

CAPÍTULO 9

TECNOLOGIA, PROTEÇÃO DE DADOS E INTELIGÊNCIA ARTIFICIAL – OS PASSOS EQUILIBRADOS PARA OS TRIBUNAIS

SOFIA WENGOROVIVUS

Juíza de direito. Encarregada da Proteção de Dados do Conselho Superior da Magistratura e dos Tribunais da Relação. Pós-graduada em Direito da Comunicação Social pelo Instituto Jurídico da Comunicação da Faculdade de Direito da Universidade de Coimbra (1997/1998) e em Proteção de Dados Pessoais pelo CIDP, da Faculdade de Direito da Universidade de Lisboa (2021/2022). Conselho Superior da Magistratura, Rua Duque de Palmela, n.º 23, 1250-097, Lisboa, email: dpo.csm@csm.org.pt

INTRODUÇÃO E ENQUADRAMENTO

A utilização das novas tecnologias e a digitalização da atividade dos tribunais (digitalização dos sistemas judiciais) é já uma realidade irreversível no nosso país e na Europa.

Entre as principais prioridades anunciadas pela Comissão Europeia está a de tornar a Europa preparada para a era digital.

A Comissão está empenhada em fazer desta década a «Década Digital» da Europa ¹.

A digitalização dos serviços públicos a 100% é uma das metas digitais anunciadas pela Comissão Europeia para 2030.

A digitalização dos sistemas judiciais é considerada crucial para proporcionar um acesso moderno à justiça num ambiente cada vez mais digitalizado, com vantagens que são manifestas, mas que comportam riscos para os cidadãos e as empresas.

1. Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho de 29 de abril de 2021 que cria o Programa Europa Digital e revoga a Decisão (UE) 2015/2240.

Este propósito está em consonância com a Jurisprudência do Tribunal Europeu dos Direitos Humanos² e com as Recomendações e práticas do Conselho da Europa relativas à utilização de tecnologias avançadas para aumentar a coerência, a qualidade e a transparência das decisões judiciais, para defender as normas em matéria de direitos humanos e de Estado de Direito nos Estados-Membros do Conselho da Europa.³

A utilização intensiva dos meios digitais e a decorrente globalização da informação veio criar desafios para a proteção de dados pessoais em todos os setores, mas também nos tribunais onde o tratamento dos dados judiciais passou a ser realizado quase exclusivamente por meios digitais e em plataformas eletrónicas.

Os benefícios da introdução de novas tecnologias na atividade dos tribunais, como a promoção da transparência, celeridade, acessibilidade e escrutínio da atividade da sua atividade, são inegáveis e potenciam a credibilidade do sistema e a confiança dos cidadãos. A tecnologia é hoje um meio necessário para assegurar a concretização do direito fundamental do acesso ao direito e a uma decisão em prazo razoável (artigo 20.º da Constituição da República Portuguesa).

Contudo, a digitalização do sistema judicial, designadamente, a tramitação dos processos judiciais em plataformas eletrónicas, o acesso eletrónico aos processos, a conservação dos dados em ambiente digital, a publicação dos dados dos processos em portais públicos na internet e, mais recentemente, a introdução de ferramentas de IA nos tribunais, comportam riscos para os direitos fundamentais do cidadão, nomeadamente para o direito à proteção dos dados pessoais, como direito à autodeterminação informativa.

É sobre estes riscos e benefícios e a conciliação dos vários direitos fundamentais aqui concorrentes, em especial com o direito à proteção de dados pessoais, que se pretende dar uma breve nota, na perspetiva do encarregado da proteção de dados, aproveitando a oportunidade para dar a conhecer algumas das ferramentas de IA que o sistema Judiciário português, designadamente, o Supremo Tribunal de Justiça e o Conselho Superior da Magistratura já desenvolveram ou projetam desenvolver.

Não se pretende neste texto realizar uma reflexão mais profunda sobre as várias aplicações de IA já testadas em alguns tribunais de outros países e das suas implicações no sistema de Justiça, mas apenas efetuar uma breve resenha das possibilidades existentes e das preocupações inerentes

2. Neste sentido, vd. TEDH - Fazliyski c. Bulgária, pedido n.º 40908/05, acórdão de 16 de abril de 2013, n.º 69; L.B. c. Hungria [GC], petição n.º 36345/16, acórdão de 9 de março de 2023; Vicent Del Campo c. Espanha, pedido n.º 25527/13, acórdão de 6 de novembro de 2018.

3. Nomeadamente Recomendação n.º R (95) 11 relativa à seleção, tratamento, apresentação e arquivo de decisões judiciais nos sistemas de recuperação de informações jurídicas.

à sua criação e desenvolvimento, nomeadamente ao nível da proteção de dados pessoais.

1 ENQUADRAMENTO LEGAL

A importância de a Europa estar preparada para a era digital e do anunciado compromisso de fazer desta década a «Década Digital», traduziu-se na aprovação de vários instrumentos de *hard law* e de *soft law* que, perante o imparável e célere avanço da tecnologia, procuram estabelecer um quadro regulamentar bem definido que assegure a necessária conciliação dos direitos fundamentais em concurso e garanta que esta seja um instrumento ao serviço do cidadão e não se traduza numa instrumentalização do ser humano.

Dos instrumentos de *hard law*, para além dos Tratados constitutivos, da Declaração Universal dos Direitos Humanos, da Convenção Europeia dos Direitos do Homem, da Carta dos Direitos Fundamentais da União Europeia, da Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108+), para o tema em análise, temos de destacar:

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

- O Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, 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;

- O Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho, de 29 de abril de 2021, que cria o Programa Europa Digital e revoga a Decisão (UE) 2015/2240;

- A Decisão (UE) 2022/2481 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, que estabelece o programa Década Digital para 2030;

- O Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, de 13 de dezembro de 2023, relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização e que altera o Regulamento (UE) 2017/2394 e a Diretiva (UE) 2020/1828 (Regulamento dos Dados), que entrou em vigor no passado dia 11 de janeiro de 2024;

- O Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho, de 30 de maio de 2022, relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados);

- O 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 e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais), instrumento diretamente aplicável em todos os Estados-membros desde 17 de fevereiro de 2024, sendo a primeira regulamentação no domínio do digital que responsabiliza as empresas digitais na UE pelos conteúdos que publicam nas suas plataformas;

- O Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho, de 14 de setembro de 2022, relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais), adotado em 18 de julho de 2022, que entrou em vigor em 2 de maio de 2023 e que visa assegurar que estas plataformas se comportam de forma justa sendo, à semelhança do Regulamento Serviços Digitais, um dos elementos centrais da Estratégia Digital Europeia;

- O Regulamento (UE) 2024/903 do Parlamento Europeu e do Conselho, de 13 de março de 2024, que estabelece medidas para um elevado nível de interoperabilidade do setor público em toda a União (Regulamento Europa Interoperável);

- O Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho, de 13 de março de 2024, sobre a transparência e o direcionamento da propaganda política;

- O Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). O Regulamento prevê como regra geral a sua aplicação direta em todos os Estados no prazo de 2 anos após a sua publicação no Jornal Oficial, com a ressalva de algumas normas relativas às proibições de sistemas de risco inaceitáveis que entram em vigor passados 6 meses e algumas obrigações que só se aplicarão ao fim de 3 anos, a 2 de agosto de 2027.⁴

