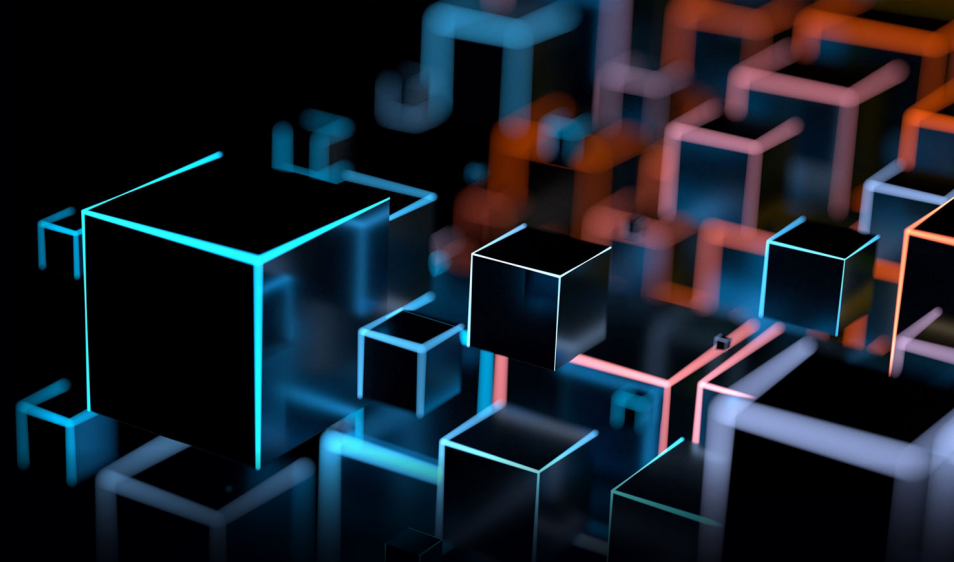




E-book CitDig

**Centro de Excelência Jean Monnet em
Cidadania Digital & Sustentabilidade
Tecnológica**

**II Congresso Ibero-Americano sobre Direito e
Tecnologias Digitais subordinado ao tema “Estado
de direito e transição digital”**

Coordenação Científica

Alessandra Silveira

Maria Inês Costa

Colaboração Editorial

Ana Cardoso

Gonçalo Matos

Bruno Saraiva

Centro de Excelência Jean Monnet CitDig é financiado pelo Programa Erasmus+ (Project 101085242).
Mais informações: <https://citdig.direito.uminho.pt/pt/>.



Universidade do Minho
Escola de Direito



INFORMAÇÕES EDITORIAIS

E-book CitDig (Centro de Excelência Jean Monnet em Cidadania Digital & Sustentabilidade Tecnológica) – II Congresso Ibero-Americano sobre Direito e Tecnologias Digitais subordinado ao Estado de Direito

Coordenação Científica:
Alessandra Silveira e Maria Inês Costa

Colaboração Editorial:
Ana Cardoso, Gonçalo Matos e Bruno Saraiva

Autores:
Alessandra Silveira | Sara Vassalo Amorim | Bruno Saraiva | Natália Gomes
Felisbela Lopes | Ana Aba | Alexandre Veronese | Inês Neves | Maria Inês Costa
Manuel Protásio | Susana Figueiredo | Francisco Garrido | Valentina Faggiani
Pedro Jacob Morais | Pedro Madeira Froufe | Ana Cardoso | Diogo Morgado
Luís Azevedo Mendes | Nuno Coelho | Joana Covelo Abreu
Paulo Novais | Larissa Coelho | Gonçalo Matos | Nuno Piçarra
Ana Maria Carmona Contreras | Francisco Pereira Coutinho | Henrique Santos

Edição:
Pensamento Sábio - Associação para o conhecimento e inovação
Universidade do Minho . Escola de Direito

Financiado pela União Europeia (Projeto 101085242 - Ações Jean Monnet - Programa Erasmus+). Os pontos de vista e as opiniões expressas são as do(s) autor(es) e não refletem necessariamente a posição da União Europeia ou da Agência de Execução Europeia da Educação e da Cultura (EACEA). Nem a União Europeia nem a EACEA podem ser tidas como responsáveis por essas opiniões.

ISBN: 978-989-36036-1-1 | DOI: 10.21814/1822.97169

Braga, setembro de 2025



Universidade do Minho
Escola de Direito



ÍNDICE

APRESENTAÇÃO	5
--------------------	---

Alessandra Silveira

SESSÃO DE ABERTURA.....	7
-------------------------	---

Sara Vassalo Amorim

PAINEL I – PLURALISMO E LIBERDADE DOS *MEDIA* – DESAFIOS AO ESTADO DE DIREITO DIANTE DA TRANSIÇÃO DIGITAL

Pluralismo e liberdade dos <i>media</i> – desafios ao Estado de direito diante da transição digital.....	11
--	----

Bruno Saraiva & Natália Gomes

Os desafios do pluralismo e da liberdade dos média diante da transição digital: o caso do Serviço Público de Média	15
--	----

Felisbela Lopes

Desinformación como problema para las democracias.....	22
--	----

Ana Aba Catoira

Hibridismo cultural e jurídico: em busca de uma nova teoria do direito para regulação dos fenômenos informacionais?	32
---	----

Alexandre Veronese

A regulação dos serviços intermediários como garantia da liberdade e pluralismo dos meios de comunicação social numa sociedade digital plataformizada.....	47
--	----

Inês Neves

PAINEL II – ENQUADRAMENTO E MECANISMOS DE COMBATE À CORRUPÇÃO – DESAFIOS AO ESTADO DE DIREITO DIANTE DA TRANSIÇÃO DIGITAL

Enquadramento e mecanismos de combate à corrupção – desafios ao Estado de direito diante da transição digital	73
---	----

Manuel Protásio & Maria Inês Costa

Transição digital e corrupção	78
-------------------------------------	----

Susana Figueiredo

Consideraciones sobre la aplicación de las nuevas tecnologías a la lucha contra el crimen organizado.....	88
---	----

Francisco Javier Garrido Carillo

La estrategia europea de lucha contra la corrupción: entre cooperación judicial y digitalización.....	108
---	-----

Valentina Faggiani

Corrupção e transição digital	123
-------------------------------------	-----

Pedro Jacob Morais

Estado de direito: notas sobre a corrupção e a transparência.....	131
---	-----

Pedro Madeira Froufe

PAINEL III – FUNCIONAMENTO DO SISTEMA DE JUSTIÇA E INDEPENDÊNCIA JUDICIAL – DESAFIOS AO ESTADO DE DIREITO DIANTE DA TRANSIÇÃO DIGITAL

Funcionamento do sistema de justiça e independência judicial – desafios ao Estado de direito diante da transição digital	142
--	-----

Ana Cardoso & Diogo Morgado Rebelo

Funcionamento do sistema de justiça e independência judicial – desafios ao Estado de direito e aos tribunais diante da transição digital.....	147
---	-----

Luís Azevedo Mendes

O digital e o Estado de direito na governação da justiça, na administração dos tribunais e na decisão jurisdicional	155
---	-----

Nuno Coelho

Sustentabilidade tecnológica e justiça eletrónica europeia numa União de direito: a interoperabilidade judiciária e o papel da inteligência artificial no domínio da justiça	175
--	-----

Joana Covelo de Abreu

O conforto do velho e a arrogância do novo: os desafios de um mundo com pressa!.....	192
--	-----

Paulo Novais

PAINEL IV – CONTROLOS E EQUILÍBRIOS INSTITUCIONAIS (CHECKS AND BALANCES) – DESAFIOS AO ESTADO DE DIREITO DIANTE DA TRANSIÇÃO DIGITAL

Controlos e equilíbrios institucionais (checks and balances) – desafios ao Estado de direito diante da transição digital	197
--	-----

Gonçalo Martins de Matos & Larissa Araújo Coelho

Checks and balances no exercício da função legislativa e da função jurisdicional da União Europeia.....	202
---	-----

Nuno Piçarra

Inteligencia Artificial y Constitución: un análisis desde la perspectiva de los controles y equilibrios institucionales	211
Ana Carmona Contreras	
A Lei dos Metadados: crónica de um fim (há muito) anunciado	218
Francisco Pereira Coutinho	
Desafios de cibersegurança no fenómeno da transição digital na Europa	234
Henrique Santos	

APRESENTAÇÃO

*Alessandra Silveira**

A Comissão Europeia publica anualmente um Relatório sobre o Estado de direito – que apresenta uma síntese da situação do Estado de direito na UE, bem como uma avaliação individualizada da situação em cada Estado-Membro. Com o referido Relatório anual a Comissão Europeia pretende detetar e prevenir desafios emergentes, bem como apoiar reformas relacionadas com o Estado de direito, sempre baseadas num contínuo diálogo com as autoridades públicas nacionais, e mediante uma ampla consulta à sociedade civil dos distintos Estados-Membros (entidades representativas, ordens profissionais, etc.).

No Relatório anual da Comissão Europeia são apreciados os desenvolvimentos do Estado de direito em quatro dimensões: *i)* funcionamento do sistema de justiça (focalizando a sua independência, qualidade e eficiência); *ii)* enquadramento anticorrupção (focalizando a efetividade das políticas nacionais de combate à corrupção); *iii)* pluralismo e liberdade dos *media* (focalizando a independência das entidades que regulam o setor, a transparência e a concentração da propriedade dos *media*, a segurança dos jornalistas e o acesso à informação, etc.), e *iv)* controlos e equilíbrios institucionais (focalizando a qualidade e abrangência do processo legislativo nacional, o papel do Tribunal Constitucional e das autoridades independentes como o Provedor de Justiça, o papel da sociedade civil nas organizações de salvaguarda de Estado de direito, etc.).

À luz desses Relatórios anuais da Comissão, no II Congresso Ibero-Americano sobre Direito e Tecnologias Digitais – organizado por CitDig (Centro de Excelência Jean Monnet em Cidadania Digital e Sustentabilidade Tecnológica) e JusGov (Centro de Investigação em Justiça e Governança), ambos da Escola de Direito da Universidade do Minho – foram abordados os desafios do Estado de direito diante da transição digital, a partir dos quatro critérios utilizados pela Comissão Europeia para avaliar a situação do Estado de direito nos distintos Estados-Membros.

Os oradores convidados a intervir representam as mais variadas perspetivas sobre o tema – dos advogados, dos governantes, da magistratura judicial nacional, da magistratura do Tribunal de Justiça, da Comissão Europeia, da Procuradoria Europeia. Mas foi contemplada também a perspetiva académica a partir de distintas mundividências (Brasil, Espanha, Portugal), de resto, verbalizada por indivíduos de distintas idades e formação de base (juristas, comunicadores, engenheiros informáticos).

Os textos dos oradores dos quatro painéis do Congresso são agora publicados neste *e-book*, antecédidos de uma apresentação da lavra de jovens investigadores associados ao Centro de Excelência CitDig (#Juniors2Seniors), que se encarregaram de fomentar o debate nos dois dias de trabalho, e agora reproduzem as inquietações verbalizadas e as pistas de reflexão recolhidas, designadamente nos seguintes painéis: Painel I – Pluralismo e liberdade dos *media* – desafios ao Estado de direito diante da

* Coordenadora Científica do Centro de Excelência Jean Monnet CitDig (Cidadania Digital e Sustentabilidade Tecnológica) da Escola de Direito da Universidade do Minho (Portugal).

transição digital; Painel II – Enquadramento e mecanismos de combate à corrupção – desafios ao Estado de direito diante da transição digital; Painel III – Funcionamento do sistema de justiça e independência judicial – desafios ao Estado de direito diante da transição digital; Painel IV – Controlos e equilíbrios institucionais (*checks and balances*) – desafios ao Estado de direito diante da transição digital.

O texto que inaugura este *e-book* corresponde à comunicação de abertura dos trabalhos do Congresso, da autoria de Sara Vassalo Amorim (DG Just, Comissão Europeia), licenciada pela Escola de Direito da Universidade do Minho, que integra atualmente a equipa responsável pela elaboração do Relatório anual da Comissão Europeia sobre o Estado de direito. Para além da dimensão simbólica que a presença de uma ex-aluna encerra, o apoio da Comissão Europeia na abertura do Congresso – e agora nesta publicação – bem ilustra a interação profícua que deve existir entre o exercício do poder público e a liberdade de pensamento crítico forjado pela academia.

Na União Europeia os académicos são financiados, precisamente, para identificar as fragilidades decisórias do poder público, e assim criticar construtivamente os desvios indesejáveis – uma lição para outras latitudes onde a liberdade académica está ameaçada, e com ela um dos pilares do controlo do poder numa sociedade democrática.

SESSÃO DE ABERTURA

*Sara Vassalo Amorim**

Ex.mos e exmas. coordenadores e coordenadoras do Congresso,
Exmos. e exmas. oradores e oradoras,
Exmas. e exmos. participantes,

É um enorme prazer poder participar neste Congresso em representação da Direcção-Geral da Justiça da Comissão Europeia, neste que é um regresso, ainda que virtual, à Escola de Direito da Universidade do Minho, onde iniciei o meu percurso académico.

Este Congresso surge oportunamente nesta fase em que se inicia um novo ciclo político na União Europeia, sendo portanto o momento de refletir sobre o papel dos direitos fundamentais e do Estado de Direito no contexto das orientações políticas e do programa da nova Comissão, e de como tal se refletirá nos Estados-Membros e no dia-a-dia de milhões de cidadãos Europeus. O Estado de Direito, além de ser um dos valores fundamentais da União Europeia consagrados no artigo 2.º do Tratado da União Europeia, desempenha um papel especial, ao garantir a proteção dos restantes valores fundamentais – um tópico que terá particular destaque durante este congresso.

O Estado de Direito é a “*garantia das garantias*”, ao assegurar o bom funcionamento das nossas democracias, da proteção dos direitos individuais e, por conseguinte, da vitalidade e da prosperidade das nossas sociedades e economias. Como afirmou o próprio Tribunal de Justiça da União Europeia, “*O valor do Estado de Direito faz parte da identidade da União em si mesma.*”

No entanto, não podemos ignorar as ameaças que põem à prova permanentemente a resiliência das sociedades e das instituições democráticas europeias. Perante grandes mudanças – sejam as crises provocadas pela COVID-19 ou pela guerra de agressão da Rússia contra a Ucrânia, ou a dupla transição ecológica e digital – os valores da União Europeia, e especialmente o Estado de Direito, permanecem fundamentais para a confiança dos cidadãos.

Ciente de que uma ameaça ao Estado de Direito num dos Estados-Membros tem o potencial de afetar o ordenamento legal e o funcionamento da União enquanto um todo, a Comissão Europeia estabeleceu como prioridade a criação de uma verdadeira política sobre o Estado de Direito a nível europeu. Assim, a Comissão tem vindo a criar vários instrumentos que lhe permitem detetar e corrigir problemas que ameacem o Estado de Direito. Por outro lado, a Comissão Europeia tem vindo a reconhecer cada vez mais a importância de uma abordagem proativa para promover e defender com êxito o Estado de Direito.

Foi neste contexto que, em 2020, surgiu um novo instrumento preventivo – o Relatório Anual sobre o Estado de Direito. Desde 2020, o relatório sobre o Estado de Direito debruça-se sobre quatro áreas chave para funcionamento do Estado de Direito – o sistema de justiça – incluindo a independência, qualidade e eficiência; o quadro de luta contra a corrupção; a liberdade e o pluralismo dos meios de comunicação; e

* Responsável pela gestão de políticas, Direcção-Geral da Justiça e dos Consumidores, Comissão Europeia.

ainda as questões institucionais relacionadas com o equilíbrio de poderes. Estas serão também, de forma geral, as áreas sobre as quais as vossas discussões incidirão durante este Congresso.

