulta que o instituto da prova por inspeção foi pensado para coisas imóveis e para coisas móveis insuscetíveis de serem apresentadas na secretaria do Tribunal.

Sendo o objeto da inspeção um facto eletrónico, como um registo que apenas existe codificado através de dígitos binários, o regime carece de ser adaptado.

Com efeito, em vez de o Juiz se deslocar ao local onde se encontra o servidor no qual é produzido ou está armazenado o código binário, é o facto eletrónico que é trazido ao Tribunal, como acontece na produção de prova por apresentação de coisa móvel, uma vez que, dadas as características do facto digital, uma mera sequência de *bits*, a sua descodificação pode ser efetuada no monitor e no computador do Tribunal.

Depois, sendo o objeto da inspeção volátil por natureza, sendo descodificado no momento em que a consulta ao suporte em que se encontra é realizada, o facto eletrónico tem de ser armazenado num formato adequado (*download* de ficheiro, armazenamento em disco ou *pen...*) e posteriormente introduzido no processo judicial eletrónico, procedimento complementado pelo *auto da diligência* no qual se descreve o que foi apreendido pelos sentidos do Juiz e se regista o modo como este teve acesso ao facto eletrónico, determina o seu armazenamento e ordena que seja junto aos autos.

Um outro ponto que distingue a inspeção a facto eletrónico da inspeção a coisa corpórea é o constrangimento que sofre a característica da imediação, uma vez que os sentidos do Juiz só têm acesso à coisa eletrónica através de uma infraestrutura (o computador, o perfil de utilizador do sistema operativo *Windows*, a gestão do *browser*, a disponibilização do provedor de acesso à internet...).[\[x\]](#)

Finalmente, nem sempre a perceção direta pelo próprio Juiz é indispensável. Quando a inspeção judicial seja legalmente admitida, mas o Juiz a não considere necessária, pode ser incumbido técnico ou pessoa qualificada de proceder aos atos de inspeção, apresentando relatório com todos os elementos úteis para o exame e decisão da causa: é a verificação não judicial qualificada, prevista no artigo 494.º do CPC, cujo resultado o Tribunal aprecia livremente. No domínio do facto eletrónico, este instituto oferece uma via intermédia entre a perícia, que pressupõe conhecimentos especiais que o julgador não possui, e a inspeção, que mobiliza os sentidos do próprio julgador.

6.1. Declaração escondida com rabo de fora?: a impugnação da autenticidade da declaração Modelo 3 de IRS

O caso: no processo n.º 13/14.5BELLE, os Impugnantes pediam a anulação de uma liquidação adicional de IRS. Alegavam ter declarado a alienação de partes sociais de uma empresa no campo 8-A do anexo G da declaração modelo 3, entregue pela internet, o que determinaria a tributação de apenas 50% do saldo das mais-valias, ao abrigo do disposto no artigo 43.º, n.º 3, do Código do IRS.

Juntaram, com a Petição Inicial, o documento n.º 3 que era o comprovativo da declaração, digitalizado a partir de impressão do ficheiro disponibilizado pelo Portal das Finanças. A Fazenda Pública defendeu-se por impugnação, sustentando que nos registos do seu sistema informático, o campo 8-A não se encontrava preenchido e - eis o detalhe digital - o número de identificação da declaração, constante do rodapé de todas as páginas do comprovativo, estava em falta nas páginas do anexo G junto pelos Impugnantes. Concluiu, então, que o anexo G junto pelos Impugnantes não correspondia à declaração que fora submetida e ao ficheiro gerado pelo Portal das Finanças, impugnando, nos termos do artigo 444.º, n.º 1, do CPC, a exatidão mecânica da reprodução.

A questão a decidir e o facto a provar: a questão de direito era a de saber se a liquidação padecia de erro nos pressupostos de facto. Tudo dependia, pois, de um único facto, a dar como provado ou não provado: se a declaração Modelo 3 de IRS entregue eletronicamente era constituída, ou não, pelo anexo G com o campo 8-A preenchido. E a resposta pressupunha a resolução de uma questão de facto - a autenticidade e a genuinidade do documento n.º 3, isto é, a sua autoria e a sua conformidade com a declaração registada no sistema da Administração Tributária. O facto a provar era, em rigor, digital: o “original” da declaração não existia em papel, existia apenas como registo binário num sistema de informação pertencente à Administração, a parte que impugnara o documento. E instalara-se um impasse típico desta nova realidade: a prova documental esgotara-se; a prova testemunhal seria inútil; e a perícia ao sistema da AT, embora possível, seria morosa e onerosa.

A fixação do meio de prova: impugnada a exatidão mecânica da reprodução, incumbia aos apresentantes a prova da sua conformidade com o registo original. Os Impugnantes, reafirmando que o documento apresentado refletia o que tinham submetido e que era a impressão do ficheiro gerado pelo Portal das Finanças, equacionaram que a falta do rodapé resultaria de uma qualquer parametrização dos documentos feita pela própria Administração, tendo requerido, ao abrigo do artigo 445.º, n.º 2, do CPC, a consulta da declaração constante do sistema informático. Pediram, no fundo, que o Tribunal fosse ver o original à fonte. O despacho que deferiu a diligência, “*face à sua pertinência*”, considerou que para comparar dois rodapés não eram necessários conhecimentos especiais que o Juiz não possuísse, pelo que determinou a realização de uma inspeção judicial, ainda que com algumas adaptações: não seria o Juiz a deslocar-se ao servidor onde o registo se encontrava, seria o facto eletrónico a ser trazido, em linha, ao Tribunal. O despacho fixou a data e a hora da diligência, convocou os Impugnantes, a sua Advogada e a Representante da Fazenda Pública, e, no caso de não terem sido os Impugnantes, as pessoas que imprimiram o documento n.º 3, a comparência e quem o fez. Foi também expressamente solicitado que os Impugnantes comparecessem na posse dos seus números de identificação fiscal e das senhas de acesso ao Portal das Finanças, tendo sido pré-definido no despacho o caminho de navegação a percorrer (Serviços: Obter – Comprovativos: IRS – Declaração – Comprovativo / Prova de Entrega).

A produção da prova: a inspeção realizou-se no Tribunal, durou vinte minutos e ficou documentada num auto que descreve todo o procedimento: que o Juiz abriu o *browser* no

computador de serviço; que este estava ligado à internet através da rede judicial; que foi introduzido o endereço do Portal das Finanças na barra de endereços do *browser*. O uso do computador foi então facultado à Advogada dos Impugnantes, que preencheu os campos de identificação fiscal e de senha “*com os dados ditados pela Impugnante*”, sem que a senha de acesso tenha sido alguma vez facultada ao Tribunal ou junta ao processo, e percorreu o caminho de navegação previamente fixado. A seleção do comprovativo abriu a declaração numa nova janela; o Juiz verificou que o ficheiro era apresentado a partir do domínio da Administração Tributária (www.portaldasfinancas.gov.pt) através de um protocolo de comunicação seguro (<https://>) e constatou que o rodapé do anexo G continha apenas a paginação no lado direito, nada constando do lado esquerdo nem da zona central - exatamente como no documento n.º 3 -, encontrando-se o campo 8-A preenchido. A perceção, volátil por natureza, foi de imediato estabilizada: o ficheiro foi gravado no ambiente de trabalho do computador, impresso, rubricado e junto aos autos ao abrigo da parte final do artigo 493.º do CPC - a versão digital das «fotografias» que o preceito autoriza.

O auto foi notificado à Representante da Fazenda Pública que não comparecera à diligência. A Fazenda solicitou esclarecimentos à Direção de Serviços do IRS que reconheceu que “*durante o tratamento das declarações de 2012 houve uma anomalia na transferência dos dados para o sistema central, não tendo sido carregada a informação relativa ao quadro 8-A do anexo G*”, sendo “*por lapso*” que o anexo G não continha a informação de rodapé.

A valoração da prova: face ao resultado da inspeção e à posição assumida pela Fazenda Pública, concluiu-se que o documento n.º 3 reproduzia de forma genuína a informação constante do Portal das Finanças. Na decisão da matéria de facto foi dado como provado que a declaração Modelo 3 de IRS entregue pelos Impugnantes era composta pelo anexo G com o campo 8-A preenchido. Na fundamentação, foi reproduzido o procedimento seguido na inspeção e o resultado alcançado.

Decisão: o incidente de impugnação foi julgado improcedente e, conseqüentemente, a Impugnação Judicial julgada procedente, anulando-se o ato de liquidação e condenando-se a Administração no pagamento de juros indemnizatórios.

Trânsito: não foi interposto recurso.

Comentário: a instrução do processo foi feita com alguma hesitação, mas com a cooperação das partes alcançou-se a composição definitiva do litígio, em prazo razoável, mediante processo equitativo. A diligência durou cerca de vinte minutos e não teve encargos com o pagamento de honorários de peritos, pelo que a inspeção se revelou uma boa opção. No entanto, como se reconhece agora, teria sido adequado guardar o ficheiro numa *pen* e, posteriormente, ser determinada a sua junção ao processo, em vez de apenas o imprimir.

Até aqui, o digital deu-nos coisas para ver: documentos, imagens, sistemas. Terminaremos com um meio de prova em que o digital não traz a coisa, mas a pessoa: a testemunha que depõe à

distância.

7. A prova testemunhal através de videoconferência eletrónica

A prova testemunhal é produzida através dos depoimentos prestados no processo pelas testemunhas que, tal como os peritos, são intervenientes accidentais. No entanto, enquanto os peritos, no seu relatório, utilizam os seus conhecimentos especiais para emitir uma apreciação sobre os factos constantes dos quesitos, as testemunhas devem apenas narrar, sob juramento e cominação da prática de crime, factos que tenham visto, ouvido ou nos quais tenham participado, sem emitir qualquer tipo de apreciação.

“A força probatória dos depoimentos das testemunhas é apreciada livremente pelo tribunal” – artigo 396.º do Código Civil -, o que significa que o Juiz pode valorar o depoimento de uma única testemunha e não dar relevo ao depoimento prestado por outras nove, ainda que estes sejam coerentes entre si. O que o Juiz tem de fazer é, na fundamentação da decisão da matéria de facto, explicar os motivos pelo qual aquela testemunha discordante o fez criar a convicção, e o das restantes não, com referência não só ao teor do depoimento, mas também ao modo como se expressa (nível de hesitação demonstrado, tom de voz utilizado, espontaneidade das respostas, reação ao contraditório...) e a eventuais elementos contextuais que o corroborem.

Por referência à baixa fiabilidade da prova testemunhal, costuma dizer-se que *“O Juiz vai para o inferno nas cavalitas da testemunha”*. A verdade é que a baixa fiabilidade da prova testemunhal não resulta, exclusivamente, da possibilidade de a testemunha querer, voluntariamente, ser parcial no seu depoimento. A falha pode ser involuntária, baseada em erros de perceção, criação de falsas memórias ou falhas de retenção, que culminam numa narração dos factos errada ou incompleta. E pode também acontecer que a falha esteja do lado do Juiz, nomeadamente por não conhecer regionalismos ou dominar vocabulário técnico.

Relativamente à inquirição das testemunhas no processo judicial tributário, dispõe o artigo 118.º do Código de Procedimento e de Processo Tributário que *“Os depoimentos são prestados em audiência contraditória, devendo ser gravados, sempre que existam meios técnicos para o efeito, cabendo ao juiz a respectiva redução a escrito, que deve constar em acta, quando não seja possível proceder àquela gravação”*. Por regra, por força do artigo 119.º, n.º 1, do CPPT, *“As testemunhas residentes na área de jurisdição do tribunal tributário são notificadas por carta registada, sendo as restantes a apresentar pela parte que as ofereceu, salvo se fundadamente se requerer a sua notificação”*, sendo que – n.º 3 – as partes *“podem requerer que o depoimento das testemunhas residentes fora da área de jurisdição do tribunal tributário seja feito”*, de preferência *“durante a mesma diligência em que são ouvidas as demais testemunhas”* – n.º 5 -, *“por teleconferência gravada a partir do tribunal tributário da área da sua residência, devendo ser identificadas perante funcionário judicial do tribunal onde o depoimento é prestado”* – n.º 4.

Por sua vez, o artigo 502.º, n.º 5, do Código de Processo Civil, epígrafado «Inquirição por meio tecnológico», que é subsidiariamente aplicável ao processo judicial administrativo e ao processo judicial tributário, estatui que *“Sem prejuízo do disposto em instrumentos internacionais ou europeus, as testemunhas residentes no estrangeiro são inquiridas através de equipamento tecnológico que permita a comunicação, por meio visual e sonoro, em tempo real, sempre que no local da sua residência existam os meios tecnológicos necessários”*.

Assim, sem prejuízo do disposto na Convenção Europeia sobre a Obtenção no Estrangeiro de Informações e Provas em Matéria Administrativa, aprovada, para ratificação, pelo Decreto n.º 58/80, de 1 de agosto, relativamente à emissão de cartas rogatórias – convenção que de acordo com o n.º 2 do seu artigo 1.º *“não é aplicável em matéria fiscal”* –, nada obsta a que as testemunhas residentes no estrangeiro sejam inquiridas por meio tecnológico, depondo a partir do local da sua residência.

Pretendeu, assim, o legislador *agilizar* a inquirição das testemunhas residentes no estrangeiro *“por meios tecnológicos fiáveis, designadamente por Skype (RL 19-11-19, 28325/17)”*, com o objetivo de afastar um *“fator de acrescida morosidade na conclusão dos processos”*. A *“falta da solenidade própria da prestação de um depoimento em plena audiência final”*, *“o maior distanciamento físico da testemunha relativamente ao Tribunal [que] poderá agravar o problema crónico da falsidade dos depoimentos”*, o beliscar do *“princípio da imediação”* e do *“princípio da livre apreciação dos meios de prova oralmente produzidos”*, *“não podem ser hipervalorizados”*, não só porque os depoimentos em sala também são falíveis e se desconhecem quais são os aspetos verdadeiramente relevantes para permitir avaliar a credibilidade dos depoimentos, mas também porque se é claro que a autoridade do Estado se manifesta através do *“ritualismo judiciário, não deve ignorar-se que, a par desse valor, existem os interesses da eficiência dos meios processuais e da celeridade na administração da justiça”*.

[\[xi\]](#)

Esta é a base legal que permite a entrada nas salas de audiências a aplicações como o Webex, Zoom, Teams, Messenger, FaceTime ou WhatsApp.

De repente, a testemunha já não tem de estar nas instalações de outro Tribunal para ser inquirida à distância, uma vez que a maioria tem no *smartphone* alternativas para ser vista e ouvida, desde que tenha uma ligação à internet.

“Na linha da jurisprudência do TEDH quanto à maior latitude na definição de um julgamento justo na jurisdição cível, e face ao quadro legal existente (pré-pandemia), nada obsta a que as partes acordem em inquirir testemunhas e/ou partes em termos mais amplos dos que os legalmente previstos (cf. art. 345.º CC; arts. 6.º, n.º 1, 7.º, n.º 1, 630.º, n.º 2, CPC), realizando mesmo videoconferência privada. Essa inquirição mais flexível pode e deve ser proposta pelo próprio juiz às partes. No limite, o assentimento das partes pretere a arguição subsequente de qualquer nulidade (cf. arts. 195.º, n.º 1, e 197.º, n.º 2, do CPC). Para esconjurar o perigo de influência indevida sobre a testemunha, no âmbito da videoconferência privada, poderão as partes – querendo e financiando – convencionar que a prestação do depoimento seja supervisionada por notário, que atestará os termos do espaço

envolvente da testemunha e a sua prestação de depoimento sem interferências de qualquer índole, podendo o depoimento ocorrer, para tal efeito, no próprio cartório, nacional ou internacional”.[\[xii\]](#)

A especificidade digital está na conversão: câmaras e microfones transformam a imagem e a voz em sinal binário, que viaja comprimido pela rede e é reconstituído no ecrã e nas colunas da sala de audiências. Esta particularidade coloca em xeque pelo menos três garantias da prova testemunhal: a identificação fiável da testemunha, no caso de não estar um funcionário/notário presente; a espontaneidade, na medida em que o Tribunal não controla o ambiente de onde a testemunha depõe, não vendo quem mais está na sala, se há documentos ou notas à vista, ou se o depoimento está a ser orientado fora do enquadramento da(s) câmara(s); e a imediação, pois a perceção do juiz fica condicionada pela qualidade da imagem e do som, pelo enquadramento e pela latência da ligação, que dilui as pausas e as hesitações.

De resto, o depoimento segue as regras do instituto: depois de, ao abrigo do artigo 513.º, n.º 1, do CPC, *fazer sentir à testemunha a importância moral do juramento e o dever de ser fiel à verdade, advertindo-o das sanções aplicáveis às falsas declarações, o Juiz “procura identificar a testemunha 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”,* sendo que – n.º 2 – *“Quando verifique pelas respostas que o declarante é inábil para ser testemunha ou que não é a pessoa que fora oferecida, o juiz não a admite a depor”.*

Ainda que o Juiz entenda que a testemunha tem capacidade para depor, a sua admissão pode ser impugnada pela parte contrária – artigo 514.º do CPC -, com fundamento em falta de aptidão mental (artigo 495.º), impedimento por poder depor como parte (artigo 496.º) ou em a pessoa que se apresenta para depor não ser a testemunha arrolada.

7.1. As testemunhas à distância de um clique. *Online*, mas sem rede?: inquirições no TAF, na comarca do vizinho e na casa da testemunha

O caso: no processo n.º 578/15.4BELLE, uma Ação Administrativa de responsabilidade civil extracontratual, a Autora, nacional da República da Irlanda e residente em Dublin, pedia a condenação do Município demandado no pagamento de uma indemnização de cerca de € 110.000,00, por danos patrimoniais e não patrimoniais. Alegava que, em agosto de 2012, durante umas férias no Algarve, ao regressar a casa de noite com o marido e os dois filhos, tropeçara num lancil degradado e sem proteção de uma via pedonal, sofrendo uma queda da qual resultou uma fratura no tornozelo do pé esquerdo, com intervenção cirúrgica e meses de incapacidade. O Município contestou, negando a perigosidade do local e a verificação dos pressupostos da responsabilidade civil.

A questão a decidir e os factos a provar: a questão de direito era a de saber se estavam reunidos os pressupostos da responsabilidade civil extracontratual das pessoas coletivas públicas: o

facto, a ilicitude, a culpa, o dano e o nexo de causalidade. Mas quase tudo dependia de prova pessoal: a dinâmica da queda não fora presenciada senão pela família da Autora, ocorrera mais de uma década antes do julgamento e os seus protagonistas residiam na Irlanda. As declarações de parte e a prova testemunhal eram, pois, incontornáveis, e a sua produção era um desafio logístico que só o digital podia resolver: as pessoas a ouvir estavam a quase três mil quilómetros do TAF de Loulé.

A fixação do meio de prova: a Autora requereu, ao abrigo do artigo 466.º do CPC, a prestação de declarações de parte e que estas tivessem lugar através da plataforma *Webex*, uma vez que residia na Irlanda, indicando para o efeito o seu endereço de correio eletrónico e, bem assim, os endereços das testemunhas que arrolara. O Tribunal deferiu, e a audiência de julgamento ficou desenhada com uma geometria probatória que seria impensável poucos anos antes: duas testemunhas do Município seriam ouvidas presencialmente, na sala de audiências; uma testemunha da Autora seria ouvida por teleconferência clássica, a partir do Tribunal Judicial da Comarca de Portimão, identificada perante funcionário judicial; e a Autora e as restantes testemunhas seriam ouvidas a partir da Irlanda, através do *Webex*, no local onde se encontrassem, apenas com a companhia de uma intérprete, nomeada e ajuramentada nos termos do artigo 133.º, n.º 2, do CPC, para assegurar a comunicação. Três regimes de inquirição, portanto, numa só audiência: a presença física, a videoconferência entre tribunais e a ligação pessoal através de programa de comunicação projetado para videochamadas, o que, numa linguagem empresarial, poderia corresponder a uma gestão *in-house* (em que a tarefa é desenvolvida nas instalações da organização, com recursos próprios), *on-site* (em que a tarefa é realizada com recursos externos que dão apoio no local) e *outsourcing* (em que a realização da tarefa é externalizada).

A produção da prova: logo na abertura da diligência, a ligação à internet mostrou que estava, literalmente, sem rede: efetuada a ligação com a Autora, verificaram-se erros técnicos no áudio que persistiram, e o Juiz, com o acordo das partes, alterou a ordem das inquirições, ouvindo primeiro a testemunha que aguardava nas instalações do Tribunal de Portimão. Restabelecida a ligação, já plenamente operacional, a Autora prestou declarações durante cerca de cinquenta minutos, confrontada com as fotografias do local juntas com a Petição Inicial, tudo gravado no sistema em uso no Tribunal, nos termos do artigo 155.º do CPC.

Seguiu-se a inquirição do marido da Autora, testemunha por esta arrolada, que se identificou com a mesma morada de Dublin, prestou juramento e foi advertido da faculdade de recusa prevista no artigo 497.º, n.º 1, alínea c), do CPC, declarando o interesse em depor. Foi então que o Mandatário do Município pediu a palavra e requereu que o depoimento não fosse admitido, uma vez que a testemunha *“acompanhou presencialmente, e ao lado da sua esposa e Autora do processo, todo o período das declarações de parte em que esta interveio, tomando conhecimento quer das questões, quer das respostas, e de todo o ocorrido no período das declarações de parte prestadas”*. A câmara revelara aquilo que não seria permitido em nenhuma sala de audiências: na divisão em que a parte prestara declarações, estava também a testemunha que iria depor a seguir. A Mandatária da Autora

respondeu que os motivos aduzidos não constituíam fundamento de impedimento. O Juiz proferiu despacho a admitir a inquirição: *“Pese embora o disposto no artigo 512.º, n.º 1 do Código de Processo Civil, não ter sido cumprido[xiii], considero que nos termos do artigo 515.º, n.º 1 do Código de Processo Civil, o que foi alegado pelo Ilustre Mandatário da Ré não põe em causa a possibilidade de a testemunha ser inquirida, sem embargo de o Tribunal ponderar o facto de ter presenciado as declarações de parte da Autora e também pela circunstância de ser marido da parte.”* A regra da incomunicabilidade das testemunhas, pensada para o corredor do tribunal, não fora cumprida na sala de estar de Dublin; a consequência, porém, não foi a exclusão do depoimento, mas a sua ponderação na valoração. A testemunha depôs, então, durante cerca de meia hora. Já de tarde, uma outra testemunha arrolada pela Autora nunca chegou a comparecer na plataforma, tendo a Mandatária prescindido do seu depoimento.

A valoração da prova: na motivação da decisão da matéria de facto, a sentença qualificou o depoimento do marido da Autora como *“parcialmente credível, pois na descrição da dinâmica do acidente a testemunha esteve presente durante a declaração da parte e o relato da testemunha indicou alguma contaminação. Em todo o caso, o seu depoimento não foi relevante, nessa parte, dada a credibilidade das declarações de parte quanto à dinâmica do acidente”*. O depoimento do marido serviu somente para dar como provados, ou corroborar, dois factos: o internamento hospitalar da Autora e a circunstância de a família passar duas a três vezes por semana pela via pedonal onde ocorreu a queda. E este último facto operou contra a parte que arrolara a testemunha: o conhecimento prévio do local, conjugado com a largura da via, a iluminação pública próxima e o consumo de álcool nessa noite, alimentou o juízo de culpa concorrente da lesada, fixada em 30%, nos termos do artigo 570.º do Código Civil.

Decisão: após a instrução, nas alegações escritas, a Autora reduziu o pedido indemnizatório de cerca de € 110.000,00 para cerca de € 22.500,00. A ação foi julgada parcialmente procedente, tendo o Município sido condenado a indemnizar a Autora em cerca de € 9.000,00, já deduzida a percentagem correspondente à culpa concorrente, com custas na proporção do decaimento.

Trânsito: o Município interpôs recurso para o Tribunal Central Administrativo Sul com fundamento, além do mais, em erro na valoração do depoimento da parte (por considerar que não ficaram provadas as circunstâncias concretas, nem a causa da queda) e erro na valoração dos depoimentos das testemunhas por si arroladas (por considerar que as testemunhas esclareceram o estado do local onde ocorreu a queda). O recurso encontra-se pendente.

Comentário: o caso é a ilustração acabada da tensão da espontaneidade enunciada na introdução deste capítulo quando a «máquina de teletransporte» é posta em funcionamento: se o depoimento é prestado fora do tribunal, o Juiz não controla o ambiente de onde a testemunha depõe. Inquirir *online*, sem a rede de segurança de um edifício público e de um funcionário ou de um notário, transfere para o momento da valoração aquilo que a lei quis prevenir no momento da produção, uma vez que a contaminação pode não ser evitada. O sistema geral volta a ter resposta

(pode equacionar-se a existência de nulidade processual, de não admissão da testemunha a depor, de consequência na livre apreciação da prova...), mas a lição prática ficou: a comodidade de uns cliques não dispensa a rede de apoio.

8. ... à Justiça na Era da Inteligência que se anuncia.

Os casos apresentados têm um fio condutor: o digital não criou um direito probatório novo. Perante o comprovativo suspeito de manipulação, a impressão de um ecrã, o ficheiro de faturação, a declaração consultada na fonte ou a testemunha inquirida à distância de um clique, os Juízes reconduziram a prova digital aos institutos gerais - o documento particular, a perícia, a inspeção, a livre apreciação... - exigindo, com especial cautela, o que sempre se exigiu: autenticidade, integridade e contraditório. As soluções estiveram na aplicação dos regimes existentes, por vezes com alguma adaptação, não na sua substituição.

Apesar da variedade dos casos, foi possível encontrar alguns fios condutores. A regra da integridade mandou procurar o original digital onde ele existe - foi assim no comprovativo de pagamento (capítulo 3.1), na base de dados de faturação (capítulo 5.1) e na declaração consultada em linha (capítulo 6.1). A conclusão de que a imagem prova o ecrã, e não o facto que o ecrã exhibe, absolveu a contribuinte no caso da notificação enviada pelos CTT (capítulo 4.1). E a exigência de fixar o que é volátil (imprimir, fotografar o ecrã, gravar numa pen...) encontrou-se na ata do julgamento do *Street View* (capítulo 4.2) e no auto da inspeção ao Portal das Finanças (capítulo 6.1).

Há quem afirme que já não nos encontramos na Era da Informação, por força de uma quarta revolução industrial caracterizada pelo papel das tecnologias - inteligência artificial, robótica, internet das coisas... - na fusão dos mundos físico, digital e biológico.[\[xiv\]](#)

E há quem equacione que o capitalismo está a evoluir para o tecnofeudalismo, com o capital a ser substituído pelos algoritmos da nuvem, que permitirão às grandes empresas tecnológicas enfraquecer as instituições democráticas e forçar a aplicação das regras que elas próprias criam.[\[xv\]](#)

Para a atividade probatória, a mudança de Era tem um significado preciso. Até aqui, a pergunta dirigida à prova, e também à digital, era a da sua integridade: este ficheiro foi adulterado depois de criado? A inteligência artificial generativa acrescenta uma pergunta diferente e mais inquietante: este ficheiro alguma vez correspondeu à realidade?

Uma fotografia, uma gravação áudio ou um vídeo podem hoje ser integralmente gerados por inteligência artificial, com uma qualidade que escapa à perceção humana - e, portanto, à inspeção judicial -, reclamando perícia especializada, leitura de metadados e, porventura, novas infraestruturas de certificação da origem dos conteúdos.

Há já também vários *softwares* de utilização corrente que permitem colocar filtros em videochamadas, alterando o aspeto físico dos intervenientes. A mensagem de René Magritte, passada no quadro *“A traição das imagens”* de 1929, em que por baixo da figura de um cachimbo surge a frase *“Ceci n’est pas une pipe”*, é totalmente atual quase um século depois. Nem tudo o que parece, é. E o *deepfake* fará pela prova digital o que a fotocópia fez, no seu tempo, pelo documento: obrigará o sistema a reforçar os seus mecanismos de confiança.

A inteligência artificial entrará também nos Tribunais pelo ecrã da frente e literalmente pelos processos dentro: é expectável e aconselhável que surjam mais instrumentos ao dispor dos juízes que incorporem ferramentas de inteligência artificial.^[xvii]

Se as nótulas que aqui ficam alguma coisa demonstram, é que os institutos gerais da prova têm tido plasticidade bastante para acolher cada vaga tecnológica. E não há razão para supor que será diferente com a da inteligência artificial generativa. Mas a livre apreciação da prova - a convicção formada por quem conhece as realidades do Mundo e as regras da experiência que nele se colhem - continuará a pressupor o que nenhum código binário substitui: um julgador humano. A «máquina do tempo» e a «máquina de teletransporte» serão cada vez mais sofisticadas; o piloto, esse, como julgamos, está para ficar.

(*) Apesar de atualmente exercer funções na Subsecção Tributária Comum do Tribunal Central Administrativo Sul, os casos apresentados foram julgados em 1.ª instância. O Autor agradece a disponibilidade dos Colegas Cláudia Monteiro e Paulo Gomes, Juízes na área administrativa do Tribunal Administrativo e Fiscal de Loulé, por terem sugerido os casos, por si julgados, que aqui são apresentados, além de terem partilhado algumas reflexões sobre a atividade jurisdicional que desenvolveram (casos 3.2, 4.2 e 4.3, e 3.1 e 7.1, respetivamente). Por último, mas não menos importante, agradece, igualmente, à Senhora Professora Ana Isa Meireles, os elementos para reflexão que muito gentilmente disponibilizou.

(**) O Sumário Executivo foi redigido com recurso ao www.chatgpt.com.

(***) O Resumo foi redigido com recurso ao www.chatgpt.com.

(****) As Palavras-Chave foram redigidas com recurso ao www.chatgpt.com.

[i] CASTELLS, Manuel. *A Sociedade em Rede*, vol. I, Fundação Calouste Gulbenkian, 2002, p. 36, refere que a terceira revolução industrial, que associa o digital à tecnologia da internet, inaugurou a Era da Informação que se caracteriza, não pela centralidade do conhecimento e da informação

transformados em dados, mas pela aplicação desses dados na produção de mais conhecimento e informação, num ciclo de alimentação cumulativo entre a inovação e o seu uso.

[ii] MEIRELES, Ana Isa. *A Prova Digital no Processo Judicial – A Blockchain e Outros Caminhos para os Tribunais*. Almedina, 2023. ISBN 978-989-40-1154-5.

BONIFÁCIO RAMOS, José Luís. *Prova Digital: Princípios e Garantias Processuais*. [Em linha]. Disponível em: https://educast.fccn.pt/vod/clips/1ajfjpl4ov/link_box?locale=pt [Visualizado em junho de 2026]

PIRES DE SOUSA, Luís Filipe. *O Conceito, o Regime e a Eficácia Probatória do Documento Eletrónico*. [Em linha]. Disponível em: https://educast.fccn.pt/vod/clips/1ajfjpl3x5/link_box?locale=pt [Visualizado em junho de 2026]

[iii] A metodologia adotada está, ainda, contaminada pelas nomeações, muito recentemente terminadas, como docente e formador externo do Centro de Estudos Judiciários. Dedico, por isso, as presentes nótulas aos Colegas e aos futuros Colegas do VI ao XII Curso de Formação de Juizes para os Tribunais Administrativos e Fiscais (2018-2025), com quem também muito aprendi.

[iv] PEREIRA RODRIGUES, Fernando. *A Prova em Direito Civil*. Coimbra Editora, 2011. ISBN 978-972-32-1922-7.

[v] ANTUNES VARELA. Comentário ao Acórdão do Supremo Tribunal de Justiça de 22 de Outubro de 1981 e ao Assento de 21 de Junho de 1983. *Revista de Legislação e Jurisprudência*. Ano 116.º, n.º 3716, p. 339.

[vi] TEIXEIRA, Inês da Silva. *A Inconstitucionalidade da Lei dos Metadados: será a alteração à Constituição uma hipótese viável?*. [Em linha]. Disponível em: <https://repositorium.uminho.pt/server/api/core/bitstreams/8af4b349-4d06-4846-8ed4-bfe2568f6023/content>. [Visualizado em: junho de 2026], apresenta as definições de:

- Benjamim RODRIGUES (*“A prova eletrónico-digital pode definir-se como qualquer tipo de informação, com valor probatório, armazenada (em qualquer dispositivo de armazenamento digital) ou transmitida (em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis), sob a forma binária ou digital”*);
- Sónia FIDALGO (a prova digital consiste *“na prova produzida a partir de dados em formato digital (na forma binária), que são manipulados, armazenados ou comunicados através de qualquer dispositivo, computador ou sistema informático, ou transmitidos através de um sistema de comunicação”*); e
- Armando DIAS RAMOS (constitui prova digital *“a informação passível de ser extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações”*).

MEIRELES, Ana Isa. *Ob. Cit.*, pp. 101-102, sustenta que *“prova digital é toda a informação, independentemente do suporte em que se apresente, que tenha sido criada ou obtida através de dispositivos (dispositivos de computação, smartphones, tablets, rastreadores de condicionamento, mediadores de energia inteligentes, sistemas de aquecimento central automatizados) ou, através de dispositivos ou não, integradas em redes digitais”*.

[vii] Curiosamente, o artigo 4.º deste Decreto-Lei prevê a prática de atos administrativos através de meio eletrónico ao estatuir que *“Nas operações relativas à criação, emissão, arquivo, reprodução, cópia e transmissão de documentos eletrónicos que formalizem atos administrativos através de sistemas informáticos, incluindo a sua transmissão por meios de comunicação eletrónica, os dados relativos à entidade emitente e à pessoa que tenha praticado cada ato administrativo devem ser indicados de forma a torná-los facilmente identificáveis e a comprovar a função ou cargo desempenhado pela pessoa signatária de cada documento”*.

[viii] A assinatura eletrónica qualificada prevista no artigo 3.º, n.º 5, do Regulamento eIDAS é a modalidade que equivale à assinatura autógrafa dos documentos com forma escrita em suporte de papel, uma vez que pressupõe a utilização de um certificado que garante a identificação do signatário e a integridade do conteúdo – é a modalidade utilizada quando se assina com o Cartão de Cidadão ou a Chave Móvel Digital, ou o Juiz com o cartão emitido pela Entidade Certificadora Comum do Estado.

A assinatura eletrónica avançada, prevista no artigo 26.º do Regulamento eIDAS, não goza de equivalência legal à assinatura autógrafa, mas também permite identificar o signatário e garantir que o conteúdo do documento não foi alterado, embora não seja certificada – é a modalidade utilizada em plataformas de assinatura, como o *Adobe Acrobat*, ou através de códigos secretos (palavra-chave ou *pin* enviado por SMS). A assinatura está sujeita à livre apreciação do Juiz.

A assinatura eletrónica simples corresponde a uma manifestação de autoria sem especial garantia de identificação do signatário, nem de integridade do conteúdo – é a modalidade que corresponde à seleção e clique numa opção «Li e Aceito os termos», ou à colocação de uma imagem com a assinatura autógrafa num documento .doc. Está também sujeita à livre apreciação do Juiz.

[ix] Esta portaria, que se encontrava em vigor à data, foi revogada pela Portaria n.º 350-A/2025/1, de 9 de outubro, já referida, cujo regime, porém, nesta parte, se mantém, no essencial, idêntico ao anteriormente vigente.

[x] Esta infraestrutura está fora do controlo do Juiz, seja através do seu Tribunal, seja através do Conselho Superior dos Tribunais Administrativos e Fiscais. É disponibilizada por um instituto público, o Instituto de Gestão Financeira e Equipamentos da Justiça, IP, que prossegue atribuições do Ministério da Justiça e faz parte do poder executivo do Estado, ainda que com o apoio pontual de Juízes, como foi o caso do Senhor Conselheiro Paulo Carvalho, antigo Presidente do TAF de Loulé,

que se jubilou muito recentemente, um dos principais, se não o principal, impulsionador do *Magistratus*.

Na verdade, não só o Juiz não dispõe da infraestrutura imediata, como não tem independência na utilização de outros recursos, como impressoras, tinteiros ou resmas de papel, ocorrendo, ocasionalmente, ruturas de stock.

O processo, que outrora estava fisicamente nas mãos do Juiz e do Funcionário Judicial ou nas prateleiras do gabinete ou da secção, está agora armazenado eletronicamente num servidor do Estado Administração que, nos processos da jurisdição administrativa e fiscal, é normalmente a parte demandada. Esta estranha forma de vida do princípio da separação e interdependência do poder judicial do Estado verifica-se, até, na prática de atos processuais: os critérios que estão no algoritmo que, diariamente, efetua a distribuição dos novos processos não são do conhecimento dos Juizes.

[xi] ABRANTES GERALDES, António, PIMENTA, Paulo e PIRES DE SOUSA, Luís Filipe. *Código de Processo Civil Anotado – Vol. I*. Almedina, 2024, 3.ª edição. ISBN 978-989-40-0535-3, notas 6 a 11 ao artigo 502.º.

[xii] Cfr. PIRES DE SOUSA, Luís Filipe. *Julgamento Presencial versus Julgamento com Telepresença. A pandemia e o futuro*, pp. 18-19 [Em linha] Disponível em: <https://julgar.pt/julgamento-presencial-versus-julgamento-com-telepresenca-a-pandemia-e-o-futuro/> [Visualizado em junho de 2026].

[xiii] O artigo 512.º, n.º 1, do CPC reza do seguinte modo: “*Antes de começar a inquirição, as testemunhas são recolhidas a uma sala, donde saem para depor pela ordem em que estiverem mencionadas no rol, primeiro as do autor, depois as do réu, salvo se o juiz determinar que a ordem seja alterada ou as partes acordarem nessa alteração.*”

[xiv] FLORIDI, Luciano. *The 4th Revolution – How the Infosphere is Reshaping Human Reality*. Oxford University Press. 2014. ISBN 9780199606726; SCHWAB, Karl. *A Quarta Revolução Industrial*. Levoir, 2018. ISBN 9789896827090; SCHWAB, Karl. *Moldando a Quarta Revolução Industrial*. Levoir, 2019. ISBN 9789896827939;

[xv] VAROUFAKIS, Yanis. *Tecnofeudalismo – Ou o Fim do Capitalismo*. Objetiva, 2025. ISBN 9789895891443, em cuja contracapa, à laia de sinopse, se pode ler o seguinte: “*O capitalismo morreu. Bem-vindos ao tecnofeudalismo. Gradualmente, a partir do próprio capital e das vertiginosas mudanças tecnológicas das últimas décadas, o capitalismo esboroou-se. Os mercados tradicionais foram substituídos por plataformas digitais e o lucro vem, agora, das rendas que pagamos por espaço na nuvem. À velocidade dos nossos scrolls e cliques, este novo sistema económico, a que Yanis Varoufakis chama «tecnofeudalismo», consolida o poder das grandes empresas tecnológicas e redesenha o mapa geopolítico (...)*”.

[xvi] O Conselho Superior dos Tribunais Administrativos e Fiscais já começou a testar o AssessorIA, uma ferramenta de inteligência artificial para apoiar os Juizes de 1.ª Instância na análise e preparação

de processos nos Tribunais da jurisdição. O mercado disponibiliza também várias ferramentas para potenciar a produtividade no trabalho, como o resumo e transcrição de áudio, bem como para pesquisa de jurisprudência a partir dos sítios da DGSJ e do Diário da República. Começam, inclusivamente, a surgir réplicas não oficiais que reproduzem os acórdãos publicados pela DGSJ, por vezes com melhor desempenho - sinal, ele próprio, de que a desmaterialização aqui descrita não se detém nas instituições. A fiabilidade e a proveniência destas alternativas reclamam, naturalmente, cautela, sobretudo quando se desconhecem os seus responsáveis. Para os Juizes, um dos desenvolvimentos que poderá ser mais relevante é o da integração de uma ferramenta de inteligência artificial no próprio *Magistratus* que, ao ter como dados de trabalho o acervo processual do Juiz, poderia ter reflexos diretos na gestão processual e no aumento da produtividade.

Fernando Silva Pereira: Professor Auxiliar da Faculdade de Direito da Universidade do Porto & Investigador do CIJ – Centro de Investigação Interdisciplinar em Justiça

Sumário Executivo (*): (1) A “navegação na internet” pelo juiz é analisada como fenómeno processual ligado à obtenção de prova e de informação em processo civil. O seu enquadramento depende da função concreta que a utilização da internet assume no caso: inspeção, fonte de prova, instrumento auxiliar ou mero suporte informativo da decisão. (2) A internet pode ser tratada como objeto de inspeção quando o facto probando consiste na existência ou conteúdo de uma página web. Nestes casos, a página é equiparada a um “lugar virtual” e sujeita a perceção direta do tribunal, nos termos da inspeção judicial. Este enquadramento levanta dificuldades técnicas relevantes, designadamente a volatilidade do conteúdo e a necessidade de registo fiável da diligência. (3) A internet pode ser utilizada pelo juiz como fonte de prova para formar a sua convicção sobre factos controvertidos, através da consulta de websites ou redes sociais. Esta utilização exige rigoroso respeito pelo princípio do contraditório e pela estrutura dispositiva do processo, sendo inadmissível quando assente em investigação privada não sindicável do juiz. (4) A internet pode funcionar como meio auxiliar de outras provas, sem constituir prova autónoma. Ferramentas como Google Maps, Street View ou Google Earth servem para contextualizar depoimentos, esclarecer localizações ou apoiar a compreensão de outros meios probatórios. Nestes casos, não substituem a prova, nem exigem contraditório reforçado. (5) A consulta da internet pode ser utilizada pelo juiz apenas como fonte de informação contextual na fundamentação da decisão, sem integrar diretamente a matéria de facto provada. Nestes casos, a informação não deve ser convertida em facto probatório implícito, servindo apenas como elemento de enquadramento ou racionalização da decisão. (6) A utilização da internet pelo juiz encontra um limite fundamental na proibição de investigação privada autónoma em processo civil de matriz dispositiva. O juiz não pode coligir prova fora do processo nem substituir-se às partes na investigação dos factos, sob pena de violação da imparcialidade e da estrutura do modelo processual. (7) O princípio do contraditório é o eixo de validação da utilização probatória da internet. Sempre que a informação obtida online seja usada como prova, deve ser assegurado que as partes conhecem o seu conteúdo e têm possibilidade efetiva de o impugnar. A sua violação pode gerar nulidade processual e afetar a validade da decisão. (8) A cibernavegação judicial não constitui um meio de prova autónomo, mas uma técnica funcionalmente variável. Pode operar como inspeção, fonte de prova, instrumento auxiliar ou mera informação contextual, mas está sempre condicionada pelo contraditório, pela estrutura dispositiva do processo e pela proibição de investigação privada do juiz.