A par de toda esta produção legislativa temos, ainda, de atender aos instrumentos de *soft law*, tais como:

4. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ%3AL_202401689

- A Resolução do Parlamento Europeu de 16 de fevereiro de 2017, com recomendações à Comissão sobre Regras de Direito Civil sobre Robótica (2015/2103(INL));⁵

- A Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente, adotada pela CEPEJ na sua 31.ª reunião plenária (Estrasburgo, 3 e 4 de dezembro de 2018);⁶

- O Livro Branco sobre Inteligência Artificial - Uma abordagem europeia de excelência e confiança (2020);⁷

- A Declaração de Lisboa – Democracia Digital com propósito (2021)
- o reforço da dimensão humana do ecossistema digital;⁸

- A Recomendação sobre a Ética da Inteligência Artificial, aprovada pela UNESCO em 23 de novembro de 2021;⁹

- A Declaração Europeia sobre direitos e princípios digitais (2022);¹⁰

- Os Princípios da OCDE sobre Inteligência Artificial, recomendação adotada em 22 de maio de 2019 e atualizada em 03 de maio de 2024¹¹.

A aprovação deste elevado número de instrumentos revela uma clara e manifesta preocupação da União Europeia e das Organizações internacionais em ditar as normas e impor os limites para, permitindo e criando condições para o avanço das novas tecnologias, designadamente dos sistemas de IA, manter o elevado padrão de proteção dos direitos fundamentais.

2 A UTILIZAÇÃO DE SISTEMAS DE IA NO SISTEMA JUDICIAL

O acelerado desenvolvimento da IA em todas as áreas com as potencialidades e ganhos manifestos e já comprovados, nomeadamente ao nível da celeridade na resposta, da eficiência na recolha e na análise de grandes volumes de dados, na conexão e sintetização de realidades e provas cada vez mais complexas, evidencia a necessidade da ponderação pelo Judiciário da utilização de aplicações de IA na sua atividade.

Os tribunais têm de se adequar a este novo mundo digital que imprimiu outra complexidade aos processos judiciais e à própria realidade que hoje é objeto dos processos e dos crimes que se investigam. Só deste

5. Textos aprovados - Disposições de Direito Civil sobre Robótica - Quinta-feira, 16 de fevereiro de 2017 (europa.eu)

6. rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0

7. EUR-Lex - 52020DC0065 - EN - EUR-Lex (europa.eu)

8. <https://www.lisbondeclaration.eu/>

9. https://unesdoc.unesco.org/ark:/48223/pf0000381137_por

10. Declaração Europeia sobre Direitos e Princípios Digitais | Moldar o futuro digital da Europa

11. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

modo, munindo-se das ferramentas que, em muitos casos, já são utilizadas por todos os outros intervenientes processuais, conseguirão dar resposta em tempo útil às solicitações e pressões do atual mundo digital e garantir o acesso ao direito e à decisão em prazo razoável.

De acordo com a nota informativa elaborada pelo Grupo de Trabalho da CEPEJ sobre Ciberjustiça e Inteligência Artificial (CEPEJ-GT-CYBERJUST), de 12 de fevereiro de 2024, sobre a “Utilização da inteligência artificial generativa (IA) por profissionais da justiça num contexto profissional”¹², dentro de um quadro claramente definido, a IA generativa parece fornecer bons resultados para:

- tradução de textos;
- geração de texto, imagens ou sons coerentes (mas não necessariamente verdadeiros);
- resumo automático dos textos;
- análise semântica e deteção de opiniões;
- mineração de texto e acesso a conteúdos.

Neste parecer, a CEPEJ elenca como riscos da utilização da IA generativa pelos juízes e outras profissões jurídicas:

- Produção potencial de informações factualmente inexatas (respostas falsas, «alucinações» e enviesamentos);
- Possível divulgação de dados sensíveis e risco de confidencialidade;
- Falta de referências para as informações fornecidas e potencial violação da propriedade intelectual e dos direitos de autor;
- Capacidade limitada de dar a mesma resposta a uma pergunta idêntica;
- Replicação potencial dos resultados;
- Estabilidade e fiabilidade variáveis dos modelos de IA generativa para processos críticos e sensíveis ao fator tempo;
- Exagero dos enviesamentos cognitivos.

Para além de elencar os riscos o grupo de trabalho enuncia recomendações sobre como as ferramentas de IA devem ser aplicadas e quando é que não devem ser utilizadas pelos juízes e outros operadores judiciais.

“Como deve ser aplicado?”

1 Certifique-se de que a utilização da ferramenta é autorizada e adequada para a finalidade pretendida.

12. <https://www.coe.int>

2 Tenha em mente que é apenas uma ferramenta e tente compreender como funciona (esteja ciente dos preconceitos cognitivos humanos).

3 Dê preferência a sistemas que tenham sido treinados em dados certificados e oficiais, cuja lista é conhecida, para limitar os riscos de viés, alucinação e violação de direitos autorais.

4 Dê à ferramenta instruções claras (prontas) sobre o que se espera dela. É através da conversação que a máquina obterá as instruções de que necessita, por isso não hesite em envolvê-la, ao contrário de um motor de busca. É possível pedir esclarecimentos ou mesmo refinar ou modificar o pedido. Por exemplo, dar à máquina um contexto (país, período de tempo), definir a tarefa (por exemplo, escrever um resumo em xx palavras), especificar a quem se destina a saída, como deve ser produzida e o tom que a ferramenta deve adotar, pedir um formato de apresentação específico, verificar se as instruções foram corretamente compreendidas (pedindo à máquina que as reformule), fornecer exemplos das respostas esperadas para perguntas semelhantes para permitir que a ferramenta imite a sua forma e estilo.

5 Introduza apenas dados e informações não sensíveis que já estejam disponíveis no domínio público.

6 Verifique sempre a exatidão das respostas, mesmo no caso de serem dadas referências (especialmente verifique a existência da referência).

7 Seja transparente e indique sempre se uma análise ou conteúdo foi gerado por IA generativa.

8 Reformule o texto gerado, caso deva ser integrado em documentos oficiais e/ou jurídicos.

9 Mantenha o controlo da sua escolha e do processo de tomada de decisão e analise criticamente as propostas apresentadas.

Quando não deve ser aplicado?

1 Caso não tenha conhecimento, não compreenda ou não concorde com os termos e condições de utilização.

2 No caso de ser proibido ou contra a sua regulamentação organizacional.

3 Caso não seja possível avaliar o resultado quanto à correção factual e à parcialidade.

4 No caso de ser obrigado a introduzir e, assim, divulgar dados pessoais, confidenciais, protegidos por direitos de cópia ou de outra forma sensíveis.

5 No caso de ter de saber como é que a sua resposta foi obtida.

6 No caso de se esperar que produza uma resposta genuinamente auto-derivada¹³.”

13. Tradução feita com recurso ao e-translation, da Comissão Europeia: <https://webgate.ec.europa>.

Esta nota, ainda que de modo muito sintético, elenca as questões essenciais e transversais a todas as aplicações que têm sido projetadas para os tribunais, com as quais se debate quem se tem dedicado à reflexão de como tirar partido das vantagens das ferramentas de IA sem esquecer as particularidades próprias do sistema da Justiça, onde cada caso judicial é um caso, exigindo uma perceção e uma ponderação da realidade que não pode deixar de ser humana.