O Relatório analisa anualmente de forma sistemática e objetiva, com base numa metodologia transparente, a evolução do Estado de Direito em todos os Estados-Membros, em pé de igualdade, demonstrando que o mesmo é importante para os cidadãos e para as empresas de toda a União Europeia. O Relatório permite detetar e prevenir desafios emergentes, apoiar reformas benéficas para o Estado de Direito, mas também fomentar o debate, contribuindo assim para uma cultura de respeito e promoção do Estado de Direito. Foi com este espírito construtivo que, em 2022, a Comissão decidiu incluir no Relatório recomendações aos Estados-Membros, destinadas a apoiá-los nos seus esforços para fazerem avançar as reformas e identificar domínios em que poderão ser necessárias melhorias ou medidas de seguimento. Tendo em conta o tópico deste Congresso, gostaria de salientar que várias dessas recomendações incidem sobre a digitalização do sistema de justiça, vista como um elemento essencial para a qualidade e eficiência destes sistemas, e deste modo para garantir o direito fundamental de acesso à justiça.

Em 24 de julho deste ano, a Comissão adotou o Relatório de 2024 sobre o Estado de Direito. Agora na sua quinta edição, o Relatório Anual tem vindo a consolidar-se como um instrumento essencial para a realização da política de Estado de Direito da Comissão, revelando-se ainda determinante na promoção de reformas a nível nacional.

Após a introdução de recomendações em 2022, como referido, o Relatório tem acompanhado a resposta dada pelos Estados-Membros a essas recomendações. Embora os desafios que persistem não possam ser ignorados, e ainda que haja também situações de retrocesso e de agravamento das ameaças ao Estado de Direito, os dados mostram uma clara determinação dos Estados-Membros em refleti-las nas suas políticas públicas. Assim, em 2023, observamos que cerca de 65% das recomendações do ano anterior tinham sido implementadas, no todo ou em parte; em 2024, este número aumentou para 68%, revelando assim uma tendência positiva. A Comissão continuará a monitorizar o progresso na implementação das recomendações nas próximas edições do Relatório. Por outro lado, a Comissão permanece em contacto com os Estados-Membros, tanto a nível político como técnico, com o intuito de apoiá-los no processo de implementação das recomendações, sendo que os Estados-Membros podem também recorrer a instrumentos de apoio técnico e financeiro disponibilizados pela Comissão para proceder à sua implementação.

É positivo observar que vários Estados-Membros também se alicerçaram nas apreciações contidas nos relatórios anuais para definirem as reformas a incluir nos seus Planos Nacionais de Recuperação e Resiliência, reconhecendo assim o papel essencial do Estado de Direito para o bom funcionamento das suas economias. Este foi, por exemplo, o caso de Portugal, que incluiu a eficiência do sistema de justiça como uma das áreas prioritárias do seu Plano Nacional de Recuperação e Resiliência. Vários outros Estados-Membros aproveitaram este financiamento extraordinário para investir na digitalização dos seus sistemas judiciais e de luta contra a corrupção. Outros tipos de financiamento da União Europeia também ajudam a reforçar não só a capacidade do sistema de justiça, mas também dos meios de comunicação social e da sociedade civil para defender o Estado de Direito, juntamente com o apoio técnico e os conhecimentos especializados para reformas específicas. Estas são áreas

em que a transição digital suscita desafios particularmente pertinentes, como terão a oportunidade de debater já na vossa primeira sessão.

Cinco anos depois da primeira edição do Relatório, a Comissão encontra-se assim mais preparada para detetar, prevenir e corrigir desenvolvimentos que possam constituir uma ameaça para o Estado de Direito na União. Em razão da avaliação positiva desta abordagem preventiva baseada nas avaliações do Relatório Anual sobre o Estado de Direito, e da influência que este tem na determinação de políticas públicas ao nível dos Estados-Membros, a Comissão tem vindo a explorar o seu potencial. Assim, em 2024, pela primeira vez, o Relatório incluiu também capítulos nacionais relativos a quatro países que se encontram em processo de adesão à União Europeia – Albânia, Macedónia do Norte, Montenegro e Sérvia.

O potencial do Relatório sobre o Estado de Direito é também reconhecido nas Orientações Políticas 2024-2029 da Presidente Ursula von der Leyen, em que se prevê que o Relatório passe a debruçar-se também sobre questões relativas ao Estado de Direito suscetíveis de afetar o mercado interno, nomeadamente questões que afetem empresas, em particular PME, com operações transfronteiriças. Outra novidade incluída nas Orientações Políticas prende-se com uma maior ligação entre as recomendações do Relatório sobre o Estado de Direito e o acesso a fundos europeus. Assim, potencia-se a utilização de fundos europeus para reformas que promovam e reforcem o Estado de Direito, ao mesmo tempo que regime geral de condicionalidade para a proteção do orçamento da União – que visa proteger a boa gestão financeira do orçamento da União e os interesses financeiros da UE contra violações do princípio do Estado de direito – continuará a ser aplicado. As orientações políticas preveem ainda a possibilidade de o Relatório vir a abranger outros países candidatos, conforme a sua evolução no processo de adesão.

Permitam-me ainda salientar outro elemento essencial do Relatório: o facto de conter uma análise e recomendações concretas sobre a situação a nível nacional, faz com que o Relatório seja também um excelente ponto de partida para um diálogo alargado. A Comissão tem também tomado a iniciativa de facilitar este diálogo. Em cooperação com as Representações da Comissão nos Estados-Membros e com a Agência dos Direitos Fundamentais, a Comissão tem realizado Diálogos Nacionais sobre o Estado de Direito, em que, com base nas conclusões e recomendações do Relatório, partes interessadas provenientes de diversos quadrantes da sociedade, têm a oportunidade de dialogar entre si e com a Comissão. Portugal foi um dos primeiros Estados-Membros a receber um destes diálogos, em novembro de 2023.

Mas a promoção e a proteção do Estado de Direito não pertencem apenas às instituições europeias e autoridades nacionais – exigem um trabalho de todos nós, enquanto cidadãos. A academia desempenha um papel importante na promoção e na proteção dos valores e direitos consagrados nos Tratados da União Europeia e na Carta dos Direitos Fundamentais, ajudando a promover o Estado de direito no terreno. Iniciativas como este Congresso são também essenciais para promover o Estado de Direito, e fomentar o debate.

Mais uma vez, muito obrigada por esta iniciativa, e muito obrigada pela vossa atenção.

PAINEL I

**PLURALISMO E LIBERDADE DOS *MEDIA* –
DESAFIOS AO ESTADO DE DIREITO DIANTE DA
TRANSIÇÃO DIGITAL**

PAINEL I

Pluralismo e liberdade dos media – desafios ao Estado de direito diante da transição digital

*Bruno Saraiva**

*Natália Gomes***

A organização do poder político na União Europeia (UE) assegura a proteção dos direitos fundamentais e salvaguarda os valores democráticos, permeando todas as dinâmicas políticas, sociais e económicas internas aos Estados-Membros. Este modelo de governação multinível assegura o desenvolvimento e a implementação de políticas comuns que promovam um equilíbrio entre a soberania nacional e a cooperação leal, de modo a garantir o bom e correto funcionamento institucional e uma governação eficaz. Entretanto, desafios surgem no contexto da transição digital – que afetam, de entre tantos, a forma como o pluralismo e a liberdade dos *media* são exercidos e protegidos. Novas dinâmicas democráticas são introduzidas nas sociedades, seja na difusão de informações ou na fiscalização do exercício do poder político – e, com elas, uma necessidade de reequilíbrio de poder no ecossistema digital.

Da mesma forma que a invenção da prensa de Gutenberg facilitou a *reforma* – religiosa e depois política –, subseqüentes inovações tecnológicas permitiram a disseminação de palavras e ideias, influenciando os processos políticos e culminando em conceitos como soberania popular e Estado de direito. Estes sucessos apenas foram possíveis pela sucessiva diminuição dos custos de transação de ideias, disseminando conhecimento e pensamentos à medida que as sociedades foram reivindicando por democratização política.¹ Não é então surpreendente que a transição digital esteja a acarretar uma profunda alteração nos *media* – que, por sua vez, altera os paradigmas, soluções e equilíbrios político-sociais que ajudaram a conceber.

A realização deste potencial transformador é fundamental para preservar o princípio do Estado de direito, baluarte do funcionamento de uma sociedade democrática. Este princípio-ferramenta foi o *leitmotif* dos debates do Congresso que dá origem ao presente *e-book*, sendo consagrado nas Constituições de todos os oradores do I painel que ora apresentamos,² e aqui balizado pelos critérios identificados no Relatório do Estado de direito da Comissão Europeia (em particular a sua versão

* Estudante de Mestrado em Direito da União Europeia e Bolseiro CitDig (Centro de Excelência Jean Monnet em Cidadania Digital e Sustentabilidade Tecnológica), Escola de Direito, Universidade do Minho.

** Mestre em Direito da União Europeia e Mestre em Direitos Humanos, Escola de Direito, Universidade do Minho.

¹ Cf. Jeremy D. Popkin, ed., *Media and revolution: comparative perspectives* (Lexington: The University Press of Kentucky, 2015).

² O Estado de direito está patente no artigo 1.º da Constituição da República Federativa do Brasil e Constituição Espanhola e no artigo 2.º da Constituição da República Portuguesa e Tratado da União Europeia.

de 2024).³ Este princípio exige a sujeição do poder a normas jurídicas, criando os equilíbrios que permitam o seu controlo e escrutínio pelos cidadãos, servindo como garante constitucional ao risco de captura da *polis*.

Apesar de a evolução dos *media* estar historicamente associada à redução de custos de transação de comunicação, algo sobejamente compatível com eficiência digital, há determinadas conquistas civilizacionais que não podem ser obliteradas sob esse pretexto. A disseminação de ideias pode ser extraordinariamente poderosa – mas a monopolização dos meios através dos quais ela ocorre pode ter efeitos nefastos. Em vez de assistir na construção de sociedades democráticas, pode servir a interesses obscuros. É por isso que um esforço contínuo de diálogo, adaptação e regulamentação que coloque o ser humano – e os seus direitos – no centro da transição digital é essencial.

Nesta senda, a UE tem desenvolvido um arcabouço normativo tendente a proteger o pluralismo e a liberdade dos *media* – o que reflete o compromisso europeu com os valores democráticos e com o Estado de direito. De entre os principais instrumentos normativos destacam-se a Carta dos Direitos Fundamentais da União Europeia, o Regulamento sobre a Liberdade dos Meios de Comunicação Social,⁴ a Diretiva Serviços de Comunicação Social Audiovisual⁵ – instrumentos que foram abordados pelos oradores do I painel que ora apresentamos.

As intervenções dos oradores revelaram uma interconexão temática evidente, ainda que com diferentes abordagens e mundividências. De todo modo, destacaram a *proteção* enquanto o cerne do debate sobre o pluralismo e a liberdade dos *media*, de modo a assegurar um ambiente democrático no qual a diversidade de vozes e perspectivas possa prosperar.⁶ O interesse público na *esfera pública* e na *participação democrática* constitui um alicerce essencial para a garantia da pluralidade e para a salvaguarda das liberdades fundamentais. Ademais, esses princípios contribuem para a equidade, calcada na existência de um espaço de debate fortalecido por mecanismos sociais de supervisão e monitoramento da comunicação, uma vez que o compromisso com a verdade permanece como um imperativo na construção de uma sociedade bem-informada.

A disseminação de desinformação em larga escala, a concentração excessiva de poder digital em determinadas organizações, bem como a manipulação com fins eleitorais representam ameaças à integridade dos processos democráticos e à proteção do Estado de direito na UE e no mundo. A comunicação imparcial desempenha um papel fundamental na preservação das informações que podem facilitar o diálogo e fomentar a cooperação de diferentes grupos. Nesta medida, a confiança nas instituições democráticas e a visibilidade das ações públicas podem ser

³ Quanto ao relatório que serviu de base para este Congresso, vide Comissão Europeia, “Relatório de 2024 sobre o Estado de direito” (Bruxelas, Serviço das Publicações da União Europeia, 2024), https://commission.europa.eu/document/download/27db4143-58b4-4b61-a021-a215940e19d0_pt?filename=COM_2024_800_1_PT_ACT_part1_v1.pdf.

⁴ Regulamento (UE) 2024/1083 do Parlamento e do Conselho, de 11 de abril de 2024, que cria um regime comum para os serviços de comunicação social no mercado interno e que altera a Diretiva 2010/13/UE (Regulamento Europeu relativo à Liberdade dos Meios de Comunicação Social).

⁵ Diretiva 2010/13/UE do Parlamento Europeu e do Conselho, de 10 de março de 2010, relativa à coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à oferta de serviços de comunicação social audiovisual (Diretiva Serviços de Comunicação Social Audiovisual).

⁶ Cf. Danielle Raeijmackers e Pieter Maesele, “Media, pluralism and democracy: what’s in a name?”, *Media, Culture & Society* 37, no. 7 (2015): 1042–59, [doi:10.1177/0163443715591670](https://doi.org/10.1177/0163443715591670).

alcançadas com uma comunicação social imparcial – eis a relevância da proteção da neutralidade e do pluralismo.⁷

Entretanto, a comunicação imparcial não é suficiente, por si só, para garantir um ambiente verdadeiramente democrático. É essencial que seja inclusiva. A clareza, a acessibilidade e o entendimento de todo conteúdo transmitido revelam-se basilares para o alcance e a preservação de um espaço público democrático. Outrossim, a literacia digital e o acesso digital tornam-se decisivos para esse processo.

Importa destacar que o acesso digital deve ser pensado em conexão com a coesão territorial, de modo a evitar a influência de apenas parte da sociedade em determinadas decisões políticas. Portanto, os meios de comunicação social devem ser articulados e abrangentes, alcançado o maior número de pessoas possíveis e em vasta extensão territorial, de modo a fortalecer o serviço público e a democracia. E, se necessário for, devem ser consideradas mudanças organizacionais para controlar e vigiar a polarização da comunicação – também no que tange às plataformas digitais.⁸ Isto porque é direito de todos o acesso à informação verdadeira.⁹

Assim, a consolidação do Estado de direito na UE e o fortalecimento da resiliência democrática exigem tanto a aplicação de mecanismos institucionais, quanto uma cidadania crítica e capacitada para lidar com os desafios impostos à comunicação social pela transição digital. A negligência na garantia da veracidade das informações, o défice na educação digital, bem como a ineficiência das entidades de verificação resultam em situações que afetam a cidadania crítica e o constitucionalismo – aqui perspectivado enquanto moderação do exercício do poder em defesa dos direitos fundamentais.

Por isso a gestão de riscos sistémicos no âmbito da moderação de conteúdos revela-se essencial para equilibrar a proteção da integridade das informações – sendo desejável fazê-lo sem comprometer a inovação ou desestabilizar os modelos de negócios já estabelecidos. Como destacado por alguns oradores do I painel, o Regulamento dos Mercados Digitais (RMD)¹⁰ desempenha papel crucial na mitigação desses riscos, pois visa garantir a concorrência justa, evitando a concentração excessiva de poder nas mãos de poucas e grandes plataformas digitais, as quais exercem práticas anticoncorrenciais que limitam a diversidade de atores no setor da comunicação, por exemplo. Já o Regulamento dos Serviços Digitais (RSD)¹¹ estabelece diretrizes para a moderação de conteúdos de forma a evitar a propagação de desinformação – e assim assegurar uma comunicação transparente e responsável. Portanto, ambos os regulamentos atuam de modo a evitar que um grupo restrito controle a narrativa política e a opinião pública iniciada no espaço digital.¹²

⁷ Felisbela Lopes *et al.*, *Serviço Público de Média Livro Branco* (Lisboa: Ministério da Cultura, 2023), 25, 62, 139-142 e 165-170.