Resumo ():** O artigo analisa a utilização da internet pelo juiz em processo civil como fenómeno probatório e decisório, centrando-se na chamada “cibernavegação”. O problema essencial consiste em delimitar quando essa atividade constitui prova, simples instrumento auxiliar ou mera obtenção de informação, e quais os respetivos limites à luz do princípio do contraditório e da estrutura dispositiva do processo: i) em primeiro lugar, a internet pode ser objeto de inspeção judicial, quando o facto a provar respeita à existência ou conteúdo de uma página web. Nesses casos, a página é tratada como um “lugar virtual”, sendo diretamente percecionada pelo juiz, com aplicação do regime da inspeção. Contudo, este enquadramento exige cautela técnica devido à volatilidade do conteúdo e à necessidade de registo fiável da diligência; ii) em segundo lugar, a internet pode funcionar como fonte de prova de factos controvertidos, quando o juiz consulta websites ou redes sociais para formar a sua convicção. Aqui o ponto crítico reside na admissibilidade dessa atuação, que deve respeitar o contraditório e não pode traduzir-se numa investigação privada autónoma do juiz, sob pena de violação da imparcialidade e do modelo dispositivo; iii) em terceiro lugar, a internet pode ser utilizada como instrumento auxiliar da prova, designadamente através de ferramentas como Google Maps ou Street View. Nestes casos, a função não é provar factos diretamente, mas apenas apoiar a compreensão, contextualização ou interpretação de outros meios de prova, sendo em regra admissível de forma mais flexível; iv) em quarto lugar, a internet pode ainda ser usada como fonte de informação para fundamentação da decisão, sem integrar diretamente a matéria de facto. Trata-se de utilização contextual ou argumentativa, que não pode converter-se em prova implícita nem substituir a atividade probatória das partes. O artigo estabelece como limite estrutural a proibição de investigação privada do juiz, decorrente do princípio do dispositivo, da imparcialidade judicial e da exigência de prova processualmente adquirida e sindicável. O juiz não pode coligir autonomamente prova fora do processo. O princípio do contraditório surge como eixo central: sempre que a informação online seja usada como prova, deve ser assegurada a possibilidade de conhecimento e impugnação pelas partes, sob pena de nulidade processual. A jurisprudência citada distingue entre uso da internet como meio auxiliar (dispensa de contraditório reforçado) e como fonte de prova (exigência de contraditório pleno), sobretudo em casos envolvendo Google Maps e Street View. Em síntese, a “cibernavegação” judicial não constitui um meio de prova autónomo, mas uma técnica funcionalmente variável, que pode operar como inspeção, fonte de prova, instrumento auxiliar ou mera informação contextual, sempre limitada pelo contraditório, pela estrutura do processo civil e pela proibição de investigação privada do juiz.

Palavras-Chave: Prova; Processo civil; Página web; Inspeção; Cibernavegação.

Keywords: Evidence; Civil proceedings; Web page; Inspection; Cyber navigation

Índice: (1) Introdução; (2) A inspeção de um lugar virtual; (3) A navegação na internet como meio para a obtenção de informações; (3.1) Utilização da informação contida na página web, enquanto fonte de prova, no juízo de formação da convicção acerca de um facto controvertido; (3.2) Utilização da informação como elemento da fundamentação da decisão, mas não inserido no *iter* decisório relativo a um concreto facto da causa.

1. Introdução

Propomo-nos, no presente artigo, olhar para a atividade de “navegação na internet” realizada pelo juiz, como meio de obtenção de provas ou de informações em processo civil^[i].

Em termos gerais, esta atividade judicial pode destinar-se: (i) a aferir o conteúdo de uma página web, sendo esse o objeto da prova (o *factum probandum* diz respeito à existência da página web x, com o conteúdo y), ou (ii) a obter uma informação, relevante do ponto de vista da decisão da causa, usada ou não como fonte de prova^[ii].

No primeiro caso, ou seja, aquele em que o *factum probandum* diz respeito à própria existência da página web, com um determinado conteúdo, existem outras formas para adquirir a prova, não sendo, aliás, a inspeção pelo juiz a forma mais frequente. Note-se que a página web é um documento eletrónico^[iii] (não assinado) que se distingue pelo seu dinamismo, e por ser acompanhado de dados (os chamados metadados), não imediatamente visíveis ao utente^[iv], os quais são de extrema importância quando se trata de demonstrar o seu carácter “original”. Isto torna mais seguro a produção de um duplicado da página web através de uma aquisição forense^[v], ou seja, com recurso a prova pericial. Mas existem outras formas de produção, que podem revelar-se úteis sempre que a página web não contenha conteúdo multimédia. É o caso da exibição de uma cópia em suporte analógico deste documento informático (acompanhada, ou não, de certificação notarial^[vi] ou outra^[vii]), ou de uma produção “self made”^[viii]. Pode também recorrer-se à prova por testemunhas, não se afastando ainda a possibilidade de as declarações de parte terem por objeto o conteúdo de uma página web.

O que distingue as hipóteses referidas em (i) e (ii) é, pois, o facto de, na primeira, a página web constituir o objeto da prova, o que não acontece na segunda, onde a página web serve apenas de meio de informação^[ix]. Ambas as hipóteses são muito desafiantes, embora por motivos diferentes. No primeiro caso, a atividade realizada pelo juiz pressupõe a existência de conhecimentos técnicos, muitas vezes não detidos pelos juizes (os quais não recebem formação específica neste campo), devendo ser atestada a conformidade da página com o que é visualizado, e com certificação dos dados anexos: a hora da operação (completada pela indicação do fuso horário de referência), o tipo e versão de *browser*, o sistema operativo e fornecedor de acesso utilizado^[x]. São, pois, de natureza técnica^[xi], sem prejuízo da possibilidade de o juiz “se fazer acompanhar” de um técnico (cf. artigo 429.º CPC), e não procedimentais^[xii] as dificuldades que aqui se colocam, relacionadas com a

natureza (virtual) do objeto da inspeção[xiii]. No segundo caso, por sua vez, o acento tónico deve ser colocado principalmente na necessidade de respeito por certos princípios de direito processual civil, em especial, o princípio do contraditório.

Pense-se no caso, não inusual, em que o juiz recorre à “navegação na internet” para obter uma determinada informação, mencionando, na sentença, a atividade por si realizada. Por ex.: no âmbito de um processo de insolvência, tendo sido pedida a exoneração do passivo restante, o juiz da causa é chamado a tomar uma decisão quanto ao montante do rendimento indisponível. A parte (o devedor insolvente) informa o tribunal de que é detentora de um direito de arrendamento para habitação, pagando de renda o valor de x. Parecendo-lhe excessivo este valor, o juiz decide consultar um “portal imobiliário para comprar e arrendar casa”, para se inteirar do preço médio praticado no respetivo mercado de arrendamento. Pode fazê-lo? É suficiente mencionar, na sentença, que realizou esta atividade, ou encontra-se ferido o princípio do contraditório?

Pense-se agora neste outro exemplo: num processo laboral, onde foi alegada uma situação de incapacidade temporária, o juiz consulta um *post* publicado pelo trabalhador numa rede social de acesso aberto, utilizando o mesmo como prova. Pode fazê-lo? E pode convocar as partes para, na sua presença, inspecionar a rede social em causa[xiv]?

Com as hipóteses referidas em (i) e (ii) não deve, entretanto, confundir-se aquela em que a página web é utilizada pelo tribunal enquanto mero instrumento ao serviço da produção de outra prova. Ou seja, os casos em que a página web (as situações mais frequentes dizem respeito à utilização do *Google Earth* e do *Street Plan*) auxilia a prática de outras provas, como o depoimento de testemunhas, as declarações de parte ou a prestação de esclarecimentos por parte de peritos[xv]. Por exemplo, numa ação de responsabilidade civil extracontratual, relacionada com um acidente de viação, o juiz solicita às partes a identificação do ponto de colisão ou determinados aspetos que podem trazer esclarecimento sobre o objeto da controvérsia (por exemplo, a existência de um sinal de stop ou de um semáforo, o sentido de circulação na respetiva rua ou a localização de uma passadeira), servindo-se, para isso, daquela ferramenta[xvi]. Conforme nota Abel Lluch[xvii], mesmo quando legalmente não estejam reconhecidos como meios de prova, estas páginas web podem configurar-se como instrumentos auxiliares, que facilitam a declaração das partes ou das testemunhas, ou os esclarecimentos dos peritos. De facto, a utilização de páginas web com esta finalidade, meramente instrumental, de auxílio à prática de outros meios de prova, não se revela particularmente problemática (note-se que a atividade probatória em causa deve, nos termos gerais, decorrer com respeito pelo princípio do contraditório). Ambas as partes estando, ou podendo estar presentes, e ambas tendo igual oportunidade de pronúncia, não vemos razão para se excluir a utilização destas ferramentas, nos casos referidos. E, de facto, isto tem-se tornado cada vez mais frequente.

No Ac. STJ, de 27.04.2023, proc. n.º 4017.20.0T8GMR.G1.S1.F3, relator Cura Mariano, o Tribunal apreciou uma hipótese afim a esta. Num recurso envolvendo uma ação de responsabilidade civil

decorrente de um atropelamento, o Tribunal da Relação recorreu imagens do *Google Maps/Street View* para apreciação da prova produzida em primeira instância^[xviii]. Trata-se, pois, de um caso em que as ferramentas em causa foram utilizadas, não como auxiliares da produção de outra prova, mas como auxiliares na apreciação de outros meios de prova. O STJ traça uma diretriz geral, tratando depois do caso concreto (a ela não subsumível).

Na apreciação de uma impugnação da decisão sobre a matéria de facto (afirma o Tribunal), os Tribunais da Relação podem utilizar, oficiosamente, as imagens do *GoogleMaps/Street View*, nos termos do artigo 662.º, n.º 2, b) CPC, devendo, no entanto, juntar as mesmas ao processo ou proceder à sua exibição, segundo o disposto no artigo 428.º CPC, facultando às partes o seu conhecimento e a possibilidade da impugnação da sua exatidão, previamente à sua utilização como meio de prova, em obediência ao princípio do contraditório em sede instrutória. Sendo imagens que retratam uma realidade no momento da sua captura (nota o Tribunal), estamos perante documentos (artigo 363.º CC), que fazem prova plena da realidade que mostram, se a parte contra quem são apresentados não impugnar a sua exatidão (artigo 368.º CC)^[xix].

No entanto (afirma o Tribunal), não é necessário assegurar o contraditório, se essas imagens não são utilizadas como um meio de prova dos factos em discussão, mas apenas como uma ferramenta de trabalho que facilita a compreensão e interpretação do conteúdo de qualquer meio de prova. Não sendo a ferramenta utilizada como meio de prova, não está o seu conteúdo sujeito ao contraditório, pelo que a ausência de notificação prévia das partes não constitui qualquer vício que invalide a sua utilização.

Foi isso – conclui o Tribunal – o que aconteceu no caso dos autos: o Tribunal da Relação usou aquelas ferramentas no trabalho de compreensão e interpretação do conteúdo do termo da inspeção judicial realizada e dos depoimentos prestados sobre o local onde ocorreu o atropelamento do Autor. Não estamos perante o recurso a um meio de prova que substituiu ou completou os meios de prova produzidos na primeira instância, mas sim perante a utilização de um instrumento que facilitou a leitura e a compreensão desses meios de prova^[xx]. Este tipo de utilização – sublinha o Tribunal – é semelhante à que ocorre com a assessoria de um técnico nos termos do artigo 601.º CPC, que também poderá ser utilizada pelo Tribunal da Relação na decisão sobre impugnação de matéria de facto, sem que a mesma constitua um meio de prova. É muito interessante esta última observação do Tribunal.

2. A inspeção de um lugar virtual

Tratemos agora da hipótese (i), acima referida, ou seja, aquela em que a prova tem por objeto a existência de uma página web x, com o conteúdo y, destinando-se a atividade de “cibernavegação”, realizada pelo juiz, a aferir dessa mesma existência.

Esta atividade de “navegação na internet” consiste numa prova por inspeção, podendo ser realizada a requerimento das partes, ou por iniciativa do tribunal (artigo 490.º, n.º 1 CPC).

A inspeção constitui um meio de prova que tem por fim a percepção direta dos factos pelo tribunal (artigo 390.º CC). É o que acontece aqui. O facto sob decisão consiste na existência de uma página web, com um determinado conteúdo, e o juiz visiona a respetiva página para aferir da conformidade entre o alegado e o objeto da sua observação. Ou seja, a inspeção tem por objeto um lugar virtual (como referimos, não é usual que se recorra ao meio de prova por inspeção para provar a existência de uma página web, e ele pode não ser eficaz, se existir o risco de a página ser apagada ou modificada. As partes costumam provar este facto através de cópia da página web, com ou sem certificação)[\[xxi\]](#).

Pode questionar-se se a existência de uma página web constitui, ou pode constituir, um facto notório. Nesse caso, como é sabido, não carecendo de prova (cf. artigo 5.º, n.º 2, al. c) CPC). Sobre o ponto, Pires de Sousa[\[xxii\]](#) sublinha a necessidade de distinguir o facto da existência da página, daquele que diz respeito ao conteúdo da mesma. Com efeito (afirma o autor), constituirá facto notório a existência de páginas *web* muito divulgadas, por ex., *Google*, bem como que as empresas de abrangência nacional costumam ter um nome de domínio tendencialmente coincidente com a sua designação comercial. Contudo, o conteúdo de tais páginas não constitui facto notório porquanto não constitui um facto do conhecimento geral sob os prismas da esfera pessoal, cognoscitiva e especial[\[xxiii\]](#).

O resultado da prova por inspeção é livremente apreciado pelo tribunal (artigo 391.º CC), encontrando-se o seu regime processual nos artigos 490.º a 493.º CPC.

Como referido, trata-se de um meio de prova de iniciativa oficiosa, ainda que a requerimento das partes (490.º, 1 CPC), dependendo apenas do juízo que o tribunal faça acerca da respetiva conveniência. Quando haja sido requerido por uma parte, compete à mesma fornecer ao tribunal os meios necessários para a realização da diligência (490.º, 2 CPC) – por ex., facultando ao juiz um computador se isso for necessário[\[xxiv\]](#) (veja-se a afinidade com o artigo 428.º CPC).

Em geral, as partes ou eventuais terceiros deverão colaborar com o tribunal na realização da diligência (417.º, 1 CPC)[\[xxv\]](#). O dever de colaboração está sujeito, porém, aos limites previstos nos artigos 490.º, 1 CPC e 417.º, 3 CPC. São ainda notificados do dia e hora da inspeção, podendo, por si próprias ou pelos seus mandatários, intervir ativamente no ato probatório, fazendo esclarecimentos ou chamando a atenção para aspetos que entendam relevantes (491.º CPC). Acresce que a inspeção, mesmo na modalidade de cibernavegação, deve ser plasmada num auto que pode, em última instância e no caso em apreço, radicar essencialmente em fotografias ou prints que sejam juntos ao processo (cf. artigo 493.º CPC)[\[xxvi\]](#).

No ato de inspeção o juiz pode fazer-se acompanhar de um técnico (492.º CPC)[\[xxvii\]](#). Da diligência é lavrado auto (493.º CPC).

No Ac. TRL, de 14.02.2023, proc. n.º 400/19.2T8CSC.L1-7, relator Pires de Sousa, pode ler-se que, a prova por inspeção, integra a modalidade cibernavegação, nos termos da qual a parte faculta ao juiz um computador, ou este utiliza um próprio, com acesso à internet, a fim de se inteirar, diretamente e na presença das partes, do conteúdo de *sites* ou de correio eletrónico trocado entre as partes. O meio de prova constituenda cibernavegação (sublinha o Tribunal) não prescinde da observância dos princípios processuais que presidem à produção de prova, a começar pelo princípio da audiência contraditória, consagrado no artigo 415.º CPC, mesmo que a cibernavegação seja de iniciativa oficiosa[xxviii]. Ao recorrer ao meio de prova cibernavegação, sem observância do regime dos artigos 415.º, 491.º e 493.º CPC, o tribunal *a quo* incorreu numa nulidade processual – neste ponto, o Tribunal adota uma tese, que tem feito curso na jurisprudência[xxix], de acordo com a qual, o proferimento de uma decisão depois da omissão de um ato obrigatório, conduz a nulidade da sentença por excesso de pronúncia (artigo 615.º, n.º 1, al. d) CPC), uma vez que o tribunal conhece de matéria de que, nas circunstâncias em que o faz, não podia conhecer. A mesma solução, em casos relacionados com a atividade de cibernavegação e com a violação do princípio do contraditório, pode encontrar-se no Ac. TRP, de 24.10.2024, proc. n.º 56/23.8T8ALB.P1, relator Paulo Dias da Silva[xxx], e no Ac. TRL, de 30.05.2023, proc. n.º 568/20.5T8MTJ.L1-7, relator Diogo Ravara, abaixo citados.

Pela nossa parte, e embora concordemos com o Tribunal no sentido de que devia ter sido observado o princípio do contraditório, não nos parece, pelas razões que apresentámos, que a atividade levada a cabo pelo tribunal deva, no caso em apreço, ser configurada como uma prova por inspeção. *In casu*, o tribunal de primeira instância recorreu ao sítio de uma imobiliária para aferir da viabilidade de arrendamento por um certo preço[xxxi]. A ação destinava-se à fixação de uma pensão de alimentos[xxxii]. O tribunal recorreu a uma pesquisa na internet para apurar o valor de mercado de arrendamento de uma casa na localidade em causa. Usou, pois, a informação constante da respetiva página web como fonte de prova[xxxiii] (a hipótese enquadra-se, a nosso ver, no ponto seguinte: 3.1.). Não estamos perante um caso em que o *facto probando* (essencial ou instrumental) diga respeito ao conteúdo de uma página web. Se assim fosse, o exame da página, pelo tribunal, corresponderia à realização de uma prova por inspeção, com aplicação – aí sim – da norma do artigo 491.º CPC.

Não é isso que acontece no caso em apreço, o qual não corresponde, tecnicamente, a uma prova por inspeção.[xxxiv] O tribunal recorre ao sítio da imobiliária como que a um perito. Do ponto de vista do exercício do contraditório[xxxv], não cremos, pela mesma razão, que o tribunal estivesse obrigado a consultar a página web na presença das partes (artigo 415.º, n.º 1 CPC). Nos termos do artigo 415.º, n.º 2 CPC, quanto às provas constituendas (como é o caso da prova por inspeção), a parte é notificada, quando não for revel, para todos os atos de preparação e produção da prova, e é admitida a intervir nesses atos nos termos da lei; relativamente às provas pré-constituídas, deve facultar-se à parte a impugnação, tanto da respetiva admissão como da sua força probatória. O conteúdo da página web pode ser introduzido no processo como prova documental, sujeitando ao

contraditório das partes (nesse sentido: Ac. STJ, de 27.04.2023, acima citado). Mas não se exclui a possibilidade de o juiz consultar o sítio da internet em audiência contraditória.[\[xxxvii\]](#)

3. A navegação na internet como meio para a obtenção de informações

Abarcamos agora, com o presente título, os casos em que o juiz se serve da “navegação na internet”, não para aferir da existência de uma página web, com um determinado conteúdo, mas para, através da consulta desse conteúdo, obter uma informação.

Importa distinguir os casos em que essa informação se destina a ser utilizada como fonte de prova, mobilizada no juízo de pronúncia sobre a matéria de facto (ou seja, sendo um elemento de fundamentação da decisão relativa a um facto controvertido – artigo 607.º, n.ºs 4 e 5 CPC), daqueles em que a informação obtida pelo juiz, sendo utilizada pelo mesmo na fundamentação da decisão, não integra, no entanto, o *iter* decisório relativo a um facto da causa.

3.1. Utilização da informação contida na página web, enquanto fonte de prova, no juízo de formação da convicção acerca de um facto controvertido

Comecemos por tratar do primeiro caso (utilização da informação, enquanto fonte de prova, no juízo de formação da convicção acerca de um facto controvertido). O ponto insere-se num problema mais amplo, que diz respeito aos limites da intervenção do juiz, no que diz respeito à recolha de provas.

A nosso ver, num sistema de base dispositiva, está vedado ao juiz realizar uma investigação privada dos factos. Uma tal atividade não se encontra a coberto do princípio do inquisitório (artigo 411.º CPC). Nos termos desta norma, incumbe ao juiz ordenar, mesmo oficiosamente, todas as diligências necessárias ao apuramento da verdade, quanto aos factos que lhe é lícito conhecer (veja-se, para isto, a norma do artigo 5.º, n.º 1 CPC). Entendemos que este poder se traduz em desencadear os meios de prova necessários para adquirir as fontes de prova de que o juiz tomou conhecimento através do processo (alegações das partes e atividade instrutória realizada). É este o poder que o artigo 411.º CPC lhe confere, não o de investigar autonomamente essas fontes. Pode também o juiz ordenar a realização de uma perícia ou de uma verificação não judicial qualificada, ou decidir realizar uma inspeção, por ser ele – a quem compete valorar a prova –, a pessoa mais bem colocada para aferir da necessidade de realização destas provas, com vista a excluir uma dúvida acerca da realidade de um (enunciado de) facto controvertido, e para conhecer dos limites do próprio conhecimento e das capacidades técnicas de que dispõe em relação a um domínio específico.

Esta vertente do princípio dispositivo sobrepõe-se ao princípio da neutralidade judicial, enquanto vertente do princípio da imparcialidade, de acordo com o qual, o juiz, deve ser alguém sem

um pré-juízo em relação aos factos da causa, formando a sua convicção (apenas) através do processo. Este elemento da imparcialidade é constitutivo da própria função jurisdicional.

Com ele também se relaciona o princípio da proibição do recurso à ciência privada (*judex judicare debet secundum allegata et probata partium, non secundum conscientiam suam* [\[xxxvii\]](#)). Com efeito, o conhecimento obtido pelo juiz, através de uma investigação privada que ele decidisse realizar, não poderia pelo mesmo ser utilizado. O conhecimento privado do juiz não pode ser sindicado por um tribunal de recurso. A convicção acerca dos enunciados de facto controvertidos deve, assim, fundar-se em elementos (de prova) objetivos, sindicáveis, controláveis, os quais devem ser apresentados na fundamentação da decisão, mediante a análise crítica do conjunto das provas realizadas (artigo 607.º, n.ºs 4 e 5 CPC). Em relação ao conhecimento privado do juiz não podem as partes exercer o direito de contraditório [\[xxxviii\]](#). Em suma, o juiz não pode ser ao mesmo tempo juiz e testemunha (cf. artigo 115.º, n.º 1, al. h) CPC).

Pode acontecer, no entanto, que, tendo procedido a uma investigação privada dos factos, ou tendo um conhecimento prévio dos factos da causa, o juiz desencadeie os meios formalmente adequados para a aquisição das respetivas fontes de prova – por ex., chamando a depor uma testemunha não arrolada pelas partes, ou ordenando a uma das partes ou a um terceiro a exibição de um documento, de cuja existência tomou conhecimento fora do processo. Ou (no caso em apreço), visualizando, em audiência contraditória [\[xxxix\]](#), o conteúdo da página web, ou submetendo uma cópia da página ao contraditório das partes. Por ex., tendo consultado uma publicação da parte no Facebook, o juiz visiona esta rede social em audiência contraditória. Neste caso, as partes terão oportunidade de pronúncia, e a decisão do juiz fundar-se-á num elemento objetivo de prova (o resultado da atividade probatória realizada) (artigo 615.º, n.º 1, al. b) CPC). Cai, portanto, este último argumento.

Não obstante, o problema mantém-se: a nosso ver, num sistema de base dispositiva, o juiz não tem poder para realizar uma tal atividade de investigação. Ao juiz não compete coligir provas, nem investigar autonomamente os factos. Trata-se de uma atividade proibida. O juiz pode ordenar a realização dos meios processuais adequados para a aquisição das fontes de prova de que toma conhecimento através do processo, para prova dos factos que lhe é lícito conhecer (factos alegados pelas partes, e factos complementares ou concretizadores e instrumentais resultantes da instrução da causa – cf. artigo 5.º CPC. No ex. referido atrás (o juiz consulta uma publicação de uma parte no Facebook, visionando esta rede social em audiência contraditória), o facto probatório em causa “a parte publicou x no Facebook” não constitui um facto de que o juiz pudesse tomar conhecimento, uma vez que o mesmo não resultou da instrução da causa (artigo 5.º, n.º 2, al. a) CPC). [\[xl\]](#)

Esta regra acompanha, no entanto, a natureza dispositiva do direito feito valer através da ação. Desaplicando-se, portanto, quando o processo envolva matéria não submetida ao poder de disposição das partes. Repare-se que, por ex., em matéria de jurisdição voluntária, o tribunal pode investigar livremente os factos, coligir provas, ordenar os inquéritos e recolher as informações

convenientes (artigo 986.º, n.º 2 CPC). Num processo como este, não vemos que exista qualquer entrave a que o juiz “navegue na internet”, com a finalidade de coligir provas. Estas provas devem, no entanto – conforme referido –, ser introduzidas no processo por meio processual adequado, sendo submetidas ao contraditório das partes.

Pode, portanto, o juiz ter ou não ter o poder para coligir provas (isso depende da natureza do processo), mas o mesmo deve sempre observar o princípio do contraditório. De onde: se o juiz investiga privadamente a realidade, e julga com base nesse conhecimento privado, a decisão é nula por violação do princípio do contraditório, e do dever de fundamentação^[xlii], mesmo que o juiz tivesse poder para realizar esta investigação^[xliii]. Se o juiz realiza uma investigação privada, introduzindo seguidamente as provas no processo através de meio processual adequado, permitindo o contraditório das partes, das duas, uma: ou o juiz não tinha poder para realizar essa investigação – caso em que comete uma irregularidade, com influência na decisão da causa – ou tinha poder para tal, caso em que nada pode ser apontado, deste ponto de vista, à decisão tomada com base no resultado da pesquisa.

No Ac. TRL, de 30.05.2023, proc. n.º 568/20.5T8MTJ.L1-7, relator Diogo Ravara, e no Ac. TRP, de 24.10.2024, proc. n.º 56/23.8T8ALB.P1, relator Paulo Dias da Silva, o Tribunal entendeu terem sido violados os princípios processuais que presidem à produção de prova, desde logo o princípio da audiência contraditória (artigo 415º CPC), pelo facto de o tribunal de primeira instância ter utilizado, privadamente, as ferramentas informáticas *Google Maps* e *Street View* como fonte de prova. Na verdade, considera o Tribunal, em ambos os arestos, que a atividade realizada corresponde a uma prova por inspeção, com violação das normas dos artigos 491.º e 493.º CPC. Não é posta em causa a admissibilidade do recurso, *ex officio iudicis*, a estas ferramentas, mas apenas o modo como o tribunal o fez: privadamente. Note-se que não se trata de casos em que as ferramentas eletrónicas referidas foram utilizadas como instrumento na prática ou na valoração de outras provas (referimo-nos a isto na introdução). Trata-se – isso sim – da utilização destas ferramentas como fonte de prova no âmbito do juízo probatório realizado sobre os factos alegados pelas partes^[xliv]. Não tem aplicação, portanto, o entendimento jurisprudencial de acordo com o qual se encontra, neste caso, dispensado o exercício do contraditório (referimo-nos, concretamente, ao Ac. STJ, de 27.04.2023, acima citado).

Concordamos inteiramente com estes arestos quanto ao aspeto do exercício do contraditório. Pode sintetizar-se do seguinte modo a orientação jurisprudencial: nos casos em que o *Google Maps* e o *Street View* sejam utilizados como mero instrumento ao serviço da prática de outras provas, não é necessário a observância do contraditório (Ac. STJ, de 27.04.2023), mas, quando os mesmos são usados como fonte de prova, o princípio do contraditório na produção da prova exige que as partes tenham a possibilidade de se pronunciar^[xlv] (Acs. TRL, de 30.05.2023, e Ac. TRP, de 24.10.2024). Tratando de uma prova constituenda, a parte é notificada para todos os atos de preparação e produção da prova, sendo também admitida a intervir nesses atos (artigo 415.º, n.º 2 CPC).

Com efeito, tratando-se de casos em que o tribunal de primeira instância se serviu do conteúdo da página web como fonte de prova, o princípio do contraditório na produção da prova obrigava a que a atividade em causa fosse realizada na presença das partes, ou, pelo menos, que as mesmas tivessem possibilidade de contraditar o seu resultado (não apenas através do recurso da decisão final – princípio da proibição de decisões-surpresa). Isto parece-nos incontroverso. A questão que nos colocamos diz respeito à possibilidade em si mesma de o tribunal recorrer às ferramentas eletrónicas referidas como fonte de prova. Ambos os arestos dizem respeito a processos contenciosos, envolvendo direitos disponíveis. O tribunal *ad quem* entendeu, em ambos os casos, que a atuação do tribunal de primeira instância se encontra coberta pela norma do artigo 411.º CPC. Entende também aquele tribunal que a atividade em causa corresponde a uma prova por inspeção. Importa submeter isto ao crivo das conclusões que apresentámos.

Defendemos que a atividade de “cibernavegação” corresponde a uma prova por inspeção somente nos casos em que o (enunciado de) facto sob decisão diga respeito à existência, e ao conteúdo, da página a examinar. Não é isso que acontece neste caso. O caso é, no entanto, peculiar. Ele não se enquadra nas categorias gerais que apresentámos. Com efeito, trata-se de hipóteses em que a consulta das ferramentas eletrónicas em causa – cuja existência, importa notá-lo, constitui um facto notório^[xlv] – funciona como um sucedâneo do facto real: ou seja, o juiz, ao observar a ferramenta, procura observar a própria realidade. Ora, a realidade em causa integra o conteúdo do enunciado de facto controvertido, ou seja, ela é o objeto da prova. Apesar de o caso não ser linear, entendemos, assim, que o juiz pode ordenar a realização desta prova, admitindo a sua qualificação como meio de prova (análogo) a uma prova por inspeção^[xlvi]. Sendo assim, o juiz tem poder para ordenar a sua realização (artigo 411.º CPC).

3.2. Utilização da informação como elemento da fundamentação da decisão, mas não inserido no *iter* decisório relativo a um concreto facto da causa

O problema assume contornos diferentes no caso em que, o conteúdo de uma página web, seja utilizado não como fonte de prova, mas como meio de informação do juiz, utilizada na fundamentação da decisão, mas não integrando o *iter* decisório relativo a um facto da causa. Ou seja, quando a consulta realizada pelo juiz, através de “cibernavegação”, se destina a recolher uma informação pelo mesmo utilizada na elaboração do juízo conducente a uma decisão de mérito, mas sem que a mesma sirva de fonte de prova dos factos alegados pelas partes.

Em primeiro lugar, deve notar-se o óbvio: o juiz pode recorrer à internet como fonte de informação, tal como pode recorrer a uma fonte de informação analógica. Não existe nenhuma discriminação da primeira, competindo, evidentemente, ao juiz apreciar (como aliás também acontece no caso de informação analógica) a fiabilidade da informação obtida – o aspeto é incontroverso.

As dúvidas que podem gerar-se dizem respeito, portanto, não ao regime aplicável (artigo 5.º, n.º 3 CPC [\[xlvi\]](#)), mas à qualificação do caso.

No Ac. TRL, de 25.09.2025, proc. n.º 546/23.2T8LSB-D.L1-8, relatora Carla Matos, relativo a uma ação destinada à resolução de questão de especial importância na vida de menores (na qual o requerente pede que os filhos menores passem a frequentar escolas públicas, sendo retiradas das escolas privadas que frequentam), o Tribunal foi chamado a pronunciar-se sobre um caso em que o tribunal de primeira instância recolheu, oficiosamente, informações de *websites* das escolas sugeridas pelo requerente, sem garantir contraditório nem produção formal de prova.

Em sentido convergente com o que dissemos anteriormente, o Tribunal começa por afirmar que: “a utilização, pelo Tribunal, de uma informação constante da Internet como meio de prova de factos em discussão, ainda que feita oficiosamente, deverá ser precedida da faculdade das partes - após lhes ser facultado o respetivo conhecimento -, a poderem impugnar”. Cita o artigo 25.º RGPTC [\[xlviii\]](#). Note-se que o processo em causa tem a natureza de processo de jurisdição voluntária, razão pela qual o tribunal tinha o poder de recolher a referida informação, e de a utilizar como fonte de prova (cf. artigos 12.º RGPTC e 986.º, n.º 2 CPC) [\[xlix\]](#). Isto não dispensa, no entanto, o tribunal do exercício do contraditório, como resulta do artigo 25.º RGPTC, e resultaria já da aplicação das normas do artigo 3.º e do artigo 415.º CPC.

No entanto, lê-se no aresto que, *in casu*, “não se tendo integrado na matéria de facto provada quaisquer factos obtidos com base nessa consulta/utilização de *sites*, não se coloca a questão da violação do princípio do contraditório na obtenção/utilização da prova”.

Ou seja, entende o Tribunal que a informação em causa não foi utilizada como fonte de prova, na medida em que não se integrou na matéria de facto provada quaisquer factos obtidos com base na referida consulta. Isto, ou seja, o facto de não ter sido violado o princípio do contraditório, não conduz, no entanto, o Tribunal à conclusão de que a informação em causa pode ser utilizada no processo em curso - nem isso teria sentido. Com efeito - nota o Tribunal - trata-se de matéria de facto, não de matéria de direito. Em suma: entende o Tribunal que se trata de matéria de facto e que, se a mesma tivesse sido tratada como tal, era necessário o cumprimento do contraditório. Não tendo sido tratada como tal (conclui o Tribunal), a informação em causa não deve ser considerada.

Este caso não serve de exemplo, portanto, do que agora tratamos (trata-se de uma hipótese subsumível ao ponto 3.2.). O tribunal de primeira instância considerou, na aplicação do direito, a informação dos *sites* da Internet, como se de direito se tratasse, mas - conforme nota o Tribunal *ad quem* - a informação em causa prende-se com as características de factos das escolas publicitadas nos respetivos sites, e não com qualquer identificação ou descrição de normas legais. O resultado da consulta/utilização dos *sites* não pode ser integrado na apreciação de direito, por não se tratar de matéria de direito. Caso a informação se inserisse no juízo de direito, o Tribunal poderia utilizá-la, sem necessidade de cumprimento do contraditório, tal como pode, na mesma circunstância, utilizar informação em suporte analógico.

Bibliografia

Abel Lluch, Xavier. "La Prueba Electrónica." In *La Prueba Electrónica. Colección de Formación Continua Facultad de Derecho ESADE Abel Luch, Picó i Junoy (org.)*, 2011.

Bechini, Ugo. *Il notaio digitale. Dalla firma alla blockchain*: Giuffrè, 2019.

Freitas, José Lebre de. *Introdução ao processo civil : conceito e princípios gerais*. 2a ed. Coimbra: Coimbra Editora, 2006.

Junoy, Joan Picó i. *El juez y la prueba : estudio de la errónea recepción del brocardo index iudicare debet secundum allegata et probata, non decundum conscientiam y su repercusión actual / Joan Picó i Junoy; pref. Manuel Cachón Cadenas*. Barcelona: Bosch, 2007.

Mata, Federico Bueno de. *Prueba Electrónica Y Proceso 2.0*: Tirant Lo Blanch, 2014.

Mendes, João de Castro, Sousa, Miguel Teixeira de. *Manual de processo civil* Lisboa: AAFDL, 2022.

Nörr, K. W. *Zur Stellung des Richters im gelehrten Prozess der Frühzeit: Iudex secundum allegata non secundum conscientiam iudicat [Münchener Universitätschriften, Reihe der Juristischen Fakultät, 2]*. Müncher: Beck, 1967.

Pereira, Fernando Silva. *Prova Eletrónica em Processo Civil*: Almedina, 2026.

Rocchi, A. d'Arminio Monforte Matteo. *Le prova digitali nel processo civile*. Pisa: Pacini Giuridica, 2021.

Sousa, Luís Filipe Pires de. *Direito Probatório Material*. 3.^a ed.: Almedina, 2023.

Sousa, Luís Filipe Pires de. *O valor probatório do documento eletrónico no processo civil*: Almedina, 2016.

Tagliaferro, Vera. "Atto pubblico informatico." In *Diritto dell'informatica, a cura di Delfini e G. Finocchiaro*. Edited by Utet, 2014.

(*) O Sumário Executivo foi redigido com recurso ao www.chatgpt.com.

(**) O Resumo foi redigido com recurso ao www.chatgpt.com.

[i] Este artigo tem por base o capítulo correspondente da nossa obra Fernando Silva Pereira, *Prova Eletrónica em Processo Civil* (Almedina, 2026).

[ii] Deve notar-se que partimos de uma noção ampla de página web, incluindo-se a execução on-line – ou seja, através da web – de uma qualquer aplicação para “telemóvel” (tais como, para citar as mais frequentes: *WhatsApp*; *Gmail*; *Youtube*; *Dropbox*; *Facebook*, *Instagram*, *Twitter*, *Linkedin*, *Pinterest*), e não só a “clássica” página de um jornal on-line ou de um sítio de *e-commerce* (A. d'Arminio Monforte Matteo Rocchi, *Le prova digitali nel processo civile* (Pisa: Pacini Giuridica, 2021), 136-137).

[iii] Um documento eletrónico pode ser definido como a representação de um facto concretizada por meio de um computador e armazenado em formato específico (*bits* e *bytes*), capaz de ser transmitido ou apreendido pelos sentidos mediante o emprego de programa (*software*) apropriado (Luís Filipe Pires de Sousa, *O valor probatório do documento eletrónico no processo civil* (Almedina, 2016), 34).

[iv] Ou à entidade certificadora (notário).

[v] A. d'Arminio Monforte Matteo Rocchi, *Le prova digitali nel processo civile*, 136-137.

[vi] Atestando a conformidade da página web ao que é visualizado pelo notário, e atestando os dados anexos, a saber: a hora da operação (completada pela indicação do fuso horário de referência), o tipo e versão de *browser*, o sistema operativo e fornecedor de acesso utilizado, e a marca e modelo da impressora e código fonte (*ibidem*). Sobre o tema, pode ver-se: Vera Tagliaferro, "Atto pubblico informatico," in *Diritto dell'informatica*, a cura di Delfini e G. Finocchiaro, ed. Utet (2014), 298.; Ugo Bechini, *Il notaio digitale. Dalla firma alla blockchain* (Giuffrè, 2019), 20. Em virtude das características deste documento eletrónico, a exibição de uma mera cópia em suporte analógico não oferece garantias de segurança, tendo pouco valor, sobretudo se não for complementada por outros meios de prova, como a prova testemunhal. Ou seja, o seu valor é meramente indiciário.

[vii] O mercado privado disponibiliza também algumas plataformas capazes de registar os conteúdos eletrónicos, sobretudo informações contidas em páginas da Internet, por meio da utilização da tecnologia *blockchain*, com o intuito de preservar as informações do momento em que os arquivos são dispostos na plataforma, como forma de auxiliar a comprovação e evitar alterações. Pode dar-se como exemplo, as plataformas da *HashCool*, *OriginalMy*, e *Verifact*. Este mecanismo garante a existência do documento numa determinada data e hora, comprovando também que o documento não foi alterado desde então. Constitui, pois, o equivalente, em meio digital, a uma autenticação notarial.

[viii] Esta última consiste em captar a página web, através de um dispositivo dotado de vídeo-câmara, enquanto a mesma é consultada pelo utente, enviando-se, para terceiro ou para si mesmo, o vídeo realizado através de correio eletrónico certificado (A. d'Arminio Monforte Matteo Rocchi, *Le prova digitali nel processo civile*, 136-137)

[ix] Repare-se que esta distinção não coincide com aquela, comumente feita pela doutrina, entre fonte e meio de prova (pode ver-se, entre outros: Xavier Abel Lluch, "La Prueba Electrónica," in *La Prueba Electrónica. Colección de Formación Continua Facultad de Derecho ESADE Abel Luch, Picó i Junoy (org.)* (2011), 26. (sobre a distinção entre fonte e meio de prova, pp. 66 ss.); Luís Filipe Pires de

Sousa, *O valor probatório do documento eletrónico no processo civil*, 37-38; Federico Bueno de Mata, *Prueba Electrónica Y Proceso 2.0* (Tirant Lo Blanch, 2014), 94). No primeiro caso, tratar-se-ia de provar um facto eletrónico (por ex., que foi enviado um determinado correio eletrónico, numa determinada data). No segundo caso, tratar-se-ia de provar eletronicamente um facto (por ex., através da exibição de um email em que o réu reconhece expressamente uma fatura não paga). Já quando se trate de provar eletronicamente um facto eletrónico (por ex., a celebração de um contrato a partir dos emails enviados dos terminais de dois computadores), a prova eletrónica seria simultaneamente objeto e meio de prova. A nosso ver, o *facto probando*, no primeiro caso, não é o correio eletrónico, mas o facto de A ter emitido uma declaração a B, em certa data, tendo essa declaração assumido a forma eletrónica (email). Mediante a apresentação do email, a parte pretende provar o *facto probando*. Da mesma forma, se A alega que B lhe enviou uma carta, recebida numa certa data, o *facto probando* não é a carta, mas o facto de B ter feito uma declaração, que assumiu a forma escrita, declaração essa que chegou à esfera de conhecimento de A no dia tal. A apresentação da carta prova este *facto probando*. Ou seja, o documento é, simultaneamente, fonte e meio de prova. A distinção acima (entre objeto/meio de prova) pode ser feita, mas são residuais os casos em que o *facto probando* diz respeito à existência do documento. Pense-se na descrição, na apreensão ou no arrolamento de um documento com muito valor, ou no caso em que o documento integra uma universalidade de facto. Sendo o documento eletrónico, como referido, uma certa informação, em código binário, armazenada num certo suporte, pode pensar-se em exemplos parecidos: pense-se no caso em que a prova tem por objeto a existência de uma obra digital certificada com um “token” não-fungível (NFT, na sigla inglesa). Concretamente no caso da cibernavegação, pode observar-se o seguinte: Nos casos “normais” de inspeção, ou seja, aqueles em que a inspeção tem por objeto uma coisa tangível, a coisa constitui o objeto da prova, sendo a inspeção o meio para a adquirir. E se a coisa for um documento? Pense-se no caso de um documento muito antigo, que não pode ser apresentado em tribunal. Pode requerer-se que o mesmo seja inspecionado, tal como que ele seja objeto de uma perícia. Neste caso, a prova por inspeção/pericial tem por objeto o documento, mas o *facto probando* não diz respeito à existência do documento, mas à declaração nele contida. Ou seja, trata-se de um caso de prova complexa, em que o meio de prova inspeção serve para provar que a “declaração tal” se encontra registada no documento, e o documento serve para provar que, uma determinada pessoa, numa determinada data, proferiu essa declaração. Não é diferente o caso, se se pede ao tribunal para observar o conteúdo de um email, ou aquele que consta de uma página web.

[x] Pode ver-se, a propósito da atividade de certificação a realizar pelo notário: Vera Tagliaferro, “Atto pubblico informatico,” in *Diritto dell' informatica*, a cura di Delfini e G. Finocchiaro, 298.; Ugo Bechini, *Il notaio digitale. Dalla firma alla blockchain*, 20.

[xi] No sentido de: técnico-informáticas.

[xii] Note-se, concretamente, que o respeito pelo princípio do contraditório está assegurado pelas regras que regem este meio de prova (a prova por inspeção).

[xiii] Abel Lluch utiliza a expressão “livre apreciação especialíssima”, no sentido de uma maior sensibilidade jurídica, para se referir à valoração de um facto ou de uma prova eletrónica, valoração essa que pode implicar uma especial atenção ou uma melhor informação sobre aspetos técnicos (Xavier Abel Lluch, "La Prueba Electrónica," in *La Prueba Electrónica. Colección de Formación Continua Facultad de Derecho ESADE Abel Luch, Picó i Junoy (org.)*, 169 ss.).

[xiv] O juiz praticaria, então, o ato de consulta da rede social na presença das partes (prova por inspeção). Mas existe uma atividade investigatória, da qual resultou o conhecimento, pelo juiz, da respetiva fonte de prova. A nosso ver, o caso é análogo, portanto, àquele em que o juiz investiga privadamente a realidade, descobrindo por sua própria iniciativa uma testemunha, chamando-a depois para depor em tribunal. Não cremos que o juiz tenha poder para isto.