Numa reflexão mais profunda sobre a “*Justiça digital e inteligência artificial nos tribunais*”, veja-se as conclusões da “Agenda da Reforma da Justiça, Uma Reflexão Aberta e Alargada do Judiciário”¹⁴, onde, entre o mais, se conclui:

(...) - A IA pode ser utilizada, numa primeira etapa, como uma espécie de assistente judicial eletrónico, para, por exemplo, preparar e auxiliar o juiz na redação das decisões finais, para reconhecer o tipo de argumentação utilizado pelas partes, o chamado *argument mining*, ou para analisar dados muito complexos – *data mining*;

- Nesta primeira fase dos processos, considera-se que não haverá grandes dificuldades ligadas à utilização da IA, embora seja importante que se perceba e reflita nos processos de que forma a mesma foi utilizada e teve influência na tomada de decisão final (por forma a que as partes se apercebam dessa utilização e possam colocar a mesma em causa, nomeadamente em sede de recurso dessa decisão);

- A IA poderá também ter aplicações perniciosas quanto ao sistema judicial, podendo utilizar os dados existentes de forma prejudicial para o mesmo, como para efetuar uma espécie de análise jurisprudencial preditiva (que pode ser individualizada quanto a cada juiz), devendo evitar-se que os dados relativos aos magistrados possam ser reutilizados para avaliar, analisar, comparar ou prever as suas práticas profissionais;

- Afigura-se mais difícil a possibilidade de serem criados algoritmos específicos para decidirem, sem interferência humana, casos judiciais ou que façam predições sobre o comportamento futuro de arguidos em processos criminais, podendo, com muita cautela, iniciar-se essa aplicação da IA em processos mais simples de natureza cível, sujeitas depois, eventualmente, a reclamação para um juiz “físico”;

- Nos processos criminais considera-se que, por ora, será de evitar o recurso à IA para a decisão de processos, o que colocaria várias questões e dificuldades, até a nível constitucional;

eu/etranslation

14. Agenda da Reforma da Justiça, Almedina, capítulo 4, pág.265 a 310, José Joaquim Fernandes Oliveira Martins “coord.”, Ana Maria Marques Flórido Pinhol, António Joaquim da Costa Gomes, Carlos Miguel, Caiado Pinho, Cláudia Marina Verdial Pina de Neves Cunha, João António Filipe Ferreira, Manuel David Masseno.

- Em qualquer intervenção legislativa relativa à aplicação da IA no sistema judicial, deve sempre atender-se à Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente adotada pela CEPEJ (Comissão Europeia para a Eficácia da Justiça) na sua 31.^a reunião plenária (Estrasburgo, 3 e 4 de dezembro de 2018), bem como a outros textos e recomendações emanados de diversas outras entidades internacionais, como a ONU ou a OCDE.

3 O REGULAMENTO SOBRE A INTELIGÊNCIA ARTIFICIAL – A UTILIZAÇÃO DE FERRAMENTAS DE IA NA JUSTIÇA

Com a aprovação do Regulamento sobre a Inteligência Artificial a 13 de março de 2024, a UE deu um passo importante na definição do primeiro quadro jurídico abrangente no domínio da inteligência artificial em todo o mundo. Neste Regulamento os sistemas de IA caracterizam-se em função do risco que lhes está inerente.

Os riscos foram classificados em quatro níveis com base na sua finalidade ou utilização:

- Risco inaceitável – será proibido tudo o que for considerado uma clara ameaça para os cidadãos europeus (como reconhecimento facial em tempo real, padrões obscuros, manipulação, ou classificação social – artigo 5.º);

- Risco elevado – a conformidade do sistema de IA de alto risco será avaliada antes destes serem introduzidos no mercado, bem como durante todo o seu ciclo de vida (caso das ferramentas de IA para a Justiça, aplicação da Lei, educação, emprego, emigração – artigos 6.º a 27.º);

- Risco limitado – estão sujeitos a obrigações de transparência [caso dos robôs de conversação (*chatbots*) e *deepfakes* – artigo 52.º];

- Risco mínimo – são de livre utilização com observação de código de conduta [caso dos jogos de vídeo ou filtros de correio eletrônico não solicitado (*spam*) baseados na inteligência artificial – artigo 69.º];

Este novo Regulamento pretende garantir que os sistemas de IA utilizados na UE são seguros, transparentes, éticos e imparciais e se mantêm sob controlo humano.

Logo no seu artigo 1.º, n.º 1, o Regulamento define como seu objeto:

A finalidade do presente regulamento é melhorar o funcionamento do mercado interno e promover a adoção de uma inteligência artificial (IA) centrada no ser humano e de confiança, assegurando simultaneamente um elevado nível de proteção da saúde, da segurança e dos direitos fundamentais consagrados na Carta, incluindo a democracia, o Estado de direito e a proteção do ambiente,

contra os efeitos nocivos dos sistemas de IA na União, bem como apoiar a inovação.

No tocante à utilização de ferramentas de IA no contexto judicial, é visível no Regulamento sobre Inteligência Artificial a preocupação, já salientada noutros instrumentos internacionais, sobre os riscos que a utilização de ferramentas de IA pode comportar para os direitos fundamentais, sendo a sua maior ou menor a potencialidade de lesão que funciona como limite à utilização de sistemas de IA.

Sobre estes riscos, nomeadamente no que toca à utilização de sistemas de IA pelo Judiciário e à necessidade de adotar especiais medidas de prevenção e de conciliação com os direitos fundamentais em causa, o Regulamento dá importantes linhas orientadoras que devem, a nosso ver, desde já, mesmo antes da sua entrada em vigor, ser seguidas pelos Estados-Membros. Assim, e mais concretamente, sobre a aplicação na atividade judicial importa salientar os Considerandos:

48) A dimensão das repercussões negativas causadas pelo sistema de IA nos direitos fundamentais protegidos pela Carta é particularmente importante quando se classifica um sistema de IA como sendo de risco elevado. Esses direitos incluem o direito à dignidade do ser humano, o respeito da vida privada e familiar, *a proteção de dados pessoais*, a liberdade de expressão e de informação, a liberdade de reunião e de associação, o direito à não discriminação, o direito à educação, a defesa dos consumidores, os direitos dos trabalhadores, os direitos das pessoas com deficiência, a igualdade de género, os direitos de propriedade intelectual, *o direito à ação e a um tribunal imparcial*, *o direito à defesa e a presunção de inocência*, e o direito a uma boa administração. (...);

(59) *Tendo em conta o papel e a responsabilidade das autoridades responsáveis pela aplicação da lei, as suas ações que implicam certas utilizações dos sistemas de IA são caracterizadas por um grau substancial de desequilíbrio de poder e podem conduzir à vigilância, detenção ou privação da liberdade de uma pessoa singular, bem como ter outras repercussões negativas nos direitos fundamentais garantidos pela Carta.* Em particular, se não for *treinado* com dados de alta qualidade, não cumprir os requisitos adequados em termos de desempenho, de exatidão ou solidez, ou não tiver sido devidamente concebido e testado antes de ser colocado no mercado ou em serviço, o sistema de IA pode selecionar pessoas de uma forma discriminatória, incorreta ou injusta. Além disso, *o exercício de importantes direitos fundamentais processuais, como o direito à ação e a um tribunal imparcial, o direito à defesa e a presunção de inocência, pode ser prejudicado, em particular, se esses sistemas de IA não forem suficientemente transparentes, explicáveis e documentados.* Como tal, é apropriado classificar como sendo de risco elevado, na medida em que a sua utilização seja permitida nos termos do direito da União e o direito nacional aplicáveis, vários sistemas de IA que se destinam a ser

utilizados no contexto da aplicação da lei, no qual a exatidão, a fiabilidade e a transparência são particularmente importantes para evitar repercussões negativas, manter a confiança do público e assegurar a responsabilidade e vias de recurso eficazes. (...)