⁸ Para uma análise empírica do papel que plataformas digitais têm na polarização política e social, cf. Emily Kubin e Christian von Sikorski, “The role of (social) media in political polarization: a systematic review”, *Annals of the International Communication Association*, vol. 45, no. 3 (2021): 188-206, doi:[10.1080/23808985.2021.1976070](https://doi.org/10.1080/23808985.2021.1976070).

⁹ Para uma análise mais ampla do direito à verdade num contexto internacional, c.f. James Sweeney, “The elusive right to truth in transitional human rights jurisprudence”, *International & Comparative Law Quarterly*, v. 67, no. 2 (2018): 353 – 387, doi: [10.1017/S0020589317000586](https://doi.org/10.1017/S0020589317000586).

¹⁰ 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).

¹¹ 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).

¹² Perspectivando a ligação entre os objetivos da UE, a base legal dos Tratados usada para implementar

Esse pacote legislativo serve não apenas para regular a atividade de gigantes tecnológicos, mas também como forma de categorização e qualificação dos mesmos e dos seus processos, servindo como base conceptual para outras formas de regulamentação e operação administrativa. O atraso na transição digital da UE em comparação com os Estados Unidos ou a China, por exemplo – como assinalado pelo relatório Draghi sobre o futuro de competitividade europeia¹³ – exige que a União desenvolva uma infraestrutura conceptual capaz de enfrentar aquele desafio.

Neste diapasão, há como prever possíveis novos e futuros desafios digitais e regulá-los de forma antecipada? A chamada *regulação antecipada* surge como um modelo inovador no campo das políticas regulatórias, que busca antecipar os desafios e impactos das transformações tecnológicas – e fazê-lo antes que se consolidem como problemas sistémicos. Este modelo é abordado no curso sobre novos modelos regulatórios da Universidade de Brasília (UnB) em parceria com a União Internacional de Telecomunicações (UIT),¹⁴ tendo sido explorado por Alexandre Veronese no debate que se seguiu ao I painel deste Congresso. Em contraposição a uma regulamentação reativa, essa abordagem visa garantir um desenvolvimento tecnológico equilibrado – que não comprometa a proteção dos direitos fundamentais diante dos desafios advindos da transição digital atual e futura.

Todavia, necessário se faz a verificação de capacidades institucionais para tal, considerando a necessidade do desenvolvimento e implementação de medidas de monitoramento contínuo capazes de identificar tendências emergentes e avaliar potenciais impactos das inovações tecnológicas. Ainda assim, relevantes são os riscos associados a *regulação antecipada*, como a restrição à inovação diante da imprevisibilidade de impactos futuros; a existência de lacunas contrapondo com excessos regulatórios; a concentração do poder regulatório, etc. De todo modo, há quem entenda que a *regulação antecipada* se consolida como um instrumento essencial para a preservação do Estado de direito democrático na era digital.

Contudo, a regulamentação do digital por parte da UE, por mais sofisticada e *antecipada* que porventura seja, não garante a sua adoção uniforme nem eficaz noutras latitudes, ou seja, em distintos contextos políticos, jurídicos e económicos. Na senda de Gomes Canotilho,¹⁵ talvez seja a hora de superar o modelo hierárquico tradicional do direito, de forma a prezar pela adoção de um sistema de governação jurídica mais flexível e adaptável às dinâmicas transnacionais – ou seja, a adoção de um sistema jurídico, de uma democracia e de um constitucionalismo multinível.¹⁶

o Regulamento dos Serviços Digitais e o combate à desinformação, c.f. Judit Bayer, “The EU policy on disinformation: aims and legal basis,” *Journal of Media Law* 16, no. 1 (2024): 18–27, doi: [10.1080/17577632.2024.2362478](https://doi.org/10.1080/17577632.2024.2362478).

¹³ Comissão Europeia, “The future of European competitiveness: Report by Mario Draghi”, 9 de setembro de 2024, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf&prefLang=pt.

¹⁴ “22.º Ciclo de Palestras sobre Novos Espaços Regulatórios,” Núcleo de Direito Setorial e Regulatório da Faculdade de Direito da Universidade de Brasília, <https://sites.google.com/ccom.unb.br/ndsr/activities>.

¹⁵ José Joaquim Gomes Canotilho, *Direito constitucional e teoria da constituição*, 7. ed. (Coimbra: Almedina, 2003), 1372-1373.

¹⁶ J. J. Gomes Canotilho, “Incomensurabilidade dos discursos ou hierarquias entrelaçadas nos sistemas jurídicos multinível,” *Católica Law Review*, vol. 1, no. 1 (2017): 35-54, doi: [10.34632/CATOLICALAWREVIEW.2017.1974](https://doi.org/10.34632/CATOLICALAWREVIEW.2017.1974).

Os desafios do pluralismo e da liberdade dos média diante da transição digital: o caso do Serviço Público de Média

*Felisbela Lopes**

1. Introdução

A transição digital, marcada pelo desenvolvimento das plataformas tecnológicas e pela crescente digitalização dos meios de comunicação social, transporta consigo um conjunto de desafios que envolvem diretamente o pluralismo e a liberdade dos média. A procura de um equilíbrio entre liberdade, regulamentação e defesa do bem público dos média, sobretudo na sua vertente jornalística, é um trabalho de uma gigantesca complexidade. O poder crescente das plataformas digitais, as desordens informativas, as desigualdades no acesso digital e a crise do jornalismo são questões que se entrelaçam nesse contexto, criando um cenário no qual o Serviço Público de Média (SPM) se torna um ator crucial para a manutenção da pluralidade informativa e da liberdade de imprensa.

O poder das grandes plataformas digitais, como *Facebook*, *X* ou *YouTube*, tem moldado significativamente a esfera pública, com algoritmos e políticas de moderação de conteúdo que condicionam a visibilidade de determinadas informações, podendo até desenvolver sofisticadas formas de censura de modo completamente arbitrário. Tal tendência pode moldar uma esfera pública asfíxiada num número restrito de temas e de atores sociais, dominada por discursos polarizadores e sensacionalistas, silenciando análises aprofundadas e plurais. Esta conjuntura apresenta sérios riscos para a consolidação das nossas democracias, uma vez que a confiança nas instituições democráticas e a participação cívica estão intimamente ligadas à qualidade da informação que circula no espaço público (mediatizado).

Neste contexto, o SPM, como espaço de bem público por excelência, desempenha um papel fundamental. A sua missão é fornecer informações rigorosas, diversas e acessíveis a todos, promovendo a coesão social e territorial, além de servir como contraponto às pressões do mercado e aos interesses privados. O SPM deve ser um pilar da democracia, garantindo a todos os cidadãos acesso a uma informação que permita fortalecer uma opinião pública bem informada.

Este artigo analisa os desafios que a transição digital impõe à liberdade de imprensa e ao pluralismo, enaltecendo a importância do SPM como um vetor de defesa desses valores fundamentais. A partir da ponderação dos principais desafios da digitalização, propõe-se uma reflexão sobre as políticas públicas necessárias para assegurar a pluralidade de vozes e a diversidade de temas num cenário cada vez mais globalizado.

* Professora do Instituto de Ciências Sociais da Universidade do Minho.

2. Pluralismo e liberdade na transição digital: riscos e oportunidades

São múltiplos os desafios que a transição digital coloca ao pluralismo e à liberdade dos média. Enunciamos quatro desafios que nos parecem significativos: o poder crescente das plataformas digitais,¹ o aumento das desordens informativas,² a desigualdade no acesso ao digital³ e a crise do Jornalismo.⁴ Em contraponto, existem também oportunidades: maior acesso à informação, mais possibilidade de escrutínio/monitorização das instituições, maior transparência dos poderes, abertura a projetos jornalísticos independentes e mais inovadores.⁵

Hoje as grandes empresas tecnológicas chamam a si uma imbatível capacidade de produção e distribuição de conteúdos. Plataformas digitais como *Facebook*, *X/Twitter*, *YouTube* são espaços centrais do debate público, controlando, nessa construção, algoritmos que determinam os conteúdos mais visíveis, aplicando regras próprias para moderação daquilo que distribuem, podendo daí resultar censuras arbitrárias ou permissões que colocam em causa o bem público.⁶

Ora, esse domínio excessivo da informação difundida à escala global tem o colossal risco de asfixiar a esfera pública num redutor número de temas e de vozes que podem ser milimetricamente controlados e dobrados a discursos sensacionalistas ou polarizadores em detrimento de análises mais profundas e plurais.⁷ Neste novo ecossistema informativo, os Estados devem motivar uma regulação eficaz, promotora do respeito dos direitos fundamentais.

Por esses caudais de comunicação, a informação verdadeira mistura-se com regularidade com informação impressiva, muitas vezes falsa. E são precisamente esses conteúdos que minam a confiança nas instituições democráticas, influenciam decisões políticas e polarizam a sociedade. Não é simples equilibrar o combate às desordens informativas com a garantia da liberdade dos média. Mas é essa espécie de quadratura do círculo que os Estados são chamados a elaborar com urgência. No entanto, nem sempre se revelam capazes para tal. No discurso de despedida, o Presidente dos EUA Joe Biden disse isto: “as redes sociais estão a desistir da verificação

¹ N. Srnicek, *Platform Capitalism* (Cambridge, UK/Malden, MA: Polity, 2016); J. Meese, *Digital platforms and the press* (Intellect, 2023).

² S. Guarino, et al., “Information disorders during the COVID-19 infodemic: the case of Italian Facebook”, *Online Social Networks Media* (2021); F. Pira, “Disinformation, emotivism and fake news: Polarising impulses and the breakdown of social bonds. Why the true-to-life can seem true”, in *Information disorder: Learning to recognize fake news*, ed. F. Biondo, G. La Rocca, V. Viviana Trapani (Peter Lang International Academic Publishers, 2022), 82-86.

³ I. Alvarez-Icaza Longoria, et al., “Systematic mapping of digital gap and gender, age, ethnicity, or disability”, *Sustainability*, 14, 3 (2022): 1-20, <https://doi.org/10.3390/su14031297>.

⁴ J. Budarick, “Media, democracy and pluralism: exploring a radical response to the crisis of journalism”, *Journalism Studies* 24, 5 (2023): 594-611. DOI: 10.1080/1461670X.2023.2173959; F. Lopes, *Jornalista: profissão ameaçada* (Alêtheia, 2015).

⁵ C. Lopezosa, et al., “Journalistic innovation: How new formats of digital journalism are perceived in the academic literature”, *Journalism*, 24, 4 (2023): 821-838, <https://doi.org/10.1177/14648849211033434>.

⁶ B. García-Orosa, et al., “Algorithms and communication: A systematized literature review [Algoritmos y comunicación: Revisión sistematizada de la literatura]”, *Comunicar* (2023): 74, <https://doi.org/10.3916/C74-2023-01>.

⁷ N. Garnham, “The media and the public sphere”, in *Habermas and the public sphere*, ed. Craig Calhoun (Cambridge: MIT Press, 1992), 359-377; M. Kischinhevsky, L. Chagas, “Diversidade não é igual a pluralidade – Proposta de categorização das fontes no radiojornalismo”, *Galáxia* 1, 36 (2017): 11-24. DOI: 10.1590/1982-2554233396; P. Staab, T. Thiel, “Social media and the digital structural transformation of the public sphere” *Theory, Culture & Society*, 39(4), (2022): 129-143, <https://doi.org/10.1177/02632764221103527>.

dos factos. A verdade é sufocada por medidas contadas pelo poder e pelo lucro” (2025). E a regulamentação tem se revelado impotente para travar a fundo essa tendência.

No entanto, nem todos têm o mesmo acesso ao universo digital e essa desigualdade provoca sérias cissuras na liberdade e no pluralismo. Sendo um dos principais espaços de debate público, de troca de informações, de construção de narrativas sociais, a Internet não constitui uma ágora aberta a todos os cidadãos e a todas as temáticas, ao contrário daquilo que postulava Jürgen Habermas para um espaço público ideal. Em *Strukturwandel der Öffentlichkeit*, obra escrita nos anos 60 do século passado, Habermas reabilitava o tipo de vida burguesa, construindo, a partir dele, um modelo de *espaço público* assente na “*comunicação ilimitada*” (aberta a todas as temáticas), na “*forma pública de debate*” (não-restrição de pessoas) e na “*racionalidade*” das discussões, traços que estão muito longe daqueles que estruturam atualmente o universo digital. Constatamos hoje que o acesso ao espaço público está limitado por múltiplos constrangimentos: de acesso, de possibilidades práticas de ação, de disseminação... E isso cria divisões entre aqueles que expressam livremente as suas opiniões e aqueles que não têm essa possibilidade, sendo, assim, atirados para espirais silenciosas e marginais. Dependendo da diversidade de vozes que têm oportunidade de se exprimir livremente, o pluralismo fica assim comprometido. Tal situação facilmente conduz à hegemonia de narrativas dominantes e à invisibilidade de grupos menos favorecidos.

Sem acesso ao universo digital, os cidadãos restringem a sua capacidade para formar opiniões informadas, fortalecendo, assim, bolhas informativas. Essa exclusão digital pode funcionar como uma espécie de censura, podendo limitar a participação cívica. Ora, o Estado deve impulsionar políticas públicas capazes de combater eficazmente a desigualdade digital, garantindo também infraestruturas e uma alfabetização digital acessíveis a todos.

Todavia, é um facto que hoje o acesso à informação é mais fácil e grande parte de nós ganhou o hábito de consumir conteúdos sem nada pagar por isso. Essa situação tem tido enormes repercussões nos média jornalísticos, sobretudo impressos. A isso acresce o facto de as empresas jornalísticas não terem conseguido alcançar uma recuperação económica desde a crise financeira de 2008, dificuldades que se acentuaram depois da pandemia da COVID-19, ainda que se procurem permanentemente modos de sobrevivência.⁸ Tal conjuntura tem impactos diretos e preocupantes na liberdade e no pluralismo, com implicações várias, nomeadamente *i)* concentração da propriedade (grandes grupos dominam o setor e isso pode levar a coberturas jornalísticas alinhadas com certos interesses); *ii)* menos meios para desenvolver um jornalismo de qualidade, principalmente de investigação; *iii)* mais dependência de fontes organizadas e de *clickbait* (fontes sofisticadas revelam mais poder de agendamento noticioso e conteúdos sensacionalistas atraem mais audiência e, por consequência, geram mais receitas); *iv)* menos diversidade de vozes e de temas (visões homogêneas e comercialmente viáveis sobrepõem-se a agendas alternativas). Enfraquecendo os meios para fiscalização dos poderes e limitando a diversidade de fontes de informação, a qualidade do jornalismo reduz-se e isso constitui-se como uma ameaça à democracia. Para mitigar esses efeitos, é fundamental apoiar modelos alternativos de financiamento e instituir novas formas de regulação.

⁸ M. Sweet, *et al.* “The pandemic and public interest journalism: crisis, survival – and rebirth?”, in *Communicating COVID-19*, ed. M. Lewis, E. Govender, K. Holland (Palgrave Macmillan, 2021), https://doi.org/10.1007/978-3-030-79735-5_2.