Pode, assim, antecipar-se a resposta a este último caso. No nosso entendimento, o juiz não pode realizar uma atividade de investigação privada dos factos da causa, a qual contenderia com o princípio dispositivo e com o princípio da proibição de recurso à ciência privada.

[xv] Referindo-se a este aspeto: Xavier Abel Lluch, "La Prueba Electrónica," in *La Prueba Electrónica. Colección de Formación Continua Facultad de Derecho ESADE Abel Luch, Picó i Junoy (org.)*, 203.

[xvi] *Ibidem*.

[xvii] *Ibidem*.

[xviii] O STJ transcreve as partes do Acórdão do tribunal *a quo* onde o mesmo afirma ter utilizado estas ferramentas: «Na presente ação, o Tribunal da Relação na apreciação da impugnação da decisão sobre a matéria de facto, alude, por três vezes à utilização do Google Maps/Street View:

- Quando descreve toda a prova produzida, na parte em que refere a inspeção ao local, finaliza com a seguinte menção, a fls. 60 do acórdão:

Consigna-se que a funcionalidade do Google Maps “Street View” está activa para a Rua do ..., ..., ..., permitindo assim visualizar o caminho percorrido pelo tribunal a quo e descrito no Auto de inspeção ao local.

- Quando analisa a dinâmica do atropelamento do Autor, relativamente à conformação da rua onde o mesmo ocorreu (...)

- Ainda na análise da dinâmica do atropelamento do Autor, a fls. 69 do acórdão, recorrido consta o seguinte:

Em primeiro lugar impõe-se referir que, percorrida a Rua em referência, através da funcionalidade “Streetview” temos alguma dificuldade em visualizar uma curva seguida de uma contracurva, como declarou o A., porquanto o sentido comum desta expressão é haver uma curva,

seja para a esquerda ou para a direita e imediatamente a seguir outra curva, mas no sentido contrário ao da primeira.

No caso concreto, a partir da curva à direita imediatamente a seguir à casa do interveniente acessório, a rua desenvolve-se em curvas sucessivas à esquerda, incluindo junto ao posto de transformação de eletricidade, em que a curva para a rua estreita é acentuada.

Em segundo lugar e tendo em consideração o auto de inspeção ao local, a consulta do Google Maps - em que é visível que antes do posto de transformação a habitação ali existente tem o n.º 218 - e o extratado dos diversos depoimentos, sobretudo do depoimento do interveniente acessório, que afirmou que o A. ia no lado esquerdo, ele ia no meio da estrada, mas depois “cheguei-me mais para aquele lado para ele me ouvir dizer “para”, cheguei-me mais para o lado dele”, que o A. declarou que foi embatido a 1/2 metros do muro da casa e o próprio interveniente declarou que o embate deu-se mais do lado esquerdo da via, a cerca de 2 m do muro (o que retira credibilidade ao depoimento da testemunha II que afirmou que o embate se deu a 4/5 m da berma, ou seja, nem é sequer do muro...), há que concluir que quando o A. se encontrava em frente ao n.º 218 da Rua ..., próximo da berma do lado esquerdo, o OI aproximou-se de tal forma do mesmo e embateu-o, na parte inferior do corpo, com a parte do veículo em que se situa a óptica esquerda, tendo o A., de seguida, caído sobre o capot e para brisas do lado do condutor, que partiu, vindo a cair no pavimento, na zona da valeta, do lado esquerdo onde ficou imobilizado sem se conseguir mexer, já que tinha os membros inferiores fraturados e hematoma na cabeça por força do embate no vidro da viatura.».

[xix] Trata-se, na verdade, de um documento eletrónico, devendo ser aplicadas as regras do artigo 3.º, n.º 10 DL 12/2021, de 9 de fevereiro.

[xx] O caso tem outra particularidade. Tendo sido requerida a junção de fotos recolhidas no Google Maps, o tribunal de 1.ª instância não admitiu a sua junção. Isto (afirma o STJ), não impede este tipo de utilização pelo Tribunal da Relação, uma vez que não foi sobre essa utilização que o mesmo se pronunciou, não ocorrendo qualquer desrespeito a um caso julgado formal.

[xxi] Repise-se que, é a esta hipótese, ou seja, aquela em que o enunciado de facto controvertido - essencial ou instrumental - diz respeito ao conteúdo de uma página web, que reservamos a aplicação, em sentido estrito, do regime da inspeção. Nos casos em que o juiz “cibernavega” com vista a obter uma informação não estamos - mesmo quando essa informação seja utilizada como fonte de prova - perante uma prova por inspeção. Não concordamos com o entendimento contrário. A nosso ver, seria o mesmo dizer que, quando o juiz consulta um livro, utilizando uma informação dele recolhida como fonte de prova, o mesmo praticou uma prova por inspeção: a inspeção do livro. Não nos parece correto este raciocínio. A prova é documental, num caso e no outro. Apenas quando o objeto da prova seja a existência da página web x, com o conteúdo y, requerendo-se ao tribunal, ou decidindo este *ex officio iudicis*, consultar a referida página, estaremos perante uma atividade subsumível ao conceito de prova por inspeção.

[xxii] Luís Filipe Pires de Sousa, *O valor probatório do documento eletrónico no processo civil*, 100.

[xxiii] Em rigor, a Google constitui um motor de busca: que leva o utilizador para uma outra página web. O conteúdo da página web pesquisada não constitui um facto notório: estamos inteiramente de acordo com isto.

[xxiv] Nesta modalidade de inspeção, «a parte faculta ao juiz um computador, ou este utiliza um próprio, com acesso à internet, a fim de o juiz se inteirar, diretamente e na presença das partes, do conteúdo de sites ou de correio eletrónico trocado entre as partes» – Luís Filipe Pires de Sousa, *Direito Probatório Material*, 3.^a ed. (Almedina, 2023), p. 206.

[xxv] Pense-se no caso em que uma parte requer ao tribunal que inspecione o computador da parte contrária, para aferir, por exemplo, do conteúdo de um email.

[xxvi] Ac. TRL, de 14.02.2023, proc. n.º 400/19.2T8CSC.L1-7, relator Pires de Sousa.

[xxvii] Pode também o juiz ordenar a realização de uma verificação não judicial qualificada (cf. artigo 494.º CPC). Não deve confundir-se esta figura, com a do artigo 492.º CPC. Nos mesmos termos em que é admitida a prova por inspeção, pode o juiz incumbir “técnico” ou “pessoa qualificada” de fazer uma verificação não judicial qualificada, que será quem pessoalmente fará o ato de inspeção (494.º, 1 CPC). As respetivas conclusões deverão constar de relatório (494.º, 1 CPC), que será livremente apreciado pelo tribunal (494.º, 2, 2.^a parte CPC). Sobre a natureza jurídica desta figura, cf., com referências, Lebre de Freitas/Isabel Alexandre, CPC Anotado, II3, 494.º.

[xxviii] Nos termos da norma do artigo 415.º, n.º 1 CPC, salvo disposição em contrário, não são admitidas nem produzidas provas sem audiência contraditória da parte a quem hajam de ser opostas.

[xxix] Cf. entre outros, os acórdãos do TRL de 12-03-2019, proc. 21183/16.2T8LSB.L1; TRL de 04-06-2019, proc. 214/16.1T8MFR.L1 e TRL de 08-10-2019, proc. 10371/18.7T8LSB.L1 consultáveis in www.dgsi.pt. E: João de Castro Mendes e Miguel Teixeira de Sousa, *Manual de Processo Civil*, Vol. I, AAFDL, 2022, p. 44; cf. ainda Teixeira de Sousa, “Nulidades do processo e nulidades da sentença: Em busca da clareza necessária”, 22.9.2020, <https://blogipcc.blogspot.com/2020/09/nulidades-do-processo-enulidades-da.html>.

[xxx] «Destarte, a sentença em crise utilizou a ferramenta Google Earth em violação do disposto nos artigos 415.º, 491.º e 493.º do Código de Processo Civil. E fazendo-o, há quem defenda que a omissão de formalidade essencial seguida da prolação de sentença configura uma nulidade processual, nos termos do disposto nos artigos 195º e segs. do Código de Processo Civil e não uma nulidade da sentença, por excesso de pronúncia, nos termos do disposto no artigo 615º, nº 1, al. d) do mesmo diploma. Acorava-se esse entendimento na consideração de que a génese da nulidade se situava a montante da prolação da sentença e bem assim na circunstância de o regime da nulidade da sentença não prever a possibilidade de o processo retroceder a fase anterior à da

prolação da decisão final (v.g. à audiência de julgamento, à audiência prévia, ou mesmo aos articulados). Contudo, alguma jurisprudência vem salientando que a preterição do direito ao contraditório seguida da prolação de sentença pode configurar simultaneamente uma nulidade processual, e uma nulidade da sentença, por excesso de pronúncia.»

O Tribunal considera que estamos perante um concurso de normas. Pode ler-se:

«Cremos, porém, que a ponderação de tais situações como de concurso das duas nulidades, com eventual conjugação de regimes permite alcançar respostas satisfatórias àquelas interrogações, respeitando a letra e espírito dos preceitos que regulam as duas figuras- Cf., neste sentido acórdão do TRL de 30-05-2023, processo 568/20.5T8MTJL1-7, consultável in www.dgsi.pt. Assim sendo, acreditamos ser de considerar que se poderá falar em concurso dos dois vícios nas situações em que a primeira nulidade por omissão de uma formalidade legal anterior à prolação da sentença não deva considerar-se sanada por falta de invocação atempada. Tal sucederá em todas as situações em que tal nulidade apenas se revela com a prolação da sentença, como se verifica no caso em análise. Nesta conformidade, conclui-se que a sentença apelada é nula, por excesso de pronúncia, devendo ser anulada e que, na impossibilidade de este Tribunal se substituir ao Tribunal a quo, nos termos previstos no artigo 665º do Código de Processo Civil, devem os autos ser remetidos ao Tribunal a quo, a fim de reabrir a audiência para a realização de cibernavegação, com observância das normas aplicáveis, nomeadamente o disposto nos artigos 415º, 491º e 493º do Código de Processo Civil.»

[\[xxxii\]](#) O caso é análogo daquele que demos como exemplo inicial: aquele em que o juiz consulta um sítio da internet para apurar o preço médio de arrendamento numa determinada zona, com vista a decidir o valor do rendimento disponível, no apenso da exoneração do passivo restante. A nosso ver, eles devem ter o mesmo tratamento.

[\[xxxiii\]](#) «O tribunal a quo fundamentou a resposta nestes termos: «Factos sob o nº9): Conforme resulta do depoimento/declarações da Autora (na parte não confessória), explicando, contudo, que já não por razões de proximidade do trabalho e poupança nos transportes, uma vez que a sociedade onde era sócia gerente encerrou a atividade e corroborado pela simples consulta do site www.idealista.pt, que consultamos, não encontrando nenhuma casa/apartamento com um mínimo de 2 quartos (já nem sequer com três, como seria o ideal), por preços inferiores.».

[\[xxxiii\]](#) Podia, a nosso ver, fazê-lo, dada a natureza do processo em causa (trataremos deste ponto mais adiante). Com efeito, deve distinguir-se a questão de saber se o juiz tem poder para realizar a atividade em causa, da questão de saber se o mesmo a pode realizar com dispensa de audiência contraditória. Apenas a segunda questão nos parece problemática no caso em apreço, não a primeira.

[\[xxxiv\]](#) No Ac. STJ, de 27.04.2023, proc. n.º 4017.20.0T8GMR.G1.S1.F3, relator Cura Mariano, acima citado, relativo a um caso em que o Tribunal da Relação recorreu imagens do Google Maps/Street View para apreciação da prova produzida em primeira instância, o Tribunal afirma que: “a

visualização de imagens do Google Maps/Street View, de forma estática ou dinâmica, apesar de colhidas na Internet, não parece consistir na realização de uma “cibernavegação”, enquanto modalidade de inspeção judicial, nos termos do artigo 450.º do Código de Processo Civil.”

[xxxv] A observância do princípio do contraditório na produção da prova «destina-se a permitir que a produção de prova por uma das partes a outra possa responder com uma contraprova (artigo 346º CC) ou com prova do contrário (artigo 347º CC)» (João de Castro Mendes, Miguel Teixeira de Sousa, *Manual de processo civil* (Lisboa: AAFDL, 2022), p. 515). A circunstância de a iniciativa da cibernavegação ser oficiosa não tolhe a necessidade de observância do princípio do contraditório, o qual persiste incólume.

[xxxvi] Um outro ponto tratado no acórdão, com o qual concordamos inteiramente, diz respeito ao facto de que, o facto em causa, não constitui um facto notório. Trata-se de um ponto alegado pelo recorrido: «(...) o tribunal a quo não deu tal facto como provado com base em inspeção, sendo um facto notório que o valor do arrendamento para habitação na zona da apelada atinge um valor mínimo mensal de quinhentos a seiscentos euros, conforme indicado na petição inicial». Conforme nota o tribunal: «(...) A exigência do conhecimento geral atua em vários âmbitos: - Na esfera pessoal, o facto notório tem de constar como certo ou falso para a generalidade de pessoas de cultura média entre as quais se encontra o juiz; - Na esfera cognoscitiva, no sentido de que tal conhecimento deve integrar a cultura média, de acesso geral, e não ser constitutivo de um saber especializado próprio de um reduzido número de pessoas que se dedica a uma atividade comum; - Na esfera espacial, no sentido de que tal facto deve ser conhecido no território que integra as instâncias de recurso. Não pode o facto ser notório para o juiz da primeira instância e desconhecido para o juiz conselheiro. Assim, um desastre nacional divulgado pela imprensa constitui um facto notório, mas já não será facto notório os prejuízos causados pelo granizo numa comarca mesmo que tenham afetado pessoalmente o juiz.» Ora, o valor de arrendamento em Queijas/Oeiras não constitui um facto de conhecimento geral a nível nacional nem integra o conhecimento de generalidade das pessoas de cultura média, estando – assim – afastada a sua natureza de facto notório.».

[xxxvii] Sobre o significado da parte final deste brocardo, referindo que a mesma foi erradamente utilizada para limitar a atividade do juiz: Joan Picó i Junoy, *El juez y la prueba : estudio de la errónea recepción del brocardo index iudicare debet secundum allegata et probata, non secundum conscientiam y su repercusión actual* / Joan Picó i Junoy ; pref. Manuel Cachón Cadenas (Barcelona: Bosch, 2007). Entende o autor que, contrariamente ao que pode, com frequência, ver-se sustentado, a doutrina do *ius commune* não comunga uma posição contrária à existência de quaisquer poderes oficiosos do tribunal, tendo a errada transcrição daquele brocardo incidido de forma direta, não apenas sobre o alcance, mas também sobre a finalidade do mesmo. O brocardo original («*iudex iudicare debet secundum allegata et probata, non secundum conscientiam*») pretende apenas destacar os limites da cognição do tribunal (*iudex iudicare debet*), rejeitando-se a possibilidade de o juiz fazer uso de qualquer conhecimento privado (*conscientiam*) dos factos. Sobre o tema pode ver-se também: K. W. Nörr, *Zur Stellung des Richters im gelehrten Prozess der Frühzeit: Iudex secundum*

allegata non secundum conscientiam iudicat [Münchener Universitätschriften, Reihe der Juristischen Fakultät, 2] (Müncher: Beck, 1967).

[xxxviii] O princípio do contraditório dirige-se à possibilidade de defesa contra a pretensão do autor/reconvinte (trata-se, na designação alemã, do direito a ser ouvido pelo tribunal (*rechtliches Gehör*), ou, no brocado latino: *audiatur et altera pars*/ que se escute também a outra parte) – artigo 3.º, n.º 1 e artigo 4.º CPC, tendo também por conteúdo, de acordo com a compreensão atual do mesmo, a possibilidade de influenciar a decisão a ser proferida na causa. Ou seja, o princípio visa conferir a possibilidade de defesa não apenas contra alegações da contraparte, mas também perante decisões do juiz. Se o juiz pretender tomar uma decisão ao abrigo de fundamento não sustentado por nenhuma das partes, deve conceder a uma e a outra a possibilidade de pronúncia (princípio da proibição de decisões surpresa). O princípio do contraditório manifesta-se, seguindo a sistematização de Lebre de Freitas, nos planos da alegação, da prova e do direito. No plano da prova, o princípio reclama que uma e outra parte: i) tenham idênticas possibilidades de proposição dos meios probatórios necessários à prova das alegações de facto; ii) que a atividade instrutória seja realizada, quando o meio de prova em causa o consinta, em audiência; iii) que se possam pronunciar sobre as provas produzidas (José Lebre de Freitas, *Introdução ao processo civil: conceito e princípios gerais*, 2a ed. (Coimbra: Coimbra Editora, 2006)).

[xxxix] Pode assim a parte impugnar a autenticidade ou a genuinidade do documento...

[xl] O problema coloca-se em termos diferentes se o facto em causa puder ser configurado como um facto notório (o que, evidentemente, não acontece no exemplo dado). Pense-se no caso em que o juiz recorre à “navegação na internet” para confirmar a distância entre um local e outro. Estamos neste caso perante um facto notório (a distância entre dois pontos), para efeitos da aplicação da norma do artigo 5.º, n.º 2, alínea c) CPC? Se não, caberia às partes alegar este facto, e requerer a prova (que podia, porventura, consistir na “navegação na internet”). Se sim, não se vê por que razão, sendo o facto notório, o juiz sente necessidade de se socorrer da “navegação na internet” para obter a confirmação do mesmo. Não deve, portanto, questionar-se se o juiz pode “navegar na internet” com vista a obter o conhecimento de um facto notório. Essa questão, pura e simplesmente, não faz sentido.

[xli] O conhecimento privado do juiz não é um meio de prova legalmente admitido. Não o é, aliás, nem mesmo se o processo tiver a natureza de processo de jurisdição voluntária. Neste caso, o juiz pode investigar livremente a realidade e coligir provas, mas deve decidir com base em elementos de prova objetivos, introduzidos pelos meios adequados.

[xlii] Coisa que acontece, designadamente, nos processos de jurisdição voluntária.

[xliii] No caso do Ac. TRL, de 30.5.2023, referente a um caso de responsabilidade civil, relacionado com um acidente de viação: «O tribunal baseou a sua convicção, no que concerne aos factos provados sob os números 1 a 7, 10, 13, 16, 17, 18, 20, 21, 27 e 31 a 33 relativos à identificação dos

intervenientes, às circunstâncias temporais, locais e de sentido em que os veículos circulavam e aos danos sofridos pelo veículo BD, na sua aceitação expressa pela ré e na sua falta de impugnação, em conjugação com a análise do teor do certificado de matrícula referente ao veículo BD, da participação do acidente de viação, do relatório de peritagem e dos orçamentos todos juntos com a petição inicial, bem como na observação da autoestrada e nas medições feitas com recurso à ferramenta de medição disponível no Google Maps”. Mas, conforme se nota seguidamente no aresto agora citado: “Muito embora o Tribunal a quo nada mais esclareça quanto às circunstâncias em que recorreu a esta ferramenta informática e aos resultados que colheu da sua utilização, do inciso citado parece resultar que tal ferramenta foi usada para observar o local e proceder a medições (sem que o Tribunal a quo esclareça que medições em concreto fez).».

No caso do Ac. TRP, de 24.10.2024, o Tribunal *a quo*, oficiosamente, «socorreu-se da ferramenta informática Google Earth para dar como provadas as áreas do prédio ...11, em concreto, que o mesmo foi «absorvido pelo prédio da Autora (...) em cerca de 560m²) e do Réu (...) em cerca de 500m²» [facto provado 16)]. Ora, tendo em consideração que a cibernavegação (medição de áreas), no caso em concreto, foi realizada oficiosamente e sem qualquer notificação às partes de que iria servir como meio de prova, ficou vedada às mesmas a intervenção no acto de produção desta prova.». Neste caso, nota também o Tribunal da Relação que, resulta das regras da experiência comum, que as medições realizadas na aplicação Google Earth é superficial e sem o devido rigor, sendo impossível determinar, com certeza, os limites e extremas dos terrenos e, consequentemente, a área dos mesmos, existindo para o efeito os levantamentos topográficos. Neste ponto, o Tribunal já não questiona a admissibilidade do recurso às referidas ferramentas eletrónicas, ou o modo (privado) como esse recurso ocorreu, mas a eficácia probatória deste meio de prova. Ou seja, a apreciação do tribunal não se coloca agora, no plano da admissibilidade da prova, mas no plano do resultado da prova.

[xliv] A observância do princípio do contraditório na produção da prova «destina-se a permitir que à produção de prova por uma das partes a outra possa responder com uma contraprova (artigo 346º do Código Civil) ou com prova do contrário (artigo 347º do Código Civil) (Cf. João de Castro Mendes, Miguel Teixeira de Sousa, *Manual de processo civil* p. 515).

[xlv] Luís Filipe Pires de Sousa, *O valor probatório do documento eletrónico no processo civil*, 100.

[xlvi] Note-se que estas hipóteses não são análogas daquela tratada no Ac. TRL, de 14.02.2023, proc. n.º 400/19.2T8CSC.L1-7, relator Pires de Sousa (caso em que repudiámos a configuração da atividade judicial realizada como uma prova por inspeção). Trata-se aqui de um caso em que o juiz recorreu ao sítio de uma imobiliária para aferir do preço médio de arrendamento de imóveis numa determinada zona. Não existe, de facto, analogia entre os casos. Este último tem, a nosso ver, afinidade – isso sim – com a prova pericial. O juiz recorre ao sítio da imobiliário como que a uma opinião técnica ou especializada.

[\[xlvii\]](#) Esta norma («o juiz não está sujeito às alegações das partes no tocante à indagação, interpretação e aplicação das regras de direito») corresponde ao princípio *iura novit curia*. Chamamos a atenção para ele neste sentido: o juiz pode recorrer à “navegação na internet” para obter informações por si mobilizadas no âmbito do juízo de direito vertido na sentença. Isto é evidente.

[\[xlviii\]](#)

«1 - As partes têm direito a conhecer as informações, as declarações da assessoria técnica e outros depoimentos, processados de forma oral e documentados em auto, relatórios, exames e pareceres constantes do processo, podendo pedir esclarecimentos, juntar outros elementos ou requerer a solicitação de informações que considerem necessárias.

2 - O juiz indefere, por despacho irrecorrível, os requerimentos apresentados que se mostrem inúteis, de realização impossível ou com intuito manifestamente dilatório.

3 - É garantido o contraditório relativamente às provas que forem obtidas pelos meios previstos no n.º 1.».

[\[xlix\]](#) Não se encontra bem calibrada, a nosso ver, a argumentação do recorrido, através das respetivas contra-alegações de recurso: «a utilização da informação constante dos websites das escolas trata-se de informação constante do domínio público (e que estava à disposição das partes) e como tal tinha o Tribunal a quo o poder de a conhecer (cf. artigo 5.ºCPC).». De facto, a informação em causa é de acesso público. No entanto, não sendo o objeto da mesma um facto notório, a questão de saber se o tribunal podia coligir e – se fosse o caso – utilizar como fonte de prova a informação em causa deve ser resolvida, não em função do acesso público ou reservado dessa informação, mas da natureza dos interesses objeto da causa, e do âmbito dos poderes instrutórios do juiz.

INTELIGÊNCIA ARTIFICIAL E PROVA EM PROCESSO CIVIL: NÓTULAS EXPLORATÓRIAS SOBRE A PRODUÇÃO, A APRESENTAÇÃO E A VALORAÇÃO DA PROVA COM CONEXÃO A SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

Joel Timóteo Ramos Pereira: Juiz Desembargador & Inspetor Judicial

Sumário Executivo: (1) O texto analisa os principais problemas probatórios suscitados pela utilização de sistemas e funcionalidades de inteligência artificial no processo civil. A inexistência de um regime processual específico obriga à adaptação das categorias probatórias tradicionais a uma realidade tecnológica que desafia os critérios clássicos de produção, apresentação e valoração da prova. (2) Enquadra-se o tema à luz do quadro regulatório europeu aplicável e as recomendações do uso de ferramentas de IA aprovadas pelo Conselho Superior da Magistratura. (3) Examina-se, em particular, a utilização de inteligência artificial nas diversas fases do processo, a qualificação jurídica da prova gerada ou assistida por sistemas algorítmicos, a autenticidade digital e a designada “cadeia de custódia”, os riscos associados às *deepfakes* e ao “dividendo do mentiroso”, a proteção de dados pessoais, o acesso às ferramentas utilizadas pela contraparte, a deteção de prova falsa, a valoração algorítmica de depoimentos e o controlo por via do recurso de atos ou decisões assistidas por inteligência artificial. (4) Conclui-se pela necessidade de reforçar o enquadramento processual através da criação de mecanismos de verificação técnica da autenticidade digital, da imposição de deveres de divulgação técnica relativos aos sistemas utilizados, da consagração da *explicabilidade* como requisito de admissibilidade probatória em determinados contextos e da institucionalização de apoio técnico especializado aos Tribunais.

Abstract: (1) The paper analyses the principal evidentiary challenges arising from the use of artificial intelligence systems and functionalities in civil proceedings. The absence of a specific procedural framework requires the adaptation of traditional evidentiary categories to a technological reality that challenges the classical criteria governing the production, submission and assessment of evidence. (2) The subject is examined in light of the applicable European regulatory framework and the recommendations concerning the use of AI tools approved by the High Council for the Judiciary. (3) Particular attention is devoted to the use of artificial intelligence throughout the various stages of civil proceedings, the legal classification of evidence generated or assisted by algorithmic systems, digital authenticity and the so-called “chain of custody”, the risks associated with deepfakes and the “liar’s dividend”, the protection of personal data, access to tools used by the opposing party, the detection of false evidence, the algorithmic assessment of witness testimony, and appellate review of acts or decisions assisted by artificial intelligence. (4) The paper concludes that there is a need to strengthen the procedural framework through the establishment of mechanisms for the technical verification of

digital authenticity, the imposition of technical disclosure obligations concerning the systems employed, the recognition of explainability as a requirement for evidentiary admissibility in certain contexts, and the institutionalisation of specialised technical support for the Courts.

Resumo (*): O texto analisa o impacto da inteligência artificial (IA) na prova em processo civil português, defendendo que o atual regime processual deve adaptar as categorias tradicionais da prova às novas realidades tecnológicas, sem perder as garantias fundamentais do processo justo. Parte do enquadramento normativo europeu, especialmente do AI Act, do Regulamento eIDAS 2.0, do RGPD e das recomendações do Conselho Superior da Magistratura, concluindo que a utilização da IA na justiça deve assentar na transparência, na supervisão humana, na explicabilidade e na responsabilização dos utilizadores. O estudo examina a utilização da IA em todas as fases relevantes do processo civil: na conciliação, na transcrição automática de depoimentos, na preparação e condução da audiência, na elaboração de peças processuais, na produção e apresentação da prova e na atividade decisória do juiz. Sustenta que a IA pode constituir um importante instrumento de apoio à organização, análise e tratamento da informação, mas nunca substituir a apreciação crítica do julgador nem a decisão jurisdicional. O autor analisa ainda problemas específicos como a autenticidade da prova digital, a cadeia de custódia, os deepfakes, as alucinações algorítmicas, a proteção de dados pessoais, o acesso às ferramentas utilizadas pelas partes, a deteção de prova falsa e a responsabilidade decorrente da utilização negligente de sistemas de IA por mandatários forenses. Quanto à qualificação jurídica, conclui que, em regra, os conteúdos produzidos por IA devem ser tratados como prova documental, sem necessidade de criar uma nova categoria probatória, embora sujeitos a exigências acrescidas de verificação da autenticidade, integridade, rastreabilidade e explicabilidade. Por fim, defende uma evolução legislativa que reforce os mecanismos de controlo da prova assistida por IA, imponha deveres de transparência relativamente aos sistemas utilizados, institucionalize apoio técnico especializado aos tribunais e assegure que a utilização da inteligência artificial permanece sempre subordinada aos princípios do contraditório, da igualdade de armas, da fundamentação das decisões e do controlo humano efetivo.

Palavras-Chave: Prova digital; inteligência artificial generativa; explicabilidade algorítmica; cadeia de custódia; *deepfake*; contraditório; dividendo do mentiroso.

Keywords: Digital evidence; generative artificial intelligence; algorithmic explicability; chain of custody; *deepfake*; adversarial principle; liar's dividend.

Índice: (§) Introdução; (1) A IA no processo civil: enquadramento dogmático; (1.1) Conceito “operativo” de IA para efeitos processuais; (1.2) Classificação dos sistemas de IA pelo nível de risco e repercussão processual; (1.3) A Carta Europeia do CEPEJ e as Diretrizes de 2025 sobre IA generativa; (1.4) Princípios processuais constitucionalmente relevantes; (1.5) Capacitação técnica do juiz; (2) Fase conciliatória: a IA como auxiliar da resolução do litígio? (2.1) Submissão de elementos documentais, periciais e outros à IA para elaboração de proposta de conciliação; (2.2) Resolução de litígios *em linha* com componente de IA; (3) Transcrição automatizada de declarações e depoimentos. (3.1) Transcrição por IA em audiência: enquadramento; (3.2) Valor probatório da transcrição gerada por IA; (3.3) Mecanismo processual de impugnação de transcrições com erros materiais; (4) Ferramentas de IA em audiência; (4.1) Utilização de ferramentas de IA pelas partes e mandatários; (4.2) Utilização de IA pelo juiz: assistência técnica ou função autónoma? (4.2.1) Enquadramento do mecanismo de assistência técnica; (4.2.2) Assistência técnica *versus* uso da IA na análise da prova; (4.2.3) A IA como instrumento de apoio à compreensão da prova tecnicamente complexa; (4.3) Pode o juiz exigir declaração de uso de inteligência artificial na elaboração das peças processuais? (4.3.1) Fundamento processual; (4.3.2) Autorresponsabilidade das partes e transparência processual; (4.3.3) Boa-fé processual, litigância de má-fé e evolução regulatória; (4.4) Especificidade do uso por mandatário de *chatbot* jurídico sem validação da informação produzida; (4.5) Práticas de IA manipuladoras e a sua aplicação a *chatbots* processuais; (5) Qualificação jurídica da prova gerada por IA; (5.1) Modalidades de prova no CPC e prova com intervenção de IA; (5.2) Prova gerada por inteligência artificial como categoria ontológica nova? (5.3) Admissibilidade e regime de junção da prova gerada por IA; (5.4) Conflito entre relatórios de IA e de perito humano; (6) “Cadeia de custódia” e autenticidade da prova digital produzida ou processada por IA; (6.1) Noção e valoração da “cadeia de custódia”; (6.2) Impugnação de documentos e prova digital gerada por IA; (6.3) *Deepfakes* (“falsificações profundas”); (6.3.1) Noção e relevo em processo civil; (6.3.2) Invocação de *deepfake*: convite ao aperfeiçoamento ou rejeição do meio de prova; (6.4) Detecção pelo juiz de prova digital falsificada; (6.5) Autenticação por carimbo (“selo”) de tempo qualificado; (7) Vigilância algorítmica, dados pessoais e dados obtidos por IA; (7.1) Prova obtida através de ferramentas de IA privadas utilizadas pelas partes; (7.2) Conflito entre direito à prova e o direito à proteção de dados pessoais; (8) Acesso às ferramentas de IA da contraparte e direito ao contraditório; (8.1) Direito de acesso ao modelo de IA, aos parâmetros de treino e aos dados utilizados; (8.2) Transparência algorítmica mínima como requisito legal de admissibilidade? (9) Valoração da prova por sistemas de IA; (9.1) Uso de IA na análise de depoimentos gravados; (9.2) Sistemas IA de análise documental em massa e cruzamento de dados entre espécies de prova; (10) Explicabilidade, recurso e controlo jurisdicional; (10.1) Explicabilidade como requisito de admissibilidade probatória; (10.2) Recurso de apelação com fundamento na ausência de *explicação* suficiente; (10.3) Controlo efetivo em sede de recurso de decisões de Primeira Instância assistidas por IA; (11) Conclusões.

A produção, a apresentação e a valoração da prova em processo civil suscitam questões específicas quando envolvem funcionalidades de modelos ou agentes de inteligência artificial (IA). A ausência de previsão expressa no Código de Processo Civil (CPC) torna essa reflexão necessária, embora ainda insuficientemente estabilizada do ponto de vista doutrinal e jurisprudencial. A prática judiciária e forense confronta-se diariamente com situações não antecipadas pelo legislador, enquanto a definição de soluções consistentes permanece dependente da evolução da doutrina e da jurisprudência.

A utilização de *chatbots* jurídicos na elaboração de articulados, o recurso a ferramentas de transcrição automatizada em audiência ou a apresentação de conteúdos probatórios cuja autenticidade depende da deteção de manipulação algorítmica ilustram diferentes manifestações do mesmo problema: a inexistência de categorias processuais adequadas para integrar uma tecnologia concebida fora do processo civil, mas que passou a influenciar a sua dinâmica por via da prática.

O presente estudo incide sobre a interseção entre a inteligência artificial e a atividade probatória no processo civil português, abrangendo a produção de prova com recurso a sistemas de inteligência artificial, a sua apresentação em juízo, a qualificação jurídica dos outputs algorítmicos à luz das categorias previstas no CPC, a respetiva valoração e a apreciação crítica realizada pelo julgador.

Ficam excluídas da análise a inteligência artificial utilizada como mero instrumento de gestão processual sem ligação à prova e a responsabilidade civil por danos causados por sistemas de inteligência artificial enquanto fonte autónoma de litígios, salvo quando tais matérias suscitem questões probatórias relevantes.

O enquadramento normativo relevante apresenta natureza transversal:

— O CPC fornece a matriz dogmática fundamental, mas o Regulamento (UE) 2024/1689 (*AI Act*) introduz deveres de transparência, supervisão humana e documentação técnica com incidência direta na apreciação da prova e o art.º 6.º da Convenção Europeia dos Direitos do Homem (CEDH) exige garantias do processo equitativo, incluindo o direito a uma decisão fundamentada e suscetível de controlo.

— O Regulamento eIDAS 2.0 (Regulamento (UE) 2024/1183) estabelece mecanismos de autenticação determinantes para a credibilidade da prova digital;

— O RGPD define os limites de admissibilidade dos dados pessoais tratados por sistemas de inteligência artificial como meio de prova;

— A Diretiva (UE) 2024/2853, relativa à responsabilidade por produtos de inteligência artificial, e o Regulamento (UE) 2023/1543, relativo à prova eletrónica transfronteiriça, completam este quadro nos casos em que a prova associada à inteligência artificial ultrapassa fronteiras nacionais ou incide sobre o funcionamento do próprio sistema.

A ordem jurídica portuguesa não prevê um regime específico para a prova produzida, processada ou valorada com recurso a sistemas de inteligência artificial. As categorias probatórias do CPC (designadamente a *prova documental, pericial, por inspeção e verificações não judiciais qualificadas*) foram concebidas para um contexto anterior à disseminação da inteligência artificial generativa, pelo que a sua aplicação exige um exercício de integração dogmática que oscila entre a adaptação das categorias existentes e a construção jurisprudencial de soluções intermédias.

As Recomendações do Conselho Superior da Magistratura relativas à utilização da inteligência artificial na atividade jurisdicional constituem a referência nacional mais atual nesta matéria. A sua relevância como parâmetro de licitude não dispensa, contudo, a apreciação autónoma das questões dogmáticas suscitadas pela atividade probatória assistida por inteligência artificial.

A estrutura adotada acompanha as fases da relação entre inteligência artificial e prova. Parte do enquadramento dogmático dos sistemas de inteligência artificial e da capacitação técnica exigível ao julgador; prossegue com a fase preliminar e conciliatória do processo, a transcrição automatizada de depoimentos e a utilização de ferramentas de inteligência artificial em audiência por partes, mandatários e juiz; analisa a qualificação jurídica da prova gerada por inteligência artificial, a designada “cadeia de custódia” e a autenticidade da prova digital, com destaque para o fenómeno das *deepfakes*; examina a tensão entre prova obtida por inteligência artificial privada e proteção de dados pessoais, o direito de acesso às ferramentas de inteligência artificial da contraparte, a deteção judicial de prova falsa e a valoração algorítmica de depoimentos; termina com a “*explicabilidade*” como requisito de admissibilidade e com o respetivo controlo em sede de recurso. Cada um destes momentos corresponde a uma fratura específica entre tecnologia e processo, concentrando-se aí o esforço interpretativo.

1. A IA no processo civil: enquadramento dogmático

1.1. Conceito “operativo” de IA para efeitos processuais

O Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, conhecido por “*AI Act*”, define, no art.º 3.º, n.º 1, como sistema de IA, o que é baseado em máquinas, concebido para operar com diferentes níveis de autonomia, que pode apresentar adaptabilidade após a implantação e que, a partir dos dados recebidos, infere a forma de gerar resultados (previsões, conteúdos, recomendações ou decisões) suscetíveis de influenciar ambientes físicos ou virtuais^[1].

Esta definição, deliberadamente ampla por razões regulatórias, abrange quer sistemas de aprendizagem automática de baixa complexidade, quer modelos de linguagem de grande escala. A sua transposição para o domínio processual exige, contudo, uma densificação concetual que o legislador europeu não realizou.

Para efeitos da atividade probatória no processo civil, a distinção relevante consiste em discernir *a inteligência artificial generativa* (sistema capaz de produzir, com base em instruções do utilizador, conteúdo novo dos sistemas de apoio à decisão, que processam dados preexistentes para deles extrair classificações, padrões ou recomendações, sem criar conteúdo *ex novo*). A primeira categoria suscita problemas de autenticidade e de autoria do conteúdo produzido; a segunda coloca problemas de fiabilidade metodológica da inferência realizada sobre prova já constituída^[2].

A tipologia de utilização judicial e processual da inteligência artificial reconduz-se, no estado atual da prática portuguesa, a quatro modalidades:

(i) *gestão processual*, em que o sistema apoia tarefas organizacionais sem interferir na substância da causa;

(ii) *assistência à pesquisa jurisprudencial e doutrinal*, modalidade já documentada e enquadrada pelas Recomendações do CSM;

(iii) *análise da prova*, em que o sistema processa documentos, depoimentos ou dados de geolocalização constantes dos autos; e

(iv) *geração (criação) de conteúdo*, categoria que abrange tanto a elaboração de minutas de decisões judiciais como a produção, pelas partes, de peças processuais ou de elementos probatórios. Esta última modalidade concentra as questões mais sensíveis, por ser aquela em que a fronteira entre o auxílio instrumental e a substituição da atividade jurisdicional ou processual assume contornos subtis.

1.2. Classificação dos sistemas de IA pelo nível de risco e repercussão processual

O AI Act assenta numa abordagem regulatória baseada no risco, qualificando como de alto risco os sistemas de inteligência artificial utilizados por autoridades judiciárias, ou em seu nome, para apoiar a apreciação dos factos e do direito e a tomada de decisões em casos concretos.

As Recomendações do Conselho Superior da Magistratura^[3] acolhem expressamente esta qualificação, submetendo tais utilizações ao regime reforçado previsto no seu art.º 6.º, n.º 2, e no anexo III, ponto 8, alínea a) ^[4]. A eventual adoção destes sistemas pelos juízes dos tribunais portugueses encontra-se, assim, sujeita ao quadro normativo mais exigente estabelecido pelo AI Act.

Deste enquadramento decorrem três ordens de obrigações com projeção processual direta.

Primeiro, a *obrigação de transparência*, que exige a documentação do funcionamento do sistema em termos compreensíveis para o operador humano, nos termos dos arts. 13.º e 14.º do AI Act.

Segundo, a *obrigação de registo e rastreabilidade das operações realizadas*, associada ao dever de manutenção de registos previsto no art.º 12.º.

Terceiro, e com particular relevância para a presente análise, a *obrigação de supervisão humana efetiva*, consagrada no art.º 14.º, que exige que o utilizador (no contexto em análise, o juiz ou o profissional forense) compreenda as capacidades e limitações do sistema, identifique anomalias ou irregularidades e conserve a faculdade de desativar ou contrariar o respetivo *output*. Esta exigência articula-se diretamente com o *princípio do controlo humano eficaz*, segundo a qual a utilização de sistemas de inteligência artificial no exercício da função jurisdicional permanece sujeita a controlo humano real, consciente e eficaz, excluindo qualquer funcionamento autónomo na tomada de decisões judiciais, na apreciação de factos ou provas e na interpretação ou aplicação do Direito[5].

A documentação técnica exigida pelo art.º 11.º do AI Act aos prestadores de sistemas de alto risco assume relevância processual para além da sua elaboração. Como se analisará *infra* 8., a sua existência condiciona o exercício efetivo do contraditório relativamente a *outputs* de inteligência artificial juntos aos autos, podendo a respetiva ausência ou insuficiência comprometer a admissibilidade da prova que neles assente.

1.3. A Carta Europeia do CEPEJ e as Diretrizes de 2025 sobre IA generativa

A Carta Ética Europeia sobre a Utilização da Inteligência Artificial nos Sistemas Judiciais, adotada pela CEPEJ em dezembro de 2018, antecipou em seis anos a arquitetura de risco do AI Act e fixou cinco princípios estruturantes: (i) respeito pelos direitos fundamentais, (ii) não discriminação, (iii) qualidade e segurança no tratamento de decisões e dados judiciais, (iv) transparência, (v) imparcialidade e equidade, e (vi) controlo pelo utilizador[6]. Este último exige que o utilizador conserve a faculdade de afastar o resultado produzido pelo sistema e decidir em sentido diverso. Em termos materiais, corresponde ao *princípio da não substituição dos juizes*, assinalado no ponto 3.º, n.º 2, das Recomendações do CSM, que veda a utilização de sistemas de inteligência artificial para substituir os juizes na decisão judicial, na apreciação de factos ou provas e na interpretação e aplicação da lei[7].

As Diretrizes da CEPEJ sobre a utilização de IA generativa nos tribunais, de 2025[8], constituem o desenvolvimento mais recente deste quadro orientador e respondem aos riscos específicos da inteligência artificial generativa, designadamente à alucinação, entendida como produção de conteúdo coerente, mas factualmente incorreto.

Estas Diretrizes consagram o *princípio da assistência estrita*: a IA generativa pode apoiar a pesquisa, a estruturação e a redação de minutas, sem substituir o juízo crítico do julgador, exigindo ainda uma declaração de transparência quanto à sua utilização. Neste âmbito, há uma correspondência direta com a previsão das “utilizações recomendadas” nas Recomendações do

CSM, que admite o recurso pelos juízes à utilização dos sistemas de IA^[9], todavia “apenas como ferramentas de apoio ou assistência”^[10].

A vinculatividade destes instrumentos no ordenamento português não se confunde com a de uma fonte de direito interno. A Carta Ética e as Diretrizes de 2025 carecem de força normativa vinculativa em sentido formal. Contudo, a sua função orientadora adquire particular relevância no contexto português, porque as recomendações do CSM (no âmbito do uso da IA na atividade jurisdicional) acolhem os mesmos princípios como referenciais, reforçando-os.

1.4. Princípios processuais constitucionalmente relevantes

1.4.1.

O *direito a um processo equitativo*, consagrado no art.º 20.º da Constituição da República Portuguesa (CRP) e no art.º 6.º da Convenção Europeia dos Direitos do Homem (CEDH), projeta sobre a utilização processual de sistemas de IA três exigências centrais.

A primeira consiste na *publicidade do processo decisório*, impondo que a intervenção destes sistemas na formação da convicção judicial ou na elaboração de peças processuais seja conhecida pelas partes e pelo tribunal de recurso (*cfr. infra* 10.3 a propósito do controlo em Segunda Instância).