A utilização de ferramentas de IA pelas *autoridades responsáveis pela aplicação da lei* e por outras autoridades pertinentes *não deverá tornar-se um fator de desigualdade nem de exclusão*. Não se deverá descurar o impacto da utilização de ferramentas de IA nos direitos de defesa dos suspeitos, *nomeadamente a dificuldade de obter informações significativas sobre o funcionamento desses sistemas e a dificuldade daí resultante de contestar os seus resultados em tribunal*, em particular quando se trate de pessoas singulares sob investigação.

61) Determinados *sistemas de IA concebidos para a administração da justiça* e os processos democráticos deverão ser classificados como sendo de risco elevado, *tendo em conta o seu impacto potencialmente significativo na democracia, no Estado de direito e nas liberdades individuais, bem como no direito à ação e a um tribunal imparcial*. Em particular, para fazer face aos riscos de potenciais enviesamentos, erros e opacidade, *é apropriado classificar como sendo de risco elevado os sistemas de IA concebidos para serem utilizados por uma autoridade judiciária ou para, em seu nome, auxiliar autoridades judiciárias na investigação e interpretação de factos e do direito e na aplicação da lei a um conjunto específico de factos*. (...)

(...) *A utilização de ferramentas de IA pode auxiliar o poder de tomada de decisão dos magistrados ou da independência judicial, mas não o deverá substituir, a decisão final tem de continuar a ser uma atividade humana. Contudo, a classificação de sistemas de IA como sendo de risco elevado não deverá ser alargada aos sistemas de IA concebidos para atividades administrativas puramente auxiliares que não afetam a administração efetiva da justiça em casos individuais, como a anonimização ou a pseudonimização de decisões judiciais, documentos ou dados, comunicações entre pessoal ou tarefas administrativas.*

(63) A classificação de um *sistema de IA como sendo de risco elevado por força do presente regulamento não deverá ser interpretada como uma indicação de que a utilização do sistema é lícita ao abrigo de outros atos do direito da União ou ao abrigo do direito nacional compatível com o direito da União*, por exemplo, *em matéria de proteção de dados pessoais ou de utilização de polígrafos e de instrumentos semelhantes ou de outros sistemas para detetar o estado emocional de pessoas singulares*. Essa utilização deverá continuar sujeita ao cumprimento dos requisitos aplicáveis resultantes da Carta e dos atos do direito derivado da União e do direito nacional em vigor. O presente regulamento não deverá ser entendido como um fundamento jurídico para o tratamento de dados pessoais, inclusive de categorias especiais de dados pessoais, se for caso disso, salvo disposição específica em contrário no presente regulamento.” *(destacados nossos)*.

No artigo 5.º, o Regulamento, no que toca a esta aplicação em contexto de investigação e/ou aplicação da Lei, define como “Práticas Proibidas de Inteligência Artificial:

(...); d) A colocação no mercado, a colocação em serviço para esta finalidade específica ou a utilização de um sistema de IA para a realização de avaliações de risco de pessoas singulares a fim de avaliar ou prever o risco de uma pessoa singular cometer uma infração penal, com base exclusivamente na definição de perfis de uma pessoa singular ou na avaliação dos seus traços e características de personalidade. Esta proibição não se aplica aos sistemas de IA utilizados para apoiar a avaliação humana do envolvimento de uma pessoa numa atividade criminosa, que já se baseia em factos objetivos e verificáveis diretamente ligados a uma atividade criminosa;

e) A colocação no mercado, a colocação em serviço para esta finalidade específica ou a utilização de sistemas de IA que criam ou expandem bases de dados de reconhecimento facial através da recolha aleatória de imagens faciais a partir da Internet ou de imagens de televisão em circuito fechado (TVCF);

f) A colocação no mercado, a colocação em serviço para esta finalidade específica ou a utilização de sistemas de IA para inferir emoções de uma pessoa singular no local de trabalho e nas instituições de ensino, exceto nos casos em que o sistema de IA se destine a ser instalado ou introduzido no mercado por razões médicas ou de segurança;

g) A colocação no mercado, a colocação em serviço para este fim específico, ou a utilização de sistemas de categorização biométrica que classifiquem individualmente as pessoas singulares com base nos seus dados biométricos para deduzir ou inferir a sua raça, opiniões políticas, filiação sindical, convicções religiosas ou filosóficas, vida sexual ou orientação sexual; esta proibição não abrange rotulagens nem filtragens de conjuntos de dados biométricos legalmente adquiridos, tais como imagens, com base em dados biométricos ou na categorização de dados biométricos no domínio da aplicação da lei; (...)

De acordo com o artigo 6.º, n.º 2 e com o Anexo III, n.º 6, são considerados sistemas de IA de alto risco os destinados a

(...) Aplicação da lei, na medida em que a sua utilização seja permitida pela legislação nacional ou da União aplicável:

a) Sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei, ou em seu nome, ou por instituições, órgãos ou organismos da União em apoio das autoridades responsáveis pela aplicação da lei, ou em seu nome, para avaliar o risco de uma pessoa singular vir a ser vítima de infrações penais;

b) Sistemas de IA concebidos para serem utilizados por

autoridades responsáveis pela aplicação da lei, ou em seu nome, ou por instituições, órgãos ou organismos da União em apoio das autoridades responsáveis pela aplicação da lei, como polígrafos ou instrumentos semelhantes;

c) Sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei, ou em seu nome, ou por instituições, órgãos ou organismos da União em apoio das autoridades responsáveis pela aplicação da lei para avaliar a fiabilidade dos elementos de prova no decurso da investigação ou ação penal relativas a infrações penais;

d) Sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei, ou em seu nome, ou por instituições, órgãos ou organismos da União em apoio das autoridades responsáveis pela aplicação da lei para avaliar o risco de uma pessoa singular cometer uma infração penal ou reincidir não exclusivamente com base na definição de perfis de pessoas singulares na aceção do artigo 3.º, ponto 4, da Diretiva (UE) 2016/680, ou para avaliar os traços e características da personalidade ou o comportamento criminal passado de pessoas singulares ou grupos;

e) Sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei, ou em seu nome, ou por instituições, órgãos ou organismos da União em apoio das autoridades responsáveis pela aplicação da lei para definir o perfil de pessoas singulares na aceção do artigo 3.º, ponto 4, da Diretiva (UE) 2016/680, no decurso da deteção, investigação ou ação penal relativas a infrações penais.