Seria, no entanto, redutor perspetivar a transição digital enquanto um tempo asfíxiado por constrangimentos. Estamos no limiar de uma era que se enche também de oportunidades. Desde logo, temos incontestavelmente um maior acesso à informação. As plataformas digitais alargam a disseminação de informação e, por consequência, as possibilidades de conhecimento, podendo fortalecer a participação cívica. Quanto mais pessoas tiverem acesso a informação, mais se reduzem barreiras de todo o tipo: geográficas, sociais, económicas... Em caso de crise, de agitação de movimentos sociais ou de ocorrência de desastres naturais, tal possibilidade assume-se como um elemento primordial pela velocidade e pela abrangência de alcance. Há também mais possibilidade de escrutínio/monitorização das instituições, por um lado, e mais transparência dos poderes, por outro. Através de plataformas digitais, muitas instituições divulgam ações/partilham dados/anunciam decisões, aumentando a confiança e o envolvimento dos cidadãos. Tendo custos mais baixos, o digital pode igualmente ajudar o jornalismo a desafiar o monopólio de grandes grupos, fortalecendo um jornalismo independente através de projetos que exigem estruturas mais pequenas e edições contínuas.

3. O papel do Serviço Público de Média na defesa do pluralismo e da liberdade

Constituindo um elemento central das sociedades democráticas e, consequentemente, um dos pontos fulcrais para a estruturação do espaço público, o SPM deve ser um referente de qualidade nos ecossistemas mediáticos nacionais e isso só acontece se se apresentar como um lugar de independência e de confiança, um meio de coesão social, um garante da diversidade, um laboratório de inovação e de experimentalismo e um eixo de responsabilidade centrado no interesse público. Em suma, se se estruturar como um exemplo de liberdade e de defesa do pluralismo.⁹

Em contextos em que um número reduzido de grupos económicos domina a atividade mediática, particularmente o jornalismo, o SPM surge em modo de contraponto às preocupações de rentabilidade. A um jornalismo concebido como indústria ou mercadoria vendido a um mercado cada vez mais saturado de produtos concorrentes, o SPM emerge como bem público, independente de interesses diversos que possam comprometer a imparcialidade e o rigor daquilo que se transmite. Esse lugar de independência e de confiança que qualquer operador público deve procurar erguer pressupõe uma independência editorial e a construção de um jornalismo alicerçado em valores fundacionais e noutros que vão emergindo enquanto agregadores de um valor público daquilo que importa reter.¹⁰

Um operador público de média deve também preocupar-se em promover a coesão social e, por extensão, territorial. Mais do que procurar audiências ou públicos estratificados, um SPM deve estar vocacionado para servir os cidadãos que é, na verdade, o fundamento da sua existência. Esse serviço pressupõe preocupações várias. Na obra *Serviço Público de Média - Livro Branco* que coordenámos, defendemos que esse recentramento nos cidadãos pressupõe, entre outros cuidados, o seguinte:

⁹ F. Lopes, *O telejornal e o serviço público* (Coimbra: Editora Minerva, 1999); G. F. Lowe, J. Bardoel, *From public service broadcasting to public service media* (Gotenburg: Nordicom, 2008); K. Donders, *Public service media beyond the digital hype: distribution strategies in a platform era*, *Media, Culture & Society*, 41(7), (2019): 1011-1028, <https://doi.org/10.1177/0163443719857616>.

¹⁰ S. Allern, E. Pollack, "Journalism as a public good: a scandinavian perspective", *Journalism* 20 (11), (2019): 1423-1439; M. Puppis, C. Alis, "Preface", in *Public service media's contribution to society: RIPE@2021*, ed. M. Puppis, C. Alis (Nordicom, University of Gothenburg, 2023), 6-8.

conhecer e servir todos os públicos, concedendo-lhes valor estratégico; definir novas métricas de medição do impacto da atividade do operador público; desenvolver práticas de literacia mediática e promover a democracia e a coesão social.¹¹ Tendo a igualdade como princípio estruturante, um operador público de média deve cultivar a proximidade com as pessoas, procurando desenvolver laços e referências comuns. Essa preocupação deve manifestar-se em relação àqueles que habitam o território nacional, mas também, no caso de Portugal, em relação à comunidade lusófona espalhada pelo mundo. Daí a existência de canais internacionais que operam na rádio, na televisão e no digital, fomentando, assim, âncoras em todas as comunidades portuguesas. Para além de funcionar como uma espécie de cola do mundo, para retomar uma expressão cara a Michel Maffesoli,¹² os canais públicos devem ser uma espécie de elos sociais, de que tanto falam Anthony Giddens, Roger Silverstone, Jean Cazenueve, Daniel Dayan, Elihu Katz, Dominique Wolton e Dominique Mehl, atendendo, de modo especial, às novas fraturas e ao crescimento de antagonismos que marcam hoje as nossas sociedades.

Ligado intrinsecamente ao princípio da igualdade está o valor da diversidade: a igualdade será tanto maior quanto maior for a diversidade das emissões. Numa obra com mais de três décadas, Wolfgang Hoffmann-Riem¹³ identifica diferentes dimensões da diversidade: *i*) uma diversidade orientada para o indivíduo ou grupo, proporcionando-lhes oportunidades de expressão; *ii*) uma diversidade que se reflete nos temas; *iii*) uma diversidade atenta a realidades de diferentes áreas territoriais; *iv*) uma diversidade que integre numa grelha diferentes formatos. Também nos anos 90, Denis McQuail¹⁴ considerava este valor algo essencial a um operador público, separando dois níveis: o *externo*, fixado pelo espectro hertziano que cria diferentes canais para públicos diversos (diversidade estrutural); o *interno*, refletido na grelha que integra diferentes programas (diversidade organizacional).

Hoje, num ecossistema mediático em transformação contínua, qualquer SPM deve ser um espaço inovador e experimental, fomentando debates públicos diversos, impulsionando novas narrativas e formatos inovadores de artistas, criadores e jornalistas, acompanhando e absorvendo transformações de diferentes campos, sem depender da aceitação comercial ou da anuência de grandes audiências massivas. A inteligência artificial, a realidade aumentada, o jornalismo imersivo são meros exemplos de áreas a que um operador público deve prestar atenção, procurando sempre um equilíbrio entre experimentalismo e responsabilidade. Fomentar a inovação não é algo contraditório com a credibilidade e a qualidade daquilo que se produz. Pelo contrário. Implica estar na vanguarda das tendências assumindo a responsabilidade de abrir caminhos para novas formas de comunicação. O caráter experimental dos conteúdos produzidos deve estar sempre ao serviço do interesse público que é o chão onde assenta toda a atividade de qualquer operador público.

Diferentemente dos média de natureza privada que priorizam o lucro e a rentabilização das audiências, um SPM deve assumir-se como um pilar da democracia e

¹¹ F. Lopes (coord.), C. Burnay, C. A. Santos, F. Sena Santos, J. Wemans, R. Romano, S. G. Silva, *Serviço Público de Média – Livro Branco* (Lisboa: Ministério da Cultura, 2023), 191-209.

¹² M. Maffesoli, *A Transfiguração do Político: a tribalização do mundo pós-moderno*, Col. Epistemologia e Sociedade (Piaget, 2004), 136.

¹³ W. Hoffmann-Riem, “Protecting vulnerable values in the german broadcasting order”, in *Television and the Public Interest*, ed. Jay Blumler (London: Sage Publications, 1992), 49.

¹⁴ D. McQuail, “The Netherlands: safeguarding freedom and diversity under multichannel conditions”, in *Television and the Public Interest*, 100-101.

como um lugar que, em cada momento, faz a apologia do bem público. A sua atividade deve guiar-se pelo compromisso de servir a sociedade e não interesses específicos. No que à informação jornalística diz respeito, o trabalho desenvolvido deve ser rigoroso e imparcial, procurando combater desordens informativas de vários tipos e neutralizar exclusões de vários tipos, criando, para isso, espaços plurais e participativos de debate, permitindo que a sociedade discuta temas relevantes de forma informada e equilibrada. A programação de entretenimento deve ser variada e valorizadora de expressões culturais nacionais, mas também locais; integradora de produtores conceituados, mas também de produções independentes menos conhecidas. Tudo isso impulsiona os cidadãos a participarem numa sociedade livre e aberta.¹⁵

4. As propostas de um Livro Branco para o Serviço Público de Média

Redigindo este artigo numa altura em que está em discussão um novo contrato de concessão para o SPM, salientamos neste ponto algumas das propostas de um Livro Branco para o SPM escrito em 2023 por uma equipa que coordenei cujas propostas tiveram acolhimento no documento elaborado no final do ano seguinte pelo Governo. Dividido em quatro partes, a obra apresenta elementos centrais para pensar de forma mais minuciosa o pluralismo e a liberdade de um operador público no contexto da transição digital.

Logo a abrir enunciam-se as missões, os princípios e os valores de um SPM.¹⁶ Nas primeiras, integram-se, por exemplo, as seguintes missões: i) *“informar e dar a conhecer, de modo rigoroso, com isenção, independência e pluralismo, o que é relevante para a sociedade portuguesa”*; ii) *“divertir os diferentes públicos, através de conteúdos diferenciados e de qualidade”*; iii) *“promover a coesão territorial e a cidadania, contribuindo para a construção da identidade nacional aberta ao mundo, ao gosto pela diferença, e pelo debate de ideias sem preconceitos”*; iv) *“servir todos(as) os(as) cidadãos(ãs) e ser responsável perante eles(as)”*; v) *“ser motor de inovação e de transformação digital.”* Continuidade, igualdade, neutralidade e adaptação são os princípios fixados como base para valores estruturantes, como qualidade, universalidade, independência, pluralismo, diversidade, inovação, acessibilidade, prestação de contas e confiança; e novos valores, como sustentabilidade, cidadania, solidariedade e proximidade.

Na última parte, apresentam-se 75 recomendações que se agrupam em cinco blocos: transformação digital, concessionária, informação e jornalismo, conteúdos e distribuição e cidadãos. Para este artigo, interessa-nos sobretudo o primeiro, o terceiro e o quinto blocos.

O primeiro bloco é o mais sucinto, e também o mais denso, na medida em que a transformação digital não é, como afirmámos, uma opção, mas uma realidade transversal a toda a atividade de um operador, exigindo um pensamento digital permanente a diversos níveis, promovendo uma mudança radical na forma como se trabalha em todas as dimensões da produção e com implicações várias, também no pluralismo e na liberdade dos média, valores críticos, quando se pensa a informação e o jornalismo. Em contextos de desordens informativas, como aquele em que

¹⁵ UNESCO, “O jornalismo é um bem público: tendências mundiais em matéria de liberdade de expressão e desenvolvimento da comunicação social, relatório global 2021/2022”, 2021, https://unesdoc.unesco.org/ark:/48223/pf0000379826_por.

¹⁶ F. Lopes (coord.), C. Burnay, C. A. Santos, F. Sena Santos, J. Wemans, R. Romano, S. G. Silva, *Serviço Público de Média – Livro Branco*, 23-26.

vivemos, e propenso à formação de bolhas de informação, esta dimensão adquire particular importância, sobretudo num SPM, mais vocacionado para uma atividade jornalística que deve ser de rigor e de exigentes padrões.

O terceiro bloco destaca a importância da informação. Diante das desordens informativas, da polarização e das mudanças no consumo de notícias, reforça-se a necessidade de um jornalismo livre, plural, ético e analítico. O SPM deve combinar rapidez com qualidade, mediatizando variados acontecimentos e dando voz a pessoas diversas em múltiplas plataformas e inovando na forma de construir narrativas. As recomendações apontam para que a informação seja a maior prioridade do SPM, garantindo-se independência editorial, descentralizando-se a produção para além dos grandes centros urbanos e promovendo-se a liberdade e o pluralismo. Também se alerta para o facto de ser imperioso um investimento grande no digital, criando-se editorias temáticas e tendo sempre a preocupação do combate à desinformação.

O último bloco destaca a missão de servir os cidadãos de forma abrangente e inclusiva, argumentando que o conceito tradicional de *público* deve ser substituído por uma visão mais pluralista, reconhecendo os *cidadãos* na sua globalidade e as respetivas necessidades. Entre as principais recomendações, inclui-se a necessidade de conhecer melhor quem consome os diferentes conteúdos, adaptar a programação às diferentes faixas etárias, valorizar a diversidade social e cultural e promover a literacia mediática. O SPM deve ainda fortalecer a relação com a sociedade civil, colaborar com instituições académicas, desenvolver parcerias estratégicas e criar mecanismos de diálogo com escolas dos diferentes ciclos de ensino. A transparência e a participação cidadã são enfatizadas, assim como a necessidade de métricas que avaliem o impacto da atividade do operador público, apreciando de modo específico o seu compromisso social e democrático.

5. Notas finais

A transição digital apresenta desafios significativos para o pluralismo e a liberdade dos média, nomeadamente o domínio das grandes plataformas digitais, a propagação das desordens informativas, as desigualdades no acesso ao digital e a crise do jornalismo. Estes fatores podem comprometer o pluralismo e, consequentemente, a qualidade da informação que circula na esfera pública, fragilizando a democracia e a participação cívica.

Neste contexto, o SPM assume um papel essencial na defesa do pluralismo e da liberdade, garantindo acesso equitativo a conteúdos informativos diversificados, imparciais e de interesse público. A sua independência editorial, o compromisso com a qualidade jornalística e a capacidade de inovação são traços distintivos que o posicionam como um pilar democrático num ecossistema mediático cada vez mais controlado por interesses privados. No entanto, para que o SPM cumpra efetivamente sua missão, é necessário que os Estados desenvolvam políticas públicas que assegurem sua sustentabilidade e relevância. Isso inclui o reforço do financiamento e a implementação de novas formas de regulação para garantir um ambiente mediático mais transparente e plural.

Se bem regulamentada, a digitalização não deve ser encarada como uma ameaça, mas como uma oportunidade para fortalecer o jornalismo independente, expandir o acesso à informação e aumentar o escrutínio público sobre as instituições. O desafio reside em equilibrar inovação e responsabilidade, garantindo que a liberdade e o pluralismo continuem a ser valores centrais em qualquer ecossistema mediático.

Desinformación como problema para las democracias

*Ana Aba Catoira**

1. Planteamiento de un problema

La irrupción de las nuevas tecnologías asociadas al entorno digital, y en particular el uso masivo de Internet, ha revolucionado los procesos de comunicación que ya nada se parecen a aquellos otros en los que desde los medios de comunicación de masas se ejercía el periodismo entendido como un flujo de información unidireccional y controlado.

El sistema de comunicación democrático es fundamental en democracia por lo que su preservación se convierte en un objetivo prioritario que, en la actualidad, está amenazado. El Derecho internacional de los derechos humanos, el Derecho de la Unión Europea y el Constitucionalismo comparado, afirman el valor de estas libertades ligadas al significado de la democracia, pues su dimensión institucional garantiza la formación y existencia de una opinión pública libre. Esta opinión pública reviste una especial trascendencia porque se erige como una condición previa y necesaria para el ejercicio de otros derechos inherentes al funcionamiento de un sistema democrático.

En el ecosistema digital el modelo de comunicación (creación, distribución y consumo), donde los medios de comunicación tradicionales están debilitados y puestos en entredicho, no permite garantizar el ejercicio de estas libertades de expresión e información, lo que parece entrar en contradicción con las posibilidades que ofrecen las tecnologías tanto en lo que se refiere a la producción de contenidos como en el acceso a la información. Los desafíos digitales como la viralización de las informaciones, el anonimato que proporciona Internet, la segmentación de la información, las cámaras de eco, las carencias en formación y capacitación digital y la falta de regulación adecuada y suficiente, favorecen la propagación de la desinformación.