A segunda corresponde à *imparcialidade*, exigindo que os dados de “treino” ou a configuração dos seus parâmetros e algoritmos não introduzam enviesamentos suscetíveis de comprometer a equidistância do julgador ou de favorecer sistematicamente uma das partes. As recomendações do CSM qualificam esse fenómeno precisamente como viés algorítmico^[11].

A terceira respeita ao *dever de fundamentação*, cuja relevância se intensifica quando a decisão beneficia da assistência de um sistema cujo funcionamento interno não é integralmente explicável.

1.4.2.

O *princípio da igualdade de armas*, corolário processual do art.º 6.º da CEDU, coloca um problema específico que apenas agora se começa a identificar: o acesso desigual a ferramentas de IA sofisticadas pode reproduzir, no plano tecnológico, a assimetria que o processo civil tradicionalmente procura corrigir através do patrocínio obrigatório e do apoio judiciário.

Uma parte representada por escritório com acesso a ferramentas avançadas de análise documental e de modelação preditiva do litígio dispõe de vantagem instrumental que a contraparte, desprovida de tal acesso, não consegue replicar por via dos mecanismos processuais tradicionais de equilíbrio.

Esta assimetria tecnológica não constitui, em si mesma, fundamento de nulidade ou irregularidade processual, mas admite-se que pode ser ponderada pelo juiz na gestão ativa do processo, em particular nos casos de uma parte não representada por mandatário judicial (*cfr. infra*, 4).

1.4.3.

A *garantia de acesso ao juiz* implica a proibição de substituição funcional da atividade jurisdicional por sistemas automatizados. As Recomendações do CSM consagram expressamente este princípio[12], que encontra fundamento adicional no art.º 22.º do RGPD[13], ao vedar, em termos gerais, a sujeição a decisões assentes exclusivamente em tratamento automatizado quando produzam efeitos jurídicos ou afetem significativamente a pessoa visada (*cfr. infra*, 7.2.).

1.5. Capacitação técnica do juiz

A questão de saber se um juiz sem competência técnica em sistemas de inteligência artificial pode julgar de forma independente quando recorre a tais sistemas não admite resposta unívoca.

A exigência de formação técnica avançada para todos os magistrados merece reserva. O juiz é, e deve permanecer, um *técnico do Direito*. A independência judicial, consagrada no art.º 203.º da Constituição, não depende de conhecimentos de engenharia informática, mas da capacidade de submeter a escrutínio jurídico os elementos que recebe, incluindo alegações das partes, relatórios periciais ou resultados produzidos por sistemas de IA.

Esta distinção não elimina a necessidade de um *nível mínimo de literacia tecnológica*, sob pena de o controlo humano previsto no art.º 14.º do AI Act assumir carácter meramente formal. Um juiz que desconheça o fenómeno da alucinação algorítmica, o risco de enviesamento associado aos dados de treino ou a natureza estatística, e não dedutiva, do raciocínio produzido por modelos de linguagem não dispõe das condições necessárias para exercer supervisão crítica sobre os respetivos resultados.

A este propósito, as Recomendações do CSM consagram o *princípio da formação e capacitação*, ao indicarem que “os juízes devem receber formação e capacitação sobre a utilização de sistemas de IA na administração da justiça” [14]. Esta formação não visa transformar magistrados em especialistas ou técnicos no uso da IA, mas garantir os conhecimentos indispensáveis ao exercício de um juízo crítico fundamentado.

O art.º 6.º-B do Estatuto dos Magistrados Judiciais consagra como *garantia de desempenho* que aos juízes sejam proporcionadas as condições de formação que lhes permitam desempenhar a sua

função com independência, *qualidade e eficiência*, a que corresponde um dever geral de atualização e formação contínua, que inclui uma dimensão tecnológica[15].

Mais complexa é a questão da *assessoria técnica* aos juízes. O seu fundamento sistemático encontra-se no art.º 601.º do CPC, que permite ao juiz requisitar técnico especializado para prestar esclarecimentos em audiência. Contudo, o uso deste mecanismo está limitado, pela previsão normativa, quando a *matéria de facto* suscite dificuldades de *natureza técnica* cuja solução dependa de conhecimentos especiais que o tribunal não possua, enquadramento que não se compagina com o recurso a este instrumento processual para o exercício de uma função de assessoria ao juiz em matéria de *IA diversa* da complexidade da *matéria de facto*.

2. Fase conciliatória: a IA como auxiliar da resolução do litígio?

A realização de tentativa de conciliação está prevista em duas fases fundamentais do processo civil: na audiência prévia (art.º 591.º, n.º 1, al. a) e 594.º) [16] e na audiência final (art.º 604.º, n.º 2). O juiz preside a esse ato e deve empenhar-se ativamente na obtenção da solução de equidade mais adequada ao litígio (art.º 594.º, n.º 3). Quando a conciliação não produz acordo total ou parcial, a ata deve registar as soluções propostas pelo juiz e os fundamentos invocados pelas partes para a subsistência do litígio (art.º 594.º, n.º 4).

2.1. Submissão de elementos documentais, periciais e outros à IA para elaboração de proposta de conciliação

Nos termos do art.º 594.º, os poderes de gestão ativa do juiz incluem a sugestão de bases de acordo, sem restringir a liberdade das partes quanto à respetiva aceitação. A utilização de sistemas de inteligência artificial para analisar documentos e elementos periciais dos autos e gerar propostas de transação suscita uma questão que ultrapassa a mera assistência técnica. Está em causa uma fase processual em que a autonomia privada assume relevância central, sem paralelo na produção de prova contenciosa.

A IA pode prestar apoio útil na identificação de aspetos não controvertidos, na modelação de cenários decisórios com base em jurisprudência análoga e na avaliação estatística das probabilidades de desfecho do litígio. Contudo, a conversão desse apoio em proposta transacional gerada por algoritmos enfrenta uma limitação estrutural: as transações judiciais raramente dependem apenas do objeto do processo delimitado pelos articulados e resultam frequentemente da consideração de elementos externos, como obrigações acessórias não controvertidas, configuração de direitos sobre outros bens, prevenção de litígios futuros, pagamentos faseados ou garantias adicionais e outros elementos que não constam do processo e, por conseguinte, inacessíveis a qualquer sistema de inteligência artificial.

Deste modo, uma potencial proposta produzida por inteligência artificial embora possa revelar plausibilidade estatística permanece inadequada à especificidade processual do litígio. A sua natureza jurídica não equivale à de uma proposta em sentido próprio, constituindo apenas informação técnica de apoio, sem eficácia ou capacidade autónoma de indução decisória.

Os limites desta utilização decorrem de três ordens de razões. Primeiro, a *autonomia das partes* impede que uma proposta produzida por inteligência artificial assuma a aparência de “*concretas soluções sugeridas pelo juiz*” (art.º 594.º, n.º 4). Tal solução pode levar o litigante a interpretá-la como antecipação do sentido da decisão, comprometendo a perceção de imparcialidade, um dos princípios estruturantes do processo justo.

Por outro lado, o *risco de condicionamento psicológico* da parte processualmente mais vulnerável (sobretudo se não beneficiar de representação forense) pode afetar a manifestação de vontade livre e esclarecida, exigida para a validade da transação.

Finalmente, o art.º 5.º, n.º 1, alínea a), do AI Act proíbe práticas de inteligência artificial que recorram a técnicas subliminares ou enganosas aptas a distorcer o comportamento decisório e a contornar a capacidade de decisão livre e informada. Esta proibição incide sobre ferramentas que apresentem uma única via de resolução do litígio sem explicitar alternativas plausíveis.

Consequentemente, a utilidade da IA nesta fase deve limitar-se a funções *instrumentais*^[17], como a identificação de elementos passíveis de mediação ou de maior proximidade para a conciliação, excluindo a formulação substantiva de propostas de transação.

2.2. Resolução de litígios *em linha* com componente de IA

As plataformas de resolução alternativa de litígios em linha, reguladas nos litígios de consumo pela Diretiva 2013/11/UE^[18], integram progressivamente sistemas de IA. Estes sistemas executam funções que variam entre a triagem inicial do litígio, mediante classificação automática da matéria e encaminhamento para o mecanismo adequado, e a formulação de propostas de acordo. Alguns modelos extraeuropeus admitem ainda decisões automatizadas vinculativas.

A admissibilidade desta última modalidade no ordenamento português suscita reservas jurídicas significativas. Uma decisão automatizada vinculativa que dirima um litígio civil sem intervenção humana na formação do juízo decisório confronta-se com a proibição do art.º 22.º do RGPD quando produz efeitos jurídicos relevantes na esfera do consumidor e com a garantia de acesso ao juiz consagrada no art.º 20.º da Constituição. A homologação judicial posterior não substitui a apreciação jurisdicional prévia inerente ao processo civil nos litígios não submetidos voluntariamente a arbitragem^[19].

Diversamente, os acordos celebrados em plataformas de resolução em linha assistidas por inteligência artificial não suscitam dificuldades dogmáticas equivalentes. Uma vez reduzidos a escrito e assinados pelas partes, ainda que resultem de proposta algorítmica, qualificam-se como documento particular nos termos gerais e submetem-se ao *regime de impugnação* [20].

Neste âmbito observa-se que, embora o art.º 362.º, do Código Civil (CC) defina *documento* “qualquer objeto *elaborado pelo homem* com o fim de reproduzir ou representar uma pessoa, coisa ou facto”, a partir do momento em que as partes *aceitem e assinem* (manuscrita ou eletronicamente) um *output* gerado por IA, esse resultado integra o conceito de documento, com a força probatória prevista no art.º 376.º, n.º 1, do CC: “faz prova plena quanto às declarações atribuídas ao seu autor, sem prejuízo da arguição e prova da falsidade do documento”. Ou seja, afigura-se que a origem algorítmica da proposta não introduz requisitos autónomos de admissibilidade face aos aplicáveis a qualquer transação extrajudicial.

O controlo jurisdicional do resultado mediado por inteligência artificial é suscetível de efetivar-se em dois momentos. Na *homologação* [21], o juiz aprecia a conformidade do acordo com a ordem pública e a capacidade das partes segundo o *regime geral* (art.º 290.º, do CPC, sem exigências adicionais decorrentes da intervenção da inteligência artificial. Em *eventual impugnação* [22]^[23], a parte pode invocar vício da vontade resultante de influência indevida exercida pelo sistema, recaindo o ónus da prova, nos termos gerais, sobre quem o invoca (art.º 342.º, do CC).

3. Transcrição automatizada de declarações e depoimentos

3.1. Transcrição por IA em audiência: enquadramento

O CPC não prevê regime específico para a transcrição automatizada de depoimentos. A matéria integra-se, por *interpretação extensiva*, no regime da gravação do art.º 155.º, que assume o registo sonoro ou vídeo [24] como meio de fixação da prova oral e não contemplam transcrições automatizadas sobre esse suporte. Embora a transcrição adquira relevância sobretudo em sede de recurso para o Tribunal da Relação, dado que o juiz e os mandatários acedem diretamente às gravações em Primeira Instância, a questão mantém particular relevância na impugnação da matéria de facto, contexto em que a fiabilidade da transcrição assume especial importância.

A transcrição recai atualmente sobre as partes, através dos respetivos mandatários e a expensas próprias, sem ferramenta oficial disponibilizada pelo sistema de tramitação processual. De acordo com o ponto 8.º, n.º 1, das Recomendações do CSM, no exercício da atividade jurisdicional, os juizes não devem utilizar sistemas de IA, a menos que lhes tenham sido fornecidos pelo sistema de tramitação processual ou pelo Conselho Superior da Magistratura (com salvaguarda de proteção de dados, designadamente sem transferência de ficheiros para servidores situados fora da União Europeia nem conservação dos conteúdos após utilização). Até à eventual disponibilização de uma ferramenta oficial de transcrição, a utilização de ferramentas comerciais de IA magistrados configura,

à luz do art.º 26.º do AI Act, situação de desconformidade regulatória por ausência de avaliação prévia da adequação ao contexto judicial.

As ferramentas comerciais atualmente existentes, desenvolvidas predominantemente para linguagem corrente (sem a vertente técnico-jurídica), revelam limitações quando processam registos orais jurídicos em português europeu, designadamente terminologia técnica, estruturas sintáticas formais e sobreposição de intervenções em interrogatório cruzado. A supervisão humana não pode, por isso, restringir-se a controlo pontual. A confiança excessiva na transcrição automática, fenómeno identificado pela doutrina como *naturalização do erro*, constitui um risco efetivo que justifica a preservação do registo áudio como meio probatório primário e insubstituível.

3.2. Valor probatório da transcrição gerada por IA

A equiparação da transcrição automatizada à ata de audiência não encontra fundamento quanto à força probatória formal. A ata, enquanto documento autêntico elaborado por funcionário de justiça no exercício das suas funções, beneficia da presunção de veracidade que o art.º 371.º do CC atribui aos factos nele documentados como praticados pela autoridade documentadora.

A transcrição produzida por sistema de IA, desprovida de autoria humana qualificada, não beneficia de presunção equivalente, constituindo apenas instrumento auxiliar de perceção da prova, sujeito a verificação e destituído de autonomia probatória relativamente ao registo de origem.

Qualquer divergência entre a transcrição e o registo áudio resolve-se a favor deste último. O suporte sonoro mantém natureza de meio probatório primário, cabendo à transcrição função meramente instrumental. Esta prevalência resulta da inexistência de fundamento legal para solução diversa e da própria natureza do erro de transcrição, suscetível de alterar significativamente o sentido de uma declaração sem deteção imediata por quem não confronte o texto com a gravação.

Sem que a transcrição assuma a natureza de documento autêntico (art.º 370.º, n.º 1, CC), a sua impugnação segue as regras gerais previstas para os documentos particulares (arts. 373.º a 377.º, CC). A parte que conteste a correspondência entre a transcrição e o registo áudio pode impugná-la nos termos gerais e requerer os meios probatórios adequados à demonstração da divergência, incluindo a audição direta da gravação pelo Tribunal de recurso.

A partir do momento em que existam ferramentas de transcrição fornecidas pelo sistema de tramitação processual, a admissibilidade da transcrição enquanto documento impugnável integra-se no regime geral dos arts. 370.º a 372.º do CC (*incidente de falsidade*) e 446.º a 450.º, *ex vi* art.º 451.º, n.º 3, todos do CPC, sem necessidade de categorização autónoma.

3.3. Mecanismo processual de impugnação de transcrições com erros materiais

O direito vigente não prevê mecanismo processual específico para reagir a *erros materiais de transcrição*.

O art.º 249.º do CC consagra o regime geral da retificação dos erros materiais (ainda que relativos a uma declaração negocial), determinando que o simples erro de cálculo ou de escrita, *revelado no próprio contexto* da declaração ou através das circunstâncias em que esta foi produzida, apenas confere ao declarante o direito à sua retificação. A norma distingue, assim, os erros materiais dos vícios da vontade ou da declaração suscetíveis de afetar a validade do ato jurídico, atribuindo-lhes um tratamento autónomo fundado na ideia de que a declaração exteriorizada não corresponde integralmente ao conteúdo efetivamente pretendido pelo declarante por mero lapso de expressão. Nestes casos, a ordem jurídica privilegia a reposição da correspondência entre a vontade real e a sua exteriorização formal, sem necessidade de recorrer aos mecanismos de invalidade do negócio jurídico.

No âmbito do processo civil, este regime constitui o fundamento dogmático da retificação de erros materiais constantes *dos atos processuais* e das decisões judiciais. A retificação destina-se exclusivamente à correção de lapsos ostensivos de escrita, cálculo, transcrição ou outras inexatidões materiais que não impliquem qualquer modificação do conteúdo decisório, da fundamentação ou da vontade juridicamente formada no ato processual. Por essa razão, o mecanismo de retificação não permite alterar o sentido da decisão nem suprir erros de julgamento, limitando-se a assegurar que o texto do ato processual reproduza com exatidão o conteúdo efetivamente pretendido. Deste modo, a retificação opera como instrumento de *correção formal e de preservação da segurança jurídica*, garantindo a fidelidade entre a vontade expressa e a respetiva formulação escrita.

Afigura-se que este regime será aplicável às situações de transcrição com uso de IA quer essa transcrição seja de *registo sonoro*, quer de *documentos de imagem com texto sem reconhecimento de caracteres*, desde que o lapso seja *ostensivo*, de mero erro de reprodução e revelado no respetivo *contexto*.

Fora desse enquadramento, a solução mais próxima encontra-se nos arts. 640.º e 662.º do CPC, que permitem impugnar a decisão sobre a matéria de facto mediante indicação dos meios probatórios que impõem solução diversa. Este mecanismo pressupõe, porém, acesso à gravação original e capacidade técnica para demonstrar a divergência entre o depoimento prestado e a respetiva transcrição, exigência particularmente gravosa para litigantes não representados ou com recursos limitados.

O erro material suscita ainda dificuldades quanto ao momento e ao modo da sua arguição. A inexistência de regime próprio para a invocação de erros de transcrição, distinto do regime aplicável à impugnação da matéria de facto, gera incerteza quanto aos respetivos limites temporais e transfere para a parte interessada o ónus de promover a correção do registo antes da produção de efeitos processuais estabilizados.

De *lege ferenda*, com a eventual disponibilização pelo CSM ou no sistema de tramitação processual, de ferramentas IA de transcrição, poderá justificar-se a criação de uma previsão autónoma de impugnação da transcrição, invocável em prazo contado da notificação da transcrição às partes e dotado de efeito suspensivo relativamente aos atos que dela dependam direta e exclusivamente. O incidente permitiria juntar a gravação original como elemento de comparação, determinar perícia técnica nos processos de maior complexidade e corrigir ou substituir a transcrição mediante decisão fundamentada. Esta solução responderia de forma mais adequada a uma matéria que permanece dispersa pelos institutos *gerais* previstos para uma realidade distinta (a declaração negocial) e que pode ser redutor para a especificidade técnica decorrente da intervenção de algoritmos avançados de IA.

4. Ferramentas de IA em audiência

4.1. Utilização de ferramentas de IA pelas partes e mandatários

O CPC *não proíbe* o uso pelas partes ou pelos mandatários de ferramentas de auxílio à normal tramitação e, por conseguinte, também não se vislumbra que possa ser impedido o uso de ferramentas de IA, inclusive em sede de audiência de julgamento.

No entanto, a inexistência de proibição específica também não legitima uma *utilização irrestrita*.

O *princípio da oralidade e da imediação* exige que o mandatário intervenha pessoalmente na produção da prova e na discussão da causa, assegurando que a perceção, a apreciação e a valoração dos meios probatórios resultem do contacto direto com os atos processuais praticados em audiência. Estes princípios não excluem, porém, a utilização de instrumentos tecnológicos de apoio à atividade forense, desde que tais instrumentos não substituam a intervenção humana nem comprometam a autenticidade, a espontaneidade e a genuinidade da produção da prova.

Neste contexto, a utilização, *em tempo real*, de sistemas de inteligência artificial baseados em modelos de linguagem de grande dimensão (Large Language Models - LLM), acessíveis através de computador utilizado pelo mandatário durante a audiência final, constitui uma modalidade de apoio técnico à condução da instância e da contra-instância que deve ser analisada à luz dos princípios do contraditório, da igualdade de armas, da lealdade processual e da boa-fé (arts. 3.º, nº 3, 4.º e 7.º, todos do CPC). Tal utilização pode ocorrer mediante a integração prévia, num ambiente controlado de IA (v.g., “Projetos”), dos articulados, dos documentos juntos aos autos, dos requerimentos probatórios, das decisões interlocutórias relevantes e dos temas da prova fixados, permitindo ao sistema *contextualizar as respostas* produzidas durante a audiência.

Nestas circunstâncias, o mandatário pode introduzir, em tempo real, os elementos emergentes dos depoimentos das partes, das declarações de parte, dos esclarecimentos prestados por peritos ou dos depoimentos testemunhais, solicitando ao sistema a identificação de aspetos relevantes para o

apuramento da factualidade controvertida. O sistema pode *sugerir* perguntas complementares destinadas a obter esclarecimentos adicionais, confirmar factos anteriormente alegados, testar a consistência interna de uma narrativa factual ou relacionar as respostas prestadas com os elementos documentais constantes dos autos e com os temas da prova objeto de apreciação.

Do mesmo modo, no âmbito da contra-instância, o sistema pode auxiliar o mandatário na deteção de *potenciais divergências* entre o depoimento prestado e anteriores declarações constantes do processo, na identificação de contradições internas ou externas, na formulação de perguntas orientadas para o teste da coerência do relato ou na sinalização de elementos suscetíveis de afetar a credibilidade, a fiabilidade ou a força probatória das declarações produzidas. Tal apoio permanece, contudo, circunscrito à formulação de sugestões analíticas ou argumentativas, competindo exclusivamente ao mandatário decidir se as acolhe, adapta ou rejeita e assumir integralmente a responsabilidade profissional pelas intervenções processuais que efetivamente realiza.

A *compatibilidade* desta utilização com os princípios estruturantes do processo depende da *preservação do controlo humano efetivo no exercício da instância*, da transparência quanto à origem das intervenções processuais quando tal se revele juridicamente relevante (arts. 7.º e 8.º, do CPC), da proteção da confidencialidade da informação processual e da observância das garantias fundamentais do processo equitativo. A IA não pode substituir a apreciação crítica do mandatário, a livre valoração da prova pelo julgador nem a formação da convicção judicial, mas pode constituir um *instrumento tecnológico de apoio* à preparação dinâmica da atividade probatória e argumentativa desenvolvida em audiência, desde que o seu uso respeite os deveres de diligência, lealdade, independência e boa-fé processual.

A confidencialidade dos *dados dos intervenientes* processados por *chatbots* jurídicos constitui questão autónoma da licitude da sua utilização. O art.º 92.º do Estatuto da Ordem dos Advogados impõe ao mandatário dever de segredo profissional sobre toda a informação obtida no exercício do mandato. A introdução de elementos processuais, ainda que imperfeitamente anonimizados, em sistemas de IA generativa cujos termos de utilização admitem o tratamento dos dados para treino do modelo cria *risco de violação desse dever*, que a utilidade da ferramenta não afasta. A diligência profissional exige a verificação prévia das condições contratuais do sistema utilizado; de outro modo, a confidencialidade dos intervenientes e dos dados do processo fica subordinada a garantias cuja existência o mandatário não confirmou.

Há ainda, no contexto dos *chatbots* jurídicos, o *risco de condicionamento algorítmico das estratégias processuais* como matéria suscetível de enquadramento na proibição de práticas manipuladoras prevista no art.º 5.º, n.º 1, alínea a), do AI Act^[25]. Esse risco intensifica-se em audiência quando o sistema é idóneo a criar condicionantes adversas ou um ambiente de constrangimento sobre um litigante (mais vulnerável ou sem representação por mandatário), num

contexto processual completo ou exigente em termos probatórios ou de aferição das respetivas consequências jurídicas.

4.2. Utilização de IA pelo juiz: assistência técnica ou função autónoma?

4.2.1. Enquadramento do mecanismo de assistência técnica

O art.º 601.º do CPC consagra um mecanismo de *apoio técnico* ao exercício da função jurisdicional, destinado a suprir limitações cognitivas do tribunal em matérias que exigem *conhecimentos especializados* estranhos ao saber jurídico comum. A norma prevê que, sempre que a *matéria de facto* suscite dificuldades de natureza técnica cuja resolução dependa de conhecimentos especiais que o julgador não detenha, o juiz pode designar uma pessoa tecnicamente habilitada para assistir à audiência final e prestar os esclarecimentos necessários à adequada compreensão dos factos controvertidos. Esta intervenção *não se confunde* com a prova pericial, nem visa substituir os meios probatórios produzidos pelas partes; destina-se, antes, a facultar ao tribunal instrumentos de *compreensão técnica* que permitam uma correta apreciação da prova e uma adequada formação da convicção sobre os factos relevantes para a decisão da causa.

A previsão legal articula-se com o *princípio da descoberta da verdade material* (art.º 411.º), e com o *dever de gestão processual* (art.º 6.º), conferindo ao tribunal poderes instrutórios complementares quando a complexidade técnica da matéria factual o justifique. O legislador admite, além da assistência técnica em audiência, a possibilidade de requisição de pareceres técnicos indispensáveis ao apuramento da verdade dos factos em qualquer fase do processo. Esta faculdade apresenta natureza instrumental e encontra fundamento na necessidade de assegurar que a decisão jurisdicional assente numa compreensão tecnicamente adequada da realidade subjacente ao litígio. O recurso a estes mecanismos exige, contudo, que a dificuldade identificada *respeite efetivamente a questões técnicas ou científicas* cuja apreciação dependa de conhecimentos especializados, não podendo servir para suprir insuficiências probatórias das partes nem para transferir para terceiros a função de julgamento, que permanece reservada ao tribunal.

Sob uma perspetiva sistemática, o art.º 601.º, n.º 1, integra o conjunto de instrumentos processuais orientados para a obtenção de uma decisão materialmente justa e tecnicamente fundada. A sua aplicação revela especial relevância em litígios que envolvam matérias de elevada complexidade científica, tecnológica, financeira, médica, contabilística ou informática, nos quais a correta perceção dos factos depende frequentemente da interpretação de elementos cuja compreensão exige competências especializadas. Nestes casos, a assistência técnica ou a requisição de pareceres constituem mecanismos destinados a reforçar a qualidade cognitiva da decisão judicial, contribuindo para uma mais rigorosa reconstrução dos factos e para uma aplicação do direito assente numa base factual adequadamente esclarecida.

4.2.2. Assistência técnica versus uso da IA na análise da prova

De qualquer modo, o regime da assistência técnica previsto no art.º 601.º do CPC pressupõe a *intervenção de técnico humano identificável*, que presta esclarecimentos sob direção processual e responde pessoalmente pelo respetivo conteúdo.

A eventual aproximação funcional dos sistemas de IA a esta figura exige uma especial cautela. Enquanto o *técnico* assume responsabilidade pelo esclarecimento prestado, o sistema de IA limita-se a *gerar resultados computacionais* desprovidos de subjetividade jurídica, diferença que condiciona a respetiva valoração processual.

Neste contexto, embora a IA possa desempenhar função auxiliar de apoio à atividade jurisdicional, *não integra autonomamente a categoria de assistência técnica*.

As Recomendações do Conselho Superior da Magistratura delimitam expressamente esse uso. Nos termos do ponto 5.º, n.º 2, os juízes devem utilizar sistemas de IA apenas como instrumentos de apoio ou assistência. O n.º 3, alínea b), admite a análise, classificação e estruturação de informações, documentos ou dados constantes do processo para efeitos de organização, compreensão ou estudo do litígio. A admissibilidade da utilização jurisdicional depende, contudo, de o sistema ter sido disponibilizado pelo sistema de tramitação processual ou pelo Conselho Superior da Magistratura, conforme determina o ponto 8.º, n.º 1.

O mesmo regime estabelece uma separação rigorosa entre *utilização jurisdicional* e *utilização para preparação ou estudo*. Fora do exercício direto da função jurisdicional, o ponto 8.º, n.º 2, permite o recurso a sistemas de IA para elaboração de resumos, traduções ou análise de fontes jurídicas, doutrinais e técnicas, desde que a informação utilizada provenha exclusivamente de fontes abertas. Mas, simultaneamente, o ponto 8.º, n.º 3, proíbe, em qualquer circunstância, o *fornecimento ou utilização de dados judiciais nesses sistemas*, impondo o n.º 4 que qualquer elemento processual utilizado se encontre previamente *anonimizado*. Estas limitações *afastam* a admissibilidade da introdução de peças processuais, prova ou outros elementos identificáveis em plataformas externas de inteligência artificial generativa, salvo se prévia e integralmente anonimizados.

O *dever de fundamentação* previsto no art.º 607.º, n.º 4, do CPC assume particular relevância quando o juiz recorra a sistemas de IA. O *princípio da transparência* (ponto 3.º, n.º 10) exige referência expressa à utilização desses sistemas, acompanhada da indicação de que a decisão foi integralmente revista pelo signatário. A exigência não possui natureza meramente formal, dado que a omissão dessa informação dificulta o controlo pelas partes da influência exercida pelo sistema na construção da fundamentação e restringe a efetividade do *contraditório*.

As Diretrizes da CEPEJ de 2025 convergem com esta orientação ao qualificarem a transparência e a ausência de carácter vinculativo como pressupostos estruturantes da utilização judicial de modelos generativos[26]. Tal solução corresponde, em substância, ao princípio da *não substituição do juiz* acolhido pelas Recomendações do Conselho Superior da Magistratura e exclui a

admissibilidade de textos decisórios produzidos por inteligência artificial sem revisão crítica integral pelo julgador.

4.2.3. A IA como instrumento de apoio à compreensão da prova tecnicamente complexa

A aproximação entre a assistência técnica prevista no art.º 601.º do CPC e a utilização de sistemas de IA revela maior pertinência quando estão em causa *meios de prova caracterizados por elevada densidade técnica*. Relatórios periciais extensos, documentação financeira ou contabilística complexa, registos clínicos, dados informáticos, elementos estatísticos ou conjuntos documentais de grande dimensão podem exigir operações preliminares de sistematização e organização que dificultam a sua apreensão imediata pelo julgador.

Neste contexto, a IA pode desempenhar uma *função instrumental* de apoio à compreensão da prova, permitindo identificar relações entre documentos, agrupar informação por temas, elaborar sínteses descritivas, destacar divergências entre versões factuais ou estruturar cronologicamente acontecimentos relevantes. Sob esta perspetiva, a tecnologia *aproxima-se funcionalmente* da assistência técnica, não porque forneça conhecimento especializado equiparável ao do técnico previsto no art.º 601.º do CPC, mas porque *facilita a inteligibilidade* de informação cuja complexidade excede a capacidade de análise imediata do decisor.

A analogia encontra, todavia, limites relevantes. O técnico intervém no processo como sujeito identificável, dotado de qualificação específica e sujeito a responsabilidade pelos esclarecimentos prestados (o art.º 601.º, n.º 2 *equipara-o* aos peritos). Em contraste, os resultados produzidos por sistemas de IA resultam de operações algorítmicas cuja formação permanece frequentemente opaca para o utilizador. Consequentemente, a informação produzida pelo sistema não pode assumir valor probatório autónomo nem substituir a apreciação crítica dos meios de prova efetivamente produzidos nos autos.

Por essa razão, a eventual utilização de ferramentas de IA para analisar ou sintetizar elementos probatórios tecnicamente complexos deve ser entendida como *mera operação preparatória* da atividade cognitiva (apreciação, valoração e decisão) da *matéria de facto* pelo julgador. A fundamentação da decisão sobre a matéria de facto continua a exigir a apreciação direta dos meios de prova relevantes, a explicitação do percurso valorativo seguido e a identificação das razões que conduziram à consideração de determinado facto como provado ou não provado, nos termos do art.º 607.º, n.º 4, do CPC.

A utilização deste tipo de instrumentos suscita igualmente *exigências acrescidas de contraditório*. Sempre que o juiz pretenda apoiar-se em análises, correlações ou sínteses produzidas por um sistema de IA para compreender ou valorar elementos probatórios, as partes *devem* poder pronunciar-se previamente sobre a metodologia utilizada, sobre os resultados obtidos e sobre a respetiva relevância para a decisão. O princípio do contraditório consagrado no art.º 3.º, n.º 3, do CPC

impede que elementos suscetíveis de influenciar o julgamento integrem o processo decisório sem possibilidade efetiva de discussão pelas partes.

Nesse âmbito, a garantia do contraditório poderá justificar a adoção de *medidas de adequação formal* ao abrigo do art.º 6.º do CPC. Tal poderá ocorrer, por exemplo, quando a análise efetuada pelo sistema origine correlações documentais, reconstruções cronológicas ou sínteses técnicas que não resultem imediatamente perceptíveis da consulta direta dos autos. Nesses casos, a gestão processual pode justificar a comunicação prévia dos resultados obtidos, a concessão de prazo para pronúncia ou, quando necessário, a realização de diligência especificamente destinada à respetiva discussão.

Acresce que a utilização de IA para tratamento de elementos probatórios tecnicamente complexos *não elimina a utilidade da assistência técnica* prevista no art.º 601.º do CPC. Pelo contrário, ambos os mecanismos podem revelar-se complementares. Enquanto a IA permite organizar e estruturar grandes volumes de informação, o técnico continua a assegurar aquilo que os sistemas algorítmicos não garantem: a *explicação especializada* do significado científico, técnico ou profissional dos dados analisados e a assunção de responsabilidade pelos esclarecimentos prestados em audiência.

A evolução tecnológica poderá justificar, no futuro, uma adaptação legislativa do regime da assistência técnica, prevendo expressamente a utilização processualmente regulada de ferramentas de IA destinadas à análise de prova tecnicamente complexa. Todavia, mesmo nesse cenário, a admissibilidade de tais instrumentos dependerá sempre da preservação dos princípios da transparência, do contraditório, da imediação e da não substituição da função jurisdicional por processos automatizados de decisão.

4.3. Pode o juiz exigir declaração de uso de inteligência artificial na elaboração das peças processuais?

4.3.1. Fundamento processual

O direito processual civil português não prevê expressamente um dever de declaração do recurso à IA na elaboração de peças processuais. Permanece, contudo, a questão de saber se o juiz pode exigir a prestação dessa informação no exercício dos poderes de gestão processual, sem norma habilitante específica. A resposta admite controvérsia, mas inclino-me afirmativamente.

O art.º 6.º do CPC atribui ao juiz o *poder-dever* de dirigir ativamente o processo e adotar os mecanismos necessários à justa composição do litígio. Este poder não se limita à condução formal da instância, abrangendo medidas instrumentais destinadas a assegurar a regularidade da instrução e a fiabilidade dos elementos submetidos à apreciação judicial. Em articulação com esse poder, os arts. 7.º e 8.º do mesmo Código impõem às partes e aos mandatários deveres de cooperação e de

boa-fé processual, exigindo uma conduta compatível com a descoberta da verdade e com a lealdade na condução do litígio.

A estes deveres acresce o *dever geral de cooperação* para a descoberta da verdade consagrado no art.º 417.º. Embora a norma tenha sido concebida sobretudo para assegurar a obtenção de meios probatórios e informações relevantes para a instrução da causa, a sua *ratio* projeta-se sobre todas as situações em que a identificação da origem, autenticidade ou credibilidade de determinado elemento processual se revele necessária ao correto exercício da função jurisdicional. Nesta perspetiva, a prestação de esclarecimentos sobre a utilização de IA não constitui um dever processual autónomo, mas uma concretização de deveres de colaboração já positivados quando tais esclarecimentos se revelem necessários para aferir a fiabilidade de conteúdos apresentados em juízo.

Consequentemente, quando existam elementos objetivos que suscitem dúvidas quanto à origem, autenticidade ou credibilidade de alegações, citações ou referências apresentadas por uma parte, a solicitação de informações adicionais traduz exercício de poderes processuais já reconhecidos pelo ordenamento jurídico. O seu fundamento não reside no controlo da opção tecnológica adotada pela parte, mas na necessidade de garantir a *veracidade* do teor de inferências, citações ou transcrições (v.g., de doutrina ou jurisprudência).

4.3.2. Autorresponsabilidade das partes e transparência processual

A questão ora em análise não reside na *licitude* do recurso a sistemas de IA para apoiar a elaboração de peças processuais. O ordenamento não proíbe essa utilização nem dela decorre, por si só, qualquer consequência processual, no entanto é dever do juiz aferir se o uso efetivado *compromete a fiabilidade* da informação apresentada ou *impede* a adequada verificação da respetiva *proveniência*.

Com efeito, a apresentação de referências jurisprudenciais inexistentes, de citações inexatas ou de elementos factuais sem correspondência com as fontes invocadas pode prejudicar o exercício do contraditório e dificultar a fiscalização do conteúdo processual pela parte contrária e pelo tribunal.

Esta conclusão decorre essencialmente do *princípio da autorresponsabilidade das partes*, inerente à estrutura do processo civil e particularmente visível nos ónus de alegação, impugnação e prova plasmados nos arts. 5.º, 552.º, 572.º do CPC e 342.º do CC. A utilização de IA não altera a imputação da responsabilidade pelo conteúdo processual nem transfere para a ferramenta qualquer dever de garantia da exatidão das informações produzidas. A parte e o respetivo mandatário conservam integralmente o *dever* de verificar a correção factual, jurídica e documental dos atos processuais que praticam.

Ou seja, a responsabilidade pela conformidade do conteúdo processual com a realidade jurídica e factual subsiste *independentemente dos instrumentos* utilizados na sua elaboração. É manifesto que o recurso a IA pode auxiliar tarefas de pesquisa, sistematização ou redação, mas não modifica o *dever de diligência* exigível nem afasta as consequências decorrentes da apresentação de informação inexata ou insuficientemente verificada.

Por essa razão, o *dever de transparência* não deve assumir a forma de uma *obrigação geral* de divulgação do recurso a qualquer ferramenta tecnológica. Isto é, a regra deve consistir em permitir e inclusive detetar-se o seu uso, como forma natural do avanço dos recursos tecnológicos, à semelhança do uso de aplicações e recursos em linha de doutrina e jurisprudência, que outrora se efetivava unicamente em formato impresso.

Todavia, quando existam *indícios objetivos* de que determinado articulado incorpora conteúdo gerado por IA suscetível de afetar a sua fiabilidade ou veracidade, o pedido de esclarecimentos encontra fundamento nos deveres previstos nos arts. 7.º, 8.º e 417.º do CPC. Nessa hipótese, a informação solicitada destina-se a aferir a autenticidade e exatidão dos elementos apresentados, bem como o cumprimento do dever de boa-fé processual que impende sobre a parte.

4.3.3. Boa-fé processual, litigância de má-fé e evolução regulatória

Nesta senda, é imperiosa a articulação entre IA e boa-fé processual, designadamente quando a utilização de IA conduza à apresentação de conteúdo falso ou que, pela sua natureza grave, não tenha sido devidamente verificado ou validado.

O art.º 542.º do CPC qualifica como litigante de má-fé quem deduz pretensão ou oposição cuja falta de fundamento não devia ignorar, altera a verdade dos factos ou faz do processo ou dos meios processuais um uso manifestamente reprovável.

A mera utilização de IA não integra qualquer destas hipóteses. Diferente é a situação em que a parte apresenta, como autênticas, referências jurisprudenciais inexistentes, excertos doutrinários fabricados ou elementos factuais sem confirmação mínima da respetiva exatidão. Nesses casos, a questão não se relaciona com a tecnologia utilizada, mas incide sobre o *incumprimento dos deveres de diligência, cooperação e boa-fé* que vinculam todos os intervenientes processuais. A IA apenas potencia riscos já contemplados pelo regime da litigância de má-fé: a introdução no processo de informação inexata, enganosa ou não verificada.

O enquadramento da questão no art.º 542.º não pressupõe a qualificação automática de qualquer erro produzido com recurso a IA como comportamento doloso ou gravemente negligente. A *relevância processual* dependerá sempre das circunstâncias concretas, designadamente da *natureza do erro*, da *possibilidade objetiva da sua deteção* e do *grau de diligência* observado pela parte ou pelo mandatário na verificação do conteúdo utilizado. Ainda assim, a crescente capacidade

destes sistemas para gerar referências fictícias ou conteúdo juridicamente plausível, mas materialmente falso, reforça a exigência de mecanismos processuais aptos a assegurar a sua *verificação*.

Neste contexto, quando o juiz solicita esclarecimentos sobre a utilização de IA perante *indícios concretos* de desconformidade ou inexatidão do conteúdo apresentado, não cria um dever autónomo de declaração, limitando-se a exercer os poderes de direção processual conferidos pelo art.º 6.º, enquanto medida instrumental destinada a preservar a integridade da instrução probatória e a verdade da informação processualmente relevante.

A experiência comparada, particularmente nos instrumentos já citados da União Europeia, apresenta uma tendência crescente para exigir a declaração da utilização de IA generativa em peças processuais. Embora esse movimento regulatório permaneça em consolidação e não disponha de equivalente vinculativo no ordenamento português, aponta para um reforço das exigências de transparência e verificabilidade associadas ao uso destas tecnologias.

Por conseguinte, de *lege ferenda*, a solução mais transparente para evitar um eventual contencioso processual, consistiria na consagração legislativa expressa de um dever de declaração, em circunstâncias específica e concretamente definidas (especialmente quando tenha sido usada IA generativa), designadamente com a identificação do sistema utilizado, da versão e, quando relevante para a aferição da fiabilidade do resultado produzido, dos respetivos *prompts* submetidos. Tal solução definiria com precisão os pressupostos, a extensão e as consequências do dever de transparência, reforçando a segurança jurídica e reduzindo as incertezas inerentes à aplicação dos deveres gerais de cooperação e boa-fé a uma realidade tecnológica em acelerado desenvolvimento.

4.4. Especificidade do uso por mandatário de *chatbot* jurídico sem validação da informação produzida

O dever de verificar as informações constantes das peças processuais constitui expressão do dever de boa-fé processual consagrado no art.º 8.º do CPC e encontra suporte deontológico adicional no art.º 100.º, n.º 1, al. *b*) do Estatuto da Ordem dos Advogados (EOA), que impõe ao mandatário o exercício da profissão com competência técnica, zelo e diligência (ainda que esse dever radique ontologicamente na relação com o *cliente*)[\[27\]](#).

A utilização de sistemas de IA generativa na preparação de articulados não altera este quadro normativo, ou seja, a responsabilidade pelo conteúdo apresentado em juízo permanece integralmente na esfera do mandatário, independentemente do grau de sofisticação ou fiabilidade da ferramenta utilizada.

Um episódio apreciado pelo Tribunal da Relação de Guimarães[\[28\]](#) ilustra a relevância prática desta exigência. A peça processual submetida continha seis acórdãos inexistentes, acompanhados

de números de processo plausíveis, datas coerentes e sumários verosímeis, integralmente produzidos por sistema de IA generativa. O tribunal qualificou a situação como absolutamente inadmissível, condenou a parte em custas e determinou a remessa do acórdão à Ordem dos Advogados para eventual apreciação disciplinar.

A relevância da decisão ultrapassa, porém, a mera deteção de jurisprudência inexistente. O acórdão aponta que o *dever de verificação* opera em níveis distintos e sucessivos, cuja diferenciação assume particular importância no contexto da utilização de sistemas generativos.

Num primeiro nível, impõe-se a *confirmação da própria existência da fonte invocada*. A referência a decisões inexistentes constitui a manifestação mais evidente do fenómeno habitualmente designado por *alucinação algorítmica*. A deteção deste vício exige a verificação elementar da existência do processo, da decisão e da respetiva identificação.

Num segundo nível, exige-se a *confirmação da correspondência* entre a fonte existente e a proposição jurídica que dela se pretende extrair. O mesmo acórdão identificou a invocação de decisões efetivamente proferidas pelo Tribunal Constitucional que, embora corretamente identificadas, incidiam sobre matérias inteiramente distintas das que lhes eram atribuídas^[29]. Nesta modalidade, a fonte existe, mas não sustenta a proposição jurídica apresentada. O risco processual deixa de residir na inexistência da decisão e passa a localizar-se na desconformidade entre o conteúdo efetivo da fonte e o conteúdo que lhe é imputado.

Num terceiro nível, impõe-se a *verificação da fidelidade das transcrições efetuadas*. Mesmo quando a decisão existe e versa matéria pertinente, subsiste a necessidade de confirmar que os excertos reproduzidos correspondem ao texto original e preservam o respetivo contexto argumentativo. A integridade da citação constitui pressuposto autónomo da sua utilização processual.