Contudo, o artigo 6.º n.º 3, ressalva desta qualificação aquelas aplicações que envolvem menos risco, as quais coincidem com as que têm sido mais frequentemente desenvolvidas pelos diversos Estados. Assim, o Regulamento, no seu n.º 3 prevê que:

Em derrogação do n.º 2, um sistema de IA a que se refere o Anexo III não pode ser considerado de risco elevado se não representar um risco significativo de danos para a saúde, a segurança ou os direitos fundamentais das pessoas singulares, nomeadamente se não influenciarem de forma significativa o resultado da tomada de decisões.

O primeiro parágrafo aplica-se nos casos em que estiverem preenchidas quaisquer das seguintes condições:

a) O sistema de IA destina-se a desempenhar uma tarefa processual restrita;

b) O sistema de IA destina-se a melhorar o resultado de uma atividade humana previamente concluída;

c) O sistema de IA destina-se a detetar padrões de tomada de decisões ou desvios em relação a padrões de tomada de decisões anteriores e não se destina a substituir nem

influenciar uma avaliação humana previamente concluída, sem que se proceda a uma verificação adequada por um ser humano; ou

d) O sistema de IA destina-se a executar uma tarefa preparatória no contexto de uma avaliação pertinente para efeitos dos casos de utilização enumerados no anexo III.

Note-se que os sistemas de IA de alto risco não são proibidos, mas ficam sujeitos a um quadro normativo com regras mais apertadas, que garanta a conformidade destes, desde a sua criação, no seu desenvolvimento e na sua utilização.

Fica, assim, patente a intenção realista do legislador de balancear a imparável evolução tecnológica com os direitos fundamentais em causa e de procurar detalhar os riscos das aplicações de IA em função da sua utilização, nomeadamente, quando estas ferramentas funcionam como auxiliar de tarefas a cargo do juiz ou para escrutínio da atividade do tribunal, mas sem terem intervenção na formação da decisão.

Aliás, grande parte do Regulamento visa precisamente estabelecer um quadro normativo para os sistemas de IA de alto risco.

Das medidas impostas relativamente a estas aplicações ressalta o paralelismo com os princípios de *compliance* previstos no Regulamento Geral sobre a Proteção de Dados (doravante “RGPD”). Esta estreita conexão e a integração dos princípios de *compliance* com o RGPD é visível no artigo 9.º, n.º 1, onde se prevê que “deve ser criado, aplicado, documentado e mantido um sistema de gestão dos riscos em relação aos sistemas de IA de alto risco”, explicitando o n.º 2 as características deste sistema, e, mais diretamente no artigo 10.º referente à “Governança de dados e dados”. Nesta disposição legal prevê-se as medidas relativas aos dados que devem ser combinadas com os princípios do RGPD. Dispõe expressamente que:

Das medidas impostas relativamente a estas aplicações ressalta o paralelismo com os princípios de *compliance* previstos no Regulamento Geral sobre a Proteção de Dados (doravante “RGPD”). Esta estreita conexão e a integração dos princípios de *compliance* com o RGPD é visível no artigo 9.º, n.º 1, onde se prevê que “deve ser criado, aplicado, documentado e mantido um sistema de gestão dos riscos em relação aos sistemas de IA de alto risco”, explicitando o n.º 2 as características deste sistema, e, mais diretamente no artigo 10.º referente a “Dados e governação de dados”. Nesta disposição legal prevê-se as medidas relativas aos dados que devem ser combinadas com os princípios do RGPD. Dispõe expressamente que:

1. Os sistemas de IA de risco elevado que utilizem técnicas que envolvam o treino de modelos com dados devem ser desenvolvidos com base em conjuntos de dados de treino, validação e teste que cumpram os critérios de qualidade a que se referem os n.ºs 2 a 5, sempre que esses conjuntos de

dados sejam utilizados.

2. Os conjuntos de dados de treino, validação e teste devem estar sujeitos a práticas de governação e gestão de dados adequadas à finalidade prevista do sistema de IA. Essas práticas dizem nomeadamente respeito:

- a) Às escolhas de conceção pertinentes;
- b) A processos de recolha de dados e à origem dos dados e, no caso dos dados pessoais, à finalidade original da recolha desses dados;
- c) Às operações de tratamento necessárias para a preparação dos dados, tais como anotação, rotulagem, limpeza, atualização, enriquecimento e agregação;
- d) À formulação dos pressupostos, nomeadamente no que diz respeito às informações que os dados devem medir e representar;
- e) À avaliação da disponibilidade, quantidade e adequação dos conjuntos de dados que são necessários;
- f) Ao exame para detetar eventuais enviesamentos suscetíveis de afetar a saúde e a segurança das pessoas, de ter repercussões negativas nos direitos fundamentais ou de resultar em discriminações proibidas pelo direito da União, especialmente quando os resultados obtidos a partir dos dados influenciam os dados de entrada para operações futuras;
- g) Às medidas adequadas para detetar, prevenir e atenuar eventuais enviesamentos identificados nos termos da alínea f);
- h) À identificação de lacunas ou deficiências pertinentes dos dados que impeçam o cumprimento do presente regulamento e de possíveis soluções para as mesmas.

3. Os conjuntos de dados de treino, validação e teste devem ser pertinentes, suficientemente representativos e, tanto quanto possível, isentos de erros e completos, tendo em conta a finalidade prevista. Devem ter as propriedades estatísticas adequadas, nomeadamente, quando aplicável, no tocante às pessoas ou grupos de pessoas em relação às quais se destina a utilização do sistema de IA de risco elevado. Essas características dos conjuntos de dados podem ser satisfeitas a nível de conjuntos de dados individuais ou de uma combinação dos mesmos.

4. Os conjuntos de dados devem ter em conta, na medida do necessário para a finalidade prevista, as características ou os elementos que são idiossincráticos do enquadramento geográfico, contextual, comportamental ou funcional específico no qual o sistema de IA de risco elevado se destina a ser utilizado.

5. Na medida do estritamente necessário para assegurar

a deteção e a correção de enviesamentos em relação aos sistemas de IA de risco elevado em conformidade com o n.º 2, alíneas f) e g), do presente artigo, os prestadores desses sistemas podem, excecionalmente, tratar categorias especiais de dados pessoais, sob reserva de garantias adequadas dos direitos e liberdades fundamentais das pessoas singulares. Para além das disposições estabelecidas nos Regulamentos (UE) 2016/679 e (UE) 2018/1725 e na Diretiva (UE) 2016/680, todas as seguintes condições para que esse tratamento ocorra devem ser cumpridas:

- a) A deteção e a correção de enviesamentos não podem ser eficazmente efetuadas através do tratamento de outros dados, nomeadamente dados sintéticos ou anonimizados;
- b) As categorias especiais de dados pessoais estão sujeitas a limitações técnicas em matéria de reutilização dos dados pessoais e às mais avançadas medidas de segurança e preservação da privacidade, incluindo a pseudonimização;
- c) As categorias especiais de dados pessoais estão sujeitas a medidas destinadas a assegurar que os dados pessoais tratados estejam seguros, protegidos e sujeitos a garantias adequadas, incluindo controlos rigorosos e uma documentação criteriosa do acesso a esses dados, a fim de evitar uma utilização abusiva e assegurar que apenas tenham acesso a esses dados as pessoas autorizadas e com as devidas obrigações de confidencialidade;
- d) As categorias especiais de dados pessoais não são transmitidos nem transferidos para terceiros, nem de outra forma consultados por esses terceiros;
- e) As categorias especiais de dados pessoais são eliminadas assim que o enviesamento tenha sido corrigido ou que os dados pessoais atinjam o fim do respetivo período de conservação, consoante o que ocorrer primeiro;
- f) Os registos das atividades de tratamento nos termos do Regulamento (UE) 2016/679, do Regulamento (UE) 2018/1725 e da Diretiva (UE) 2016/680 incluem os motivos pelos quais o tratamento de categorias especiais de dados pessoais foi estritamente necessário para detetar e corrigir enviesamentos e os motivos pelos quais não foi possível alcançar esse objetivo através do tratamento de outros dados.