Dicho lo anterior, aparece ante nosotros el gran problema, desaparece la calidad informativa y se dificulta la exigencia de responsabilidades. En efecto, mientras que el modelo anterior se caracterizaba por un proceso comunicativo vertical y mayoritariamente profesional, el avance tecnológico ha democratizado el acceso y la participación en la comunicación, permitiendo que cualquier individuo con acceso a Internet forme parte activa del proceso (prosumidor), sin necesidad de someterse a estándares éticos, editoriales y técnicos que tradicionalmente regían la práctica periodística. Como se dice en el Informe sobre el Estado de Derecho de 2024 es esencial para el Estado de Derecho garantizar un entorno mediático libre y plural porque unos medios de comunicación libres e independientes desempeñan un papel importante como guardianes de la democracia y hacen que el poder rinda cuentas. La

* Profesora de Derecho Constitucional en la Facultad de Derecho de la Universidad de Coruña.

presión política sobre los medios no solo pone en peligro su libertad sino también la libertad de las personas para buscar, recibir y transmitir información, lo que se agrava con la concentración del mercado. En este sentido, es necesario aumentar la transparencia de la propiedad de los medios de comunicación como garantía de la libertad y el pluralismo de los medios de comunicación porque permite a las personas usuarias formarse opiniones mejor fundamentadas, pues los propietarios de los medios pueden controlar o influir directa o indirectamente en las decisiones editoriales y los contenidos informativos.

Así pues, el mayor riesgo que enfrenta la democracia en la actualidad es, en palabras de Hasen, que el público no puede determinar lo que es verdad o decidir su voto en base a información precisa, por lo que es susceptible de manipulación política a través de contenidos de relevancia electoral que pueden ser falsos o sesgados y que se viralizan utilizando la segmentación de datos y los perfiles de los usuarios.

Así pues, entre los riesgos de la desinformación podemos establecer los siguientes:

- Conduce a tomar decisiones equivocadas basadas en información falsa o engañosa con los consiguientes efectos negativos.
- Disminución de la confianza ciudadana en las instituciones y en los medios de comunicación tradicionales con su consiguiente impacto negativo en el funcionamiento del sistema.
- Aumento de la discriminación y del odio hacia determinados grupos sociales.
- División y segmentación de la sociedad cada vez más polarizada.

Según datos de la Comisión Europea de 2023 se ha reducido mucho la credibilidad de la ciudadanía hacia los diferentes canales de información. Menos de la mitad de la población europea confía en las televisiones y radios públicas siendo todavía más baja cuando se trata de prensa escrita (38%) o cuando los medios son privados (29%).

Si atendemos a las cuentas de grupos o amistades que se sigue en redes sociales descende a un 16%, Youtube o plataformas de video a un 14% alcanzando un 9% en el caso de influencers. La preocupación por la desinformación es una realidad siendo considerada un problema nacional por un 83% de los españoles y para un 86% un problema para la democracia en general. El 68% de la ciudadanía europea reconoce que ha sido expuesta a desinformación y fake news en los últimos 7 días: el 33% a veces, el 22% a menudo y el 13% muy a menudo. Este dato alcanza el 83% en España: un 29% a veces, un 31% a menudo y un 23% muy a menudo.

La probabilidad de consumir noticias falsas es más elevada en las redes sociales (64%) mientras que en los demás medios bastante menos probable: televisión (36%) periódicos y revistas online (22%), webs de videos (21%), plataformas de mensajería (17%), periódicos y revistas en papel (14%) y radio (10%). En España las redes sociales son el medio donde se percibe el mayor riesgo de consumir desinformación (57%) seguidas de la televisión (44%), periódicos y revistas digitales (28%), plataformas de mensajería (21%), prensa escrita (17%) y radio (12%).

En definitiva, la profunda transformación de los procesos comunicativos impulsada por la era digital ha supuesto avances significativos en términos de acceso y participación ciudadana, pero también ha planteado retos complejos para la preservación de los estándares de calidad informativa. Este cambio estructural exige reflexionar sobre cómo equilibrar los beneficios de un sistema más inclusivo y plural con la necesidad de garantizar una información fiable y responsable.

2. La protección de las libertades de expresión y su esencialidad democrática: la lucha contra la desinformación

En el análisis de la calidad de los procesos de comunicación es una cuestión poco menos que delicada. En efecto, se trata de analizar el alcance del ejercicio de libertades básicas para el funcionamiento de la democracia en cuanto que garantizan la participación ciudadana, el pluralismo y el control del poder y, al mismo tiempo, determinar qué medidas se pueden establecer para frenar el avance imparable de las campañas de intoxicación informativa que ponen en serio riesgo los sistemas democráticos.

La magnitud del problema es preocupante porque la desinformación ya es una amenaza estructural que se dirige directamente contra la estabilidad de las democracias y la libertad y seguridad de la ciudadanía. En la Unión Europea este problema está presente en la agenda política desde hace ya tiempo y no son pocos los esfuerzos de prevención y lucha contra las campañas de manipulación informativas dirigidas no solo a influir en la opinión pública sino a debilitar a la institucionalidad e incitar al odio y la violencia.

No obstante, el año 2016 está marcado en la historia de la desinformación, no solo por su influencia en las elecciones presidenciales de Estados Unidos, sino también porque a partir de ese momento aumentaron exponencialmente los casos de manipulación e influencia política a través de campañas montadas sobre mentiras intencionadas viralizadas en redes sociales y el consiguiente socavamiento de las instituciones.

La digitalización sirve para esta finalidad e impacta directa e intensamente en el ejercicio de las libertades de expresión e información. Como hemos indicado en el ecosistema digital, las redes sociales son las infraestructuras comunicativas de la actualidad, que se rigen por unas normas de organización y funcionamiento propias y sobre las que el control de los Estados no es eficaz además de tener diferente intensidad en el contexto europeo y en el norteamericano. El monopolio de las redes sociales, que se sirven de los algoritmos para su funcionamiento, ha impactado negativamente en los procesos de comunicación democráticos que han dejado de ser libres y plurales, introduciendo una serie de amenazas para las democracias a través de la manipulación del discurso público para satisfacer el interés económico y no el interés general.

Sin embargo, en este escenario, los Estados y las empresas multinacionales no tienen poderes equilibrados estando los primeros debilitados y diluidos frente a los gigantes tecnológicos que no solo poseen las infraestructuras sino también los datos personales. En esta situación de desequilibrio los poderes privados determinan el ejercicio de las libertades dictando sus propias normas.

En este contexto, la respuesta europea dista mucho de la norteamericana, en lógica con su historia jurídico-política, y ello impacta de forma distinta en el sistema constitucional. En Europa se aplica una perspectiva pro derechos fundamentales a través de una regulación y limitación de las libertades mientras que en los Estados Unidos rige una perspectiva a favor del mercado de las ideas que convierte a la libertad de expresión en una libertad absoluta. Lógicamente ambas concepciones se proyectan de forma distinta en la realidad digital y así el marco regulatorio europeo es profuso como también lo son los marcos nacionales que siguen la estela europea, en un escenario de confrontación entre el poder estatal y el poder de las tecnológicas que se proyecta en el abordaje de la desinformación a través de obligaciones y responsabilidades impuestas a las empresas en un marco de colaboración público-

privada. Podríamos decir que la respuesta adecuada reside en el equilibrio regulatorio que permita garantizar los valores y principios democráticos, pero sin caer en el intervencionismo “*censor*” que supondría el fin de las libertades.

En Estados Unidos, estos riesgos se enfrentan de forma peculiar debido a la arraigada tradición de libertad de expresión en internet, un contexto que se intensificó bajo el Gobierno de Trump y que, en general, favorece soluciones de mercado o autorregulación por encima de intervenciones normativas. La Primera Enmienda, interpretada de manera amplia, limita significativamente la capacidad de las autoridades para regular plataformas y contenidos, lo que supone dejar en manos de las empresas la lucha contra la desinformación y la manipulación informativa. Las reglas del mercado poco contribuyen a garantizar los procesos democráticos y el ejercicio de los derechos fundamentales si la rentabilidad económica se sigue incrementando gracias a los algoritmos.

En el análisis de la desinformación hay que establecer una clara delimitación de las libertades en juego. Como bien es sabido podemos hablar de una libertad de comunicación genérica que se desdobra en la libre expresión de pensamientos e ideas y en una libertad de información que recae sobre hechos noticiables, dos libertades con un contenido y alcance diferentes.

Así pues, la libre expresión nos permite manifestar cualquier concepción intelectual, creencias, juicios de valor, opiniones o pensamientos, a través de cualquier medio. Sin duda una libertad amplísima, pero no absoluta. Esta amplitud engloba las ideas que pueden chocar o generar repulsa a parte de la sociedad¹ y que si se refieren a personas o personajes públicos todavía disfrute de unos contornos más amplios. Además, hemos de recordar que en los sistemas que no son democracias militantes están amparadas opiniones contrarias al sistema constitucional.²

Por tanto, en el ámbito de la libertad de expresión cabe mentir, es decir, expresar opiniones que en sí mismas sean falsedades.

La libertad de información es otra cosa porque ya no se trata de difundir opinión sino un relato de la realidad de los hechos que tienen interés público y que, en este sentido, su comunicación cumple un papel fundamental para mantener a la ciudadanía informada. La libertad informativa que tiene amparo constitucional es aquella que cumple con el requisito de la veracidad, no verdad, pero sí un mínimo de diligencia informativa que asegura que no se difunden contenidos falsos o manipulados intencionadamente. La exigencia de veracidad es indiscutible y supone una garantía frente a la desinformación en el sentido de excluir las *fakes* o informaciones construidas desde la falsedad.

Resulta interesante que en el Derecho internacional la libertad de información se presenta como derivada de la libertad de expresión que integra el derecho a buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección (artículo 19 del Pacto Internacional de Derechos Civiles y Político).

El derecho a informar es una libertad y el derecho a recibir información (veraz) y, por tanto, a estar informado, se proyecta en la posibilidad de elegir entre los contenidos publicados en ejercicio del primero. Este derecho a recibir información veraz se ve amenazado en el entorno digital por varias razones como la dificultad de

¹ Sentencia STEDH *Handyside v. Reino Unido*, 7 diciembre 1976, 5493/72.

² Sentencia STC 235/2007, 7 noviembre 2007.

distinguir entre libre expresión e información y por el incremento exponencial de contenidos no verificados. Por tanto, disminuye la garantía de estas libertades.

La protección de las libertades de expresión e información es un derecho también en los entornos digitales. Por ello, como bien ha declarado el Tribunal Constitucional español, la configuración de estas libertades debe ser revisada ante la irrupción de nuevos actores en este contexto digital porque la doctrina constitucional, elaborada en torno a estas libertades, es de aplicación también cuando la comunicación se realiza a través de Internet. Ahora bien, teniendo en cuenta que concurren unas características específicas cuando la comunicación se realiza a través de estos medios y, muy concretamente, a través de las redes sociales.³

La doctrina constitucional establece los elementos que determinan si estamos ante un ejercicio legítimo del derecho a informar. En un primer orden de cosas, el requisito de la veracidad que funciona como un criterio delimitador del derecho, límite inmanente, y, en segundo orden, los límites que derivan de la existencia de otros derechos y valores garantizados en el sistema constitucional con los que esta libertad puede colisionar en un caso concreto.

El primero de los elementos o requisitos, siguiendo al Tribunal Europeo de Derechos Humanos, implica que los hechos hayan sido contrastados con la debida diligencia profesional.⁴ Por lo que ahora nos interesa, recordaremos que la veracidad no se entiende como total exactitud ni es equivalente a verdad, por lo que están protegidas aquellas informaciones que puedan resultar inexactas o erróneas si han sido contrastadas. Por el contrario, esta protección no le corresponde a quienes a sabiendas defraudan el derecho a recibir información veraz difundiendo engaños o falsedades bajo la apariencia de veracidad.

Se ha indicado la creciente preocupación de los gobiernos ante esta grave amenaza. Es cierto que el legislador español se ha preocupado por regular el funcionamiento de los medios de comunicación y el ejercicio profesional del periodismo. En este sentido, la Ley 13/2022 general de comunicación audiovisual establece expresamente el requisito de la veracidad en su artículo 9.1º cuando dice que los noticiarios y programas de contenido informativo se elaborarán de acuerdo con el derecho ciudadano a recibir información veraz y el deber de diligencia profesional en la comprobación de los hechos. En este orden de cosas, serán respetuosos con los principios de veracidad, calidad de la información, objetividad e imparcialidad, diferenciando de forma clara y comprensible entre información y opinión, respetando el pluralismo y fomentando la libre formación de opinión del público.

En este sentido, el artículo 15 de la Carta de Derechos Digitales dedicado al derecho a recibir información veraz se refiere a los prestadores de servicios intermediarios, a través de los que se ejercen estas libertades, que deben contar con protocolos para garantizar a los usuarios dicho derecho. Estos protocolos deben asegurar la transparencia de la información y las opiniones dando a conocer si han sido elaboradas sin intervención humana, si han sido clasificadas o priorizadas por el proveedor con técnicas de perfilado y si tienen carácter publicitario o han sido patrocinadas por un tercero. En la Carta se afirma el papel esencial de las plataformas en las campañas de intoxicación informativa siendo necesario que asuman responsabilidades y obligaciones para evitar convertirse en un medio de difusión viral de este tipo de contenidos y garantizar la transparencia en todo momento.

³ Sentencia STC 8/2022, 27 enero 2022.

⁴ Sentencia STC 6/1988, 21 enero 1988.

En consonancia con lo anterior y con el objetivo de crear un entorno digital libre y seguro en términos de acceso a informaciones veraces que contribuyan a el mantenimiento del sistema democrático con una sociedad informada, en la Carta de Derechos Digitales se recogen los derechos de rectificación, de oposición a técnicas de análisis de usuarios que puedan afectar a las libertades ideológicas y el derecho de la persona a solicitar la inclusión de un aviso de actualización junto a las noticias que le conciernan. La redefinición de los derechos fundamentales en los entornos digitales, a la que nos referíamos anteriormente, se proyecta en estos derechos digitales que, realmente, constituyen actualizaciones o concreciones del derecho de rectificación tradicional ahora aplicado a un nuevo ecosistema.

Estos derechos ya se recogían en la Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales. La regulación del derecho de rectificación en Internet, contenida en el artículo 85, establece que los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio de rectificación ante los usuarios que difundan contenidos que atenten contra los derechos de la personalidad en Internet y el derecho a comunicar o recibir libremente información veraz.

Entendemos que este derecho sirve para reaccionar frente a informaciones falsas dolosamente o negligentemente, pero, el ejercicio de este derecho de rectificación frente a las informaciones inexactas que perjudican a la persona interesada (no todas las noticias falsas son inexactas pueden ser engañosas o sesgadas) solo cabe frente a los medios de comunicación no frente a personas o entidades.

En su artículo 86 recoge el derecho a la actualización de informaciones en medios digitales que no parece adecuado para frenar la desinformación porque se piensa en noticias que son correctas, pero que se quedan anticuadas con el paso del tiempo perjudicando a alguna persona (decisión judicial que revoca otra anterior).

En definitiva, sucede que estos derechos no son exigibles frente a esta suerte de periodismo ciudadano que nos asola, entendido como las noticias que producen y divulgan personas que no son profesionales de la información en ejercicio de su derecho a comunicar recogido en el artículo 20.1º, d) de la norma constitucional, pero sin sujeción a los códigos deontológicos del periodismo tradicional. En efecto, resulta complicado exigir algún tipo de responsabilidad por no cumplir con la veracidad de la información. Y tampoco, como se ha dicho, cabe ejercitar el derecho de rectificación configurado como protección frente a la divulgación de noticias a través de los medios de comunicación social.

Por tanto, aquí encontramos un elemento a favor de la diseminación de noticias falsas.