Esta distinção demonstra que o dever de verificação não se esgota na confirmação formal da existência da fonte: o cumprimento diligente desse dever exige um controlo material da informação produzida pelo sistema, mediante confronto entre a decisão efetivamente proferida, o respetivo conteúdo e a utilização argumentativa que dela se pretende fazer.

Sem prejuízo, a identificação do padrão pela Relatora do citado Acórdão, em resultado da sua experiência e atenção crítica, não permite concluir que a fiabilidade do sistema processual possa depender da capacidade individual de deteção de cada julgador. O próprio CSM reconheceu essa vulnerabilidade ao incluir, no ponto 12.º, n.º 2, al. a) das Recomendações, como *indícios de uso de IA*, “citação de acórdãos sem existência real e produzidos por alucinação do algoritmo”

Nesse âmbito, o referido ponto 12.º, n.º 1 das Recomendações impõe um *dever de vigilância do juiz*, “enquanto responsável pelos dados judiciais do processo”, para prestar especial atenção ao uso de IA, designadamente: “a) informações jurídicas obtidas por intervenientes sem representação por profissional forense; b) produção de peças processuais com indícios de uso de IA”.

Neste contexto, a eventual relevância disciplinar da conduta assume caráter acessório relativamente ao problema central, que reside no incumprimento do dever de verificação. A referência *supra* (4.3.3.) ao regime da litigância de má-fé é suficiente para reiterar que a apresentação de informação juridicamente falsa ou inexata pode adquirir relevância processual quando se verificarem os respetivos pressupostos legais. A questão decisiva, porém, situa-se a montante: a *utilização de IA não cria deveres processuais novos*, antes amplia o risco de violação de deveres preexistentes de diligência, lealdade e veracidade.

A mesma lógica explica a autonomia da responsabilidade disciplinar perante a Ordem dos Advogados. A comunicação efetuada pelo Tribunal da Relação de Guimarães enquadra-se no art.º 545.º, do CPC e articula-se com o regime disciplinar previsto nos arts. 115.º e ss. do EOA. Isto é, afigura-se que incumprimento do dever de verificação pode ter consequências em planos distintos, processual e deontológico, sem que a apreciação num deles determine necessariamente o resultado do outro.

Conclui-se, assim, que, a *natureza* dos deveres profissionais e processuais *precede* as soluções tecnológicas, quaisquer que elas sejam. Por conseguinte, o dever de verificar a existência, o conteúdo e a exatidão das fontes invocadas constitui a condição mínima de utilização diligente das ferramentas de IA no exercício do patrocínio forense.

4.5. Práticas de IA manipuladoras e a sua aplicação a *chatbots* processuais

O art.º 5.º, n.º 1, alínea a), do AI Act proíbe a colocação no mercado, a colocação em serviço ou a utilização de sistemas de inteligência artificial que empreguem técnicas subliminares, manipuladoras ou enganosas destinadas a distorcer substancialmente o comportamento de uma pessoa, contornando a sua capacidade de decisão informada e causando, ou podendo razoavelmente causar, dano significativo.

A subsunção de um *chatbot* jurídico que orienta de forma sistemática um utilizador (mandatário, parte) para determinada *estratégia processual*, em função de parâmetros definidos por um fornecedor com interesse económico no resultado, depende da configuração concreta do sistema, afastando qualificações abstratas aplicáveis a todas as ferramentas desta natureza.

A enunciada proibição não pressupõe o recurso a técnicas subliminares em sentido estrito. Pode abranger a omissão deliberada de informação relevante, designadamente quando o sistema apresenta uma única via processual como juridicamente correta, ocultando alternativas disponíveis em resultado de parâmetros de treino inacessíveis ao utilizador. Ou seja, o preceito centra-se na *distorção da capacidade decisória* e não no mecanismo utilizado para a produzir, abrangendo formas de manipulação menos ostensivas incompatíveis com uma decisão verdadeiramente informada.

Esta proibição não esgota, contudo, o quadro regulatório europeu aplicável aos *chatbots* jurídicos utilizados por partes e mandatários, impondo-se a sua articulação o Regulamento dos Serviços Digitais^[30] (art.º 25.º), transposto para a ordem jurídica nacional pela Lei n.º 12-A/2026, de 15 de abril, que no seu art.º 18.º, n.º 3, al. s) qualifica de contraordenação “a conceção, organização ou exploração das suas interfaces em linha de forma a enganar ou manipular os destinatários do seu serviço ou de forma a distorcer ou prejudicar substancialmente a capacidade dos destinatários do seu serviço de tomarem decisões livres e informadas”.

Embora este regime normativo não tenha por destinatário principal a atividade jurisdicional, a sua lógica fornece um critério complementar ao previsto no art.º 5.º do AI Act, sobretudo quando o constrangimento do cidadão não decorra do teor da resposta da IA, mas da *forma* como o sistema estruturou o processo de elaboração dessa resposta, de *engano, manipulação e distorção*.

Neste âmbito, não pode deixar de ser feita uma referência aos designados *dark patterns*, expressão utilizada para designar opções de arquitetura digital concebidas para orientar, influenciar ou condicionar o comportamento do utilizador através da configuração da interface, sem recurso a imposições formais ou comandos explícitos.

A *manipulação não resulta da falsidade da informação* transmitida, mas da forma como as escolhas são apresentadas, ordenadas ou destacadas. Entre os exemplos mais frequentes encontram-se a ocultação de alternativas mais ajustadas ou favoráveis, a apresentação visual privilegiada de determinada opção, a utilização de linguagem a induzir urgência ou conformidade, a multiplicação de obstáculos para aceder a escolhas alternativas ou a criação de percursos de navegação que conduzem o utilizador para uma solução previamente favorecida pelo operador da plataforma.

Transpondo para o domínio dos *chatbots* jurídicos, esta lógica permite identificar situações em que a influência exercida sobre o cidadão não decorre de uma falsidade jurídica da resposta fornecida, mas da forma como o sistema apresenta a resposta (a solução). Tal pode suceder quando o sistema destaca repetidamente determinada *estratégia processual*, relega opções importantes para planos secundários, exige passos adicionais para consultar soluções alternativas ou estrutura a interface de modo a induzir a perceção de que existe apenas uma via juridicamente plausível. Nestas hipóteses, o efeito potencialmente lesivo para a autonomia decisória do utilizador aproxima-se da preocupação subjacente tanto ao art.º 5.º do AI Act como ao art.º 25.º do Regulamento dos Serviços Digitais.

A *igualdade de armas entre as partes*, já analisada *supra* 1.4, projeta-se assim sobre o desenho funcional do *chatbot* jurídico. O problema deixa de residir exclusivamente na correção substantiva da informação disponibilizada e passa igualmente *pela forma* como o sistema aponta o caminho para que o utilizador tome uma decisão.

À semelhança do *supra* referido, ainda que noutra vertente (4.4.), a sanção estatuída no art.º 18.º da Lei n.º 12-A/2026, de 15 de abril *não exclui* a eventual responsabilização processual da parte que

utilizou conscientemente o sistema manipulador, nem afasta a relevância da manipulação na apreciação do consentimento livre exigido para a validade da prática de atos processuais, designadamente para a obtenção de transação no litígio (*cf. supra*, 2.1.).

5. Qualificação jurídica da prova gerada por IA

5.1. Modalidades de prova no CPC e prova com intervenção de IA

Para efeitos de qualificação da espécie probatória do *output* de sistemas de IA é necessário distinguir a IA como *instrumento* de produção da prova da IA como *objeto* do tema de prova. Esta distinção corresponde à separação entre a *utilização da ferramenta* e a *qualificação* jurídica do resultado produzido.

O regime da *prova documental* está previsto nos arts. 362.º e ss. do CC e 423.º e ss. do CPC. Afigura-se, nesta sede, que quaisquer relatórios, análises comparativas ou sínteses gerados por sistemas de IA generativa, quando reproduzidos em suporte duradouro impresso ou digital e, nesse formato, juntos aos autos, integram a noção de *documento particular*. Na prática, o documento é criado mediante a incorporação de um conteúdo suscetível de reprodução, não exigindo, em termos literais, autoria humana acompanhada de assinatura tradicional.

Diversa é a questão suscitada pela *prova pericial*, regulada nos arts. 467.º e ss. do CPC. Quando o perito utiliza sistemas de IA para tratamento estatístico, análise de grandes volumes de dados ou simulação de cenários, a responsabilidade pelo parecer mantém-se integralmente na sua esfera jurídica. O perito subscreve o relatório, responde pelo respetivo conteúdo e sujeita-se à prestação de esclarecimentos nos termos gerais (arts. 484.º a 486.º). Já a atribuição ao próprio sistema da função de fonte autónoma do juízo pericial não encontra correspondência na teleologia do que consiste o exercício da função de perito. Na verdade, o art.º 467.º pressupõe um perito identificável (arts. 467.º a 472.º), sujeito à prestação de compromisso (art.º 479.º), responsabilização pela fundamentação do relatório (art.º 484.º) e obrigação de comparência na audiência final (art.º 485.º). Um sistema de IA, desprovido de personalidade jurídica, não satisfaz nenhum destes requisitos.

Por outro lado, a prova por *inspeção* e a *verificação não judicial qualificada*, previstas nos arts. 490.º a 494.º, admitem uma forma distinta de utilização instrumental da IA. Estes sistemas podem auxiliar o tribunal ou o técnico que o coadjuva ao abrigo do art.º 601.º na análise de evidência física ou digital durante a diligência inspetiva. A solução aproxima-se da assistência técnica anteriormente analisada e assume particular relevo quando a inspeção incide sobre objetos digitais, designadamente dispositivos eletrónicos ou sistemas informáticos.

5.2. Prova gerada por inteligência artificial como categoria ontológica nova?

A qualificação da prova gerada por sistemas de IA é suscetível de oscilar entre duas posições.

Por um lado, pode apontar-se para uma *categorização autónoma*, fundada nas especiais características do *processamento* e do *output* dos sistemas de IA, a saber: (i) a *opacidade algorítmica*, que dificulta a reconstrução do percurso lógico subjacente ao *output*; (ii) a *inexistência de um autor humano identificável* nos moldes pressupostos pela prova documental; (iii) e o *processo de geração*, que distingue o output algorítmico tanto do documento, cujo conteúdo permanece fixo após a criação, como do parecer pericial, assente num método tendencialmente replicável e explicável pelo respetivo técnico.

Em sentido oposto, pode argumentar-se que ordenamento português não criou nem carece de criar uma categoria probatória autónoma para a prova produzida por inteligência artificial e que o *princípio da tipicidade probatória* exige o enquadramento de cada elemento probatório num regime jurídico existente. Nesta, o output algorítmico deve integrar as categorias disponíveis mediante adaptação interpretativa. Para este entendimento pode também sustentar-se que origem algorítmica do conteúdo não compromete, por si só, a adequação funcional dos regimes documental e pericial, dado que o problema principal reside na fidedignidade e na explicação do resultado, matérias que os mecanismos de impugnação documental e o regime pericial podem absorver com a interpretação extensiva adequada.

Face ao estado do desenvolvimento dos sistemas de IA, afigura-se ser de acompanhar esta segunda orientação, sem ignorar a especificidade e a rápida possibilidade de alteração exponencial dos seus métodos de configuração e dos respetivos critérios de criação de resultados.

Por conseguinte, a prova gerada por IA deve, em regra, qualificar-se como *prova documental*, sujeita a exigências acrescidas de controlo da autenticidade e da integridade do processo de geração. Quando o output incorporar apreciações técnicas ou especializadas, o respetivo valor probatório justifica exigências reforçadas de explicação e verificação, aproximando o seu tratamento processual do regime pericial. Tal aproximação não determina, porém, a equiparação à prova pericial, por ser incompatível com a inexistência de personalidade e subjetividade jurídicas.

Esta solução dispensa, no estado atual, a criação de uma nova categorização probatória e permite responder aos riscos específicos da produção algorítmica através da interpretação dos regimes vigentes. Ainda assim, poderá permanecer desejável uma clarificação legislativa futura, com a integração expressa da prova produzida por IA numa das modalidades probatórias tipificadas no CPC.

5.3. Admissibilidade e regime de junção da prova gerada por IA

O enquadramento da prova gerada por IA nos arts. 423.º a 425.º do CPC não suscita, quanto ao momento da apresentação ou ao regime de preclusão, dificuldades distintas das aplicáveis aos

documentos particulares. A prova deve acompanhar o articulado em que a parte alega os factos correspondentes, sob pena de aplicação do regime geral de junção extemporânea. A especificidade reside na *qualificação* do elemento apresentado, sobretudo quando a própria parte recorre à IA para o produzir.

Nesta hipótese, a distinção entre *prova de parte* e *prova por junção de pareceres* assume relevância decisiva. Quando a parte submete documentos processuais a um sistema de IA e junta aos autos a análise obtida, o respetivo *output* constitui *prova de parte*, sujeita a apreciação crítica reforçada de verificação e análise dos documentos fonte, não configurando prova por junção de pareceres, por falta de personalidade e autoria na qualidade de advogado, professor ou técnico (art.º 426.º). Quem produz o elemento probatório através de ferramenta sob o seu controlo não pode atribuir-lhe a aparência de “neutralidade” que fundamenta um parecer técnico.

O controlo judicial da admissibilidade destes *outputs* não dispõe de regime autónomo no direito português. Todavia, os poderes de gestão processual previstos no art.º 6.º permitem exigir à parte elementos mínimos sobre o processo de geração antes da produção da prova. Essa exigência não cria um requisito adicional de admissibilidade, limitando-se a concretizar os poderes de direção da instrução.

Neste contexto, os *metadados*, os registos de processamento e a “rastreadibilidade” do *output* constituem elementos essenciais para a respetiva apreciação. Embora a falta de informação sobre o sistema utilizado, a versão do modelo, os *prompts* introduzidos ou as fontes consultadas não determine, por si só, a inadmissibilidade da prova, podem constituir elementos determinantes na *valoração* que o juiz atribua a esses elementos probatórios.

5.4. Conflito entre relatórios de IA e de perito humano

A divergência entre relatórios de dados produzidos por sistemas de IA (prova documental) e pareceres de peritos humanos (prova pericial ou técnica) sobre o mesmo objeto probatório submete-se ao *princípio da livre apreciação da prova*, consagrado no art.º 607.º, n.º 5 do CPC. Nenhuma das fontes beneficia de primazia apriorística: o julgador não deve privilegiar o parecer humano apenas em razão da sua origem, nem afastar o resultado algorítmico por resultar de um sistema não humano.

Neste âmbito, a apreciação comparativa deve atender, designadamente, à metodologia utilizada, ao grau de concretização das fases da produção, à transparência dos “dados de treino” e à existência de validação técnica externa e independente. Um resultado produzido por sistema de IA que omita fontes, critérios analíticos ou fundamentos não apresenta força valorativa equivalente à de um parecer pericial fundamentado nos termos processualmente exigidos. Nessa hipótese, o défice de explicabilidade constitui fator de desvalorização probatória, mas sem determinar a exclusão automática do elemento apresentado.

O *contraditório* assume, neste contexto, função material de controlo da fidedignidade da prova. Sem acesso aos elementos essenciais de funcionamento do sistema cuja conclusão pretende impugnar, a parte não dispõe de meios adequados para contestar eficazmente o respetivo resultado. Esta questão relaciona-se diretamente com a *transparência algorítmica* enquanto projeção do princípio do contraditório previsto no art.º 3.º do CPC.

Neste quadro, poderá justificar-se a criação, designadamente mediante adaptação processual com prévia auscultação das partes (art.º 6.º), de um mecanismo ou incidente de verificação técnica dos sistemas de IA, ao abrigo do *princípio do inquisitório*, previsto no art.º 411.º, nos termos do qual “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”, eventualmente com aproveitamento extensivo do regime previsto no art.º 601.º, do CPC, ou seja, nomeando um técnico para assistir o juiz na realização de uma análise independente à metodologia e fiabilidade do sistema utilizado, designadamente à validade técnica do instrumento algorítmico, o qual prestará ao juiz os “esclarecimentos necessários” (art.º 601.º, n.º 1).

6. “Cadeia de custódia” e autenticidade da prova digital produzida ou processada por IA

6.1. Noção e valoração da “cadeia de custódia”

O termo “cadeia de custódia” é derivado do âmbito da prática policial para garantir a integridade das provas físicas e digitais de um crime, com origem anglo-saxónica e consolidada nos Estados Unidos sob a designação “*chain of custody*”.

À semelhança do direito penal em que a “cadeia de custódia” consiste no registo cronológico detalhado que fixa a posse, custódia, controlo e transferência de uma prova (como uma arma, vestígios de ADN ou um disco rígido) desde que é recolhida no local do crime até à sua apresentação em tribunal, usa-se esse termo relativo a um sistema de IA para descrever o registo cronológico e documentado de todo o ciclo de vida do sistema, com anotação da origem, alterações, responsáveis pela sua configuração, histórico das diversas versões do modelo de processamento.

A sua aplicação no processo civil resulta dos princípios gerais da prova documental, para aferição da integridade da prova digital, sobretudo quando sistemas de IA intervêm entre a captação e a junção aos autos, mediante a anotação de todo o seu percurso, visando a salvaguarda de verificação que o conteúdo apresentado coincide ou tem conexão direta com o originalmente produzido.

Os mecanismos técnicos atualmente disponíveis ultrapassam a simples assinatura eletrónica: (i) o *hash* criptográfico permite detetar qualquer alteração do ficheiro mediante comparação dos respetivos valores; a tecnologia *blockchain* assegura, através de registo distribuído e cronológico, a anterioridade e a integridade de conteúdos digitais; (iii) o carimbo temporal qualificado, regulado

pelo eIDAS 2.0, acrescenta a intervenção de prestador qualificado de serviços de confiança sujeito a supervisão regulatória.

A verificação da integridade assenta em procedimentos que são imprescindíveis para a posterior valoração da prova pelo juiz. Com a “cadeia de custódia”, é possível: (i) efetivar a correlação de datas, horários e metadados provenientes de fontes distintas; (iii) detetar manipulações mediante análise de inconsistências em imagens, áudio ou vídeo; (iii) fazer a comparação sucessiva de *hashes* para identificar regravações ou alterações posteriores. Estes procedimentos não substituem a prova pericial, mas podem constituir a sua própria base técnica. A ausência deste registo aquando da apresentação de uma prova digital pode suscitar reservas de valoração relativas à preservação da integridade do elemento probatório.

Não havendo “cadeia de custódia” de um determinado resultado produzido por sistema de IA, assim como se a mesma tiver sido quebrada, afigura-se que o juiz pode: (i) *não admitir* a sua junção ao processo, por não poder integrar o objeto da instrução (art.º 410.º) ou por não ser apto a fazer prova dos fundamentos da ação ou da ação (art.º 423.º, n.º 1 *a contrario*); (ii) *ponderar* o respetivo conteúdo ao abrigo do princípio da livre apreciação da prova (art.º 607.º, n.º 5). Sem prejuízo, se o juiz admitir a sua junção, a quebra da cadeia de custódia é suscetível de reduzir o seu valor probatório, pela diminuição da credibilidade que lhe pode ser atribuída, dependendo da gravidade ou da justificação para a falta ou deficiência da cadeia de custódia.

Em caso de adulteração ou perda de rastreabilidade de prova digital processada por inteligência artificial, o ónus de demonstrar a integridade da cadeia de custódia recai sobre a parte que invoca o meio probatório, nos termos do art.º 342.º, do CC. A impossibilidade de comprovar essa integridade não deve, por regra, prejudicar a parte contrária, alheia ao processo de produção ou de tratamento algorítmico da prova.

6.2. Impugnação de documentos e prova digital gerada por IA

A força probatória do documento particular, regulada pelo art.º 376.º, do CC assenta numa distinção que conserva pela aplicação perante prova digital produzida ou processada por sistemas de IA.

A *autoria do documento*, expressa na letra e assinatura ou nos respetivos equivalentes eletrónicos, presume-se verdadeira quando a parte contrária a reconhece ou não a impugna. Essa presunção não abrange, porém, a veracidade intrínseca das declarações nele contidas, cuja valoração permanece sujeita à livre apreciação. A intervenção de sistemas de IA não altera este regime, mas exige *impugnação tecnicamente fundamentada* quando se pretende contestar a autenticidade do documento. A simples alegação de origem algorítmica, desacompanhada de

elementos concretos que ponham em causa a autoria, integridade ou genuinidade do ficheiro, não é suficiente para afastar a presunção legal aplicável aos documentos não impugnados.

Já o *incidente de ilisão da autenticidade ou da força probatória de documento* previsto nos arts. 444.º a 450.º do CPC distingue-se da mera *impugnação de documentos*[\[31\]](#) por incidir sobre a alegação de falsificação do documento ou de alteração do respetivo conteúdo. Quem invoca a falsidade de prova digital com fundamento em manipulação algorítmica deve deduzi-la no prazo legal e requerer os meios probatórios adequados à sua demonstração (art.º 449.º, n.º 1). Em contrapartida, a parte que apresentou o documento pode requerer prova da respetiva genuinidade no prazo correspondente (art.º 448.º). Esta repartição dos ónus probatórios assume particular relevância perante *deepfakes*, contexto em que emerge também o problema do designado “*dividendo do mentiroso*”.

Finalmente, o art.º 46.º do Regulamento eIDAS consagra o princípio da *não discriminação dos documentos eletrónicos*, proibindo a recusa de eficácia jurídica fundada exclusivamente no formato digital (sem suporte físico tradicional)[\[32\]](#). Por isso, a origem algorítmica do documento ou a utilização de sistemas de inteligência artificial no respetivo processamento não justificam, por si só, qualquer exclusão ou desvalorização probatória. A apreciação processual deve centrar-se na *autenticidade, integridade e fiabilidade do documento*, e não no suporte utilizado ou no modo tecnológico da sua produção.

6.3. Deepfakes (“falsificações profundas”)

6.3.1. Noção e relevo em processo civil

O art.º 3.º, ponto 60, do AI Act define *deepfake* como conteúdo de imagem, áudio ou vídeo gerado ou manipulado por IA que reproduz pessoas, objetos, lugares, entidades ou eventos reais e pode induzir terceiros a considerá-lo autêntico ou verídico. A definição abrange, designadamente, a substituição facial em vídeo e a clonagem de voz, constituindo o referencial normativo para a qualificação processual destes conteúdos quando integrem a atividade probatória em processo civil.

Por sua vez, o denominado “*dividendo do mentiroso*” (*liar’s dividend*) traduz a erosão da credibilidade da prova digital decorrente da possibilidade generalizada de manipulação algorítmica. A parte confrontada com prova autêntica desfavorável pode contestar a sua genuinidade mediante a simples alegação de manipulação por inteligência artificial, criando dúvida suficiente para afetar a convicção do julgador sem suporte técnico minimamente sólido.

Neste âmbito, é elevado o risco da apresentação da prova digital, face à crescente dificuldade em distinguir conteúdos autênticos de conteúdos “*sintéticos*”, associada à ampla disponibilidade de ferramentas de geração artificial, conduzindo à exposição do processo a duas consequências paralelas: a possibilidade de o juiz admitir e valorar prova manipulada como *genuína* e desacreditar

ou desvalorizar prova autêntica, com fundamento na existência de *suspeitas* sobre a qualidade da prova digital apresentada.

Esta dupla vulnerabilidade suscita a questão de saber se se deve reconhecer uma *presunção de autenticidade dependente* do cumprimento de requisitos técnicos mínimos ou manter, em todos os processos, um *dever de verificação autónoma* sem qualquer efeito presuntivo. A segunda solução implicaria custos processuais dificilmente compatíveis com uma gestão eficiente da prova digital. Em contrapartida, uma presunção condicionada (*cfr. infra*, 6.5 a propósito do carimbo temporal qualificado), permite compatibilizar eficiência processual e controlo da autenticidade, sem afastar a impugnação fundamentada prevista no regime vigente.

O art.º 50.º do AI Act impõe aos prestadores e responsáveis pela implantação de sistemas de inteligência artificial generativa o dever de assegurar a deteção dos conteúdos sintéticos ou manipulados, recorrendo, entre outros mecanismos, a marcas de água digitais, metadados de proveniência compatíveis com o protocolo C2PA (Coalition for Content Provenance and Authenticity) ou formas equivalentes de divulgação da origem artificial do conteúdo.

Se essa exigência for cumprida, ficará salvaguardada a verificação da autenticidade e fidedignidade da prova digital. Porém, existem aplicações pelas quais é possível remover ou adulterar marcas de água sem degradação perceptível do conteúdo. Sem instrumentos processuais especificamente dirigidos à utilização não consentida da imagem ou da voz em *deepfakes*, tornar-se-á cada vez mais difícil efetivar uma valoração segura desse tipo de conteúdos.

6.3.2. Invocação de *deepfake*: convite ao aperfeiçoamento ou rejeição do meio de prova

A apreciação da impugnação da autenticidade de prova apresentada com fundamento em alegada manipulação por *deepfake* impõe que se faça a distinção entre *prova cuja autenticidade suscita dúvida fundada* e *prova que apresenta, prima facie, sinais de falsificação*. Embora o regime geral da impugnação do art.º 446.º do CPC não formule expressamente esta distinção, a natureza das situações é suscetível de conduzir à prolação de decisões distintas.

Assim, quando a alegação de manipulação assenta em elementos que geram *dúvida razoável*, sem indícios técnicos imediatamente perceptíveis e sem permitir a confirmação da autenticidade através da análise direta do conteúdo, afigura-se que o juiz poderá determinar, oficiosamente ou a requerimento, a realização de uma perícia (art.º 467.º, n.º 1, CPC), visando o esclarecimento da origem, integridade e autenticidade do elemento probatório[33].

Diversamente, quando a prova apresenta sinais evidentes de manipulação ou quando a própria parte reconhece intervenção algorítmica não declarada, se a prova digital não puder ser rejeitada ao abrigo do art.º 443.º, do CPC, a sua junção aos autos fica sujeita à valoração a efetivar na decisão da matéria de facto, motivando a desconsideração da prova digital, fundada na sua falsidade ou, se

houver dúvida, no princípio estatuído no art.º 414.º (“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”).

Também neste contexto importa distinguir entre *suprimento de insuficiências formais e comprometimento substancial do meio probatório*. O convite ao aperfeiçoamento destina-se ao suprimento de vícios formais ou a deficiências sanáveis e não a situações em que a autenticidade da prova se encontra comprometida. Apenas quando a parte possa juntar elementos adicionais de autenticação aptos a dissipar a dúvida suscitada (art.º 414.º), deve admitir-se uma solução de convite à apresentação complementar de prova.

6.4. Detecção pelo juiz de prova digital falsificada

Os meios processuais de detecção de prova falsa produzida mediante sistemas de IA coincidem, na sua tipologia, com os instrumentos gerais já analisados: prova pericial (art.º 467.º), assistência técnica (art.º 601.º, convocada a propósito do conflito entre conclusões de IA e perícia humana, *cfr.* supra 5.4) e da apreciação de *deepfakes* (supra 6.3.2).

A especificidade ora em análise reside numa perspetiva exclusivamente funcional, a saber, *em que circunstâncias e perante que indícios* o juiz deve suspeitar da falsidade e oficiosamente cumprir o princípio do inquisitório no exercício dos seus poderes de gestão e de direção processual.

As Recomendações do CSM fornecem o *quadro indiciário* mais concreto e atual. No ponto 12 (*dever de vigilância*) são identificados como sinais de utilização de IA a citação de acórdãos inexistentes gerados por alucinação algorítmica, a referência a legislação inaplicável em território nacional, o emprego de expressões estranhas ao português europeu e vestígios de respostas a *prompts*. Embora concebido para a “vigilância” de peças processuais, este conjunto de indícios aplica-se igualmente à apreciação da autenticidade da prova documental, porque as incongruências internas que revelam alucinação textual resultam do mesmo mecanismo que pode gerar elementos probatórios fabricados.

A distinção entre *prova produzida com auxílio de IA* e *prova falsificada mediante IA* constitui o eixo primordial desta questão.

A primeira categoria abrange, entre outros exemplos, relatórios assistidos por ferramentas de análise documental, transcrições automatizadas ou cronologias geradas a partir de elementos verídicos constantes dos autos. Tais elementos não apresentam qualquer vício pelo simples recurso instrumental à tecnologia, permanecendo sujeitos ao regime geral de admissibilidade e de livre apreciação analisado *supra*. Diversamente, a *prova falsificada* mediante IA não corresponde a prova menos fiável, mas à inexistência da realidade representada, estando em causa a sua admissibilidade e licitude.

6.5. Autenticação por carimbo (“selo”) de tempo qualificado

O Regulamento (UE) 2024/1183, que revê o quadro eIDAS, consolidou o regime da *assinatura eletrónica qualificada* e do carimbo de tempo eletrónico qualificado, atribuindo-lhes efeitos equiparáveis, respetivamente, à assinatura manuscrita e à certificação notarial da data de documento físico. O carimbo de tempo qualificado certifica, por meios criptograficamente verificáveis, que determinado conteúdo digital existia, com conteúdo idêntico, num momento temporal definido, mas à semelhança dos documentos autênticos, essa certificação não abrange a veracidade substantiva do conteúdo declarado.

Sendo certo que esta autenticação confere à prova digital a garantia de integridade desde a data da aposição do “carimbo”, não assegura que o conteúdo não incorporasse já uma manipulação algorítmica anterior. Esta ressalva é importante, sobretudo nas *deepfakes*, em que a falsificação *precede* a fixação do conteúdo em suporte estável.

Sem prejuízo, face à *autenticação* atribuída, a parte que impugne um documento no qual tenha sido aposto carimbo de tempo qualificado não pode invocar genericamente a sua suspeita de manipulação; deve apresentar elementos técnicos concretos aptos a demonstrar que a integridade certificada foi comprometida ou que a manipulação antecedeu a carimbagem (art.º 376.º, n.º 1, CC). Esta consequência decorre da elevada fiabilidade técnica do mecanismo e da dificuldade prática de produzir carimbos qualificados falsos, funcionando ainda como resposta ao problema do “dividendo do mentiroso”.

Nesta perspetiva, o carimbo de tempo qualificado desempenha função análoga à do reconhecimento notarial no domínio da prova digital (art.º 375.º, CC). Tal como o reconhecimento notarial não certifica a veracidade do conteúdo documental, limitando-se à autenticidade da assinatura e à data da sua aposição, também o carimbo qualificado não certifica a veracidade do conteúdo digital, mas garante com força probatória equiparável, a integridade e a anterioridade temporal do ficheiro desde a aposição do carimbo.

7. Vigilância algorítmica, dados pessoais e dados obtidos por IA

7.1. Prova obtida através de ferramentas de IA privadas utilizadas pelas partes

A produção de prova por iniciativa das partes, mediante o uso de ferramentas privadas ou comerciais de IA, diversas das que venham a ser integradas no sistema de tramitação processual, é suscetível de consubstanciar violação de dados pessoais. Com efeito, muitas dessas ferramentas incluem o reconhecimento facial aplicado a imagens de videovigilância para identificar pessoas em litígios de responsabilidade civil, a análise de padrões comportamentais extraídos de comunicações

eletrónicas para sustentar alegações de assédio ou incumprimento contratual, sistemas de avaliação de risco utilizados em fase pré-contenciosa e inferências de geolocalização baseadas em metadados de dispositivos móveis.

Ainda que no âmbito do dever de cooperação para a descoberta da verdade, o art.º 417.º, n.º 3, prevê a licitude da recusa na junção de documentos quando a mesma implicar a violação da integridade física ou moral das pessoas e a intromissão na vida privada ou familiar, no domicílio, na correspondência ou nas telecomunicações.

A transposição das garantias do art.º 32.º, n.º 8, da Constituição[34] para o processo civil permanece controvertida, mas a jurisprudência portuguesa tem admitido essa aproximação em matéria de gravações obtidas sem consentimento, com fundamento na unidade dos direitos fundamentais protegidos pela Constituição[35].

A utilização de IA exige uma efetiva aferição da aplicação do *princípio da concordância prática* (art.º 335.º, CC), dado que apesar do regime geral da licitude da prova em processo civil, os sistemas de reconhecimento facial ou de análise comportamental processam grandes volumes de dados pessoais e produzem inferências sobre a conduta dos visados com intensidade intrusiva superior à mera gravação de uma conversa, circunstância que deve integrar o correspondente juízo de ponderação.

O princípio da *prevenção dos enviesamentos algorítmicos*, apontado pelo Conselho Superior da Magistratura para a utilização jurisdicional de sistemas de IA[36], projeta-se igualmente na apreciação da prova produzida pelas partes. A exigência de escrutínio crítico impõe-se com especial intensidade quando a prova assenta em sistemas de avaliação de risco ou de reconhecimento facial cuja parametrização e dados de treino permanecem fora do controlo processual.

Situação diversa ocorre nos litígios relativos a veículos autónomos ou sistemas de decisão automatizada. Nesses processos, *a IA constitui o próprio objeto do litígio*. Os registos de funcionamento, os dados recolhidos pelos sensores e as decisões algorítmicas anteriores ao evento danoso assumem frequentemente valor probatório essencial, ou mesmo exclusivo. A obtenção desses elementos depende, em regra, da colaboração do fabricante ou operador do sistema, questão diretamente ligada ao direito de acesso às ferramentas de inteligência artificial da contraparte, e particularmente relevante à luz da Diretiva (UE) 2024/2853.

7.2. Conflito entre direito à prova e o direito à proteção de dados pessoais

O tratamento de dados pessoais por sistemas de IA para fins probatórios em processo civil submete-se ao Regulamento (UE) 2016/679 e à Lei n.º 58/2019, de 8 de agosto. A articulação entre o direito à prova, enquanto corolário do direito de ação consagrado no art.º 20.º da Constituição, e o direito à proteção de dados pessoais não admite prevalência abstrata de qualquer destes interesses,

exigindo ponderação casuística estruturada pelos fundamentos de licitude previstos no art.º 6.º do RGPD.

A licitude do tratamento pode assentar em diferentes fundamentos do art.º 6.º, n.º 1, do RGPD: cumprimento de obrigação jurídica, quando a obtenção da prova decorre diretamente da lei processual; exercício de funções de interesse público, no âmbito da atividade jurisdicional; ou interesses legítimos do responsável pelo tratamento, fundamento que sustenta frequentemente a produção probatória por iniciativa da parte. Nesta última hipótese, impõe-se a ponderação entre o interesse prosseguido e os direitos e liberdades fundamentais do titular dos dados.

A *anonimização* e a *pseudonimização* dos dados processuais utilizados no *treino de modelos de inteligência artificial* decorrem do princípio da minimização previsto no art.º 5.º, n.º 1, alínea c), do RGPD. As recomendações do CSM acolhem expressamente esta exigência ao determinarem que qualquer elemento processual utilizado por sistemas de IA seja previamente anonimizado^[37]. Embora dirigidas à atividade jurisdicional, estas orientações exprimem um padrão geral de cautela aplicável, por identidade funcional, à utilização de dados processuais por entidades privadas para treino ou aperfeiçoamento de sistemas de IA, sem prejuízo de estas se regerem pelo regime geral de proteção de dados e não pelas referidas recomendações.

O art.º 22.º do RGPD proíbe, em regra, decisões baseadas exclusivamente em tratamento automatizado, incluindo definição de perfis, quando produzam efeitos jurídicos ou consequências significativamente equivalentes na esfera do titular dos dados.

No contexto processual civil, esta proibição não suscita dificuldade relevante, uma vez que o *princípio da não substituição dos juízes* (cfr. *supra* 1.4), impede que uma decisão judicial resulte exclusivamente de tratamento automatizado sem intervenção humana efetiva.

O problema desloca-se para decisões pré-processuais ou extraprocessuais, designadamente sistemas de *scoring* de risco (*supra* 7.1), nos quais a automatização integral permanece tecnicamente viável e juridicamente mais sensível por faltar o conjunto de garantias institucionais inerentes ao exercício da função jurisdicional.

8. Acesso às ferramentas de IA da contraparte e direito ao contraditório

8.1. Direito de acesso ao modelo de IA, aos parâmetros de treino e aos dados utilizados

A questão de saber se o acesso da parte ao modelo de IA utilizado pela contraparte integra o princípio do contraditório, consagrado no art.º 3.º do CPC, coloca em confronto o direito de defesa e a proteção da propriedade intelectual, do sigilo profissional e dos “segredos de negócio” (da ferramenta de IA).

O *contraditório* exige que a parte disponha de oportunidade efetiva para se pronunciar sobre os fundamentos invocados contra si. Essa garantia fica comprometida quando a prova ou a pretensão assenta em sistema de IA cujo funcionamento permanece inacessível. A parte não consegue impugnar eficazmente conclusões cuja origem, metodologia ou critérios decisórios desconhece.

O fundamento principal do *direito de acesso* reside nesta limitação. A utilização de sistemas opacos transfere para a parte contrária um *ônus de impugnação* que exige, pelo menos, conhecimento suficiente da metodologia empregue, dos dados de treino relevantes e dos parâmetros que contribuíram para o resultado produzido. Todavia, este interesse não prevalece automaticamente sobre os direitos de propriedade intelectual e de segredo de negócio que protegem o desenvolvedor ou o utilizador do sistema. O art.º 5.º da Diretiva (UE) 2016/943 admite a divulgação de segredos de negócio quando necessária ao exercício do direito de ação, ao recurso efetivo e aos direitos de defesa em processo judicial, solução que favorece *mecanismos de divulgação controlada* em vez da exclusão de qualquer dos interesses em conflito.

O RGPD não prevê expressamente um “*direito à explicação*” sobre a utilização dos dados pessoais, mas este direito resulta da articulação de vários preceitos relativos às decisões individuais automatizadas e à definição de perfis (*profiling*). Assim, o art.º 15.º, n.º 1, alínea *h*), em conjugação com o art.º 22.º, consagra o direito de acesso e impõe ao responsável pelo tratamento o dever de facultar informações claras acerca da lógica subjacente às decisões automatizadas. Os arts. 13.º, n.º 2, alínea *f*), e 14.º, n.º 2, alínea *g*), reforçam este regime através da imposição de deveres de informação prévios, determinando que o responsável pelo tratamento informe o titular dos dados, antes da realização do tratamento, sobre a existência de decisões automatizadas, incluindo a definição de perfis, bem como sobre a lógica subjacente, a importância e as consequências previstas desse tratamento. Por fim, o Considerando 71, embora não possua natureza normativa autónoma, explicita que o titular dos dados deve ter o direito de «obter uma explicação da decisão adotada após essa avaliação», constituindo, por isso, um elemento hermenêutico relevante para a densificação do denominado direito à explicação no contexto das decisões automatizadas.

Estas regras devem ser conjugadas com o disposto nos arts. 13.º e 86.º do AI Act. O primeiro normativo impõe aos prestadores de sistemas de alto risco deveres de transparência que permitam interpretar adequadamente o respetivo resultado; por seu turno, o art.º 86.º reconhece à pessoa afetada por decisão baseada no resultado de sistema de alto risco o direito de obter explicações claras e significativas sobre a intervenção desse sistema no processo decisório.

A convergência destes normativos com o princípio do contraditório sustenta o reconhecimento de um direito de acesso alicerçado no exercício da defesa, cuja concretização exige mecanismos de divulgação compatíveis com a tutela dos “segredos de negócio”.

No entanto, enquanto não ocorrer uma alteração do CPC, a única forma de regular o acesso será por via do regime previsto no art.º 417.º, aferindo concretamente ao abrigo do art.º 335.º, do CC, da

legitimidade da invocação de recusa (art.º 417.º, n.º 3), sem prejuízo da dispensa de confidencialidade nas situações previstas no art.º 418.º.

8.2. Transparência algorítmica mínima como requisito legal de admissibilidade?

O nível mínimo de *explicabilidade* exigível aos sistemas de IZ utilizados em litígios cíveis suscita a distinção entre a *transparência procedimental* e a *transparência substantiva*.

A *transparência procedimental* respeita à documentação do funcionamento do sistema, incluindo *prompts*, fontes consultadas e versão do modelo.

A *transparência substantiva* refere-se à compreensão dos mecanismos internos de inferência que conduzem ao resultado. Nos modelos de grande escala, essa compreensão permanece frequentemente inacessível, mesmo para os respetivos desenvolvedores, em virtude da sua estrutura de “caixa negra”.

Nestes termos, a transparência procedimental constitui exigência mínima, tecnicamente viável e juridicamente inoponível. Já a transparência substantiva plena pode revelar-se inalcançável com os meios atualmente disponíveis. O processo civil deve acomodar essa limitação tecnológica sem a transformar em obstáculo geral à admissibilidade da prova assistida por IA, sob pena de inviabilizar a utilização processual destes sistemas sem acréscimo proporcional de fiabilidade.

A documentação técnica exigida pelo art.º 11.º do AI Act (*cf. supra*, 1.2.) relativamente aos sistemas de alto risco, fornece o suporte documental necessário à transparência procedimental. A sua articulação com o art.º 429.º do CPC suscita a questão de saber se o tribunal *pode ordenar a exibição dessa documentação para assegurar o contraditório* relativamente a prova produzida mediante sistema de inteligência artificial de alto risco.

A resposta deve ser afirmativa. O art.º 429.º não exige que o documento tenha sido elaborado para o processo; basta a sua relevância para a demonstração dos factos controvertidos e a sua detenção pela parte ou por terceiro identificável. A documentação técnica prevista no art.º 11.º do AI Act satisfaz, em princípio, ambos os pressupostos, por constituir elemento cuja produção e conservação incumbem ao prestador do sistema.

Impõe-se, por isso, um *dever específico de divulgação técnica* aplicável aos sistemas de IA utilizados na produção ou processamento da prova. Tal solução concentra a articulação entre o dever de exibição previsto no art.º 429.º do CPC e as obrigações de documentação técnica impostas pelo AI Act aos sistemas de alto risco. Um despacho proferido nestes termos (sustentado nas regras do CPC e no Regulamento Europeu) evita que a efetividade do contraditório dependa da adesão voluntária da parte apresentante, sem prejuízo da compatibilização com o “segredo de negócio”, aferida de forma concreta (caso a caso), ao abrigo do art.º 335.º, do CC.

9. Valoração da prova por sistemas de IA

9.1. Uso de IA na análise de depoimentos gravados

As ferramentas de análise de padrões de veracidade aplicadas a depoimentos, designadamente o processamento de microexpressões faciais captadas por vídeo, a deteção de *stress* vocal em registo áudio e a análise de padrões linguísticos associados à fabricação de relatos, constituem a utilização processual da IA em que o conflito entre inovação tecnológica e garantias fundamentais assume maior intensidade, por incidirem diretamente sobre a *credibilidade* de quem depõe.

A análise de microexpressões ou de *stress* vocal incide sobre matéria de elevada especialização técnica e aproxima-se, em abstrato, da faculdade prevista no art.º 601.º, do CPC (assistência técnica ao juiz), mas suscita muitas reservas (que, se existem na simples produção durante a audiência de julgamento, mais graves se tornam quando se pretenda a sua sujeição aos algoritmos da IA).

Entre as reservas mais relevantes, figura o valor constitucional da *dignidade do interveniente* (da testemunha ou parte), que se opõe à conversão do depoimento em objeto de escrutínio biométrico não consentido e potencialmente estigmatizante. Por outro lado, a proibição de prova ilícita prevista nas alíneas *a)*, *b)* e *c)*, do n.º 3, do art.º 417.º (sem prejuízo do referido *supra* 7.1.) exclui meios probatórios obtidos mediante ingerência na integridade moral da pessoa (enquadramento suscetível de abranger a análise não consentida de reações vocais). E, finalmente, o RGPD sujeita os dados biométricos ao regime reforçado do art.º 9.º, exigindo fundamento jurídico específico para o seu tratamento, requisito que a mera utilidade probatória não satisfaz.