Esta disposição impõe a necessária conciliação entre o Regulamento sobre a Inteligência Artificial e os princípios do RGPD, perante os riscos que estes sistemas podem comportar para o direito à proteção de dados pessoais. Salienta a necessidade de, quando os sistemas de IA impliquem o tratamento de dados pessoais, serem respeitados os princípios consagrados no RGPD, designadamente o princípio da licitude, lealdade e transparência [artigos 5.º, 6.º, 7.º, 8.º, 9.º, 10.º considerando (39); 8.º e 52.º da carta de direitos fundamentais da UE]; o princípio da limitação das finalidades

(artigos 5.º, n.º 1, al. b) e 6.º); o princípio da limitação da conservação (artigos 5.º, 1, al. e), 9.º, n.º 2, al. j) e 89.º); o princípio da minimização dos dados [artigo 5.º, n.º 1, al. c)]; o princípio da exatidão (artigos 5.º, n.º 1, alínea d), 15.º, 16.º e 17.º); o princípio da integridade e confidencialidade (artigo 5.º, 1, al. f); o princípio da responsabilidade proativa – *accountability* (artigos 5.º, n.º 2, 24.º a 36.º) e o princípio *privacy by design and by default* (artigo 25.º e considerando 78).

O conceito de risco presente no RGPD e na ISO 31000 resulta da combinação entre a probabilidade de um evento incerto acontecer com a magnitude das consequências que resultam da sua materialização.

Nos sistemas de alto risco, como as ferramentas de IA para a Justiça e aplicação da Lei, acima descritas, a avaliação de conformidade imposta pelo Regulamento, terá de ser realizada desde a sua criação e introdução no mercado como em todo o seu ciclo de vida.

Ao encarregado da proteção de dados (usualmente designado pela sigla inglesa *DPO*), no exercício das funções elencadas no artigo 39.º do RGPD, cumpre identificar as potenciais consequências indesejáveis, ou seja, identificar os riscos de acordo com a definição do Regulamento sobre a Inteligência Artificial e com os princípios do artigo 5.º do RGPD. Após o enquadramento e a qualificação do sistema de IA como sendo de risco elevado, de risco limitado ou de risco mínimo deve o encarregado da proteção de dados aconselhar o responsável a proceder em conformidade com estes Regulamentos. Em caso de sistemas de risco elevado há que identificar os riscos, definir as medidas e quantificar o impacto para, após, emitir parecer sobre a avaliação de risco e sobre a conformidade do mesmo, como dispõe os artigos 35.º e 39.º, n.º 2, do RGPD. Cabe ao responsável pelo tratamento, mediante o parecer do encarregado da proteção de dados, a decisão sobre ou documentar e utilizar o sistema, ou reavaliar a sua utilização com vista a reduzir os impactos.

Assume particular importância o cumprimento do princípio *privacy by design and by default* (previsto no artigo 25.º e no Considerando 78) do RGPD), do qual resulta a obrigatoriedade de o responsável pelo tratamento aplicar as medidas técnicas e organizativas adequadas desde a primeira fase (no desenho) do desenvolvimento de um sistema de informação ou de um novo projeto com sistemas de IA que implique tratamento de dados pessoais, e durante toda a execução do mesmo. Para tal, é essencial o envolvimento do encarregado da proteção de dados desde o início do projeto, de forma adequada e em tempo útil, conforme resulta do disposto o artigo 38.º, do RGPD.

O desenvolvimento das aplicações de IA gerou uma verdadeira “corrida aos dados” e tal pressão sente-se, também, relativamente aos dados constantes dos processos judiciais.

Para a proteção dos dados pessoais, numa perspetiva mais pragmática e na visão do encarregado da proteção de dados do Conselho Superior da Magistratura e dos Tribunais da Relação, para além dos riscos já acima enunciados, destacam-se as seguintes questões:

- No tratamento de dados necessários para desenvolvimento destas ferramentas (abrangendo a recolha, registo, estruturação, utilização, divulgação e conservação de dados) é indispensável assegurar que as bases de dados contendo dados judiciais não anonimizados se mantêm sob tutela do Judiciário. Os princípios da responsabilidade, da segurança dos dados, da licitude e da transparência, não permitem a recolha massiva de dados dos processos judiciais para constituição de bases de dados por outras entidades que não os Tribunais, quer estas entidades sejam públicas, quer sejam privadas.

- Na qualidade dos dados, para cumprimento do princípio da minimização, da limitação da finalidade e da proporcionalidade, tem de ser assegurado que os dados tratados para desenvolvimento destas ferramentas são confiáveis e fidedignos e são os adequados, pertinentes e limitados ao que é necessário e proporcionais às finalidades daquele tratamento. O Regulamento sobre a Inteligência Artificial sublinha a importância da qualidade dos dados introduzidos para treinar a ferramenta de IA. Garantir a qualidade dos dados no desenvolvimento destas ferramentas é a única forma de evitar os perigos de preconceito induzido, enviesamento e discriminação. Como salienta a CEPEJ na citada nota informativa: “Mais importante ainda, toda a inteligência artificial é profundamente determinada pelos dados sobre os quais foi treinada: por conseguinte, nunca é neutra e, pelo contrário, incorpora todos os preconceitos, imprecisões, lacunas ou falhas contidas na base de dados de formação e/ou os preconceitos culturais de quem concebeu o sistema e orientou a sua formação através da (in)validação de algumas das suas respostas. Pode haver até mesmo casos em que o viés foi construído deliberadamente no algoritmo. A opacidade da forma como o algoritmo é programado e como os dados subjacentes são conectados leva a uma maior incompreensibilidade e, portanto, dificuldades na verificação das respostas dadas.” Se as medidas técnicas e organizativas não forem adotadas no desenho destas aplicações será muito difícil detetar o que falha no algoritmo, sendo que, como resulta das algumas experiências práticas já efetuadas noutros países nos dados introduzidos, os preconceitos, enviesamento ou discriminação induzidos pelos dados de treino são muitas vezes reforçados pelo *machine learning* num círculo vicioso difícil de cortar.