En este contexto de desórdenes informativos concurre otro elemento que favorece la desinformación: los intereses geopolíticos. Desde países poco o nada democráticos se recurre frecuentemente a las estrategias de desinformación para influir en la sociedad, la política y la economía, e incidir notablemente en la opinión pública. Los procesos electorales, los conflictos bélicos o una pandemia, han estado y están determinados por las campañas de manipulación intencionadas que se sirven de una industria a su servicio. Los datos que proporciona el Servicio Europeo de Acción Exterior en su informe sobre interferencia y manipulación extranjera son esclarecedores.

En materia de desinformación consideramos que los gobiernos mantienen dos tipos de respuestas que obedecen a diferentes perspectivas o formas de abordar este

problema. Por una parte, aquella que aborda la manipulación informativa desde un enfoque de derechos fundamentales y que apuesta por garantizar su ejercicio efectivo y no regular excesivamente para no caer en restricciones injustificadas; y, por otra, desde una perspectiva de seguridad, que responde a las interferencias extranjeras.

Estamos convencidas de que los retos jurídicos que plantea la digitalización de la comunicación no deben ser respondidos con medidas restrictivas de derechos sino con la aplicación de las reglas ya existentes al entorno digital. La desinformación, ya catalogada como grave problema estructural, requiere de soluciones para proteger los valores y principios sobre los que se asienta nuestra convivencia, pero, en ningún caso, estas soluciones deben conllevar más problemas en forma de vulneración de derechos fundamentales, restringiendo el acceso a contenidos digitales a través de bloqueos o de supresión. Tampoco la opción de establecer una verdad oficial parece adecuada en democracia sobre todo en democracias no militantes.

Ya los Relatores internacionales para la libertad de expresión afirmaron que las prohibiciones generales de difusión de información basadas en conceptos imprecisos y ambiguos, incluidos noticias falsas o información no objetiva, son incompatibles con los estándares internacionales sobre restricciones a la libertad de expresión y deberían ser derogadas.⁵

Así nos encontramos ante un obstáculo, es decir, cómo definimos la desinformación, cómo se determina qué es desinformación y qué no lo es, para no restringir injustificadamente el ejercicio de la libertad a través del control de contenidos.

La institucionalización de la lucha europea contra la desinformación se formalizó en 2015 a partir de la campaña rusa para desestabilizar Ucrania y la ocupación de Crimea. A partir de este momento se adoptan diferentes medidas desde la afirmación por el Consejo Europeo de la necesidad de contrarrestar las campañas de desinformación procedentes de Rusia. Ese año se creó el Grupo de Trabajo East StratCom, adjunto al Servicio Europeo de Acción Exterior, para la comunicación de las políticas y actividades de la Unión Europea en Rusia y que se enmarca proyecto denominado EU vs Disinformation.

A partir de 2015 se aprobaron diferentes medidas y ya, en 2018, en el seno de la Comisión Europea, se constituyó un grupo de expertos de alto nivel (HLEG) para asesorar sobre las acciones a realizar para luchar contra la desinformación. En este marco de trabajo se alcanzan algunas conclusiones respecto a las líneas de actuación: aumentar la transparencia de las publicaciones garantizando la privacidad de los datos; fomentar la alfabetización mediática e informacional para generar entornos seguros; capacitación digital contra la desinformación; fomentar la investigación sobre el impacto de la desinformación en Europa, evaluando las medidas para establecer las respuestas adecuadas.

Este mismo año se aprobaron dos comunicaciones de la Comisión Europea siendo una de ellas la Comunicación sobre la lucha contra la desinformación en línea. En el marco del Plan Europeo contra la Desinformación se aprobó el Código de Buenas Prácticas de la Unión en materia de desinformación que entró en vigor ese 2018.

⁵ Organización de los Estados Americanos, “Declaración conjunta sobre libertad de expresión y noticias falsas, desinformación y propaganda”, 2017, consultado en febrero 24, 2024, <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1056&IID=2>.

El año 2020 fue el año del COVID-19, una pandemia que protagonizó infinidad de informaciones falsas que intoxicaron a una sociedad mundial vulnerable. La Comisión Europea adoptó la Comunicación titulada *“La lucha contra la desinformación acerca de la COVID-19, y puesta en marcha del programa de vigilancia de la desinformación relativa a la COVID-19”* como primera medida de reacción frente a la intoxicación informativa que fue calificada como *“infodemia”* desde la OMS. La creación ese mismo año del Observatorio Europeo de Medios Digitales (EDMO) integrado por agencias de verificación, academia y universidad, además de otros grupos de interés relevantes, persigue promover investigaciones sobre el fenómeno de la desinformación.

El Plan de Acción para la Democracia Europea busca reforzar las democracias europeas frente a los desafíos que plantea la desinformación durante los procesos electorales y en la garantía de las libertades de expresión e información con instrumentos adecuados contra las interferencias extranjeras. A finales del 2020 el Parlamento Europeo aprobó una resolución *“sobre el refuerzo de la libertad de los medios de comunicación: protección de los periodistas en Europa, discurso del odio, desinformación y papel de las plataformas”* donde se recalca la necesidad de proteger a los medios de comunicación y la seguridad de los profesionales.

Frente al papel de las plataformas como propagadoras de desinformación se insiste en la necesidad de adoptar medidas legislativas en orden a aumentar la transparencia y la responsabilidad de las plataformas, así como programas con medidas que fomenten el periodismo de calidad independiente. La importancia de la alfabetización mediática y la educación digital de la ciudadanía como herramientas para protegerse frente a la desinformación.

Ya en junio de 2022 se aprobó una actualización mejorada del Código de buenas prácticas en materia de desinformación, el Código de Prácticas Reforzado, con 18 firmas más que la versión de 2018. Sus firmantes, las plataformas, empresas de publicidad, verificadores, sociedad civil y organizaciones especializadas en desinformación; y entre sus medidas reforzadas: el incremento de la participación de plataformas y verificadores, la reducción de incentivos económicos como ingresos publicitarios para difundir desinformación, atender a nuevas formas de manipulación como son las cuentas falsas, bots o ultrafalsificaciones, reforzar la alfabetización mediática de las personas usuarias, garantizar la transparencia de la publicidad política además de la creación de un grupo de trabajo y un centro de transparencia. El consejo asesor de contenido de Facebook-Meta actúa a modo de tribunal que revisa las decisiones de la empresa cuando se alegue afectación de derechos individuales o colectivos de las personas usuarias.

La posición europea es más intervencionista que la norteamericana, por lo que la autorregulación, los códigos de conducta, los mecanismos internos de resolución de conflictos, las políticas de uso, etc., se complementan con las medidas legislativas como el Reglamento Europeo de Servicios Digitales (DSA) que busca la supervisión de las actividades de las plataformas para proteger los intereses públicos y los derechos fundamentales de las personas. Con el fin de preservar la integridad de los procesos democráticos y de proteger derechos fundamentales, las normas europeas buscan la supervisión algorítmica, es decir, poder someter a un escrutinio los algoritmos y sistemas de IA que incidan de manera significativa en la formación de la opinión pública. Para alcanzar este objetivo, la DSA introduce obligaciones específicas de transparencia y responsabilidad para grandes plataformas (VLOPs), exigiéndoles la implementación de mecanismos de gestión de riesgos sistémicos y auditorías

periódicas. Este enfoque pretende atajar la manipulación política y la difusión de desinformación a gran escala, garantizando un acceso plural a la información.

Pero, en el cumplimiento de las reglas de moderación de contenidos pesan mucho los intereses propios de las empresas. Tras los atentados de Hamás del 7 de octubre de 2023, con la difusión de terribles imágenes y videos en redes sociales, la Comisión instó a las empresas a llevar a cabo un mayor control y vigilancia sobre las notificaciones falsas publicadas. Sin embargo, acogiéndose a la libertad de expresión y al principio de neutralidad, defienden la política empresarial y deciden libremente sobre los contenidos que publican. En esta línea, el dueño de X defiende su modelo de negocio que se sirve de la mentira y la desinformación, argumentando la utilización de código abierto y transparente.

En 2023 se aprobó la Resolución del Parlamento Europeo “*sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación*”, donde se aborda como, a través de la desinformación, se producen injerencias de terceros en los procesos democráticos. En 2024 el Parlamento aprobó la *European Media Freedom Act* (EMFA), que la Comisión aprobó en 2022, que contiene un conjunto de normas para garantizar la libertad, el pluralismo y la independencia editorial en los medios de comunicación en el entorno digital.

La desinformación ha aumentado de forma exponencial gracias a la digitalización y a la inteligencia artificial específicamente. Por ello, aunque no se trate de una medida específica dirigida a la lucha contra este fenómeno, es interesante conocer las regulaciones contenidas en el Reglamento Europeo de Inteligencia Artificial relacionadas con la desinformación. La norma europea contempla la generación de imágenes o videos falsos muy realistas y deepvoice o voz humana sintética que son herramientas que favorecen la manipulación. El Reglamento sigue un enfoque basado en los riesgos de los sistemas que se clasifican como de riesgo inaceptable, riesgo alto y riesgo bajo o mínimo.

Entre los sistemas prohibidos se engloban aquellos que utilizan técnicas subliminales que alteran el comportamiento provocando o siendo probable que provoquen daños físicos o psicológicos o los sistemas que aprovechen vulnerabilidades de un grupo específico para alterar su comportamiento y provocar daños.

La norma establece requisitos y obligaciones específicas de transparencia para los sistemas de alto riesgo que pueden resultar muy lesivos para los derechos fundamentales y la seguridad como son aquellos que generan o manipulan contenidos (ultra falsificaciones) que tendrán que proporcionar información suficiente para identificar que contenidos están creados artificialmente.

Dentro de esta batería normativa se sitúa el Reglamento Europeo sobre Transparencia y Segmentación de la Publicidad Política, que dispone requisitos muy estrictos en la publicidad segmentada. En este sentido, prohíbe la utilización de datos sensibles para fines de microsegmentación política y exige la trazabilidad de la publicidad en repositorios públicos.

Siguiendo el Informe de Naciones Unidas para contrarrestar la desinformación podemos hacer dos grupos de propuestas, unas dirigidas a los Estados y otras a las empresas que son las principales difusoras de desinformación dado su modelo de negocio.

Los Estados deben:

- Proteger y garantizar la libertad de expresión, el acceso a la información y el pluralismo de los medios de comunicación;

- Evitar las regulaciones basadas en definiciones vagas, imponer sanciones desproporcionadas y no criminalizar nunca los contenidos legítimos;
- Abstenerse de los cierres/bloqueos de Internet de sitios web y puntos de venta;
- Asegurarse de que desde las instituciones se comparte información veraz y exigir responsabilidades a las autoridades que difundan información falsa;
- Involucrar a la sociedad civil en el diseño de políticas y otros esfuerzos destinados a contrarrestar la desinformación como son los verificadores de noticias.

Las empresas tecnológicas deben:

- Evitar que sus actividades provoquen o contribuyan a provocar consecuencias negativas sobre los derechos humanos y que hagan frente a esas consecuencias cuando se produzcan;
- Divulgar políticas y prácticas pertinentes para contrarrestar la desinformación;
- Revisar sus modelos de negocio para asegurarse que respetan los principios de los derechos humanos;
- Garantizar una mayor transparencia y facilitar el acceso a los datos y la información pertinentes;
- Velar para que sus prácticas de moderación de contenidos sean coherentes y cuenten con recursos suficientes en todos los lugares en los que operan y en todos los idiomas pertinentes.

En definitiva, contamos con abundante regulación, pero su eficacia práctica se ve dificultada por la dimensión transnacional de las plataformas cuyo alcance no se limita a la Unión Europea siendo necesario establecer estándares globales y acuerdos basados en la cooperación público-privada. A modo de cierre, solo nos queda insistir en que la desinformación es ya un grave problema estructural que afecta a todas las sociedades tanto desde dentro como desde fuera. Las medidas para luchar contra ella deben ser variadas y aplicarse de forma coordinada en un abordaje integral de este fenómeno.

En todo caso, como ya hemos señalado, consideramos que, en lugar de imponer restricciones, se debe optar por otro tipo de medidas positivas que fomenten la comunicación de calidad que genera la confianza de la ciudadanía en el funcionamiento de nuestro sistema y deben implementarse desde tres ámbitos fundamentales: las empresas tecnológicas, la sociedad civil y las instituciones académicas.

En definitiva, queda mucho por hacer, pero sin concienciación y compromiso público y privado no será posible.

Hibridismo cultural e jurídico: em busca de uma nova teoria do direito para regulação dos fenômenos informacionais?

Alexandre Veronese *

1. Introdução

As ciências sociais, na atualidade, já possuem, cada vez mais, uma visão clara de que o mundo social não deveria ser separado das interações comunicacionais existentes por meios das novas tecnologias da informação e da comunicação. Essa é a visão de Lee Rainie e Barry Wellman para a sociologia, por exemplo.¹ As pesquisas da área de comunicação, também, já possuem uma literatura que aponta para essa conclusão.² As vidas humanas são digitais e, ao mesmo tempo, não-digitais. Nos primórdios do fenômeno, ainda havia autores das ciências sociais que identificavam esse aparecimento como uma novidade. A noção filosófica de virtual ou de inteligência coletiva, tão bem descritas por Pierre Lévy, evidenciam isso.³ Porém, com o passar dos anos, ficou evidente, em especial com a obra de Manuel Castells, que a visão reticular da vida social iria impor desafios novos aos pesquisadores, apesar das críticas que são dirigidas aos excessos no uso desse conceito.⁴ Porém, o mundo jurídico continuou a trabalhar com a perspectiva teórica de sistemas jurídicos logicamente perfeitos, apesar de suas imperfeições para aplicação de meios regulatórios. A frase mais comum ainda é “o direito sempre estará atrasado em relação aos avanços tecnológicos.” Para lidar com esse dilema, a teoria contemporânea da regulação – que sempre foi mais ampla do que a teoria jurídica clássica – começou a produzir soluções.⁵

* Professor de Teoria Social e do Direito da Universidade de Brasília. Membro do Centro de Excelência Jean Monnet em Cidadania Digital e Sustentabilidade Tecnológica da Universidade do Minho (Portugal).

É necessário agradecer aos meus alunos e minhas alunas das disciplinas de Direito, Internet e Sociedade, bem como de Sociologia do Direito, lecionadas ao longo dos anos, na graduação e na pós-graduação da Universidade de Brasília. Sem as suas observações, eu jamais teria me debruçado sobre esse tema de pesquisa da mesma forma. Igualmente, agradeço à Universidade de Brasília pelo período outorgado de licença para capacitação que permitiu essa pesquisa. Ainda, agradeço a recepção na Universidade do Minho (Portugal) e na *Vrije Universiteit Brussel* (Bélgica). Por fim, é necessário agradecer ao meu anfitrião, na licença, Professor Fernando de Castro Fontainha, o qual me recebeu no Instituto de Estudos Sociais e Políticos da Universidade do Estado do Rio de Janeiro, contribuindo significativamente para a concretização dessa pesquisa.

^{**} Uma versão deste artigo redigida em língua inglesa foi publicada na Revista *UNIO - EU Law Journal* (Vol. 11, No. 1, June 2025).

¹ Lee Rainie and Barry Wellman, *Networked: the new social operation system* (Cambridge, MA: The MIT Press, 2014).

² Andrew Chadwick, *The hybrid media system: politics and power* (Oxford: Oxford University Press, 2017).

³ Pierre Lévy, *Cyberculture* (Minneapolis: University of Minnesota Press, 2001). Pierre Lévy, *Collective intelligence: mankind's emerging world in cyberspace* (Rutgerlen: Platum Trade, 1997).

⁴ Manuel Castells, *The information age: economy, society, and culture*, 3 volumes (Hoboken: Wiley, 1999).