9.2. Sistemas IA de análise documental em massa e cruzamento de dados entre espécies de prova

As ferramentas de *e-discovery* e de análise documental em massa, orientadas para o tratamento de volumes elevados de documentação eletrónica com vista à identificação de elementos relevantes para o processo, não suscitam, em termos de admissibilidade, dificuldades equiparáveis às das ferramentas de análise comportamental.

O processamento automatizado de grandes massas documentais para seleção e organização da prova assume *natureza instrumental*, essencialmente classificatória, não substituindo o juízo de relevância e de credibilidade reservado ao julgador, aproximando-se funcionalmente da *assistência organizacional* (cfr. *supra* 1.1, no quadro da tipologia de utilização jurisdicional da IA).

A utilização de IA na *identificação de contradições entre depoimentos e documentos* suscita ponderação diversa. Quando o sistema ultrapassa a organização e classificação e *formula conclusões sobre incongruências* substantivas entre meios de prova, como a sinalização de

discrepância entre uma data referida em depoimento e a constante de documento, a sua função aproxima-se da *apreciação crítica da prova*.

A qualificação dessa intervenção como auxiliar ou substitutiva da apreciação jurisdicional depende da *natureza* do respetivo objeto: (i) a deteção de contradições objetivamente verificáveis constitui auxílio instrumental legítimo, por reduzir carga analítica sem interferir na função jurisdicional; (ii) a avaliação de contradições que exige ponderação de credibilidade relativa entre fontes probatórias distintas excede a assistência técnica admissível, por incidir sobre o núcleo da função de julgar, reservado ao juiz.

O *princípio da livre apreciação da prova*, consagrado no art.º 607.º, n.º 5, do CPC, deve funcionar como *regra de valoração* e como *garantia* da centralidade da apreciação humana realizada pelo julgador, independentemente da sofisticação das ferramentas de cruzamento de dados utilizadas na instrução.

Na verdade, a livre apreciação não se confunde com a “adesão” a conclusões algorítmicas. O dever de fundamentação da decisão final (*cfr. supra*, 4.2. no contexto da fundamentação reforçada em decisões assistidas por IA) impõe a concreta *explicitação* do percurso crítico autónomo que sustenta a valoração adotada, sem prejuízo da análise, ponderação e consideração das sinalizações produzidas por sistemas IA de análise documental.

10. Explicabilidade, recurso e controlo jurisdicional

10.1. Explicabilidade como requisito de admissibilidade probatória

O nível mínimo de transparência algorítmica exigível a ferramentas de inteligência artificial em litígios cíveis, delimitado *supra* 8.2 quanto à distinção entre transparência procedimental e substantiva, projeta-se também na estrutura decisória do juiz, na medida em que a explicabilidade de um sistema de IA (futuramente integrado na aplicação de tramitação processual) pode condicionar a possibilidade de a decisão judicial cumprir o dever constitucional de fundamentação.

A natureza de “*caixa negra*” dos modelos de IA de grande escala introduz um desafio ao artigo 607.º, n.º 4, do CPC, que exige análise crítica da prova e enunciação dos fundamentos decisivos da convicção.

Quando o juiz integra na decisão um raciocínio ou conclusão sugerida por um sistema opaco de IA e não consegue *explicar autonomamente* a sua génese, a parte de fundamentação assente no output desse sistema é processualmente insubsistente. Ou seja, ainda que conste *formalmente* no texto decisório, fica subtraída ao controlo efetivo das partes e do tribunal de recurso.

É importante consignar que não se exclui a possibilidade do *uso instrumental* desses sistemas de IA. Aliás, as Recomendações do CSM permitem esse uso, contudo circunscrito a “fins de

preparação ou estudo, como a elaboração de resumos ou traduções, ou a análise de fontes jurídicas, doutrinais ou técnicas, desde que a informação utilizada para o efeito provenha única e exclusivamente de fontes abertas” (ponto 8.º, n.º 2).

No entanto, o uso de ferramentas de IA não pode *transferir* para esse sistema a “tarefa” de fundamentação; cabe apenas ao juiz a construção e explicitação motivada do percurso decisório, ainda que *informado* por output algorítmico devidamente *verificado*.

A jurisprudência portuguesa recente antecipa esta exigência. A título meramente exemplificativo, o Ac. TRG, 28-05-2026, ao apreciar a motivação da decisão de facto, assinalou que “a fundamentação da decisão de facto não pode assumir a feição de um discurso meramente compositivo, resultante da agregação de enunciados ou categorias abstratas, nem reduzir-se a um produto indiferenciado de combinação textual, *tal como sucede nos modelos de linguagem próprios da denominada inteligência artificial*, antes devendo traduzir um efetivo processo cognoscitivo individualizado, no qual se revele, de forma racional e sindicável, a formação da convicção do julgador” [38].

Este critério, embora não dirigido à utilização de sistemas de IA pelo juiz, fornece um parâmetro negativo útil: a decisão não pode assumir estrutura análoga à produção indiferenciada de modelos de linguagem, sob pena de erosão do dever de fundamentação.

Trata-se, em essência, na distinção entre *explicabilidade* e *fundamentação*. A primeira, refere-se à descrição do mecanismo interno do sistema que conduz ao resultado, exigência que pode exceder as capacidades técnicas atuais dos modelos mais complexos; já a *fundamentação*, corresponde ao dever do juiz de expor, em linguagem própria, as razões da decisão, sem delegação ou remissão para conclusões elaboradas por ferramentas de IA.

As consequências são igualmente diversas: o vício da indevida explicabilidade integra-se nos *requisitos* para a efetiva valoração da prova, enquanto o vício da falta ou deficiência da *fundamentação* configura vício próprio da decisão [art.º 662.º, n.º 2, al. c), CPC].

10.2. Recurso de apelação com fundamento na ausência de *explicação* suficiente

O regime do recurso de apelação, estruturado nos artigos 635.º e 640.º do CPC, não prevê fundamento autónomo assente na falta ou insuficiente *explicação* relativa ao uso de sistemas de IA, designadamente quando efetivados ao abrigo do ponto 5.º, n.º 3, das Recomendações do CSM [39].

O artigo 640.º impõe ao recorrente a especificação dos pontos de facto incorretamente julgados, dos meios probatórios relevantes e da decisão alternativa, numa matriz concebida para aferição *tradicional* da valoração da prova, cuja transposição para défice de explicabilidade algorítmica impõe uma extensão interpretativa.

A questão central consiste em determinar se a utilização de IA opaca na valoração da prova configura nulidade da decisão ou mero erro de julgamento.

Quando o juiz utiliza o sistema como instrumento auxiliar e constrói fundamentação própria e sindicável, a insuficiência de explicabilidade reconduz-se a *erro de julgamento*, no âmbito da apreciação da matéria de facto[\[40\]](#), passível de anulação da decisão de Primeira Instância, ao abrigo do disposto no art.º 662.º, n.º 2, al. d), do CPC[\[41\]](#).

Quando a fundamentação da sentença assenta de forma determinante em raciocínio produzido por sistema de IA não controlado nem explicitado pelo julgador, a questão desloca-se para o plano da fundamentação da decisão e para vício de maior gravidade, designadamente (se aplicável no caso concreto) nulidade da sentença, por força do art.º 615.º, n.º 1, al. b), do CPC[\[42\]](#), na medida em que a fundamentação que transfere o núcleo decisório para um sistema não explicável pelo julgador não especifica adequadamente os fundamentos de facto e de direito (ainda que a sentença apresente uma estrutura formal decisória).

10.3. Controlo efetivo em sede de recurso de decisões de Primeira Instância assistidas por IA

A possibilidade de os Tribunais da Relação exercerem controlo efetivo sobre decisões de Primeira Instância assistidas por IA[\[43\]](#), quando não têm acesso ao sistema utilizado, aos resultados concretos ou às respetivas explicações de funcionamento, desloca o problema da relação entre o juiz e o sistema de IA para a relação entre tribunal de recurso e uma decisão cuja génese algorítmica é insindicável.

Se a documentação (ou declaração[\[44\]](#)) relativa ao uso de IA não integra os autos nem a decisão, o tribunal de recurso apenas controla o que consta do processo, e a ausência de documentação impede qualquer reexame, independentemente da eventual capacidade técnica abstrata para o realizar caso a informação estivesse disponível. Esta limitação compromete o disposto no artigo 6.º, n.º 1, da CEDH, na vertente do direito a processo equitativo, enquanto exigência de controlo jurisdicional efetivo em sistemas com instância de recurso. A falta de acesso a uma componente relevante da fundamentação do tribunal recorrido introduz uma opacidade incompatível com esse parâmetro de revisão.

Afigura-se, todavia, que o dever de invocação da questão recai primariamente sobre a parte recorrente. A parte que disponha de conhecimento ou suspeita fundamentada sobre a utilização de sistema de IA sem declaração de transparência, poderá invocar em sede de recurso a violação do dever de fundamentação ou a ausência de transparência processual, com apoio nos indícios de utilização elencados nas alíneas do ponto 12.º, n.º 2, da Recomendações do CSM.

Em sede de *lege ferenda*, poderá prever-se o registo (preservação e junção aos autos) da documentação técnica dos sistemas de IA utilizados na instrução do processo e, se aplicável, os

elementos previstos no artigo 11.º do AI Act. Apenas a preservação sistemática e tempestiva desta documentação assegura efetividade ao artigo 6.º, n.º 1, da CEDH, na sua integralidade.

11. Conclusões

1. A ausência de um regime processual específico para a prova produzida ou valorada com recurso a sistemas de inteligência artificial no Código de Processo Civil exige um exercício de integração dogmática de adaptação das modalidades existentes.
2. A distinção entre a *inteligência artificial generativa* e os *sistemas de apoio à decisão* revela-se fundamental para a atividade probatória, uma vez que a primeira categoria suscita problemas de autenticidade e autoria, enquanto a segunda coloca desafios à fiabilidade metodológica das inferências realizadas.
3. O quadro regulatório europeu, designadamente o Regulamento (UE) 2024/1689, introduz obrigações de transparência, supervisão humana e documentação técnica que condicionam diretamente a admissibilidade e a valoração da prova assistida por algoritmos.
4. O princípio do controlo humano eficaz impede o funcionamento autónomo de sistemas de IA na tomada de decisões judiciais ou na apreciação de factos, exigindo que o juiz compreenda as capacidades e limitações da ferramenta utilizada para exercer uma supervisão crítica efetiva.
5. O direito a um processo equitativo impõe a transparência e a publicidade da intervenção de sistemas algorítmicos na formação da convicção judicial, garantindo que as partes e os tribunais de recurso conheçam o seu uso na decisão.
6. A assimetria tecnológica decorrente do acesso desigual a ferramentas avançadas de IA pode reproduzir desigualdades processuais, cabendo ao juiz ponderar esse desequilíbrio no exercício da gestão processual, especialmente perante partes não representadas.
7. A independência judicial exige um nível mínimo de literacia tecnológica dos juízes para evitar que a supervisão humana assuma natureza meramente formal, sem prejuízo de o juiz permanecer essencialmente um técnico do Direito apoiado por assessoria técnica especializada quando necessário.
8. A utilização de sistemas de IA na fase conciliatória deve limitar-se a funções instrumentais de apoio, excluindo a formulação de propostas de transação substantivas, de modo a evitar o risco de condicionamento psicológico ou de distorção da vontade livre dos litigantes.

9. As transcrições automatizadas de depoimentos produzidas por sistemas de IA carecem de força probatória autónoma face ao registo sonoro, constituindo apenas instrumentos auxiliares de perceção da prova, sem beneficiar da presunção de veracidade atribuída aos documentos autênticos.

10. O juiz aplica o regime da retificação de erros materiais às situações de lapsos ostensivos em transcrições geradas por algoritmos, desde que a divergência resulte do próprio contexto da declaração ou das circunstâncias da sua produção.

11. A utilização de ferramentas de IA pelas partes e pelos mandatários em audiência é admissível como apoio técnico à condução da instância, mas não pode substituir a intervenção humana nem violar os deveres de lealdade, boa-fé e segredo profissional.

12. O juiz pode recorrer a sistemas de IA para a análise, classificação e estruturação de dados constantes do processo, mas a admissibilidade dessa utilização jurisdicional depende da prévia anonimização dos elementos processuais e da revisão crítica integral pelo julgador.

13. Os poderes de gestão processual conferidos ao juiz autorizam a exigência de uma declaração de utilização de IA na elaboração de peças processuais sempre que existam indícios objetivos de que tal recurso compromete a fiabilidade ou a veracidade da informação apresentada.

14. A autorresponsabilidade das partes e o dever de diligência dos mandatários impõem a verificação material da exatidão das citações doutrinárias e jurisprudenciais geradas por sistemas algorítmicos, sob pena de responsabilidade disciplinar e condenação por litigância de má-fé.

15. A prova gerada por IA integra, em regra, a categoria da prova documental particular, embora a sua densidade técnica justifique exigências reforçadas de explicação e verificação próximas do regime da prova pericial.

16. A “cadeia de custódia” da prova digital constitui o registo cronológico indispensável para garantir a integridade do elemento probatório, sendo que a sua ausência ou quebra fundamenta a redução do valor probatório ou a inadmissibilidade da respetiva junção ao processo.

17. O “carimbo temporal qualificado”, regulado pelo eIDAS 2.0, assegura a integridade e a anterioridade de conteúdos digitais com eficácia equiparável à certificação notarial, dificultando a impugnação genérica fundada no fenómeno do dividendo do mentiroso.

18. O fenómeno das *deepfakes* exige um escrutínio jurisdicional rigoroso perante indícios de manipulação, podendo o tribunal ordenar perícias técnicas destinadas a dissipar

dúvidas fundadas sobre a autenticidade de conteúdos de imagem, áudio ou vídeo.

19. O tratamento de dados pessoais para fins probatórios através de sistemas de inteligência artificial deve observar o princípio da minimização e os fundamentos de licitude previstos no RGPD, exigindo uma ponderação entre o direito à prova e a proteção da privacidade.

20. O princípio do contraditório fundamenta o direito de acesso da parte à metodologia e aos parâmetros de funcionamento do sistema de IA utilizado pela contraparte, salvaguardando-se a proteção de “segredos de negócio” mediante mecanismos de divulgação controlada.

21. A explicabilidade algorítmica constitui um requisito de admissibilidade probatória e um pressuposto da validade da fundamentação judicial, impedindo a integração de conclusões sugeridas por sistemas opacos sem fundamentação autónoma pelo julgador.

22. A falta de explicação suficiente sobre a intervenção de um sistema de IA na formação da convicção judicial configura nulidade da sentença ou erro de julgamento suscetível de controlo e anulação pelos tribunais de recurso.

Bibliografia

BRANDÃO, Diogo de Matos. *A Prova Digital no Processo Civil*. Famalicão: Nova Causa, 2020. ISBN 9789895481286.

CABRAL, Tiago Sérgio Cabral. *Proteção de Dados e Inteligência Artificial - Sinergias Interpretativas e Potenciais Conflitos Entre o RGPD e o AI Act*. Lisboa: Quid Juris, 2026. ISBN 9789727249299.

FERREIRA, Ana Miguel Neto. *Deepfake e (des)caracterização da Intelectualidade - Implicações no Direito de Autor e Direitos Conexos e a Blockchain como Caminho para a Autenticidade*. Coimbra: Almedina, 2026. ISBN 9789894032519

MEIRELES, Ana Isa Dias. *A Prova Digital no Processo Judicial - A Blockchain e Outros Caminhos para os Tribunais*. Coimbra: Almedina, 2023. ISBN 9789724098764.

MONTEIRO, António Pedro Pinto. Garantias processuais e prova digital. *Revista da Ordem dos Advogados*, ano 83 (2024), Vol. III e IV, pp. 551-567.

PEREIRA, Fernando Silva. *Prova Eletrónica em Processo Civil*. Coimbra: Almedina, 2026. ISBN 9789894031512.

SILVA. Nuno Sousa e. *Lições de Direito Digital*. Coimbra: Almedina, 2026. ISBN 9789894032458.

SOUSA. Luís Filipe Pires. *Direito Probatório Comentado*. 4.^a ed. Coimbra: Almedina, 2026. ISBN 9789894030966.

STJ. *Tribunais e Inteligência Artificial*. Uma Odisseia no Século XXI (Colóquio STJ, 11 de maio de 2023). Lisboa:STJ, 2023. ISBN 9789895305889 [em linha]. Disponível em: <https://www.stj.pt/wp-content/uploads/2024/05/Livrodigital-Inteligencia-Artificial-2023-4.pdf>.

WENGOROVIOUS, Sofia. Tecnologia, Proteção de dados e inteligência artificial – os passos equilibrados. *A inteligência artificial e os tribunais em Portugal e no Brasil*. Londrina: Thoth Editora, 2024. ISBN 9786559598915, pp. 197-220.

Fontes institucionais e regulatórias

CEPEJ. *Assessment Tool for the Operationalisation of the European Ethical Charter* (CEPEJ(2023)16rev). 2023. Disponível em: <https://rm.coe.int/cepej-2023-16rev-operationalisation-ai-ethical-charter-en/1680b65218>.

CEPEJ. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*. Estrasburgo: Conselho da Europa, 2018. Disponível em: <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>.

CEPEJ. *Guidelines on the Use of Generative Artificial Intelligence for Courts* (CEPEJ(2025)18Final). 2025. Disponível em: <https://rm.coe.int/cepej-2025-18final-en-draft-guidelines-on-the-use-of-generative-ai-for/48802a4ad1>.

CONSELHO SUPERIOR DA MAGISTRATURA. *Recomendações para o uso de inteligência artificial na atividade jurisdicional*. [Em linha]. Disponível em: https://csm.org.pt/wp-content/uploads/2026/05/Recomendacoes_Uso_IA.pdf.

TEDH. *Background Paper for the Judicial Seminar 2025: AI and the ECHR*. Estrasburgo: TEDH, 2025. Disponível em: <https://www.echr.coe.int/documents/d/echr/seminar-background-paper-2025-eng>.

(*) O Resumo foi redigido com recurso ao www.chatgpt.com.

[1] Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. JO L, 12.07.2024. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689>.

[2] O Considerando 12 do Regulamento (UE) 2024/1689: “Uma característica principal dos sistemas de IA é a sua *capacidade de fazer inferências*. Esta capacidade de fazer inferências refere-se ao processo de obtenção dos resultados, tais como previsões, conteúdos, recomendações ou decisões, que possam influenciar ambientes físicos e virtuais, e à capacidade dos sistemas de IA para obter modelos ou algoritmos, ou ambos, a partir de entradas ou dados. As técnicas que permitem fazer inferências durante a construção de um sistema de IA incluem abordagens de aprendizagem automática que aprendem com os dados a forma de alcançarem determinados objetivos, e abordagens baseadas na lógica e no conhecimento que fazem inferências a partir do conhecimento codificado ou da representação simbólica da tarefa a resolver”. *Cfr.* igualmente a definição (17) do Glossário das Recomendações do CSM.

[3] Conselho Superior da Magistratura. Recomendações no uso de inteligência artificial na atividade jurisdicional, aprovadas pelo Plenário de 8 de abril de 2026. Disponível em: https://csm.org.pt/wp-content/uploads/2026/05/Recomendacoes_Uso_IA.pdf.

[4] São considerados sistemas de alto risco, no âmbito da “administração da justiça e processos democráticos”, de acordo com o Anexo III, n.º 8.º, al. a) os “sistemas de IA concebidos para serem utilizados por uma autoridade judiciária, ou em seu nome, para auxiliar uma autoridade judiciária na investigação e na interpretação de factos e do direito, bem como na aplicação da lei a um conjunto específico de factos, ou para serem utilizados de forma similar na resolução alternativa de litígios”.

[5] CSM. Recomendações, *cit*, ponto 3.º (Princípios), n.º 1: “*Princípio do controlo humano eficaz*. A utilização de sistemas de IA no exercício da atividade jurisdicional estará sempre sujeita ao controlo humano real, consciente e eficaz por parte dos juízes, não podendo tais sistemas operar autonomamente para a tomada de decisões judiciais, a avaliação de factos ou provas, ou a interpretação e aplicação da lei”.

[6] CEPEJ. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment. Estrasburgo: Conselho da Europa, 2018. Disponível em: <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>.

[7] CSM. Recomendações, *cit*, ponto 3.º (Princípios), n.º 2: “*Princípio da não substituição dos juízes*. No exercício da atividade jurisdicional, a utilização de sistemas de IA não poderá, em caso algum, substituir os juízes na tomada de decisões judiciais, na avaliação de factos ou provas, ou na interpretação e aplicação da lei”.

[8] CEPEJ. Guidelines on the Use of Generative Artificial Intelligence for Courts (CEPEJ(2025)18Final). 2025, adotadas na 45.ª reunião plenária de 4 e 5 de dezembro de 2025. Disponível em: <https://rm.coe.int/cepej-2025-18final-en-draft-guidelines-on-the-use-of-generative-ai-for/48802a4ad1>.

[9] CSM. Recomendações, *cit*, ponto 5.º (Utilizações recomendadas), n.ºs 3 e 4 e ponto 6.º (Minutas de decisões judiciais).

[10] CSM. Recomendações, *cit*, ponto 5.º (Utilizações recomendadas), n.º 2: “No exercício da sua atividade jurisdicional, os juízes devem utilizar os sistemas de IA apenas como ferramentas de apoio ou de assistência”.

[11] De acordo com o ponto 3.º, n.º 7 (*Princípio da prevenção dos vieses algorítmicos*), “os juízes devem tomar as precauções necessárias para identificar e evitar os enviesamentos algorítmicos decorrentes da utilização de sistemas de IA”. No respetivo glossário, define-se “viés algorítmico” (33), “o desvio sistemático nos resultados gerados por um sistema de inteligência artificial, derivado dos dados, modelos ou processos utilizados, que seja suscetível de produzir efeitos arbitrários ou discriminatórios”.

[12] CSM. Recomendações, *cit*, ponto 7.º (Usos não recomendados): “No exercício da sua atividade judicial, os juízes não devem utilizar os sistemas de IA para (...) a) A substituição, automatização ou delegação da tomada de decisões judiciais, da avaliação de factos ou provas, ou da interpretação e aplicação da lei”.

[13] Regulamento (UE) n.º 679/2016, de 27 de abril, art.º 22.º, n.º 1: “O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar”.

[14] CSM. Recomendações, *cit*, ponto 3.º, n.º 9 e ponto 13.º.

[15] Apesar de o art.º 10.º-B, do EMJ, que previa expressamente o direito/dever de formação contínua, ter sido revogado pelo art.º 8.º, da Lei n.º 67/2019, continua a apontar-se a frequência de duas ações de formação anuais (art.º 30.º, n.º 3; art.º 30.º-A, n.º 2 e art.º 30.º-B, n.º 2), a competência do CSM para “elaborar e aprovar o elenco das necessidades formativas e apresentá-lo ao Centro de Estudos Judiciários, propondo, quanto à formação contínua, áreas prioritárias e objetivos anuais” [art.º 149.º, n.º 1, al. *m*)], em particular a competência da Secção de acompanhamento e ligação aos tribunais para “acompanhar as atividades de formação inicial e de formação contínua realizadas pelo Centro de Estudos Judiciários” [art.º 152.º-C, n.º 1, al. *j*)] e “apresentar sugestões e propostas relativamente a planos de estudo e de atividades destinadas à formação inicial e contínua de juízes” [art.º 152.º-C, n.º 1, al. *k*)].

[16] Em rigor, se couber no âmbito dos poderes de disposição das partes, a tentativa de conciliação pode ter lugar, *em qualquer estado do processo*, desde que as partes conjuntamente o requeiram ou o juiz a considere oportuna, mas as partes não podem ser convocadas exclusivamente para esse fim mais que uma vez (art.º 594.º, n.º 1).

[17] Importa ainda assinalar que as Recomendações do CSM preveem no seu ponto 6.º que os juízes só *podem* “utilizar minutas geradas por sistemas de IA que lhes sejam fornecidas pelo sistema de tramitação processual previsto na lei processual ou pelo Conselho Superior da Magistratura como ferramentas de apoio ou assistência ao exercício da sua atividade jurisdicional”, daqui decorrendo que *não lhes é admissível* o recurso a LLM ou ferramentas comerciais,

[18] Transposta para o ordenamento jurídico interno pela *Lei n.º 144/2015, de 8 de setembro*.

[19] Cfr. CSM, Recomendações, cit., ponto 3.º, n.º 2, ponto 7.º, al. a) e b).

[20] Regime previsto nos arts. 444.º a 450.º, do CPC.

[21] Mesmo quando a instância é suspensa para que o litígio seja resolvido por mediação, quando o acordo é alcançado, “o mesmo é remetido a tribunal, preferencialmente por via eletrónica, seguindo os termos definidos na lei para a homologação dos acordos de mediação” (art.º 273.º, n.º 5, do CPC).

[22] Ação de declaração de nulidade ou anulabilidade ou revisão da sentença: cfr. art.º 291.º, n.ºs 1 e 2, do CPC. Cfr. Ac. TRL, 12.09.2023, proc. 7624/15.0T8LSB.L1-7: “(...) 10. Uma vez transitada em julgado a sentença homologatória da transação, a parte que pretenda reabrir a discussão no processo, de modo a que venha a conhecer-se do pedido formulado por todos ou um por um dos autores, em função dos factos carreados para os autos, tem que, fora do processo, lograr: - por um lado, a destruição dos efeitos substantivos da transação e o processual resultante do caso julgado atribuído a esses efeitos pela homologação da transação; e, - por outro lado, a destruição do efeito processual decorrente da extinção da instância no processo em que foi produzida a sentença homologatória, o que poderá fazer por via: - de ação destinada à declaração de nulidade ou anulação da mesma; ou, - de recurso de revisão, conforme arts. 291.º, n.º 2 e 696.º, al. d)”.

[23] A transação é um *contrato processual* e, por isso, só pode ser anulada se padecer de vícios da vontade ou do negócio jurídico, designadamente (i) vícios da vontade: erro, dolo ou coação (arts. 247.º a 257.º e 287.º do CC) (ii) outros fundamentos: simulação, falta de capacidade das partes ou falta de poderes do mandatário (art. 289.º e ss. do CC).

[24] Nos termos do art.º 155.º, n.º 2, “a gravação é efetuada em sistema vídeo ou sonoro, sem prejuízo de outros meios audiovisuais ou de outros processos técnicos semelhantes de que o tribunal possa dispor, devendo todos os intervenientes no ato ser informados da sua realização”, a qual *deve ser disponibilizada* (enquanto tal, *sem transcrição*) às partes, no prazo de dois dias a contar do respeito ato (art.º 155.º, n.º 3), estando sujeito ao regime de *arguição de falta ou deficiência da gravação* (art.º 155.º, n.º 3), sem qualquer referência à *transcrição*.

[25] De acordo com este normativo, são proibidas práticas de um sistema de IA que “(...) empregue técnicas subliminares que contornem a consciência de uma pessoa, ou técnicas manifestamente manipuladoras ou enganadoras, com o objetivo ou o efeito de distorcer substancialmente o comportamento de uma pessoa ou de um grupo de pessoas prejudicando de forma considerável a

sua capacidade de tomar uma decisão informada e levando, assim, a que tomem uma decisão que, caso contrário, não tomariam, de uma forma que cause ou seja razoavelmente suscetível de causar danos significativos a essa ou a outra pessoa, ou a um grupo de pessoas”.

[26] CEPEJ, Diretrizes, *cit*, ponto 2.2.6.1 (Explicabilidade e fundamentação transparente), Diretriz n.º 74: “(...) Os sistemas de IA utilizados na esfera judicial devem fornecer explicações claras e compreensíveis do percurso seguido para cada resultado ou recomendação, permitindo que os operadores judiciais os verifiquem criticamente. Para esse efeito, os sistemas devem divulgar o seu processo interno de inferência de forma transparente e auditável, assegurando uma conformidade substancial e evitando simulações de cumprimento meramente superficiais que ocultem a sua lógica real⁴⁰. Os sistemas devem ser capazes de indicar as fontes específicas de cada afirmação geradas”.

[27] Estatuto da Ordem dos Advogados (Lei n.º 145/2015, de 09-09, com as alterações introduzidas até à Lei n.º 6/2024, de 19-01), art.º 100.º, n.º 1, al. b): “Nas relações com o cliente, são ainda deveres do advogado: (...) b) Estudar com cuidado e tratar com zelo a questão de que seja incumbido, utilizando para o efeito todos os recursos da sua experiência, saber e atividade”.

[28] Cfr. *sumário* do Ac. TRG, 10.02.2026, proc. 986/23.7GAFAF.G1, Cristina Xavier da Fonseca: «(...) 4-É inadmissível – porque, ao contrário da inteligência artificial, não se espera que a inteligência humana “alucine”, sobretudo na administração da Justiça – que, no recurso, sejam identificados e transcritos excertos de seis (alegados, mas inexistentes) acórdãos de Tribunais Superiores». No texto do Acórdão pode ainda ler-se: “Nesta fase de mudanças tecnológicas galopantes, sabemos todos que a inteligência artificial reveste uma característica que habitualmente se aplica aos seres humanos: alucina, no sentido de produzir informações falsas para preencher lacunas de dados – fornece ao utilizador títulos de livros que não foram escritos, de filmes que não foram feitos ou fontes que não existem, como se fossem credíveis. Porém, é de exigir bastante mais da inteligência humana, sobretudo quando ao serviço de uma função tão decisiva no tecido social como é a de administrar – e auxiliar – a Justiça e os Tribunais. É absolutamente inadmissível – e não pode deixar de se refletir na condenação em custas do recorrente, caso haja sucumbência, bem como do envio de cópia deste acórdão à Ordem dos Advogados, face à possível violação dos deveres profissionais por parte de um dos seus membros – que, ao longo das citadas peças processuais, sejam identificados e transcritos excertos de seis (alegados) acórdãos daqueles Tribunais que não estão publicados na fonte indicada pelo recorrente nem em qualquer outra”.

[29] Ac. TRG, 10.02.2026, proc. 986/23.7GAFAF.G1, *cit.*: “(...) quanto à existência de fenómeno semelhante à aludida alucinação da inteligência artificial: apesar de os dois acórdãos do Tribunal Constitucional citados pelo recorrente, desta vez, existirem, nenhum deles versa matéria relevante para os autos ou contém sequer os excertos que o recorrente lhe atribui – um (n.º 85/2010) situa-se no âmbito do direito fiscal (!) e outro (n.º 262/12) versa direito laboral”.

[30] Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais, JO L 277 de 27.10.2022, disponível em:

[31] Ac. TRL, 15.01.2015, proc. 5643/11.4YYLSB-A.L1-6 (Maria de Deus Correia): “A mera impugnação genérica dos documentos juntos aos autos, sem que seja posta em causa a genuinidade dos mesmos, nem a sua força probatória, não impede que seja dado como provado o facto por eles documentado”; Ac. TRE, 21.04.2016, proc. 1004/14.1T8FAR.E1 (Paula Amaral): “A simples afirmação de que se impugna um documento apresentado pela parte não é impugnação da letra ou assinatura a que se refere o art.º 374.º nem arguição da falsidade do documento a que se refere o art.º 376.º, ambos do Código Civil”.

[32] Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, art.º 46.º; quanto à receção deste princípio na doutrina portuguesa, cfr. Monteiro, António Pedro Pinto. Garantias processuais e prova digital. *Revista da Ordem dos Advogados*, ano 83 (2024), Vol. III e IV, pp. 551-567.

[33] A necessidade da realização da perícia pode ser aferida pela análise de diversos elementos, designadamente se houver divergências entre a data de criação alegada e os metadados do ficheiro, descontinuidades na sequência temporal de registos áudio ou vídeo e discrepâncias entre o cabeçalho técnico de uma mensagem eletrónica e a origem que a parte lhe atribui. Estes elementos não substituem a perícia quando subsista dúvida fundada, mas permitem formular um juízo preliminar sobre a necessidade e pertinência da sua realização.

[34] No processo criminal, as garantias são reforçadas por esta previsão constitucional de nulidade relativamente a “todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações”.

[35] Ac. TRL, 15-04-2021, proc. 705/18.0T8CSC-A.L1-2 (Carlos Castelo Branco): “(...) V) A licitude da prova constitui um limite intrínseco do direito à prova, que se deduz da tutela constitucional de diversos direitos fundamentais – embora, em si mesmo, não diretamente do art.º 32.º, n.º 8, da CRP, preceito previsto em sede de garantias do processo criminal – e se concretiza naqueles pressupostos ou condições que, por natureza, devem ser observados por qualquer prova. VI) Assim, constituirá prova ilícita toda aquela que seja obtida ou produzida, mediante a violação de normas de direito material, que tutelam direitos fundamentais dos cidadãos, ou aquela cuja formação ou produção em si mesma consubstancie um ilícito. VII) A lei processual civil – muito embora estabeleça diversas regras limitativas da produção de prova ou de certos meios de prova, por exemplo, nos arts. 433.º e 607.º n.º 2 do CPC ou nos arts. 364.º, n.º 1, 393.º e 394.º do CC – é omissa quanto à questão da inadmissibilidade da prova ilícita, contrariamente ao que sucede no processo penal (cfr. art. 125º do CPP). VIII) Relativamente às provas relativamente ilícitas – em que está em questão a violação de direitos fundamentais, como o direito à intimidade da vida privada ou familiar, o direito à inviolabilidade do domicílio, ao segredo de correspondência ou das telecomunicações, o direito à imagem, à palavra, etc., e a que se referem as alíneas b) e c) do n.º 3 do art. 417.º do CPC – o

consentimento do titular do respetivo direito é relevante em termos de retirar ilicitude ao ato lesivo. IX) Face à colisão de direitos fundamentais, impõe-se proceder a uma ponderação concreta dos interesses em jogo (cfr. art.º 335.º do CC), ponderando se o meio de prova ilicitamente obtido é, não obstante, relevante, imprescindível, justificado, adequado e proporcionado para prova dos factos em presença, que, em concreto, sobrelevam sobre outros direitos fundamentais em presença, justificando a sua compressão em detrimento de tal direito à prova, ou se, tal compressão, não se mostra justificada”.

[36] CSM, Recomendações, *cit.*, ponto 3.º, n.º 7: “Princípio da prevenção dos vieses algorítmicos. Os juízes devem tomar as precauções necessárias para identificar e evitar os enviesamentos algorítmicos decorrentes da utilização de sistemas de IA”.

[37] CSM. Recomendações, *cit.*, ponto 8.º, n.ºs 3 e 4: “3. Os juízes não podem, em caso algum, fornecer ou utilizar dados judiciais nestes sistemas de IA. 4. Na utilização destes sistemas de IA o uso de qualquer elemento processual deve estar devidamente anonimizado”.

[38] Ac. TRG, 28.05.2026, proc. 172/24.9T8GMR-G.G1, Gonçalo Oliveira Magalhães.

[39] Recorda-se que de acordo com o ponto 3.º, n.º 10, das Recomendações (princípio da transparência), “o uso de sistemas de IA *deve ser assumido e declarado* nas decisões judiciais”.

[40] Ac. TRP, 23-05-2024, proc. 3278/21.2T8PRT.P2 (Isoleta de Almeida Costa): “O erro de julgamento (*error in judicando*) resulta de uma distorção da realidade factual (*error facti*) ou na aplicação do direito (*error juris*), de forma a que o decidido não corresponda à realidade ontológica ou à normativa, traduzindo-se numa apreciação da questão em desconformidade com a lei e/ou consiste num desvio à realidade factual”. No mesmo sentido, cfr. Reis, José Alberto dos. *Código de Processo Civil Anotado, Volume V*. Coimbra: Coimbra Editora, 1981, pp. 124,125: “(...) o magistrado comete erro de juízo ou de julgamento quando decide mal a questão que lhe é submetida, ou porque interpreta e aplica erradamente a lei, ou porque aprecia erradamente os factos; comete um erro de atividade quando, na elaboração da sentença, infringe as regras que disciplinam o exercício do seu poder jurisdicional. Os erros da primeira categoria são de carácter substancial: afetam o fundo ou o efeito da decisão; os segundos são de carácter formal: respeitam à forma ou ao modo como o juiz exerceu a sua atividade”.

[41] Esta previsão confere à Relação o *poder-dever* de intervir, mesmo oficiosamente, quando a fundamentação da decisão de facto não está devidamente alicerçada (que é exatamente o que está em causa quando a fundamentação é estruturalmente tributária de um sistema de IA opaco, sem que o julgador tenha explicitado o percurso *cognoscitivo próprio*). Nesse cenário, a Relação não substitui simplesmente a valoração (como no n.º 1 do artigo 662.º), nem anula por deficiência do objeto da prova [al. c)], mas determina que o tribunal de 1.ª instância fundamente devidamente a decisão de facto, com base nos depoimentos gravados e na demais prova produzida, *expurgando* assim a dependência algorítmica não declarada.

[42] Esta matéria carece de consolidação na jurisprudência. A jurisprudência dominante tem entendido que o vício de falta de fundamentação, gerador de nulidade, verifica-se apenas nos casos em que é absoluta a falta de fundamentação, assim se devendo entender a alusão legal à ausência de especificação dos fundamentos que justifiquem a decisão. Uma fundamentação meramente insuficiente não basta, em regra, para integrar a nulidade da alínea *b*), configurando antes erro de julgamento. Há, porém, jurisprudência que alarga ligeiramente este critério: o Tribunal da Relação de Coimbra (Ac. TRC, 03.11.2020, proc. 2000/17.2T8LRA.C1, Fernando Monteiro) entendeu que, para efeitos desta nulidade, “também a fundamentação de facto ou de direito insuficiente, em termos tais que não permitam ao destinatário da decisão judicial a perceção das razões de facto e de direito da decisão judicial, deve ser equiparada à falta absoluta de especificação dos fundamentos de facto e de direito e, consequentemente, determinar a nulidade da sentença”. Esta segunda corrente jurisprudencial fornece o suporte mais adequado à hipótese em análise: uma fundamentação que delega, de forma não declarada e não controlável, num sistema de IA opaco o percurso lógico conducente à decisão impede ao destinatário (incluindo as partes e o tribunal de recurso) a apreensão das razões de facto subjacentes à convicção formada, aproxima-se, por essa via, da insuficiência equiparável à falta absoluta de fundamentação. O vício não reside numa fundamentação discutível ou incorreta, mas numa fundamentação cuja componente determinante assume natureza estruturalmente inescrutável.

[43] Paralelamente, a possibilidade de o Supremo Tribunal de Justiça exercerem controlo efetivo sobre decisões *em matéria de Direito* proferidas pelos Tribunais da Relação, assistidas por sistemas de IA.

[44] CSM. Recomendações, *cit.*, ponto 3.º, n.º 10.

INTELIGÊNCIA ARTIFICIAL E ESTADO DE DIREITO: PARA UMA JUSTIÇA AUMENTADA E JURIDICAMENTE RESPONSÁVEL

Luís Paulo Reis: Professor Catedrático da Faculdade de Engenharia da Universidade do Porto & Diretor do LIACC - Laboratório de Inteligência Artificial e Ciência de Computadores da Universidade do Porto

Sumário Executivo: (1) O texto analisa os impactos da Inteligência Artificial (IA) no setor jurídico, considerando a sua utilização transversal na advocacia, na magistratura judicial, no Ministério Público, nos tribunais, na administração da justiça, nas entidades reguladoras e no acesso dos cidadãos ao direito. Parte-se da constatação de que o direito, enquanto prática intensiva em linguagem, informação, interpretação, argumentação e decisão, é particularmente exposto à transformação provocada por sistemas de IA generativa, modelos de linguagem, ferramentas de análise documental e mecanismos de apoio à decisão. (2) O artigo propõe a noção de “justiça aumentada” como modelo intermédio entre a rejeição defensiva da tecnologia e a sua adoção acrítica. A IA pode apoiar a pesquisa jurídica, a sumarização de processos, a revisão contratual, a gestão processual, a anonimização de decisões, a triagem administrativa, a comunicação com o cidadão e a organização da prova. Contudo, a tecnologia deve permanecer como instrumento auxiliar, subordinado ao juízo humano, à responsabilidade profissional, à independência judicial e às garantias fundamentais do processo. (3) No domínio da advocacia, o texto destaca o potencial da IA para aumentar a produtividade, melhorar a gestão do conhecimento, apoiar a revisão documental, acelerar a pesquisa jurídica e tornar os serviços jurídicos mais acessíveis. Todavia, sublinha riscos relevantes, como alucinações, erro jurídico, utilização de fontes inexistentes ou desatualizadas, violação do segredo profissional, exposição de dados sensíveis, dependência excessiva da tecnologia e fragilização da formação dos advogados mais jovens. A utilização responsável da IA na advocacia exige validação humana, dever de diligência reforçado e políticas claras de confidencialidade e segurança. (4) Relativamente à magistratura judicial, o artigo sustenta que a IA pode auxiliar tarefas de pesquisa, organização processual, identificação de jurisprudência relevante, sumarização de articulados, transcrição e comunicação em linguagem clara. Porém, quando se aproxima da apreciação da prova, da formação da convicção, da avaliação de risco ou da recomendação de soluções decisórias, os riscos tornam-se particularmente elevados. A decisão judicial deve permanecer um ato humano, fundamentado, sindicável e institucionalmente responsável, não podendo ser substituída por inferências estatísticas ou recomendações algorítmicas opacas. (5) No Ministério Público, na investigação criminal e no processo penal, o texto assinala oportunidades de utilização da IA na análise de grandes volumes de dados, deteção de padrões, gestão de denúncias, priorização de processos e organização de prova digital. Contudo, alerta para riscos acrescidos em matéria de presunção de inocência, liberdade individual, igualdade

de armas, vigilância, discriminação algorítmica, prova digital e contraditório. Uma pontuação de risco, uma classificação automática ou uma recomendação algorítmica não podem substituir factos, prova admissível, fundamentação individualizada e decisão humana responsável. (6) Na administração da justiça, o artigo identifica a IA como instrumento potencialmente relevante para triagem processual, gestão de prazos, distribuição de trabalho, anonimização e pseudonimização de decisões, transcrição de audiências, tradução, estatística judicial, interoperabilidade e atendimento ao cidadão. Estes usos podem produzir ganhos significativos de eficiência e acessibilidade. Ainda assim, devem respeitar o princípio do juiz natural, a transparência dos critérios de distribuição, a qualidade dos dados, a cibersegurança, a proteção de informação sensível e a possibilidade de correção humana. (7) O texto analisa também a utilização da IA no acesso dos cidadãos ao direito, destacando o seu potencial para explicar conceitos jurídicos, simplificar linguagem, orientar pedidos, apoiar o preenchimento de formulários, traduzir informação e tornar as instituições jurídicas mais compreensíveis. Esta dimensão pode reforçar a inclusão e a literacia jurídica, mas comporta riscos de falsa segurança, aconselhamento incorreto, desinformação jurídica, exposição de dados pessoais e aumento de desigualdades entre cidadãos com diferentes níveis de acesso e literacia digital. A IA deve informar e orientar, mas não substituir o aconselhamento jurídico qualificado quando estejam em causa direitos relevantes. (8) O artigo propõe uma matriz de princípios para uma IA juridicamente responsável, assente em supervisão humana efetiva, explicabilidade suficiente, rastreabilidade das fontes, confidencialidade e segredo profissional, auditabilidade, responsabilidade clara, separação entre apoio técnico e decisão jurídica, literacia em IA para juristas e certificação ou validação dos sistemas usados em contexto judicial. Estes princípios são apresentados não como obstáculos à inovação, mas como condições de legitimidade, confiança e sustentabilidade da adoção da IA no setor legal. (9) Neste enquadramento, o JurisVis é apresentado como exemplo de sistema de IA concebido para apoiar advogados e sociedades de advogados no contexto do direito português. O artigo destaca a importância de sistemas jurídicos baseados em fontes oficiais ou rastreáveis, conhecimento jurídico validável, segurança da informação, supervisão profissional e articulação entre modelos de linguagem e bases normativas controladas. O exemplo permite ilustrar a diferença entre ferramentas generalistas de IA e soluções orientadas para o contexto jurídico nacional. (10) Conclui-se que a IA pode contribuir para uma justiça mais eficiente, acessível, informada e compreensível, mas apenas se permanecer subordinada ao juízo humano, às garantias processuais, à proteção de dados, à responsabilidade profissional e aos direitos fundamentais. A alternativa não deve ser entre tecnofilia e tecnofobia, mas entre uma adoção acrítica e uma inovação juridicamente responsável. A tecnologia deve aumentar a capacidade dos juristas e das instituições, não substituir a responsabilidade humana que legitima a decisão jurídica.