- No cumprimento do princípio da transparência. É preciso evitar a falta de transparência decorrente de modelos de *deep learning* e *black box*. Como já em 2016 alertava Giovanni Buttarelli (Autoridade Europeia de Proteção de Dados):

Uma das grandes preocupações em relação ao big data é a informação facultada aos indivíduos: transparência. Se não lhes for prestada informação adequada e entregue o controlo, as pessoas ficam «sujeitas a decisões que não entendem e sobre as quais não têm controlo». Quando são usadas máquinas inteligentes para tratar *big data*, não adianta às autoridades de proteção de dados (APD) verificar a caixa negra do algoritmo. A análise precisa de ser feita ao processo de ‘aprendizagem’ da máquina em si mesmo e aos dados inseridos (para detetar um eventual preconceito)¹⁵.

- As ferramentas utilizadas pelos tribunais devem ser desenvolvidas dentro da UE e para as finalidades específicas definidas pelo Judiciário. É de evitar a utilização pelos juízes e magistrados do Ministério Público de ferramentas de empresas que concentram demasiado poder e atuam de acordo com os seus interesses lucrativos (como a Open AI, Microsoft, Google, etc), para além de que, muitas vezes, estas estão sediadas fora da Europa. A utilização das ferramentas já desenvolvidas como as ferramentas de conversação com sistema de IA (caso do ChatGPT, do Google Bard ou do CoPilot), que sabemos serem já utilizadas em muitos tribunais, como auxílio do trabalho do juiz, não revestem os mesmos requisitos de *compliance* com o RGPD do que uma aplicação desenvolvida unicamente para essa finalidade e de acordo com as orientações dos tribunais ou dos Conselhos Superiores.

4 FERRAMENTAS DE IA DESENVOLVIDAS E/OU PROJETADAS PELO SUPREMO TRIBUNAL DE JUSTIÇA E PELO CONSELHO SUPERIOR DA MAGISTRATURA PARA OS TRIBUNAIS

A utilização das novas tecnologias e a digitalização da atividade dos tribunais (digitalização dos sistemas judiciais) é já uma realidade em Portugal. De acordo com a 11.ª Edição do Painel de Avaliação da Justiça na UE, da Comissão Europeia instrumento de acompanhamento das reformas da justiça nos Estados-Membros, relativamente à utilização de tecnologia pelos tribunais e serviços do Ministério Público, Portugal é o sexto país da UE com maior digitalização do sistema judiciário, resultados nos quais se avalia os sistemas de comunicação à distância, a gestão eletrónica de processos, a distribuição automática, o teletrabalho para juízes e o recurso a aplicações de inteligência artificial¹⁶.

Como refere Gabriela Cunha Rodrigues, Juíza Desembargadora, Chefe do Gabinete do Presidente do Supremo Tribunal de Justiça, no texto “A inteligência artificial e o projeto IRIS/SAMA no Supremo Tribunal de

15. Texto disponível na revista “Forum da Proteção de Dados”, Comissão Nacional de Proteção de Dados, n.º 04 julho, 2017, semestral.

16. Painel de Avaliação da Justiça na UE, in <https://commission.europa.eu>

Justiça¹⁷”: “O Supremo Tribunal de Justiça de Portugal tem procurado ser pioneiro na implementação de técnicas de inteligência artificial.

Apresentou uma candidatura em 2020 ao Projeto IRIS/SAMA – Informação, Racionalização, Integração e Sumarização, desenvolvido pelo INESC-ID – Instituto de Engenharia de Sistemas e Computadores e financiado através do Programa Operacional COMPETE 2020, enquadrado no Programa Portugal 2020, e pelo Fundo Social Europeu.

Está em fase final de produção e de testagem.

O âmbito do Projeto IRIS/SAMA, atualmente definido, é o desenvolvimento de ferramentas que cumpram três grandes objetivos:

- Apoio à análise de processos e elaboração de acórdãos;
- Apoio na elaboração de sumários, na sugestão de descritores, na anonimização dos acórdãos e na transcrição para formato digital de acórdãos antigos que só existam em papel;
- Divulgação pública da jurisprudência do Supremo Tribunal de Justiça através da sua publicação no site deste Tribunal, na forma de documentos previamente anonimizados.”

No âmbito deste projeto o Supremo Tribunal de Justiça visa o desenvolvimento dos seguintes serviços:

“• Serviços de «biblioteca digital», com o objetivo de disponibilizar a pesquisa e o acesso aos textos em formato digital e aos metadados das decisões proferidas pelo Supremo Tribunal e Justiça;

• Serviço de divulgação ao público em geral dos textos anonimizados dessas decisões, permitindo a sua descoberta por mecanismos variados de pesquisa e navegação em índices;

• Serviço de pesquisa restrito de Jurisprudência do Supremo Tribunal de Justiça, apenas acessível na rede interna do Tribunal, em que se permite a descoberta e o acesso aos textos das decisões não anonimizadas;

• Serviço de apoio à anonimização de acórdãos;

• Serviço de apoio à sumarização e geração de descritores de acórdãos: serviço que sugere a um utilizador que lhe forneça um texto e indica quais os parágrafos que podem ser considerados mais relevantes para uma tarefa de sumarização desse texto. Este serviço é realizado através de três módulos interligados de forma transparente para o utilizador, designadas de «Sumarizador», «Descritores» e «Interface».

• Serviço de apoio à realização de OCR (acrónimo de «Optical Character Recognition»): serviço que permite a um utilizador que lhe forneça um conjunto de imagens de apoio na tarefa de transcrição para um formato de texto editável.

17. Disponível in <https://www.stj.pt/wp-content>

Todas as soluções foram desenvolvidas utilizando código livre e, sempre que possível, código aberto.

Todas elas fazem uso de «tecnologia web», o que implica que são destinadas a ser instaladas em servidores acessíveis em redes com tecnologia normalizada da Internet e a ser acedidas através de «navegadores de www» usuais.

Já a elaboração de sumários em linguagem formal, com base no texto original do acórdão, é uma tarefa extremamente complexa, representando o desafio de maior exigência científica deste projeto.

Um sumário é uma construção intelectual única, obviamente relacionada com o texto do acórdão, mas bastante distinta no seu conteúdo.

Há que reconhecer que este desafio vai para além do estado da arte das tecnologias atuais, pelo que deveria ser reconhecidamente classificado como de investigação científica avançada.

Todas as aplicações desenvolvidas podem vir a ter um potencial de utilização mais alargado, tornando-as eventualmente úteis para outros tribunais em Portugal e noutros países, designadamente os países e territórios de língua portuguesa¹⁸.”

O desenvolvimento de aplicações de IA para pseudonimização das decisões judiciais de forma automatizada com vista à sua publicação na internet torna indispensável a fixação de regras uniformes já que o seu desenvolvimento pressupõe a fixação prévia dos critérios de seleção e a enumeração dos dados pessoais a ofuscar para desenvolvimento inicial e treino da ferramenta.

Com vista a harmonização das regras essenciais a observar, sempre que haja lugar à publicação de decisões, o Conselho Superior da Magistratura elaborou, com o contributo e em consonância com a prática do Supremo Tribunal de Justiça, um parecer aprovado por deliberação do Plenário, de 11 de abril de 2023, onde se fixaram os critérios e regras da pseudonimização, com enumeração dos dados pessoais a ocultar. Estas regras foram aprovadas para serem tidas em consideração, não só para a base de dados de tratamento de informação legal (ECLI), mas também para outras situações de publicação de decisões judiciais *online*, independentemente das plataformas ou das bases de dados utilizadas para tal finalidade¹⁹.