⁵ Jonathan E. Nuechterlein and Philip J. Weiser, *Digital crossroads: telecommunications law and policy in the internet age*, 2.^a ed. (Cambridge, MA: The MIT Press, 2013).

A ideia de governança transnacional e multissetorial foi uma delas. Ela deu azo para a construção de estruturas globais de gestão, assim como já havia normas técnicas para lidar com problemas que não conhecem fronteiras. Um veículo que se pretenda global precisa ser apto a transitar em estradas de diversos países com os mesmos níveis de segurança. Os padrões de qualidade para fármacos ou insumos médicos fornecem outro exemplo. Eles precisam ser seguros para uso por diversas pessoas diferentes em escala global. Logo, existem sistemas de certificação para tanto. Todavia, os sistemas jurídicos sempre estiveram definidos por alguns elementos que os relacionam com os Estados-nação, apesar de sabermos que existem normas privadas que possuem uso social ao largo dos Estados. É evidente que os Estados não desapareceram. Porém, os meios de responder aos fenômenos sociais trazidos pelas novas tecnologias da informação e da comunicação mostrou os seus limites. A pretensão do presente estudo é grande. Ele visa propor um novo conceito de Estado de Direito (*Rule of Law*), que possa lidar com esses fenômenos. A conclusão pode ser adiantada. A proposta é uma mescla do conceito de Estado-em-Rede, de Manuel Castells⁶ com o conceito de hibridismo cultural de Néstor García Canclini⁷ e de Peter Burke.⁸ A postulação conclusiva é clara: as sociedades somente conseguirão produzir regulação em dois cenários possíveis. Os dois cenários exigem alguma concessão de soberania. O primeiro cenário seria marcado pela abertura internacional, de cunho global dos sistemas jurídicos nacionais. Ela seria definida pela adesão e integração de quase duas centenas de Estados-nação em tratados internacionais, com plena efetividade. Essa solução preservaria o caráter tradicional do conceito de Estado de Direito, tal como vem ocorrendo há alguns séculos. Porém, existe uma crise no sistema de governança global. O segundo cenário seria a reformulação do conceito de Estado de Direito para abranger o conceito de híbrido cultural e jurídico, que é uma forma reelaborada de pluralismo jurídico. Esse Estado de Direito, aberto aos influxos normativos de outras fontes, teria que aceitar e incorporar várias normas externas, mesmo que fossem conflitantes com estipulações de direito nacional. Inclusive normas técnicas, normas sociais e práticas econômicas, entendidas como forças normativas. Um caminho para amenizar esses processos de “interferência” de outras “soberanias” sem anuência prévia em relações sociais seria o conceito de hibridismo cultural e jurídico, que é a proposição dessa pesquisa. O texto possui a seguinte estrutura. Na parte subsequente, será analisado o dilema da regulação atual de fenômenos novos. Essa parte tratará, também, da parte central da pesquisa, que é a demonstração do problema. Esse problema é o conceito de sistema jurídico nacional e de ordem jurídica internacional, com seus reflexos regulatórios. Depois, serão indicados os limites jurídicos dos meios tradicionais de resolução de conflitos, seja por meio do direito internacional público (decisões de órgãos multilaterais, por exemplo), seja por meio do direito internacional privado (a aceitação de normas estrangeiras para a solução de problemas específicos, por exemplo).

2. Regulação? Nacional, internacional ou transnacional?

Os conceitos de regulação nacional, internacional e transnacional não são novidades, mesmo no mundo da Internet.⁹ Os dois primeiros são mais novos do

⁶ Manuel Castells, *Communication power*, 2.^a ed. (Oxford: Oxford University Press, 2009).

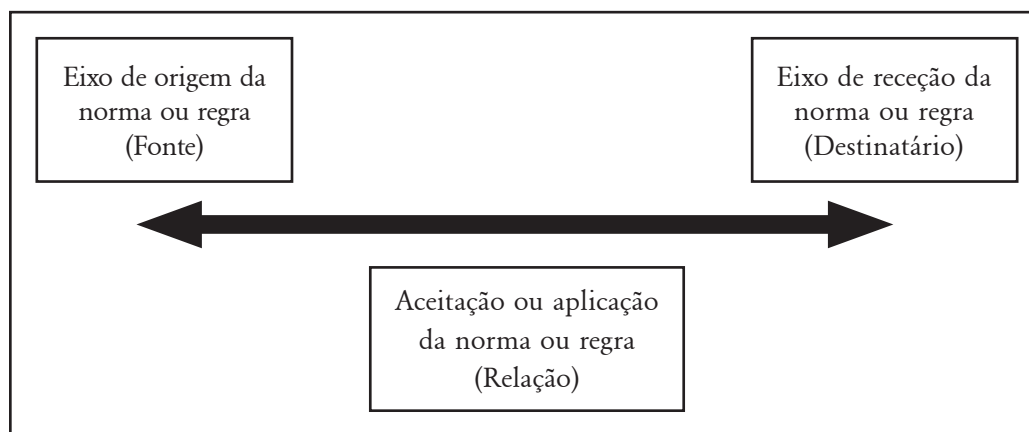
⁷ Néstor García Canclini, *Hybrid cultures: strategies for entering and leaving modernity* (Minneapolis, University of Minnesota Press, 2006).

⁸ Peter Burke, *Cultural hybridity* (Cambridge: Polity Press, 2009).

⁹ Christopher T. Marsden, ed., *Regulating the global information society* (London, Routledge, 2000).

que o último. A diferença do terceiro conceito é a sua amplitude para incluir atores privados como entes reguladores. Assim, é possível imaginar produtores de padrões técnicos, como a ISO, o IEEE, o W3C, dentre outros, como fontes normativas. Note que será necessário trabalhar com o conceito de normatividade para além do Estado, em uma chave analítica, derivada de Max Weber.¹⁰ Essa chave analítica é a base para debates comportamentais, que serão o eixo. Assim, a primeira pressuposição é que não apenas o direito nacional ou o direito internacional – incluído o direito regional, como o direito da União Europeia – são fontes de justificativas para ações e relações sociais. Ainda, essa pressuposição se desdobra no fato de que o direito (nacional ou internacional) não é, necessariamente, a fonte normativa mais forte para influenciar e justificar ações. Normas sociais e padrões técnicos fixos e normalizados podem ter mais força normativa do que o direito, do que um Estado-nação, ou mesmo do que o direito internacional. A análise da força normativa em questão dependerá de avaliações empíricas específicas. O contexto será absolutamente relevante. Nem todo direito nacional é igual, assim como o direito internacional não é recepcionado pelos Estados-nação de forma idêntica. Logo, a pluralidade de fontes normativas varia pelo eixo de receção. Por fim, o ponto central para avaliação empírica está no resultado relacional, ou seja, na receção ou na aplicação. De modo simplificado, a figura abaixo demonstra esses dois eixos:

Figura 1. Simplificação dos eixos



Fonte: elaboração própria

Cabe notar que esse modelo é uma simplificação, uma vez que é considerada a existência de uma pluralidade de fontes e destinatários, bem como variações de grau de receção ou aplicação. No caso da receção, o que se está a tratar é do fato de que determinadas normas ou regras podem ser seguidas pelos destinatários, sem a necessidade de coerção. Para Max Weber, esse seria o grau máximo de legitimidade de uma ordem normativa. O usual seria a aplicação, que se baseia no fato de que existe algum aparato de coerção para garantir a validade das normas ou regras, mesmo em casos nos quais os destinatários as considerem ilegítimas. A outra simplificação é o fato de que as normas ou regras não podem ser entendidas sem o contexto mais amplo. O exemplo mais simples é a ordem jurídica nacional. Posteriormente, serão discutidos os limites das teorias tradicionais do direito para lidar com os fenômenos reticulares. Alguns desses limites já existiam no contexto

¹⁰ Max Weber, *Economy and society: a new translation* (Cambridge, MA: Harvard University Press, 2019).

não-reticular. Mas, a radicalização da conexão e da digitalização tornaram esse quadro mais complexo. A tabela a seguir busca colocar dois eixos em ordem. Não será usado um gráfico, pois, como indicado, a pluralidade de situações empíricas é grande.

Tabela 1. Fontes normativas, aplicação e recepção

Eixo das fontes	Eixo da aplicação (necessidade de coerção)	Eixo da recepção (aceitação por legitimidade)
Direito nacional	Nulo. O Estado-nação possui normas jurídicas, mas não as consegue aplicar.	Nulo. As normas jurídicas existem. Mas, não são seguidas, de forma geral, pois os indivíduos ou grupos não as consideram legítimas.
	Mínimo. Poucos indivíduos ou grupos seguem as regras jurídicas, sob coerção.	Mínimo. Uma parte bem pequena dos indivíduos ou grupos considera as normas jurídicas legítimas e as seguem.
	Médio. As regras são – em boa parte – aplicadas e seguidas, com coerção.	Médio. As regras jurídicas são seguidas por uma média razoável das pessoas ou grupos, que as consideram legítimas.
	Máximo. Há alta efetividade coercitiva e as regras são seguidas pela grande maioria das pessoas e grupos.	Máximo. Alta adesão social às regras jurídicas em razão da sua ampla legitimidade.
Direito internacional ou regional	Nulo. O Estado-nação aderiu aos tratados e aceitou suas regras. Mas, o direito nacional e transnacional, bem como as outras fontes normativas, induzem a inaplicabilidade das normas jurídicas, mesmo com risco de sanções internacionais ao país.	Nulo. A adesão do Estado-nação aos tratados não garante a legitimidade das normas jurídicas internacionais ou regionais, seja nos aparatos estatais, seja na vida social.
	Mínimo. As normas jurídicas derivadas de tratados estão acolhidas no Estado-nação. Porém, sua aplicação é baixa, em razão de várias questões fáticas. Há possibilidade de coerção. Mas, ela não alcança efetividade.	Mínimo. Uma parte bem pequena dos indivíduos ou grupos considera as normas jurídicas legítimas e as seguem.
	Médio. As regras são, em boa medida, aplicadas e seguidas, com coerção.	Médio. As regras jurídicas são seguidas por uma média razoável das pessoas ou grupos, as quais consideram-nas legítimas.
	Máximo. Há alta efetividade coercitiva e as regras são seguidas pela grande maioria das pessoas e grupos.	Máximo. Alta adesão social às regras jurídicas em razão da sua ampla legitimidade.

Direito transnacional (privado)	Nulo. As regras para formar acordos entre partes privadas, como contratos arbitráveis existem. Mas, mesmo aderindo aos acordos, as partes não os cumprem, dando preferência para outras fontes normativas. Isso ocorre a despeito de haver meios coercitivos privados (exclusão do grupo) ou estatais (sanções).	Nulo. A aceitação de relações jurídicas com base em fontes normativas transnacionais não se traduz – necessariamente – na sua legitimidade. Logo, o cumprimento esperado não ocorre. Ou, ainda, as regras são consideradas tão ilegítimas, que sequer permitem a formação de relações.
	Mínimo. Uma pequena parte dos convenientes aceita participar de relações privadas, com base em normas e regras privadas. Essa situação ocorre mesmo que haja sanções sociais (como a exclusão das relações econômicas ou maior custo por alternativas) ou sanções técnicas (produtos e serviços mais complexos ou menos eficientes).	Mínimo. Há uma pequena adesão às normas e regras privadas, com base no consentimento, em razão da legitimidade. Pode haver até preferências por elas, em detrimento de outras fontes normativas, como o direito estatal e internacional.
	Médio. As normas e regras privadas são usadas por parte das pessoas e grupos em razão dos riscos de sanções sociais econômicas ou técnicas. Outra parte pode contornar essas normas e regras; ou mesmo usar outras fontes normativas.	Médio. Uma parte das pessoas e dos grupos considera que essas normas e regras são legítimas. Pode ser em razão da eficiência, em comparação com outras fontes normativas ou por aversão às normas jurídicas.
	Máximo. O uso dessas normas e regras é generalizado entre pessoas e grupos. Isso ocorre em razão do objetivo de contornar o direito local ou internacional público, em comparação com outras vantagens potenciais. Ainda, o uso dessas normas e regras pode ser imperativo para a existência da relação.	Máximo. As normas e regras de direito transnacional gozam de legitimidade superior em comparação com as demais fontes normativas. Esse juízo de pessoas e de grupos é amparado por comparação em relação às demais fontes normativas.
Normas e regras sociais	Nulo. Existem normas e regras sociais de conduta que não são seguidas pela maior parte das pessoas e grupos. Elas podem aderir às outras fontes normativas por diversos motivos, independentemente da existência de potenciais represálias.	Nulo. As normas e regras sociais – apesar de existirem e serem reconhecidas – não fruem de legitimidade social, em comparação com as outras fontes normativas.

	Mínimo. As normas e regras sociais possuem sanções sociais. Porém, elas são seguidas por uma minoria dos indivíduos e grupos, os quais preferem outras fontes normativas.	Mínimo. As regras e normas sociais possuem legitimidade reconhecida apenas por poucos indivíduos e poucos grupos. A maioria considera que outras fontes normativas possuem maior legitimidade.
	Médio. Pode ser que haja múltiplas normas e regras sociais, o que induz seu cumprimento não majoritário, nem minoritário. O fato é que uma parte sensível dos indivíduos e grupos as seguem, independentemente das sanções.	Médio. De modo similar à efetividade por sanção social, pode existir pluralidade de normas e regras sociais. Isso induz uma legitimidade parcial. Parte dos indivíduos e grupos reconhece e legitimidade das normas e das regras sociais. Outra parte, não o faz.
	Máximo. A maioria dos indivíduos e dos grupos segue as normas e regras sociais. As sanções sociais contribuem para sua efetividade, mesmo que uma minoria divirja.	Máximo. A legitimidade das normas e das regras sociais é ampla. Uma minoria pode delas discordar e não as seguir. Todavia, a maioria nelas acredita.
Normas e padrões técnicos	Nulo. Os padrões técnicos existem, mas não são seguidos pelos indivíduos ou grupos. Eles podem usar padrões alternativos. Em grau radical, a negativa de uso pode dificultar ou inviabilizar relações; o que, por si, já é uma sanção técnica.	Nulo. Independentemente do uso, a legitimidade dos padrões e das normas técnicas não é reconhecida. Pode haver uso generalizado. Mas, não haverá anuência. Se possível for, grupos e indivíduos procurarão alternativas.
	Mínimo. As normas técnicas e os padrões são seguidos por uma quantidade pequena de indivíduos e de grupos. Pode haver alternativas, mesmo que sejam menos eficientes (ou até perigosas), o que já é uma sanção técnica.	Mínimo. Apenas uma quantidade pequena de pessoas ou grupos reconhece que os padrões e normas técnicas gozam de legitimidade. A maioria não acredita nelas.
	Médio. Pode haver padrões e regras em concorrência, como ocorre com as normas e regras sociais. A maior sanção é o risco de menor interoperabilidade entre sistemas ou dispositivos.	Médio. As crenças sobre a legitimidade dos padrões e normas técnicas é dividida. Alguns indivíduos ou grupos podem não crer na sua legitimidade e negar o seu uso. Outra parte pode buscar padrões e regras técnicas concorrentes.
	Máximo. As normas e regras técnicas gozam de ampla efetividade, em razão do seu uso generalizado. Isso decorre da sanção de exclusão (ou, maior risco; ou, menos eficiência), a qual é muito eficaz.	Máximo. A maior parte dos indivíduos e grupos acredita na legitimidade técnica, tornando os padrões e as regras generalizados. Um pequeno grupo pode discordar da sua legitimidade e até prover alternativas.