Resumo: A Inteligência Artificial está a transformar de forma acelerada o setor jurídico, afetando a advocacia, a magistratura judicial, o Ministério Público, os tribunais, a administração da justiça, os reguladores e o próprio acesso dos cidadãos ao direito. A sua utilização promete ganhos relevantes de eficiência, qualidade, rapidez e acessibilidade, nomeadamente na pesquisa jurídica, análise

documental, sumarização de processos, revisão contratual, gestão processual, triagem administrativa, comunicação com o cidadão e apoio à decisão. Contudo, a integração de sistemas de IA no universo jurídico suscita riscos particularmente sensíveis: erro, enviesamento, opacidade, alucinações, violação da confidencialidade, desigualdade de acesso, dependência tecnológica, fragilização da fundamentação e diluição da responsabilidade profissional e institucional. Este artigo analisa a IA como instrumento transversal de transformação das profissões jurídicas e da justiça, defendendo que a sua adoção não deve ser orientada nem por entusiasmo tecnológico acrítico nem por rejeição defensiva. Propõe-se a noção de “justiça aumentada” como modelo intermédio: uma justiça apoiada por sistemas inteligentes, mas preservando o juízo humano, a independência judicial, o contraditório, a proteção de dados, a responsabilidade profissional e os direitos fundamentais. O artigo propõe ainda uma matriz de princípios para uma IA juridicamente responsável, assente em supervisão humana efetiva, explicabilidade suficiente, rastreabilidade das fontes, confidencialidade e segredo profissional, auditabilidade, responsabilidade clara, separação entre apoio técnico e decisão jurídica, literacia em IA para juristas e validação dos sistemas usados em contexto judicial. Neste enquadramento, apresenta-se o JurisVis como exemplo de sistema de IA concebido para apoiar advogados e sociedades de advogados no contexto do direito português, privilegiando a utilização de fontes jurídicas rastreáveis, a segurança da informação, a supervisão profissional e a articulação entre modelos de linguagem e conhecimento jurídico validável. Conclui-se que a IA pode contribuir para uma justiça mais eficiente, acessível e informada, mas apenas se permanecer subordinada ao Estado de Direito. A tecnologia deve aumentar a capacidade dos juristas e das instituições, não substituir a responsabilidade humana que legitima a decisão jurídica.

Abstract: Artificial Intelligence is rapidly transforming the legal sector, affecting lawyers, judges, public prosecutors, courts, justice administration, regulators and citizens’ access to legal information and remedies. Its use promises significant gains in efficiency, quality, speed and accessibility, particularly in legal research, document analysis, case summarisation, contract review, case management, administrative triage, citizen communication and decision support. However, the integration of AI systems into the legal domain raises particularly sensitive risks: error, bias, opacity, hallucinations, breaches of confidentiality, unequal access, technological dependency, weakened legal reasoning and the dilution of professional and institutional responsibility. This article analyses AI as a cross-cutting instrument of transformation in legal professions and justice systems, arguing that its adoption should be guided neither by uncritical technological enthusiasm nor by defensive rejection. It proposes the notion of “augmented justice” as an intermediate model: a justice system supported by intelligent systems, while preserving human judgement, judicial independence, adversarial proceedings, data protection, professional responsibility and fundamental rights. The article further proposes a matrix of principles for legally responsible AI, based on effective human oversight, sufficient explainability, traceability of sources, confidentiality and professional secrecy, auditability, clear responsibility, separation between technical support and legal decision-making, AI literacy for legal professionals and validation of systems used in judicial contexts. Within this

framework, JurisVis is presented as an example of an AI system designed to support lawyers and law firms in the context of Portuguese law, prioritising traceable legal sources, information security, professional supervision and the articulation between language models and verifiable legal knowledge. The article concludes that AI can contribute to a more efficient, accessible and informed justice system, but only if it remains subordinated to the Rule of Law. Technology should augment the capacity of legal professionals and institutions, not replace the human responsibility that legitimises legal decision-making.

Palavras-Chave: Inteligência Artificial; Inteligência Artificial no Direito; Justiça aumentada; Profissões jurídicas; Estado de Direito; Responsabilidade jurídica; Supervisão humana; Explicabilidade; JurisVis.

Keywords: Artificial Intelligence; Artificial Intelligence in Law; Augmented justice; Legal professions; Rule of Law; Legal responsibility; Human oversight; Explainability; JurisVis.

Índice: (1) Introdução; (2) Da digitalização da justiça à justiça aumentada; (3) IA para advogados e sociedades de advogados; (4) IA para magistrados judiciais; (5) IA para tribunais e administração da justiça; (6) Princípios para uma IA juridicamente responsável; (7) Jurisvis - IA responsável para advogados e sociedades de advogados; (8) Conclusão: nem tenofilia nem tecnofobia.

1. Introdução

A Inteligência Artificial [Turing, 1950], [McCarthy, 1955] deixou de ser uma realidade periférica no mundo jurídico. Aquilo que, há poucos anos, era sobretudo discutido em termos de digitalização dos tribunais, bases de dados jurisprudenciais ou automatização administrativa, passou a incluir sistemas capazes de pesquisar, resumir, classificar, comparar, redigir, prever, argumentar e interagir em linguagem natural [Magesh, 2024], [Dehghani, 2025]. Ferramentas de aprendizagem computacional [Mitchell, 1997], [Vapnik, 1995], IA generativa, modelos de linguagem de grande escala [Vaswani 2017], [Brown, 2020], sistemas de análise documental, mecanismos de apoio à decisão e agentes computacionais começam a ser usados, ou pelo menos testados, em sociedades de advogados, departamentos jurídicos, tribunais, entidades reguladoras, administrações públicas e serviços de apoio ao cidadão.

Esta transformação é particularmente relevante porque o direito é, em larga medida, uma prática intensiva em linguagem, informação, interpretação e decisão. A IA intervém precisamente nesses domínios. Pode acelerar a pesquisa jurídica, identificar padrões jurisprudenciais, sintetizar peças processuais extensas, apoiar a revisão contratual, detetar inconsistências documentais, organizar

prova, anonimizar decisões, traduzir documentos, simplificar comunicações jurídicas e melhorar o acesso dos cidadãos a informação legal compreensível. Em sistemas judiciais sobrecarregados, estes ganhos potenciais não devem ser desvalorizados.

Mas a mesma tecnologia que promete eficiência pode também introduzir novas formas de risco. Um sistema que produz uma resposta juridicamente plausível pode estar errado. Uma ferramenta treinada sobre dados históricos pode reproduzir ou amplificar desigualdades. Um modelo opaco pode dificultar o contraditório e a fiscalização. Uma decisão apoiada por IA pode tornar-se menos transparente se o decisor humano se limitar a validar uma recomendação técnica que não compreende. Uma peça processual redigida com apoio de IA pode violar deveres de diligência, confidencialidade ou lealdade se não for adequadamente verificada. E uma justiça excessivamente dependente de sistemas automáticos pode comprometer aquilo que a distingue: a fundamentação, a responsabilidade, a independência e a consideração concreta da pessoa perante o caso.

Por isso, a pergunta relevante já não é apenas saber se a IA deve ou não ser usada no direito. A pergunta decisiva é outra: em que condições institucionais, profissionais, técnicas e normativas pode a IA ser usada sem degradar o Estado de Direito? Este artigo parte da premissa de que a IA pode ser um instrumento importante de modernização da justiça, mas apenas se for integrada como tecnologia de apoio, sujeita a controlo humano, auditabilidade, transparência adequada, proteção de dados, responsabilidade profissional e respeito pelas garantias processuais.



Figura 1: Inteligência Artificial no Ecosistema Jurídico (Fonte: Elaboração própria do autor, com recurso a ferramenta de IA generativa para apoio visual)

A noção de “justiça aumentada” permite captar esse equilíbrio. A IA pode aumentar a capacidade de trabalho dos juristas, melhorar o acesso à informação, reduzir tarefas repetitivas e apoiar decisões mais informadas. Mas não deve substituir a responsabilidade do advogado, a independência do juiz, a titularidade da ação penal pelo Ministério Público, o contraditório das partes ou o direito do cidadão a uma decisão fundamentada por uma autoridade competente. A justiça pode ser tecnologicamente assistida; não deve tornar-se juridicamente desresponsabilizada.

2. Da digitalização da justiça à justiça aumentada

A relação entre tecnologia e justiça não começou com a Inteligência Artificial. Durante várias décadas, a modernização tecnológica dos sistemas jurídicos foi essencialmente entendida como um processo de digitalização: substituição do papel por suporte eletrónico, criação de bases de dados de legislação e jurisprudência, informatização dos tribunais, submissão eletrónica de peças processuais, videoconferência, assinatura digital, notificações eletrónicas e gestão processual digital. Estes instrumentos alteraram a forma de trabalho dos juristas, mas não modificaram substancialmente a natureza das tarefas jurídicas. O computador era, em regra, um meio de armazenamento, comunicação, pesquisa ou tramitação.

A Inteligência Artificial introduz uma mudança qualitativamente diferente. Não se limita a transportar para o meio digital atos que antes eram praticados em papel. Passa a intervir em tarefas cognitivas até agora reservadas ao trabalho humano: classificar documentos, identificar padrões, extrair entidades relevantes, comparar decisões, resumir autos, sugerir argumentos, prever riscos, redigir minutas, responder a perguntas em linguagem natural e, em certos contextos, recomendar opções de decisão. A passagem da digitalização para a IA corresponde, assim, à passagem de uma tecnologia de suporte para uma tecnologia de colaboração cognitiva.

Esta distinção é essencial para evitar equívocos. Digitalizar a justiça significa tornar os processos, documentos e comunicações acessíveis por meios eletrónicos. Automatizar a justiça significa executar, por meios técnicos, tarefas repetitivas ou regras previamente definidas. Utilizar IA na justiça significa permitir que sistemas computacionais aprendam com dados, reconheçam padrões, produzam inferências ou gerem conteúdos que podem influenciar a atuação de profissionais jurídicos. A diferença não é apenas técnica; é institucional. Quanto mais a tecnologia se aproxima do núcleo da interpretação, da argumentação e da decisão, maior deve ser a exigência de controlo, explicabilidade, responsabilidade e legitimidade.

Importa também distinguir entre diferentes tipos de IA. Em muitos contextos jurídicos, continuam a ser relevantes sistemas clássicos de aprendizagem automática [Mitchell, 1997], [Vapnik, 1995], usados para classificação, previsão, deteção de anomalias, priorização de casos ou análise estatística. Estes sistemas podem, por exemplo, apoiar a gestão processual, identificar processos semelhantes, sinalizar risco de incumprimento, agrupar reclamações ou detetar padrões em grandes

volumes documentais. Já a IA generativa, em especial os modelos de linguagem de grande escala, tem uma natureza diferente: produz texto, responde a perguntas, simula diálogo, estrutura argumentos e gera documentos com aparência de coerência jurídica. Esta capacidade torna-a particularmente útil, mas também particularmente perigosa, porque a fluência linguística pode ocultar erro, incerteza ou falta de fundamento.

Neste contexto, a expressão “justiça aumentada” é o proposto e pressupõe que a IA deve reforçar, e não substituir, a capacidade humana de compreender, ponderar e decidir. A tecnologia pode ampliar a memória institucional, acelerar a pesquisa, melhorar a organização da informação, reduzir tarefas repetitivas e facilitar o acesso ao direito. Mas a decisão jurídica, quando envolve direitos, deveres, responsabilidades, sanções ou liberdades, deve permanecer sujeita a uma autoridade humana identificável, responsável e capaz de fundamentar a sua decisão.

A justiça aumentada deve, por isso, ser compreendida como uma arquitetura de colaboração entre humanos e sistemas inteligentes. Nesta arquitetura, a IA pode desempenhar funções instrumentais: pesquisar jurisprudência, resumir documentos, sugerir linhas argumentativas, identificar contradições, organizar prova, auxiliar a gestão de agendas, apoiar a triagem de processos ou facilitar a comunicação com o cidadão. Mas a validação, interpretação e decisão têm de permanecer no domínio da responsabilidade profissional humana. A questão fundamental não é saber se a IA “decide”, mas perceber em que medida condiciona, orienta ou influencia quem decide.

Esta influência pode ser subtil. Um sistema que ordena resultados de pesquisa pode tornar certas decisões mais visíveis do que outras. Um algoritmo que resume um processo pode omitir elementos relevantes. Uma ferramenta que sugere jurisprudência pode reforçar uma determinada linha interpretativa. Um sistema de predição de risco pode induzir uma percepção de perigosidade ou probabilidade que afeta a decisão humana. Mesmo quando a IA não decide formalmente, pode estruturar o campo cognitivo em que a decisão é tomada. Por isso, a supervisão humana não pode ser meramente nominal. Tem de ser efetiva, informada e crítica.

A transição para a justiça aumentada exige também uma reflexão sobre a divisão do trabalho jurídico. Tarefas tradicionalmente desempenhadas por advogados estagiários, assessores, oficiais de justiça, juristas internos ou consultores podem passar a ser parcialmente executadas por sistemas automáticos. Isto pode libertar profissionais para atividades de maior valor, mas pode também reduzir oportunidades de aprendizagem, alterar modelos de negócio e criar novas assimetrias entre organizações com forte capacidade tecnológica e profissionais ou cidadãos sem acesso a ferramentas equivalentes. A IA não é apenas uma ferramenta; é também um fator de reorganização institucional e profissional.

Outro aspeto relevante é a mudança na relação entre conhecimento jurídico e fontes. O trabalho jurídico assenta na autoridade das fontes: Constituição, lei, regulamentos, jurisprudência, doutrina, contratos, prova documental e factos processualmente adquiridos. Sistemas de IA, especialmente os modelos generativos, podem produzir respostas que parecem fundadas, mas que não indicam

corretamente as fontes, confundem regimes jurídicos, inventam referências ou misturam informação válida com informação desatualizada. Num domínio em que a validade depende da fonte, da hierarquia normativa, da data, da jurisdição e do contexto, a rastreabilidade é condição essencial de confiança.



Figura 2: Da Digitalização da Justiça à Justiça Aumentada (Fonte: Elaboração própria do autor, com recurso a ferramenta de IA generativa para apoio visual)

Daqui resulta que a adoção de IA no direito não pode ser reduzida a uma decisão de eficiência. A eficiência é importante, sobretudo em sistemas judiciais com pendências elevadas e recursos limitados. Porém, no domínio da justiça, a eficiência não é um valor isolado. Deve ser compatibilizada com a legalidade, a igualdade, o contraditório, a imparcialidade, a independência, a proteção de dados, o segredo profissional e a fundamentação das decisões. Uma justiça mais rápida, mas menos transparente ou menos controlável, não é certamente uma justiça melhor.

A justiça aumentada exige, por fim, uma nova literacia profissional. Advogados, magistrados, oficiais de justiça, reguladores e demais profissionais jurídicos não precisam de se tornar engenheiros ou especialistas em IA, mas devem compreender os seus conceitos fundamentais, limitações e riscos. Devem saber que um modelo pode errar com confiança, que os dados de treino podem ser enviesados, que uma resposta plausível não é necessariamente verdadeira, que a confidencialidade pode ser comprometida por ferramentas inadequadas e que a utilização de IA não

elimina a responsabilidade de quem a utiliza. A competência jurídica do futuro incluirá, inevitavelmente, uma dimensão de competência tecnológica crítica.

Em síntese, a passagem da digitalização da justiça para a justiça aumentada representa uma transformação profunda. A tecnologia deixa de ser apenas infraestrutura e passa a participar na produção do conhecimento jurídico. Essa participação pode ser benéfica, desde que enquadrada por princípios claros, instituições vigilantes e profissionais capazes de exercer controlo crítico. A IA pode ajudar a justiça a ser mais acessível, eficiente e informada. Mas só será compatível com o Estado de Direito se permanecer subordinada à responsabilidade humana, à transparência possível, à qualidade das fontes e às garantias fundamentais.

3. IA para advogados e sociedades de advogados

A advocacia é uma das áreas jurídicas em que a Inteligência Artificial tem revelado maior potencial de transformação imediata. A razão é compreensível: grande parte do trabalho dos advogados envolve pesquisa, leitura, comparação, redação, revisão, argumentação, análise de risco e comunicação com clientes. Estas tarefas são intensivas em linguagem e informação, precisamente os domínios em que os atuais sistemas de IA, em especial os modelos de linguagem de grande escala, apresentam maior capacidade operacional.

Nas sociedades de advogados, departamentos jurídicos de empresas e práticas individuais, a IA pode apoiar a pesquisa de legislação, jurisprudência e doutrina, a elaboração de pareceres, a preparação de peças processuais, a revisão de contratos, a organização de prova documental, a sumarização de reuniões, a identificação de cláusulas problemáticas, a deteção de inconsistências, a produção de minutas entre muitas outras tarefas. Pode ainda ajudar na gestão do conhecimento interno, permitindo recuperar precedentes, modelos, argumentos e experiências anteriores de forma mais rápida e estruturada.

A utilização de IA na advocacia deve, todavia, ser distinguida em função do grau de proximidade ao núcleo do aconselhamento jurídico. Há tarefas de baixo risco, como organizar documentos, converter linguagem técnica em linguagem mais acessível, gerar listas de verificação ou produzir primeiros rascunhos internos. Há tarefas de risco intermédio, como resumir contratos, comparar versões de documentos ou identificar jurisprudência relevante. E há tarefas de risco elevado, como formular estratégias processuais, avaliar probabilidades de sucesso, aconselhar clientes em matérias sensíveis ou redigir peças que serão submetidas a tribunal. Quanto mais a ferramenta se aproxima do aconselhamento jurídico substantivo, maior deve ser o dever de verificação humana.

A promessa de produtividade é evidente. Um advogado pode analisar em minutos um conjunto documental que antes exigiria horas de leitura preliminar. Uma equipa de contencioso pode obter rapidamente um resumo dos principais argumentos de várias peças processuais. Um departamento de corporate pode comparar múltiplas versões contratuais e identificar alterações relevantes. Um

advogado individual pode beneficiar de ferramentas que antes apenas estavam ao alcance de grandes estruturas. Neste sentido, a IA pode democratizar capacidades técnicas e reduzir barreiras de acesso a serviços jurídicos mais sofisticados.

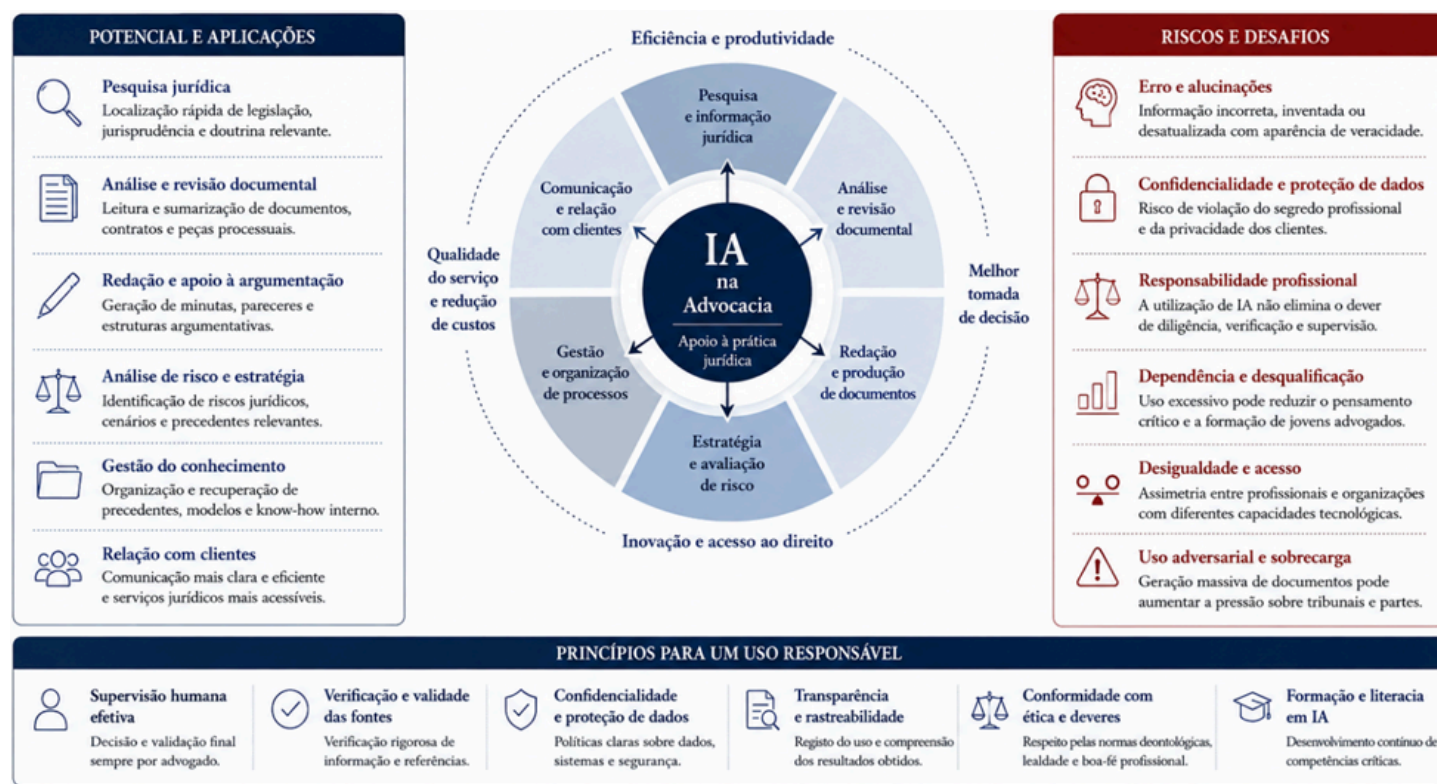


Figura 3: IA para Advogados e Sociedades de Advogados (Fonte: Elaboração própria do autor, com recurso a ferramenta de IA generativa para apoio visual)

Mas a mesma tecnologia pode também aprofundar desigualdades. Grandes sociedades de advogados poderão desenvolver sistemas internos treinados sobre bases documentais próprias, com equipas técnicas, políticas de segurança e mecanismos de validação. Pequenos escritórios ou profissionais individuais poderão depender de ferramentas generalistas, menos controladas e eventualmente inadequadas para informação confidencial. Clientes empresariais com grande capacidade tecnológica poderão exigir níveis de rapidez e análise que alteram a relação tradicional com os seus consultores jurídicos. A IA pode, assim, redistribuir vantagens competitivas no mercado jurídico.

O primeiro risco central é o erro. Os modelos generativos são capazes de produzir respostas linguisticamente convincentes, mas juridicamente incorretas. Podem inventar jurisprudência, citar normas inexistentes, confundir regimes legais, misturar jurisdições, omitir alterações legislativas ou apresentar conclusões sem fundamento suficiente. Na advocacia, estes erros não são meramente técnicos: podem afetar direitos de clientes, prazos processuais, estratégias negociais, deveres

profissionais e responsabilidade civil ou disciplinar. A aparência de autoridade da resposta automática é, precisamente, uma das suas maiores fragilidades.

Por isso, a IA não deve ser entendida como fonte jurídica autónoma. Deve ser tratada como instrumento auxiliar de trabalho, sujeito a validação profissional. O advogado que utiliza IA continua obrigado a confirmar a validade das fontes, a atualidade da legislação, a relevância da jurisprudência, a adequação dos argumentos e a conformidade da peça ou parecer com o caso concreto. A delegação técnica não elimina a responsabilidade profissional. Pelo contrário, pode reforçar o dever de diligência, porque quem recorre a uma ferramenta poderosa deve compreender as suas limitações.

Um segundo risco é a confidencialidade. O segredo profissional é uma das bases da relação advogado-cliente. A introdução de dados, documentos, estratégias ou informações sensíveis em sistemas externos de IA pode levantar problemas graves de proteção de dados, confidencialidade contratual e segredo profissional. Mesmo quando a ferramenta afirma não utilizar os dados para treino, subsistem questões sobre armazenamento, localização dos servidores, acesso por terceiros, segurança, auditoria e enquadramento contratual. A utilização de IA na advocacia exige, portanto, políticas claras sobre que informação pode ser introduzida, em que sistemas, com que garantias e sob que responsabilidade.

A proteção de dados pessoais assume aqui especial relevância. Muitos processos jurídicos envolvem dados sensíveis: saúde, vida familiar, situação económica, antecedentes criminais, relações laborais, dados de menores ou informação empresarial reservada. A utilização de IA deve respeitar princípios de minimização, finalidade, segurança, limitação de conservação e controlo de acesso. Não basta perguntar se a ferramenta “funciona”; é necessário perguntar se é juridicamente admissível, segura e proporcional ao fim pretendido.

Um terceiro risco prende-se com a relação com o cliente. A IA pode facilitar a prestação de informação jurídica preliminar, a preparação de respostas rápidas e a criação de documentos acessíveis. Contudo, pode também criar uma aparência de certeza onde existe incerteza jurídica. O cliente pode não distinguir entre uma análise validada por advogado e uma resposta automática. Por isso, deve ser ponderado quando e como revelar a utilização de IA, especialmente se a sua intervenção for material para o resultado entregue. A transparência perante o cliente pode tornar-se uma componente relevante da confiança profissional.

A IA coloca ainda desafios à formação dos advogados. Durante muito tempo, a aprendizagem da profissão fez-se através de tarefas como pesquisa, elaboração de minutas, revisão documental, preparação de memorandos e análise de jurisprudência. Se estas tarefas forem excessivamente automatizadas, há o risco de reduzir oportunidades de desenvolvimento do raciocínio jurídico dos profissionais mais jovens. O ganho de eficiência a curto prazo pode gerar perda de competência a médio prazo se as organizações não redesenharem os processos de formação. A advocacia

aumentada exige, portanto, não apenas novas ferramentas, mas novos modelos de aprendizagem profissional.

Também a autoria e a qualidade do trabalho jurídico devem ser repensadas. Uma peça processual, um parecer ou um contrato podem ser redigidos com apoio de IA, mas a responsabilidade pelo seu conteúdo continua a pertencer ao advogado que os subscreve. A assinatura profissional não pode converter-se num ato meramente formal de validação superficial. Deve significar que o advogado compreendeu, verificou e assumiu o conteúdo produzido. A IA pode sugerir formulações; não pode substituir o juízo jurídico que confere sentido, adequação e responsabilidade ao texto.

No plano da litigância, a IA pode ser usada para analisar decisões anteriores, identificar tendências, mapear argumentos frequentes, estimar durações processuais ou organizar estratégias. Estas capacidades podem ser úteis, mas devem ser utilizadas com prudência. A análise estatística de decisões judiciais não deve ser confundida com previsão determinística do resultado de um processo. O direito não é apenas regularidade empírica; é também interpretação normativa, argumentação, prova, contexto e decisão institucional. A redução da justiça a padrões preditivos pode empobrecer a compreensão do caso concreto.

Há ainda uma dimensão ética na utilização adversarial da IA. Ferramentas generativas podem produzir grandes volumes de requerimentos, incidentes, comunicações ou documentos, aumentando a pressão sobre tribunais e partes contrárias. Podem ser usadas para explorar assimetrias de recursos, automatizar litigância de massa ou dificultar a gestão processual. A eficiência de uma parte pode transformar-se em sobrecarga sistémica. Por isso, o uso de IA na advocacia deve ser compatível com deveres de lealdade, cooperação, boa-fé processual e respeito pela administração da justiça.

Ao mesmo tempo, seria errado ignorar o potencial positivo da IA para o acesso ao direito. Muitos cidadãos e pequenas empresas não conseguem obter aconselhamento jurídico atempado por razões económicas, geográficas ou culturais. Ferramentas de IA, devidamente reguladas e supervisionadas, podem ajudar a explicar direitos, preparar informação preliminar, orientar cidadãos para os meios adequados, simplificar linguagem jurídica e apoiar advogados em modelos de prestação de serviços mais acessíveis. A IA pode contribuir para uma advocacia mais próxima, preventiva e compreensível.

A questão decisiva é, pois, a governação profissional da IA na advocacia. Cada escritório, sociedade ou departamento jurídico deveria definir regras internas sobre seleção de ferramentas, tratamento de dados, validação de resultados, deveres de revisão, comunicação ao cliente, conservação de registos, formação dos profissionais e resposta a incidentes. Estas regras não devem ser vistas como obstáculos à inovação, mas como condições de confiança. Num domínio em que o erro pode afetar direitos e responsabilidades, a confiança é parte integrante da própria utilidade da tecnologia.

Em síntese, a IA pode aumentar significativamente a capacidade de trabalho dos advogados e melhorar a qualidade, rapidez e acessibilidade dos serviços jurídicos. Mas essa promessa só se realiza de forma legítima se a tecnologia for usada como instrumento auxiliar e não como substituto do juízo profissional. O advogado do futuro não será certamente aquele que rejeita a IA, nem aquele que nela delega cegamente. Será aquele que sabe utilizá-la criticamente, preservando a confidencialidade, a independência, a diligência, a lealdade e a responsabilidade que definem a profissão.

4. IA para magistrados judiciais

A utilização de Inteligência Artificial no contexto da magistratura judicial exige uma ponderação particularmente exigente. Ao contrário de outros domínios jurídicos, em que a IA pode ser sobretudo entendida como ferramenta de produtividade, no exercício da função jurisdicional a tecnologia aproxima-se de um núcleo institucional sensível: a decisão sobre direitos, deveres, responsabilidades, liberdades e conflitos. Por isso, a questão não é apenas saber se a IA pode ajudar os juízes a trabalhar melhor, mas em que medida a sua utilização é compatível com a independência judicial, a fundamentação das decisões, a apreciação da prova, o contraditório e a confiança pública nos tribunais.

A IA pode ter utilidade significativa em várias tarefas de apoio à atividade judicial. Pode auxiliar a pesquisa de legislação e jurisprudência, identificar decisões semelhantes, resumir peças processuais extensas, organizar cronologias factuais, extrair questões jurídicas relevantes, comparar argumentos das partes, apoiar a redação preliminar de despachos ou decisões simples, sugerir estruturas de fundamentação, sinalizar prazos e facilitar a gestão de processos. Em tribunais sobrecarregados, estas funcionalidades podem contribuir para reduzir tempos mortos, melhorar a organização da informação e libertar o magistrado para tarefas de maior densidade decisória.

Contudo, a utilidade administrativa ou cognitiva da IA não deve ser confundida com legitimidade decisória. O juiz não decide apenas com base em informação; decide no quadro de uma função constitucionalmente legitimada, sujeita à lei, às garantias processuais, à independência e ao dever de fundamentação. A decisão judicial é um ato institucional de autoridade, não uma mera inferência estatística nem uma recomendação tecnicamente otimizada. Por isso, qualquer sistema de IA utilizado na atividade judicial deve permanecer numa posição instrumental, sem substituir a responsabilidade pessoal e funcional do magistrado.

A distinção entre apoio e substituição é essencial. Um sistema que ajuda a encontrar jurisprudência relevante pode reforçar a qualidade da decisão. Um sistema que resume articulados pode facilitar a compreensão inicial do processo. Um sistema que organiza a prova documental pode melhorar a eficiência da análise. Mas um sistema que recomenda a solução do litígio, sugere a credibilidade de uma testemunha, estima a probabilidade de condenação, calcula o risco de

reincidência ou propõe a medida concreta de uma pena entra num domínio de risco elevado. Nestes casos, a IA pode condicionar a própria formação da convicção judicial.

Mesmo quando o juiz mantém formalmente a decisão, a influência da IA pode ser substancial. A literatura sobre sistemas de apoio à decisão mostra que os utilizadores tendem, em muitos contextos, a atribuir peso excessivo a recomendações automáticas, sobretudo quando estas são apresentadas com aparência de objetividade, quantificação ou neutralidade técnica xxx. Este fenómeno, frequentemente designado por enviesamento de automação xxx, é especialmente problemático na justiça. Uma recomendação algorítmica pode criar uma âncora cognitiva difícil de afastar, levando o decisor humano a confirmar, mais do que a avaliar criticamente, o resultado sugerido.

A fundamentação das decisões judiciais é outro ponto crítico. Uma decisão judicial não deve apenas ser correta; deve ser compreensível, sindicável e racionalmente justificada. A fundamentação permite às partes compreenderem as razões da decisão, possibilita o recurso, disciplina o próprio decisor e reforça a legitimidade pública da justiça. Se a decisão for influenciada por um sistema de IA opaco, não auditável ou incapaz de explicar os critérios relevantes, a fundamentação pode tornar-se aparente. O juiz poderá reproduzir uma conclusão sem conseguir reconstruir plenamente o percurso que conduziu a ela.

Por isso, a utilização de IA pelos magistrados judiciais deve obedecer a uma exigência de explicabilidade suficiente. Isto não significa que todos os modelos tenham de ser totalmente transparentes em sentido técnico absoluto, o que muitas vezes não é possível. Significa, porém, que o juiz deve compreender a finalidade do sistema, os dados utilizados, as suas limitações, o grau de fiabilidade esperado, os critérios relevantes e o tipo de erro que pode ocorrer. A explicabilidade juridicamente relevante não é apenas matemática; é funcional, institucional e processual. O decisor deve saber o bastante para poder usar, questionar, corrigir ou rejeitar a recomendação.

A apreciação da prova constitui talvez o domínio mais delicado. A prova não é apenas um conjunto de dados a classificar. Envolve contexto, oralidade, imediação, contraditório, credibilidade, coerência narrativa, regras de experiência e valoração prudencial. Sistemas de IA podem apoiar a organização da prova, a transcrição de depoimentos, a identificação de documentos, a comparação de versões ou a deteção de inconsistências. Mas devem ser usados com extrema prudência quando se aproximam da avaliação da credibilidade, da inferência sobre intenção, da previsão de comportamentos ou da qualificação de risco pessoal. Nestes domínios, os perigos de enviesamento, simplificação e desumanização são particularmente elevados.

O processo penal acentua estes riscos. A utilização de IA em matérias como prisão preventiva, perigosidade, reincidência, investigação criminal, prova digital ou determinação da pena pode afetar diretamente a liberdade das pessoas e a presunção de inocência. Um sistema treinado sobre dados históricos pode reproduzir padrões discriminatórios ou desigualdades anteriores. Uma pontuação de risco pode ser interpretada como facto, quando é apenas uma estimativa probabilística baseada em

determinados dados e pressupostos. A defesa deve poder conhecer, questionar e contraditar os elementos que influenciam a decisão. Sem essa possibilidade, o contraditório fica enfraquecido.

A independência judicial também pode ser afetada por vias menos visíveis. Se os tribunais passarem a depender de sistemas desenvolvidos por entidades externas, com modelos proprietários, dados não acessíveis ou critérios não transparentes, cria-se uma nova forma de dependência institucional. A independência não é apenas independência face a poderes políticos ou económicos; é também capacidade de decidir sem condicionamentos técnicos opacos. A infraestrutura tecnológica da justiça deve, por isso, ser compatível com soberania institucional, auditabilidade pública e controlo democrático.

A IA pode ainda influenciar a uniformização da jurisprudência. Ferramentas que identificam decisões dominantes ou sugerem soluções alinhadas com padrões anteriores podem promover coerência e previsibilidade. Estes são valores importantes. Contudo, existe o risco de cristalização jurisprudencial, reduzindo a abertura à evolução do direito, à distinção do caso concreto e à inovação interpretativa. O precedente estatístico não deve converter-se em precedente normativo automático. A decisão judicial deve poder afastar-se de padrões anteriores quando existam razões jurídicas para o fazer.

No plano da gestão processual, a IA oferece oportunidades relevantes e menos controversas, embora também aqui sejam necessários cuidados. Sistemas de triagem, distribuição, deteção de urgência, gestão de agendas, previsão de duração processual ou identificação de processos repetitivos podem melhorar a eficiência dos tribunais. No entanto, devem respeitar critérios transparentes, evitar discriminação indireta e garantir mecanismos de correção. A distribuição de processos, em particular, é matéria sensível, pois se relaciona com o princípio do juiz natural e com a imparcialidade do sistema.

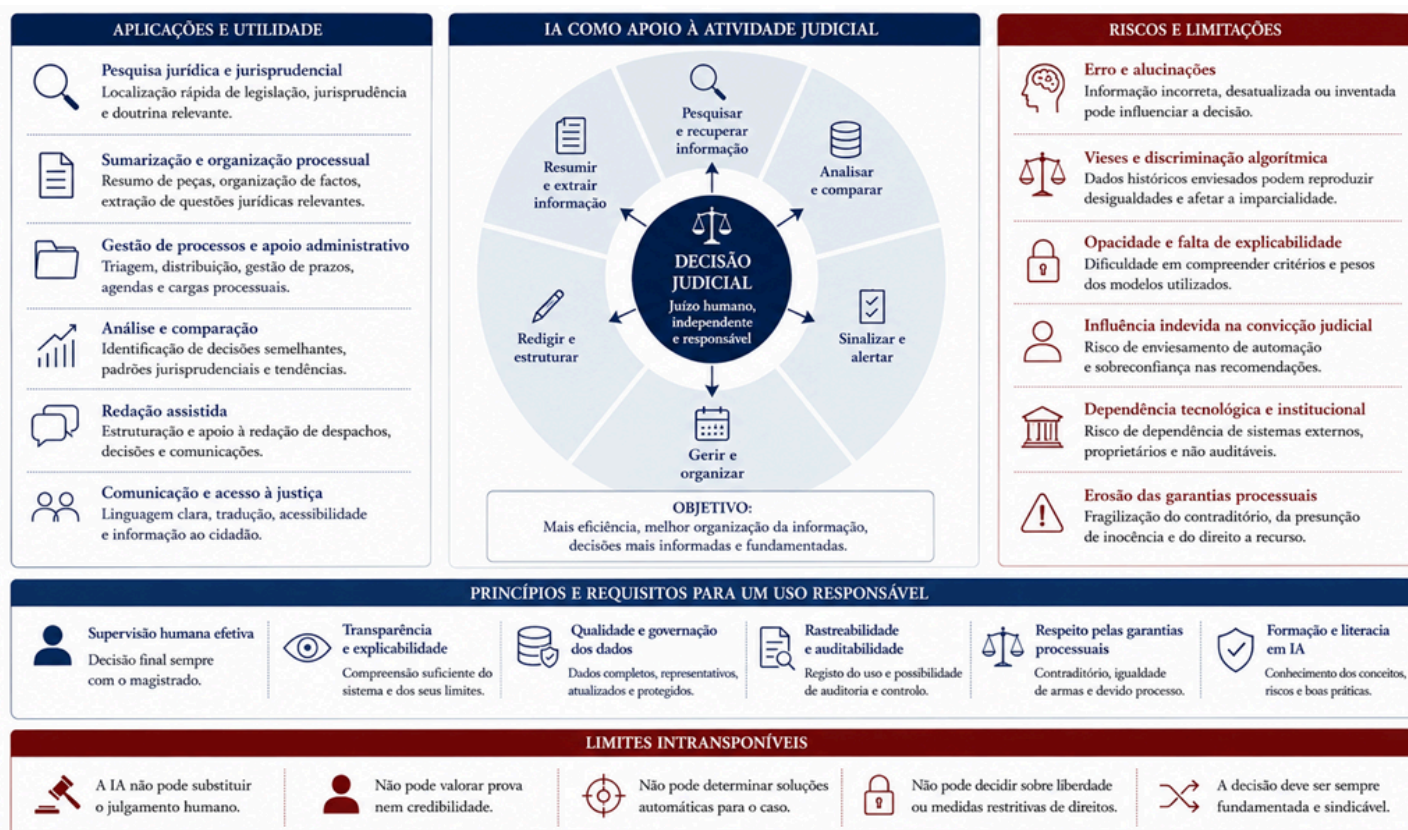


Figura 4: Inteligência Artificial para Magistrados Judiciais (Fonte: Elaboração própria do autor, com recurso a ferramenta de IA generativa para apoio visual)

Uma área promissora é a simplificação da comunicação judicial. A IA pode ajudar a produzir versões em linguagem clara de decisões, notificações ou informações processuais, sem substituir o texto jurídico oficial. Pode também apoiar tradução, acessibilidade para pessoas com deficiência, atendimento inicial ao cidadão e explicação de etapas processuais. Esta utilização pode reforçar o acesso à justiça e a compreensão pública dos tribunais. Todavia, deve ficar claro quando se trata de uma explicação auxiliar e não de uma decisão ou interpretação oficial vinculativa.

A formação dos magistrados é, neste contexto, indispensável. Não se pode exigir aos juízes que se tornem especialistas em aprendizagem computacional, mas é necessário que compreendam os principais conceitos, riscos e limitações da IA. Devem saber distinguir sistemas baseados em regras, modelos estatísticos, IA generativa, ferramentas de pesquisa semântica e sistemas preditivos. Devem conhecer fenómenos como enviesamento de dados, alucinação, opacidade, sobreconfiança, erro probabilístico e dependência tecnológica. A literacia em IA torna-se uma condição prática da independência judicial no século XXI.

Também os tribunais superiores terão um papel relevante. À medida que decisões assistidas por IA forem questionadas, será necessário construir critérios jurisprudenciais sobre admissibilidade, transparência, contraditório, prova algorítmica, dever de fundamentação e responsabilidade. A utilização de IA não deve permanecer invisível quando tenha influência material na decisão. Pelo

contrário, deve ser suficientemente documentada para permitir escrutínio pelas partes, pelos tribunais de recurso e, quando aplicável, por entidades de auditoria ou supervisão.

A responsabilidade final deve permanecer clara: a decisão é do juiz. A IA pode assistir, organizar, sugerir ou alertar, mas não pode assumir a responsabilidade institucional de julgar. Essa responsabilidade inclui a obrigação de compreender o caso concreto, ouvir as partes, valorar a prova, interpretar o direito, fundamentar a decisão e responder pelas razões apresentadas. Uma decisão judicial não deve ser o resultado de uma delegação silenciosa em tecnologia, mas de um juízo humano informado, eventualmente apoiado por instrumentos digitais, mas nunca substituído por eles.

Em síntese, a IA pode contribuir para uma magistratura mais eficiente, informada e acessível, sobretudo nas tarefas de pesquisa, organização, gestão e comunicação. Mas a sua utilização no exercício da função jurisdicional deve obedecer a limites particularmente rigorosos. Quanto mais a IA se aproxima da formação da convicção, da apreciação da prova e da decisão sobre direitos fundamentais, maior deve ser a exigência de transparência, auditabilidade, contraditório e controlo humano. A justiça aumentada só será compatível com o Estado de Direito se preservar o que torna a decisão judicial legítima: independência, responsabilidade, fundamentação e humanidade.