Outra ferramenta de IA projetada e a ser desenvolvida pelo Conselho Superior da Magistratura é o “Assistente Virtual do Juiz - Sistema de apoio à decisão”.

18. Texto citado e acessível em <https://www.stj.pt/wp-content/uploads/2024/05/Livrodigital-Inteligencia-Artificial-2023.pdf>

19. Parecer aprovado em 11 de abril de 2023, disponível em <https://www.csm.org.pt>

Ao longo dos últimos anos, tem sido notório o aumento do número e da complexidade dos casos levados aos tribunais, os quais requerem, cada vez mais, para além de conhecimento técnico especializado, um significativo trabalho de pesquisa e análise, resultando num aumento da sua morosidade. Este incremento do número e da sofisticação dos processos tem também vindo a colocar uma pressão acrescida junto dos juízes por eles responsáveis impactando a sua capacidade de tomada de decisão e potencialmente uma deterioração da qualidade da administração da Justiça. Como agravante deste cenário, tem-se verificado ao longo dos últimos anos uma diminuição significativa dos funcionários ao serviço dos tribunais, ao ponto de alguns tribunais não conseguirem, sequer, dispor do número mínimo de funcionários legalmente obrigatório, apontando as mais recentes previsões no sentido de esta tendência se continuar a verificar.

A elevada responsabilidade decisória, a necessidade de garantir a solidez das decisões dos tribunais e a imperatividade de libertar o juiz para a sua tarefa mais científica tem justificado a existência de assessores nos principais tribunais do país. Contudo, a disponibilização deste tipo de apoio a todos os tribunais não se afigura possível e representa um esforço financeiro muito elevado.

Ciente da necessidade sentida pelos juízes de suporte da sua atividade diária, este projeto visa o desenvolvimento de uma ferramenta digital que, atendendo aos mais recentes avanços na área da IA, seja capaz de prestar este auxílio.

Pretende-se que esta ferramenta, este assistente virtual, tenha um desempenho o mais aproximado possível ao auxílio prestado pelos atuais assessores humanos. O desenvolvimento desta ferramenta visa ajudar o juiz na elaboração de trabalhos de fundo e será desenvolvido enquanto aplicação autónoma ao sistema de gestão processual.

Neste contexto o assistente virtual deverá ser capaz de:

- Facilitar a extração e tratamento de informação de documentos;
- Realizar pesquisas automáticas em documentos, ou em partes de documentos; e
- Possibilitar o tratamento da informação catalogada de modo a facilitar a elaboração de decisões judiciais.

Com a implementação desta ferramenta, o Conselho Superior da Magistratura tem por objetivo:

- Reduzir o tempo com análise de documentos, de realização de pesquisas de legislação, jurisprudência e casos semelhantes;
- Reduzir os encargos administrativos com tarefas de seleção e catalogação de informação;

- Aumentar o tempo disponível, pelos juízes, para a análise de tomada de decisão;

- Diminuir a fadiga dos juízes, provocada pela execução de tarefas mecanizadas e repetitivas, melhorando deste modo a qualidade de trabalho dos juízes.

O desenvolvimento desta ferramenta já foi adjudicado e encontra-se em fase de desenvolvimento.

CONCLUSÃO

A aplicação de sistema de IA na atividade dos tribunais é uma realidade inevitável. Aceitando-se esta premissa, é esta a altura de quem tem responsabilidades de gestão e de decisão assumir a projeção, o desenvolvimento e a execução destas aplicações dentro do contexto e para as finalidades do Judiciário. Devem ser os Tribunais e os seus órgãos de gestão a definir as regras e a assegurar os direitos de quem a eles recorre para tutela dos seus direitos.

Os Tribunais têm de acompanhar os avanços da tecnologia, nomeadamente o desenvolvimento dos sistemas de IA, pois só assim estarão preparados para os desafios deste novo mundo digital. Contudo, é agora com um quadro normativo bem definido, decorrente dos Regulamentos Europeus aprovados, e ciente da importância dos princípios que se impõem que, perante cada projeto com aplicações de IA a utilizar no campo da Justiça, se deve ponderar e avaliar a conformidade com os princípios estabelecidos assegurando *ab initio* a avaliação do seu impacto de forma a implementar as medidas técnicas e organizativas necessárias a garantir os direitos fundamentais suscetíveis de serem afetados. Os direitos fundamentais, como o direito à dignidade do ser humano, o respeito da vida privada e familiar, a proteção de dados pessoais, o direito à não discriminação, o direito à ação e a um tribunal imparcial, o direito à defesa e à presunção de inocência têm de funcionar como limite e contrabalanço desta acelerada evolução a que o Fórum Económico Mundial (World Economic Forum) denominou de a “quarta revolução industrial” e que certamente irá operar a maior transformação deste século.

Como alertava Giovanni Buttarelli, Autoridade Europeia de Proteção de Dados, na 38.^a Conferência Internacional de Comissários de Proteção de Dados e da Privacidade, em outubro de 2016, numa visão que se mantém muito atual e agora ainda mais pertinente face à aceleração dos últimos desenvolvimentos, a respeito da dimensão ética e da oportunidade do momento:

“Em relação à inteligência artificial e à robótica, temos neste momento uma oportunidade crucial de nelas incorporar os valores corretos antes que se concretize uma adoção massiva destas tecnologias.

Tal exige uma nova avaliação sobre se os seus potenciais benefícios dependem verdadeiramente da recolha e análise de informação pessoalmente identificável de milhões de indivíduos. Essa avaliação poderia desafiar os investigadores a encontrarem soluções baseadas num paradigma diferente daquele usado nas máquinas inteligentes ou que, pelo menos, restringisse a utilização de dados pessoais. (...)

As autoridades de proteção de dados, sendo conhecedoras e realmente independentes, têm um papel fulcral na prevenção de um futuro em que a vida das pessoas seja determinada por inteligências artificiais que vivem na nuvem acima de nós. (...)

Não só os engenheiros, mas também os investigadores têm de começar a integrar os princípios de conceção da privacidade como o *privacy by default e privacy by design* na nova investigação, tanto de produtos como de serviços.

Como a inteligência artificial, através das máquinas inteligentes, precisa de grande volume de dados para ser eficiente, os investigadores deviam explorar a conceção e aplicação de algoritmos que ocultem as identidades e agreguem os dados, de modo a proteger o indivíduo enquanto aproveitam o poder preditivo dos mesmos dados.

É imperativo que lancemos hoje as bases para lidar com estes desafios, juntando em rede investigadores e criadores de diferentes áreas e peritos de proteção de dados a exemplo da *Internet Privacy Engineering Network* (IPEN), que contribui para um frutífero intercâmbio multidisciplinar de ideias e perspetivas.

É indispensável desenvolver um quadro ético que sustente os tijolos do ecossistema da inteligência artificial e da robótica.”

Esperamos que a efetiva aplicação do Regulamento sobre a Inteligência Artificial seja o garante dos direitos fundamentais em risco e que, para além de estabelecer o quadro normativo para toda a UE, seja também uma influência para todos os demais Estados, à semelhança do que foi o Regulamento Geral sobre a Proteção de Dados.