5. IA para tribunais e administração da justiça

A utilização de Inteligência Artificial nos tribunais não se limita ao apoio direto a advogados, magistrados ou Ministério Público. Uma parte substancial do seu potencial transformador encontra-se na administração da justiça enquanto sistema organizado: secretarias judiciais, gestão processual, distribuição de processos, atendimento ao cidadão, tramitação, notificações, anonimização, transcrição, tradução, estatística, arquivo, interoperabilidade e planeamento de recursos. Neste domínio, a IA pode contribuir para uma justiça mais eficiente, acessível e compreensível, desde que não comprometa garantias processuais, transparência institucional e controlo humano.

Os tribunais são organizações intensivas em informação. Recebem, produzem, classificam, armazenam e circulam grandes volumes de documentos, prazos, atos, requerimentos, decisões, notificações e dados administrativos. Muitas das tarefas realizadas diariamente são repetitivas, morosas e suscetíveis de apoio automatizado. A IA pode ajudar a ordenar esta complexidade, reduzindo trabalho manual, evitando erros formais, sinalizando incongruências e permitindo que os profissionais se concentrem em tarefas de maior valor jurídico e humano.

Uma primeira área de aplicação é a triagem e classificação processual. Sistemas inteligentes podem auxiliar a identificar a natureza do processo, o tipo de pedido, a matéria jurídica predominante, a existência de urgência, a repetição de causas, a conexão com outros processos ou a falta de elementos essenciais. Esta funcionalidade pode acelerar a entrada e organização dos processos, melhorar a distribuição interna de trabalho e reduzir atrasos iniciais. Contudo, a triagem

automática deve ser sempre verificável e corrigível, pois uma classificação incorreta pode afetar prazos, competência, prioridade ou tramitação subsequente.

A distribuição de processos constitui matéria especialmente sensível. Ferramentas de apoio podem ajudar a equilibrar cargas de trabalho, identificar incompatibilidades, respeitar regras de especialização e prevenir concentração indevida de processos. Porém, qualquer intervenção tecnológica neste domínio deve respeitar o princípio do juiz natural, a aleatoriedade ou os critérios legalmente definidos de distribuição, a imparcialidade e a auditabilidade. Um sistema opaco de distribuição, ainda que eficiente, poderia afetar a confiança pública nos tribunais. Por isso, a IA pode apoiar a gestão da distribuição, mas não deve introduzir critérios ocultos ou manipuláveis.

A gestão de prazos é outro domínio com elevado potencial. A IA pode sinalizar prazos críticos, detetar processos parados, identificar atos pendentes, antecipar necessidades de agendamento, alertar para situações urgentes e apoiar a priorização administrativa. Em sistemas judiciais com elevada pendência, estas ferramentas podem reduzir atrasos evitáveis e melhorar a capacidade de resposta. No entanto, a priorização automática deve ser compatível com critérios jurídicos transparentes. A urgência processual não pode ser definida apenas por padrões estatísticos ou conveniência administrativa.

A anonimização e pseudonimização de decisões judiciais representam uma aplicação particularmente relevante. A publicação de jurisprudência é essencial para a transparência, previsibilidade e desenvolvimento do direito, mas deve ser compatibilizada com a proteção de dados pessoais, a privacidade das partes e a salvaguarda de informação sensível. Sistemas de IA podem identificar nomes, moradas, números de identificação, dados de saúde, menores, vítimas ou outros elementos que devam ser ocultados. Ainda assim, a anonimização automática exige revisão e controlo de qualidade, porque tanto a omissão indevida como a divulgação indevida podem gerar consequências relevantes.

A transcrição automática de audiências, declarações e depoimentos constitui outra área promissora. A conversão automática de voz em texto pode melhorar o registo processual, facilitar a pesquisa, acelerar a elaboração de atas e apoiar a consulta posterior da prova. A tradução automática pode também facilitar processos com intervenientes estrangeiros, documentação multilingue ou cooperação judiciária internacional. Contudo, estes sistemas devem ser usados com consciência das suas limitações: erros de transcrição, dificuldades com sotaques, linguagem técnica, ruído, sobreposição de vozes ou expressões ambíguas podem alterar o sentido do que foi dito. Em contexto probatório, a revisão humana continua indispensável.

A comunicação com o cidadão é uma das áreas em que a IA pode produzir ganhos democráticos significativos. Muitos cidadãos não compreendem notificações, prazos, decisões ou etapas processuais. Sistemas de IA podem ajudar a explicar, em linguagem clara, o significado de atos processuais, os passos seguintes, os documentos necessários ou os canais adequados de contacto. Podem também apoiar atendimento inicial, encaminhamento, respostas a perguntas

frequentes e preenchimento orientado de formulários. Esta utilização pode aproximar os tribunais dos cidadãos e reduzir barreiras de acesso à justiça.

No entanto, a comunicação assistida por IA deve ser cuidadosamente delimitada. Um chatbot judicial não deve prestar aconselhamento jurídico personalizado, substituir advogado, interpretar de forma vinculativa uma decisão ou criar expectativas incorretas sobre resultados processuais. Deve ser claro para o cidadão se está perante informação geral, orientação administrativa, explicação simplificada ou comunicação oficial. A distinção entre informação, aconselhamento e decisão deve permanecer transparente.

A IA pode também apoiar a gestão de processos repetitivos ou de litigância de massa. Em áreas como consumo, cobrança, contraordenações, trabalho, segurança social ou pequenas causas, pode identificar padrões, agrupar casos semelhantes, detetar argumentos recorrentes e apoiar a criação de fluxos de tratamento mais eficientes. Esta capacidade pode reduzir duplicação de trabalho e promover coerência. Mas existe o risco de tratar como idênticos casos que têm diferenças juridicamente relevantes. A massificação processual não deve conduzir a uma justiça indiferenciada.

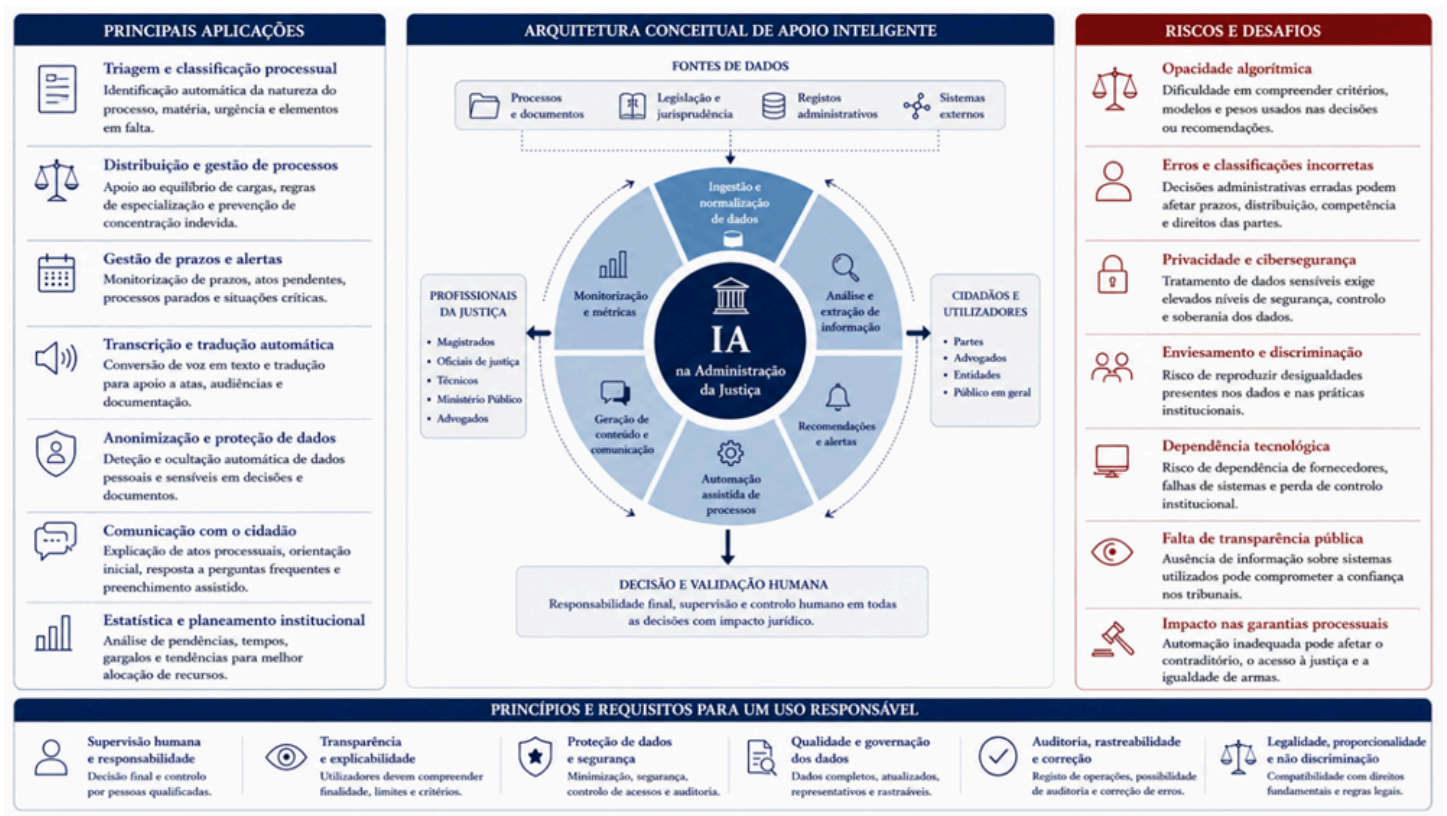


Figura 5: IA para Tribunais e Administração da Justiça (Fonte: Elaboração própria do autor, com recurso a ferramenta de IA generativa para apoio visual)

A estatística judicial e o planeamento institucional são igualmente beneficiados por ferramentas inteligentes. A IA pode ajudar a compreender pendências, tempos médios, gargalos organizacionais,

distribuição territorial de litígios, evolução de matérias emergentes, impacto de reformas legislativas ou necessidades de recursos humanos. Estes dados podem apoiar políticas públicas de justiça mais informadas. Contudo, deve evitar-se uma governação puramente quantitativa dos tribunais. Indicadores são úteis, mas não captam integralmente a qualidade da decisão, a complexidade do caso ou a proteção efetiva dos direitos.

A interoperabilidade entre sistemas é uma condição essencial para que a IA tenha utilidade real na administração da justiça. Tribunais, Ministério Público, polícias, entidades administrativas, serviços prisionais, segurança social, registos, plataformas europeias e sistemas de gestão documental produzem dados em formatos e estruturas distintas. Sem interoperabilidade segura, qualidade de dados e normalização, a IA tenderá a operar sobre informação incompleta, duplicada ou inconsistente. A modernização tecnológica da justiça não depende apenas de algoritmos; depende também de arquitetura de dados, processos claros e governação institucional.

A qualidade dos dados é, por isso, um requisito central. Dados processuais incompletos, mal classificados, desatualizados ou enviesados podem gerar resultados errados. A IA aplicada aos tribunais não deve partir da ficção de que os dados administrativos são neutros ou perfeitos. Pelo contrário, deve reconhecer que os dados refletem práticas, rotinas, omissões e desigualdades institucionais. Antes de automatizar, é necessário compreender, limpar, documentar e governar os dados. Uma má base de dados pode produzir uma má justiça aumentada.

A cibersegurança e a soberania tecnológica assumem especial importância. Os tribunais lidam com informação extremamente sensível: dados pessoais, segredos comerciais, informação penal, dados de menores, vítimas, saúde, família, património e prova documental. A adoção de ferramentas de IA deve ser compatível com elevados padrões de segurança, controlo de acessos, encriptação, localização dos dados, registo de operações e resposta a incidentes. A dependência de fornecedores externos deve ser avaliada com cuidado, sobretudo quando estejam em causa sistemas críticos para o funcionamento da justiça.

A transparência institucional é outro elemento indispensável. Os cidadãos e profissionais devem saber que tipos de sistemas de IA são utilizados nos tribunais, com que finalidade, em que fases do processo, com que limites e sob que mecanismos de supervisão. Nem todos os detalhes técnicos têm de ser públicos, mas a existência e função dos sistemas não devem ser invisíveis. A opacidade administrativa pode corroer a confiança, mesmo quando a intenção é apenas aumentar eficiência.

O controlo humano deve adaptar-se ao tipo de utilização. Em tarefas administrativas simples, pode bastar validação por amostragem, controlo estatístico e mecanismos de correção. Em tarefas que afetam prazos, direitos das partes, distribuição de processos, urgência, comunicação oficial ou acesso a informação processual, o nível de supervisão deve ser mais elevado. A regra deve ser proporcionalidade: quanto maior o impacto jurídico da decisão ou recomendação, maior a exigência de controlo humano, documentação e possibilidade de contestação.

A introdução de IA na administração da justiça exige também mudança organizacional. Não basta adquirir software. É necessário redesenhar procedimentos, formar profissionais, definir responsabilidades, atualizar regulamentos internos, criar canais de reporte de erros, estabelecer métricas de qualidade e envolver utilizadores finais. Oficiais de justiça, magistrados, advogados, técnicos de informática e cidadãos devem ser considerados no desenho dos sistemas. A tecnologia imposta de cima, sem compreensão das práticas reais, tende a falhar ou a gerar resistência legítima.

Os oficiais de justiça e funcionários judiciais não devem ser vistos como destinatários passivos da automação. Pelo contrário, são atores fundamentais na identificação de tarefas repetitivas, problemas de fluxo, riscos práticos e oportunidades de melhoria. A IA pode libertá-los de trabalho burocrático excessivo, mas pode também criar novas exigências de verificação, correção e supervisão. A transição deve valorizar competências profissionais e evitar a percepção de substituição indiferenciada por tecnologia.

A acessibilidade deve ser um princípio orientador. Sistemas de IA podem melhorar o acesso à justiça para pessoas com deficiência, cidadãos com baixa literacia jurídica, migrantes, idosos ou pessoas geograficamente afastadas. Podem produzir versões simplificadas de informação, apoiar leitura automática, tradução, navegação assistida e orientação inicial. Mas devem ser desenhados de forma inclusiva. Uma justiça digital ou aumentada que exclui quem tem menor capacidade tecnológica seria uma contradição nos seus próprios termos.

Em síntese, a IA pode ter um impacto profundo na administração da justiça, talvez até mais imediato do que na própria decisão judicial. Pode melhorar triagem, organização, prazos, comunicação, anonimização, transcrição, gestão de recursos e acesso ao cidadão. Mas a eficiência administrativa não deve ser separada das garantias processuais. A administração dos tribunais não é uma empresa comum; é a infraestrutura institucional através da qual se realizam direitos fundamentais. Por isso, a IA deve ser introduzida com prudência, transparência, segurança, controlo humano e compromisso com o Estado de Direito.

6. Princípios para uma IA juridicamente responsável

A aplicação da Inteligência Artificial ao setor jurídico exige uma matriz própria de responsabilidade. Não basta importar princípios genéricos de ética tecnológica, nem confiar apenas na conformidade formal com normas de proteção de dados ou regulação de IA. O direito tem características específicas: trabalha com fontes normativas hierarquizadas, interpreta factos e provas, protege direitos fundamentais, decide conflitos, impõe sanções, regula relações de poder e atribui responsabilidade institucional. Por isso, a IA utilizada por advogados, magistrados, Ministério Público, tribunais, reguladores e demais profissionais jurídicos deve obedecer a princípios especialmente exigentes.

O primeiro princípio é o da **supervisão humana efetiva**. A IA deve permanecer sob controlo de profissionais qualificados, capazes de compreender a finalidade do sistema, avaliar criticamente os seus resultados, corrigir erros e rejeitar recomendações inadequadas. A mera presença formal de um utilizador humano não basta. A supervisão só é efetiva se houver tempo, competência, informação e autoridade para questionar o resultado produzido pela máquina. No setor jurídico, o humano não pode ser um simples homologador de uma sugestão algorítmica; deve ser o responsável pela validação substantiva da decisão, do parecer, da peça, da acusação, da defesa ou do ato administrativo.

O segundo princípio é o da **explicabilidade suficiente**. A utilização de IA em contexto jurídico não exige necessariamente transparência técnica absoluta, muitas vezes impossível em sistemas complexos, mas exige uma compreensão adequada do funcionamento, finalidade, limitações e critérios relevantes do sistema. A explicabilidade deve ser proporcional ao impacto jurídico da utilização. Uma ferramenta de apoio à formatação documental exige menor explicação do que um sistema que influencia a avaliação de risco, a distribuição de processos, a priorização de investigação ou a decisão sobre direitos. A explicação juridicamente relevante é aquela que permite compreender, discutir, controlar e, se necessário, impugnar a influência da IA.

O terceiro princípio é o da **rastreabilidade das fontes**. No direito, a qualidade de uma resposta depende da autoridade, atualidade e pertinência das fontes utilizadas. Um sistema de IA que gera uma conclusão sem indicar a legislação, jurisprudência, doutrina, documentos ou dados que a sustentam tem utilidade limitada e risco elevado. A rastreabilidade permite verificar se a norma está em vigor, se a jurisprudência é aplicável, se a fonte é oficial, se o documento foi corretamente interpretado e se a conclusão resulta de elementos juridicamente relevantes. Sem fontes identificáveis, a IA corre o risco de produzir textos plausíveis, mas juridicamente frágeis.



Figura 6: Princípios para uma IA Juridicamente Responsável (Fonte: Elaboração própria do autor, com recurso a ferramenta de IA generativa para apoio visual)

O quarto princípio é o da **confidencialidade e do segredo profissional**. O setor jurídico lida com informação particularmente sensível: estratégias processuais, comunicações entre advogado e cliente, dados pessoais, dados criminais, segredos comerciais, informação familiar, dados de saúde, dados de menores e elementos probatórios. A utilização de IA deve respeitar deveres de confidencialidade, segredo profissional e proteção de dados desde a conceção do sistema. Antes de introduzir informação em ferramentas externas, devem ser avaliados o armazenamento, a localização dos dados, o acesso por terceiros, a possibilidade de reutilização para treino, as garantias contratuais e os mecanismos de segurança. A eficiência tecnológica não pode justificar a exposição indevida de informação protegida.

O quinto princípio é o da **auditabilidade**. Sistemas de IA utilizados em contexto jurídico devem permitir controlo posterior. Deve ser possível reconstruir, quando necessário, que dados foram usados, que versão do sistema foi aplicada, que resultado foi produzido, que intervenção humana ocorreu e de que modo esse resultado influenciou o ato final. A auditabilidade é indispensável para corrigir erros, apurar responsabilidade, avaliar enviesamentos, garantir conformidade e preservar a confiança pública. Uma IA que influencia decisões jurídicas mas não permite escrutínio adequado é incompatível com a exigência de controlo própria do Estado de Direito.

O sexto princípio é o da **responsabilidade clara**. A IA não deve servir para diluir responsabilidade. Deve estar definido quem escolhe o sistema, quem valida a sua utilização, quem controla os dados, quem verifica os resultados, quem responde por erros e quem assume a decisão final. No direito, a responsabilidade não pode ser transferida para “o algoritmo”, “a plataforma” ou “o fornecedor tecnológico”. O advogado continua responsável pelo conselho que presta; o magistrado continua responsável pela decisão que profere; o Ministério Público continua responsável pelo despacho que assina; a instituição continua responsável pelos sistemas que coloca em funcionamento.

O sétimo princípio é o da **separação entre apoio técnico e decisão jurídica**. A IA pode apoiar a pesquisa, a organização da informação, a análise documental, a deteção de padrões, a sumarização, a transcrição, a tradução, a gestão de prazos e a elaboração preliminar de textos. Mas deve manter-se uma fronteira clara entre aquilo que é auxílio técnico e aquilo que constitui decisão jurídica. A decisão sobre direitos, deveres, responsabilidade, culpa, medidas restritivas, estratégia profissional ou solução de um litígio exige juízo humano, fundamentação e assunção de responsabilidade. A IA pode informar a decisão; não deve ocupar o lugar institucional de quem decide.

O oitavo princípio é o da **literacia em IA para juristas**. Uma utilização responsável da IA pressupõe que os profissionais jurídicos compreendam, pelo menos em termos fundamentais, as

capacidades e limitações destes sistemas. Devem saber que modelos generativos podem alucinar, que dados históricos podem reproduzir enviesamentos, que uma resposta fluente não é necessariamente correta, que uma previsão estatística não é prova, que a proteção de dados depende de escolhas técnicas e contratuais, e que a utilização de IA não elimina deveres profissionais. A formação jurídica contemporânea deve integrar competências mínimas de literacia tecnológica, não para transformar juristas em engenheiros, mas para lhes permitir exercer responsabilidade crítica.

O nono princípio é o da **certificação ou validação de sistemas usados em contexto judicial**. Ferramentas utilizadas em tribunais, investigação criminal, administração da justiça ou decisões com impacto relevante sobre direitos devem ser objeto de avaliação prévia, validação independente e revisão periódica. Esta validação deve considerar não apenas desempenho técnico, mas também qualidade dos dados, segurança, enviesamentos, explicabilidade, conformidade legal, impacto em direitos fundamentais e adequação ao contexto jurídico concreto. Um sistema aceitável para uso administrativo interno pode ser inadequado para influenciar decisões judiciais ou processuais. A validação deve, por isso, ser proporcional ao risco.

Estes princípios não devem ser entendidos como obstáculos à inovação. Pelo contrário, são condições para que a inovação seja confiável, legítima e sustentável. A ausência de princípios claros pode conduzir a erros, abusos, desconfiança pública e rejeição institucional da tecnologia. Uma matriz de IA juridicamente responsável permite aproveitar os benefícios da automação e da inteligência computacional sem abdicar das garantias que definem o direito.

Em síntese, a IA no setor jurídico deve ser adotada segundo uma lógica de prudência ativa: nem rejeição apriorística, nem delegação acrítica. A tecnologia deve aumentar a capacidade dos juristas, melhorar o acesso à informação, reduzir tarefas repetitivas e apoiar decisões mais bem fundamentadas. Mas deve fazê-lo sob supervisão humana efetiva, com explicabilidade suficiente, fontes rastreáveis, confidencialidade protegida, auditabilidade, responsabilidade clara, separação entre apoio e decisão, literacia profissional e validação adequada dos sistemas. Só assim a IA poderá servir a justiça sem enfraquecer o Estado de Direito.

7. Jurisvis - IA responsável para advogados e sociedades de advogados

A discussão anterior evidencia que a adoção de Inteligência Artificial no setor jurídico não deve ser avaliada apenas em função da sua capacidade técnica, mas sobretudo em função da sua compatibilidade com os deveres profissionais, a qualidade das fontes, a confidencialidade, a auditabilidade e a responsabilidade humana. É neste contexto que se insere o JurisVis [Jurisvis, 2026], um sistema de Inteligência Artificial concebido pelo LIACC/FEUP e Hiperbole Pioneira especificamente para apoiar advogados e sociedades de advogados no contexto do direito

português, procurando materializar, em termos práticos, a noção de justiça aumentada defendida neste artigo.

O JurisVis não deve ser entendido como um substituto do advogado, nem como uma entidade autónoma de aconselhamento jurídico. A sua função é instrumental: apoiar a pesquisa, a análise, a organização e a redação jurídica, mantendo sempre a decisão, a validação e a responsabilidade no domínio do profissional. O sistema foi pensado como um copiloto jurídico, isto é, como uma ferramenta que aumenta a capacidade de trabalho do jurista, mas que não elimina o dever de verificação, prudência e juízo crítico que caracteriza a profissão [Jurisvis, 2026].

A principal preocupação na conceção do JurisVis é a adaptação ao contexto jurídico português. Muitos sistemas generalistas de IA produzem respostas aparentemente convincentes, mas sem garantia de que utilizam fontes adequadas, atualizadas ou pertencentes à jurisdição relevante. No direito, esta limitação é particularmente grave. Uma resposta juridicamente plausível pode ser inútil, ou mesmo perigosa, se se basear em legislação estrangeira, jurisprudência desatualizada, normas revogadas ou referências inexistentes. Por isso, um sistema de IA para uso jurídico deve ser construído em torno de fontes jurídicas identificáveis, rastreáveis e verificáveis [Jurisvis, 2026].

O JurisVis procura responder a este problema através de uma arquitetura orientada para a recuperação e utilização de fontes jurídicas relevantes. Em vez de depender exclusivamente da capacidade generativa de um modelo de linguagem, o sistema deve privilegiar a consulta estruturada de legislação, jurisprudência, doutrina, documentos internos e outros materiais previamente selecionados. Esta opção reduz o risco de respostas infundadas e permite aproximar a utilização de IA das exigências tradicionais do trabalho jurídico: indicar fontes, verificar autoridade, respeitar a hierarquia normativa e atender ao contexto concreto do caso [Jurisvis, 2026].

Neste sentido, a rastreabilidade das fontes constitui um elemento central do sistema. Uma resposta produzida por IA só tem utilidade profissional se o advogado puder perceber de onde resulta a informação apresentada. O JurisVis deve, por isso, permitir que o utilizador identifique os diplomas, artigos, decisões, excertos documentais ou peças internas que sustentam determinada resposta. A transparência das fontes não elimina a necessidade de validação humana, mas torna essa validação possível. Sem rastreabilidade, a IA transforma-se numa máquina de plausibilidade; com rastreabilidade, pode tornar-se uma ferramenta de trabalho juridicamente controlável [Jurisvis, 2026].

Outra dimensão essencial é a confidencialidade. A advocacia trabalha frequentemente com informação protegida por segredo profissional, dados pessoais sensíveis, estratégias processuais, documentos empresariais reservados e comunicações entre advogado e cliente. A utilização de ferramentas generalistas, sem garantias adequadas de segurança e controlo de dados, pode ser incompatível com estes deveres. Um sistema como o JurisVis deve ser concebido de modo a respeitar princípios de minimização, controlo de acesso, segurança, segregação de informação e

proteção dos dados introduzidos pelos utilizadores. A confiança técnica e jurídica no sistema depende, em larga medida, da forma como trata a informação confidencial [Jurisvis, 2026].

O JurisVis pode apoiar diferentes tarefas do quotidiano profissional dos advogados. Entre elas incluem-se a pesquisa de legislação e jurisprudência, a identificação de normas aplicáveis, a sumariação de documentos extensos, a comparação de versões contratuais, a preparação de minutas, a organização de argumentos, a análise preliminar de risco, a criação de listas de verificação, a extração de pontos relevantes de peças processuais e o apoio à gestão de conhecimento interno das sociedades de advogados. Estas funcionalidades são particularmente relevantes em contextos de elevada pressão temporal, grande volume documental ou necessidade de resposta rápida ao cliente [Jurisvis, 2026].

Contudo, a utilidade destas funcionalidades depende da forma como são integradas no processo de trabalho. O JurisVis não deve ser usado como fonte final de verdade jurídica, mas como mecanismo de apoio à construção da resposta profissional. O advogado deve continuar a verificar a legislação aplicável, confirmar a atualidade das normas, avaliar a pertinência da jurisprudência, adaptar a argumentação ao caso concreto e assumir a responsabilidade pelo conteúdo entregue ao cliente ou submetido a tribunal. A IA pode acelerar etapas preparatórias, mas não substitui o raciocínio jurídico nem a responsabilidade da assinatura profissional.

Um dos contributos mais relevantes de um sistema como o JurisVis é a possibilidade de reforçar a gestão do conhecimento jurídico dentro das organizações. As sociedades de advogados acumulam ao longo do tempo pareceres, minutas, cláusulas, memorandos, peças processuais, notas internas, experiências setoriais e conhecimento tácito disperso por equipas e departamentos. A IA pode ajudar a recuperar esse conhecimento, relacioná-lo com novos problemas e torná-lo mais acessível aos profissionais. Deste modo, o sistema não serve apenas para pesquisar direito externo; pode também ajudar a preservar e reutilizar conhecimento interno, desde que tal seja feito com regras claras de confidencialidade e controlo de acesso.

O JurisVis pode igualmente contribuir para a formação de advogados mais jovens. Em vez de substituir o processo de aprendizagem, pode ser usado como instrumento pedagógico interno, ajudando a estruturar problemas, sugerir caminhos de pesquisa, explicar conceitos, identificar lacunas argumentativas e comparar alternativas de redação. No entanto, esta utilização deve ser acompanhada por supervisão sénior. A aprendizagem jurídica exige contacto direto com as fontes, com a complexidade dos casos e com a responsabilidade da decisão. A IA pode orientar, mas não deve empobrecer a formação através da automatização acrítica das tarefas fundamentais da profissão.

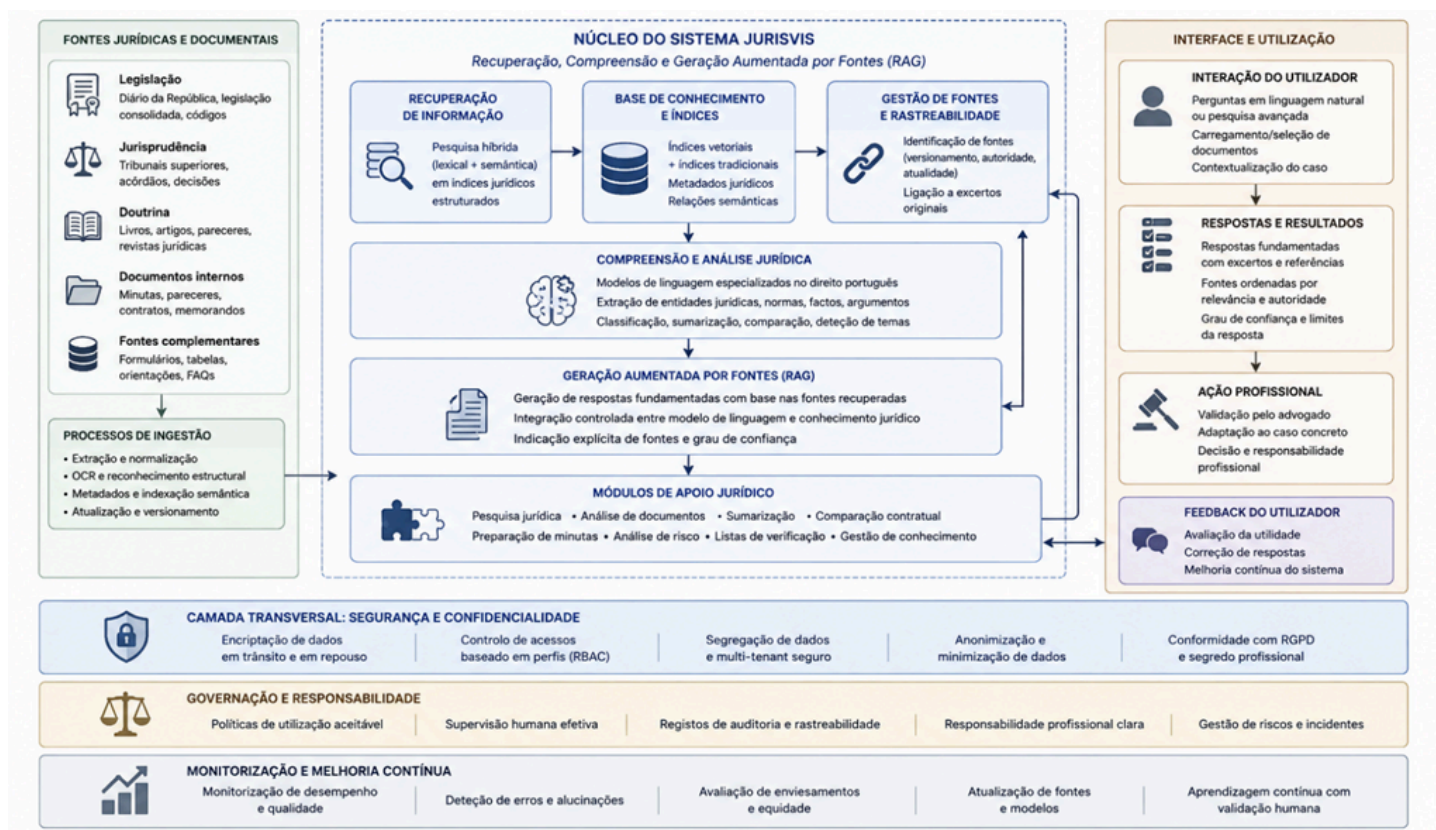


Figura 7: Jurisvis - IA Juridicamente Responsável (Fonte: Elaboração própria do autor, com recurso a ferramenta de IA generativa para apoio visual)

A interface do sistema deve refletir esta filosofia de utilização responsável. Não basta apresentar uma caixa de diálogo capaz de gerar respostas. É importante que o ambiente de trabalho evidencie as fontes consultadas, o grau de confiança, os limites da resposta, os documentos utilizados, as alternativas possíveis e a necessidade de validação profissional. A experiência de utilização deve induzir uma atitude crítica, e não uma relação de dependência. Um bom sistema jurídico de IA não é necessariamente aquele que responde com mais fluência, mas aquele que ajuda o jurista a trabalhar melhor, com maior controlo e consciência das incertezas.

A Figura 7 sintetiza a lógica de responsabilidade subjacente ao JurisVis. O sistema deve articular modelos de linguagem, bases documentais, mecanismos de recuperação de informação, módulos de análise jurídica e interfaces de utilização, mas sempre sob supervisão humana. A sua arquitetura deve refletir os princípios anteriormente propostos: fontes rastreáveis, confidencialidade, auditabilidade, responsabilidade clara e separação entre apoio técnico e decisão jurídica. A tecnologia é colocada ao serviço da prática profissional, e não no lugar da prática profissional.

A Figura 8 ilustra a dimensão operacional do sistema. Uma interface jurídica responsável deve permitir que o advogado formule perguntas, carregue ou selecione documentos, consulte respostas fundamentadas, aceda às fontes relevantes e refine a análise de acordo com o caso concreto. Esta interação deve ser concebida para apoiar ciclos sucessivos de trabalho: pergunta, resposta, verificação, aprofundamento, comparação, redação e validação. O objetivo não é produzir

automaticamente a solução jurídica final, mas melhorar a qualidade e a eficiência do processo de construção dessa solução.

A adoção de um sistema como o JurisVis também exige governação organizacional. As sociedades de advogados que utilizem IA devem definir políticas internas sobre tipos de utilização permitida, categorias de dados que podem ser introduzidas, níveis de revisão obrigatória, procedimentos de validação, formação dos utilizadores, conservação de registos e resposta a erros ou incidentes. A qualidade do sistema tecnológico é apenas uma parte da equação. A outra parte é a maturidade institucional com que a ferramenta é integrada no trabalho jurídico.



Figura 8: Jurisvis – Interface do Sistema [Jurisvis, 2026]

Em termos mais amplos, o JurisVis representa uma tentativa de operacionalizar a ideia de IA juridicamente responsável. A sua relevância não está apenas nas funcionalidades que oferece, mas no modelo de utilização que propõe: uma IA orientada por fontes, controlada pelo profissional, respeitadora da confidencialidade, auditável, contextualizada no direito português e subordinada à responsabilidade humana. Este modelo permite distinguir a inovação legítima da automação imprudente.

Em síntese, o JurisVis demonstra que é possível desenvolver sistemas de IA para o setor jurídico sem abdicar dos princípios fundamentais da profissão. A IA pode apoiar advogados e sociedades de advogados na pesquisa, análise, redação e gestão do conhecimento, mas deve fazê-lo de forma rastreável, segura e supervisionada. A promessa da tecnologia não está em substituir o jurista, mas

em libertá-lo para tarefas de maior valor: interpretar, ponderar, argumentar, aconselhar, decidir e assumir responsabilidade. Nesse sentido, o JurisVis pode ser visto como uma concretização prática da justiça aumentada: uma justiça mais informada e eficiente, mas ainda profundamente humana, profissional e subordinada ao Estado de Direito.

8. Conclusão: nem tecnofilia nem tecnofobia

A Inteligência Artificial entrou definitivamente no universo jurídico. Já não se trata de uma hipótese futurista, nem de uma discussão reservada a especialistas em tecnologia. Advogados, magistrados, Ministério Público, tribunais, reguladores, administrações públicas, empresas e cidadãos começam a utilizar, testar ou ser afetados por sistemas capazes de pesquisar, resumir, classificar, prever, redigir, traduzir, organizar e recomendar. O direito, enquanto prática intensiva em linguagem, informação, interpretação e decisão, é um dos domínios mais expostos à transformação provocada pela Inteligência Artificial.

Perante esta realidade, a resposta jurídica não deve ser nem a rejeição defensiva nem a adesão acrítica. A tecnofobia ignora o potencial da IA para melhorar a eficiência, reduzir tarefas repetitivas, facilitar o acesso ao direito, apoiar a gestão processual, melhorar a comunicação com os cidadãos e reforçar a qualidade da informação disponível para os profissionais jurídicos. Mas a tecnofilia esquece que a justiça não é apenas um problema de produtividade. A justiça é uma função essencial do Estado de Direito, estruturada por garantias, responsabilidades, procedimentos, direitos fundamentais e confiança pública.

A IA pode ajudar muito, mas pode também errar de forma convincente, reproduzir enviesamentos, ocultar critérios, fragilizar a fundamentação, expor dados sensíveis, criar dependências tecnológicas, acentuar desigualdades de acesso e diluir responsabilidades. Estes riscos não são argumentos para impedir a inovação, mas são razões para a governar com especial exigência. No setor jurídico, a eficiência só é desejável quando permanece compatível com a legalidade, a independência, o contraditório, a igualdade de armas, a proteção de dados, o segredo profissional, a imparcialidade e o direito a uma decisão fundamentada.

A ideia de justiça aumentada permite sintetizar esta posição. A IA deve aumentar a capacidade dos juristas, não substituir o seu juízo. Deve melhorar a pesquisa, não inventar autoridade. Deve organizar informação, não determinar automaticamente soluções. Deve apoiar a decisão, não ocupar o lugar institucional de quem decide. Deve simplificar o acesso do cidadão ao direito, não criar uma falsa segurança jurídica. Deve reforçar a qualidade do serviço público de justiça, não tornar invisíveis critérios técnicos que afetam direitos.

Esta distinção entre apoio e substituição é decisiva. O advogado que utiliza IA continua responsável pelo aconselhamento que presta e pelos documentos que subscreve. O magistrado judicial continua responsável pela decisão que profere e pela respetiva fundamentação. O Ministério

Público continua responsável pela direção do inquérito, pela promoção da ação penal e pelos despachos que assina. Os tribunais continuam responsáveis pela organização, distribuição e tramitação dos processos. As instituições públicas continuam responsáveis pelos sistemas que adotam. A IA não deve servir como intermediário opaco entre a decisão e a responsabilidade.

Também o cidadão deve permanecer no centro da transformação digital da justiça. A IA pode ajudar a explicar direitos, simplificar linguagem, preencher formulários, orientar pedidos, traduzir informação e tornar o sistema jurídico mais acessível. Mas o acesso ao direito não pode ser confundido com acesso a respostas automáticas. Quando estejam em causa direitos relevantes, prazos, sanções, contratos, família, trabalho, habitação, imigração ou responsabilidade penal, a orientação tecnológica deve saber reconhecer os seus limites e encaminhar para apoio humano qualificado.

A governação da IA no direito deve, por isso, assentar numa matriz própria: supervisão humana efetiva, explicabilidade suficiente, rastreabilidade das fontes, confidencialidade, auditabilidade, responsabilidade clara, separação entre apoio técnico e decisão jurídica, literacia em IA para juristas e validação de sistemas usados em contexto judicial. Estes princípios não são acessórios éticos; são condições de legitimidade. Sem eles, a IA pode aumentar a velocidade do sistema jurídico, mas diminuir a sua qualidade democrática.

O desafio não é escolher entre justiça humana e tecnologia. O verdadeiro desafio é construir instituições jurídicas capazes de usar tecnologia sem perder humanidade, responsabilidade e legitimidade. A IA pode libertar tempo, revelar padrões, melhorar a informação e aproximar cidadãos das instituições. Mas deve permanecer subordinada ao direito, aos direitos fundamentais e ao controlo humano. A justiça não deve tornar-se automática; deve tornar-se mais informada, mais acessível, mais transparente e mais responsável.

Em conclusão, a Inteligência Artificial representa uma oportunidade estrutural para modernizar o setor jurídico, mas também um teste à maturidade do Estado de Direito. Se for usada sem regras, pode fragilizar garantias e concentrar poder em sistemas opacos. Se for recusada sem reflexão, pode desperdiçar instrumentos úteis para enfrentar atrasos, complexidade e desigualdade no acesso à justiça. Entre estes dois extremos, impõe-se uma via de prudência ativa: inovar, mas com controlo; automatizar, mas com responsabilidade; apoiar a decisão, mas preservar o juízo humano; aumentar a justiça, mas nunca substituir o direito.

Referências bibliográficas

[Brown, 2020] BROWN, Tom B.; MANN, Benjamin; RYDER, Nick; et al. Language Models are Few-Shot Learners. In *Advances in Neural Information Processing Systems* 33. Red Hook, NY: Curran Associates, 2020, pp. 1877–1901.

[Dehghani, 2025] DEHGHANI, Fatemeh; DEHGHANI, Reza; ARDEBILI, Yashar Naser; RAHNAMAYAN, Shahryar. Large Language Models in Legal Systems: A Survey. Humanities and Social Sciences Communications. 2025, vol. 12. DOI 10.1057/s41599-025-05924-3.

[Jurisvis, 2026] REIS, Luis Paulo; Restivo, André; Pimenta, João et al, JURISVIS - JurisVis: Assistente de Investigação Jurídica com IA. [Em linha]. 2026. Disponível em: <https://jurisvis.com/>. [Visualizado em: 5 julho 2026].

[Magesh, 2024] MAGESH, Varun; SURANI, Faiz; DAHL, Matthew; SUZGUN, Mirac; MANNING, Christopher D.; HO, Daniel E. Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools. [Em linha]. arXiv, 2024. DOI 10.48550/arXiv.2405.20362

[McCarthy, 1955] McCARTHY, John; MINSKY, Marvin L.; ROCHESTER, Nathaniel; SHANNON, Claude E. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. [Em linha]. 1955. Disponível em: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>. [Visualizado em: 20 junho 2026].

[Mitchell, 1997] MITCHELL, Tom M. Machine Learning. New York: McGraw-Hill, 1997. ISBN 978-0070428072.

[Siino, 2025] SIINO, Marco; FALCO, Mariano; CROCE, Danilo; ROSSO, Paolo. Exploring LLMs Applications in Law: A Literature Review on Current Legal NLP Approaches. IEEE Access. 2025, vol. 13, pp. 18253–18276. DOI 10.1109/ACCESS.2025.3533217.

[Turing, 1950] TURING, Alan M. Computing Machinery and Intelligence. Mind. 1950, vol. 59, n.º 236, pp. 433–460. ISSN 0026-4423.

[Vapnik, 1995] VAPNIK, Vladimir N. The Nature of Statistical Learning Theory. New York: Springer, 1995. ISBN 978-0387987804.

[Vaswani 2017] VASWANI, Ashish; SHAZEER, Noam; PARMAR, Niki; USZKOREIT, Jakob; JONES, Llion; GOMEZ, Aidan N.; KAISER, Łukasz; POLOSUKHIN, Illia. Attention Is All You Need. In Advances in Neural Information Processing Systems 30. Red Hook, NY: Curran Associates, 2017, pp. 5998–6008.