Fonte: elaboração própria

Cabe notar que os interesses econômicos (objetivos) e religiosos, morais ou sociais (subjetivos) podem ser elementos para o descumprimento. Essas motivações podem ocorrer tanto em contextos nos quais há coerção forte e eficiente (uma manifestação contra o governo mesmo sob forte repressão), quanto noutros, nos quais há baixa legitimidade (descontentamento geral com as normas ou regras). Os interesses econômicos, usualmente, são entendidos como escolhas racionais de cumprimento. Todavia, mesmo esses interesses racionais podem não ser suficientes para aceitação de regras consideradas ilegítimas, por exemplo.

Para quem conhece o debate sobre direito e ciberespaço, não será surpreendente ver que a tabela reflete uma complexificação do modelo de Lawrence Lessig, que define quatro forças “regulatórias.”¹¹ A diferença desse texto é que os interesses econômicos e parte dos interesses sociais (que ele consideraria “normas sociais”) foram retirados da análise, em prol de um alinhamento à teoria sociológica de Max Weber sobre ações e relações sociais. Outro ponto é que o mesmo poderia ser feito com as normas e padrões técnicos. Elas não são, assim como as normas jurídicas, um bloco monolítico. Existem normas e padrões técnicos com diferentes graus de efetividade de coerção e de legitimidade social. O modelo de Lawrence Lessig possui diversas críticas.¹² Porém, ele certamente abriu um debate que estava truncado. Na década de 1990, a questão central era a possibilidade, ou não, de regular o ciberespaço. A postulação de Lawrence Lessig era que o ciberespaço seria passível de “regulação”, com a combinação eficiente das quatro forças: direito; normas sociais, incentivos e desincentivos econômicos; normas e padrões técnicos. A sua maior contribuição ao debate foi jogar luz nas normas e nos padrões técnicos como uma força “regulatória.” Isso permitiu que vários autores identificassem os desenvolvedores de hardware, software e firmware, como atores centrais na fixação dos comportamentos dos usuários. Mas, é importante repassar essas críticas.

2.1. As fronteiras físicas têm relevância

É certo que David Johnson e David Post são os autores mais conhecidos no debate sobre a questão das fronteiras nacionais como um empecilho para aplicação dos direitos nacionais às aplicações de Internet.¹³ O argumento central deles é que os usuários estariam num local físico e, ao mesmo tempo, num local virtual, como um ciberespaço. A solução deles é algo que vai retornar na obra de Andrew D. Murray, de uma forma sofisticada: os usuários podem escolher usar normas e regras não estatais, por vários modos.¹⁴ Aliás, se um conjunto amplo de usuários assim o fizer, as normas e regras jurídicas perdem força normativas, em razão da baixa efetividade. Existem diversos modos de contornar o direito estatal por meios técnicos (criptografia forte, por exemplo). Ainda, o Estado-nação pode não possuir um aparato de vigilância e punição que faça valer suas regras em detrimento das outras fontes normativas. Ou, mesmo elas podem ser tão fortes (normas e padrões técnicos), que seria contraproducente tentar fazer isso (como não usar protocolos TCP/IP e sistemas de

¹¹ Lawrence Lessig, *Code: and other laws of cyberspace, version 2.0*, 2.^a ed. (New York: Basic Books, 2006).

¹² Viktor Mayer-Schönberger, “Demystifying Lessig”, *Wisconsin Law Review*, v. 4 (2008): 713-746. Andrew D. Murray, *The regulation of cyberspace: control in the online environment* (Abington: Routledge-Cavendish, 2007).

¹³ David R. Johnson and David G. Post, “Law and borders: The rise of Law in cyberspace”, *Stanford Law Review*, v. 48, no. 5 (1996): 1367-1402. David G. Post, “What Larry doesn’t get: code, Law, and liberty in cyberspace”, *Stanford Law Review*, v. 52, no. 5, (1999): 1439-1459.

¹⁴ Andrew D. Murray, *The regulation of cyberspace: control in the online environment* (Abington: Routledge-Cavendish, 2007).

DNS da ICANN). Apesar das críticas de Lawrence Lessig contra essa perspectiva, que visualiza a possibilidade de o direito nacional controlar normas e padrões técnicos, o argumento deles ainda têm relevância, especialmente ao se considerar que nem todos os Estados-nação possuem as mesmas capacidades institucionais.

2.2. *As normas e os padrões técnicos são burláveis*

A segunda crítica à teoria de Lawrence Lessig é a força que ele impõe ao conceito de Código como força “regulatória.” Em diversas passagens do seu livro mais importante sobre o tema, fica claro que ele possui uma proposição de que é possível conjugar o direito e o Código como meio reforçáveis para obrigar o comportamento dos indivíduos.¹⁵ É claro que, tanto ele, quanto Joel R. Reidenberg, têm ciência de que é possível mudar o Código. Todavia, o elemento normativo da solução de usar o Código em prol da conformação de potencial ação de indivíduos faz com que parte da literatura considere seu modelo determinista do ponto de vista tecnológico, segundo Viktor Mayer-Schönberg. Outros autores seguem esse caminho, como Jonathan Zittrain¹⁶ e, também, Primavera De Filippi e Aaron Wright.¹⁷ Um outro elemento do tecno-determinismo é a pressuposição de que a tecnologia – de forma usual – é imbuída de valores sociais. Nenhum dos dois argumentos é completo e absoluto. A teoria de Lawrence Lessig não é simplória. Ela não chega a abraçar o determinismo tecnológico. Mas, é certo que ela acata algum grau de autonomia majorada da tecnologia em detrimento dos usos sociais alternativos. Um exemplo seria a produção de um sistema que, por si mesmo, quase obriga um comportamento social. Ainda, que uma situação dessas possa ocorrer, existem vários exemplos de uso social de tecnologias criadas para uma finalidade, cujo uso social modifica.

2.3. *O direito (nacional, internacional, regional ou internacional) não possui tanta força normativa*

É possível entender que a grande solução de Lawrence Lessig – e, também, de Joel R. Reidenberg – seria a combinação do direito com o Código. O último autor não indica uma prevalência do direito; ao contrário, ele alertava para o fato de que as normas e regras dos sistemas criariam uma “*Lex Informatica*.”¹⁸ Mas, Lawrence Lessig estava num cenário no qual postula um modelo em que o direito pode controlar a tecnologia. A questão central, tratada em tópico anterior é que o direito não possui essa força normativa, em vários graus. Um Estado-nação pode ter leis e não possuir o aparato para as aplicar. Os destinatários das normas e regras jurídicas podem não as considerar legítimas e não as seguirem, a despeito dos riscos.

3. O que é um sistema jurídico? Um conceito a ser revisto

A concepção mais clássica de norma jurídica positiva é derivada de John Austin.¹⁹ Esse autor define a norma jurídica como um comando derivado de uma autoridade

¹⁵ Lawrence Lessig, *Code: and other laws of cyberspace, version 2.0*, 2.^a ed. (New York: Basic Books, 2006).

¹⁶ Jonathan Zittrain, *The future of the internet – and how to stop it* (New Haven: Yale University Press, 2008).

¹⁷ Primavera de Filippi and Aaron Wright, *Blockchain and the Law: the rule of the code* (Cambridge, MA: Harvard University Press, 2019).

¹⁸ Joel R. Reidenberg, “Lex informatica: The formulation of information policy rules through technology”, *Texas Law Review*, v. 76, no. 3 (1998): 553-598.

¹⁹ David Campbell e Philip A. Thomas, eds., *The province of jurisprudence determined by John Austin* (London: Routledge, 2019).

soberana. Ele não produz um debate muito amplo sobre legitimidade e pluralidade de normas. No seu ponto de vista, há uma relação entre um súdito e um soberano. O soberano determina normas jurídicas e os súditos as cumprem. O descumprimento atrai uma sanção. O debate sobre legitimidade – ou fundamentação – do sistema jurídico será feito posteriormente, por autores como Hans Kelsen, Herbert L. A. Hart, John Finnis e Joseph Raz. Isso será feito com base na busca de um reconhecimento social (Herbert L. A. Hart), ou um fundamento estritamente jurídico (Hans Kelsen), ou na natureza do direito (John Finnis e Lon. L. Fuller), ou na autoridade do direito e não do soberano (Joseph Raz). O que une todos esses autores modernos é a identificação de que as normas jurídicas não podem ser compreendidas sem um conceito de sistema jurídico, independentemente das muitas divergências sobre a fonte da legitimidade.

O foco de exame precisa ser limitado à contraposição entre normas e regras não jurídicas e normas e regras jurídicas. As contraposições clássicas, na teoria do direito, estão na existência de duas ou mais normas e regras jurídicas aplicáveis para situações similares (antinomia). Ainda, na inexistência de uma norma ou regra jurídica, a qual precisa ser suprida (lacuna). Existem vários modos para buscar essas soluções. No caso das lacunas, é possível recorrer às analogias, aos princípios, sejam eles juridicamente fixados ou derivados como “*gerais de direito*.” A questão central para a análise das ciências sociais (sociologia, antropologia, economia, dentre outras) sobre o direito é a aferição de efetividade e de legitimidade. Essa será a chave de interpretação.

3.1. Comando e controle pelo soberano

O primeiro autor a ser examinado precisa ser John Austin. Seria possível recuar para Edward Coke, por exemplo, para manter a análise no mundo anglo-americano. Ou, ainda, autores longevos do direito natural. Contudo, é notório que John Austin buscou uma teoria para fundamentar a validade das normas, sem recorrer diretamente a busca de elementos universais, religiosos ou laicos, em vários graus. É razoável colocá-lo no início do positivismo jurídico. A sua solução é muito próxima de Thomas Hobbes, no qual o conceito de autoridade está baseado na síntese do mundo social. O soberano seria o corporificar da pluralidade social. A visão de John Austin pode ser considerada simplificadora. Haveria um soberano – grupo ou indivíduo – que deteria o poder para emitir comandos, os quais seriam seguidos pelas pessoas sob o risco de sanção. É possível considerar sua visão pragmática, já que o autor escreve no início do século XIX, sob forte influência do modelo utilitarista. A necessidade de afirmar o conceito de Estado-nação e de soberania está impregnado em seu modelo.

3.2. Norma jurídica e sistema jurídico como derivados de fundamentação própria

O autor mais importante para essa postulação é Hans Kelsen. Além da teoria pura do direito, ele produziu uma obra em estágio mais avançado da vida, quando já estava exilado nos Estados Unidos da América.²⁰ Essa obra mais tardia possui a relevância de ter sido objeto de maior reflexão temporal, assim como de diálogos críticos, havidos ao longo de décadas. O conceito de norma jurídica de Hans Kelsen busca uma legitimidade no sistema jurídico, o qual, por conseguinte, é legitimado por uma norma fundamental. O seu objetivo é apartar da análise do direito (nacional ou

²⁰ Hans Kelsen, *General theory of Law and State* (New York: Routledge, 2005).

internacional), seja para fins práticos, seja para metas científicas, a moral, costumes e outros elementos não-jurídicos.

Uma diferenciação importante que Hans Kelsen faz é separar o conceito de norma jurídica daqueles de normas moral, social e técnica. Assim, ele busca um conceito de norma jurídica como “*dever-ser*”, em contraposição às condutas humanas, as quais são relacionadas ao “*ser*.” Pode haver vários tipos de “*dever-ser*” (moral, social ou técnico). Mas, a diferença crucial para Hans Kelsen reside na sua fundamentação de validade. Ele não usa o conceito de legitimidade, já que isso poderia induzir a introdução de elementos extrajurídicos na apreciação de validade normativa. A fundamentação de uma norma jurídica é o próprio ordenamento jurídico, o qual se baseia em escalas de validade, cujo cume é uma norma abstrata: a norma fundamental. Ele não nega o papel da sanção e da coerção. Mas, reduzir o conceito de norma jurídica apenas à possibilidade de sanção seria introduzir um elemento de factualidade, o qual não permitiria ao jurista entender e aplicar a norma jurídica como uma derivação de um ordenamento sem recorrer à vida social, às questões morais e políticas; ou, ainda, às considerações técnicas. Há exemplos clássicos de normas e regras não-jurídicas que possuem sanções, como uma punição pelo desvio da conduta social esperada. Isso vale também para normas técnicas. Não seguir uma norma técnica pode ter consequências, como a impossibilidade de autorização para licenciar um produto ou mesmo danos efetivos. Logo, tal conceituação não permitiria uma separação clara entre o não-jurídico e o jurídico.

Essa diferenciação clara entre o não-jurídico e o jurídico tem pontos positivos e negativos. O ponto positivo é tentar afastar o consequencialismo – e outros elementos – da avaliação de validade da criação e aplicação das normas jurídicas. O lado intermediário é a teoria ser separada de considerações morais de toda e qualquer ordem, que é um risco em determinados casos, como indicam as teorias de Ronald Dworkin²¹ e de Robert Alexy.²² Por fim, o lado negativo é negar a pluralidade normativa do direito. Esse é um objetivo da teoria de Hans Kelsen. Mas, o uso estrito dessa negação é a limitação da compreensão de que existem normas jurídicas – igualmente fundamentadas – ao mesmo tempo. É essa compreensão que exigiria um esforço teórico dos juristas para ampliar seus horizontes de análise para entender a realidade. É nesse ponto que ele seguirá um caminho – sem divergir – de Max Weber. Para esse autor, as outras ordens normativas podem ser mais efetivas do que uma ordem jurídica. Hans Kelsen não diverge disso. Porém, ele não focaliza atenção nessa temática, considerando-a fora da teoria do direito. Por fim, tanto Hans Kelsen, quanto Herbert L. A. Hart, estarão preocupados com o conceito de *Rule of Law*. Para ambos, o direito só pode ser entendido como apartado da moral e das normas e regras sociais, bem como possui a função de ordenar a sociedade. A conclusão mais interessante desse ponto de vista é que a força (sanção) serve ao direito, ao invés de o fundamentar.

3.3. Herbert L. A. Hart

O modelo de Herbert Hart é construído para não buscar soluções metafísicas ao problema da legitimidade e da fundamentação. Ele avança muito em comparação com o modelo de John Austin, pois está ciente da necessidade de construir uma

²¹ Ronald Dworkin, *Taking rights seriously: with a new appendix, a response to critics* (Cambridge, MA: Harvard University Press, 1978). Ronald Dworkin, *Law's Empire* (Cambridge, MA: Belknap Press of Harvard University Press, 1986).

²² Mathias Klatt, ed., *Institutionalized reason: the jurisprudence of Robert Alexy* (Oxford: Oxford University Press, 2012).

teoria do ordenamento jurídico para tratar do conceito de norma jurídica.²³ O seu conceito de direito não foge da relação entre súditos e o poder soberano. Contudo, a sua fundamentação para o conceito de sistema jurídico é complexa. Ela é baseada na regra de reconhecimento. Diferentemente do conceito de norma fundamental, de Hans Kelsen, as normas de reconhecimento pressupõem a análise da existência de pessoas (sociedade), as quais aceitam a legitimidade do sistema. Além disso, ele cria dois tipos de normas jurídicas. As primeiras são normas de estrutura e reconhecimento. Elas são normas para a construção de outras normas, bem como para organizar as mudanças no sistema e para adjudicar. As segundas normas jurídicas são os comandos normativos (obrigações). Em sua obra, há uma preocupação muito efetiva em diferenciar as normas jurídicas das normas sociais e das normas morais.

3.4. *Joseph Raz*

Esse autor está mais próximo da contemporaneidade. Ele identifica a necessidade de um sistema jurídico como pressuposto para o Direito (*Rule of Law*).²⁴ Porém, ele não vai lidar – assim como os demais autores resenhados – com o problema da pluralidade normativa do mundo atual. O seu conceito ainda está relacionado com o Estado-nação, o qual produz um sistema jurídico, cuja base se encontra na autoridade. Mas, a autoridade para Joseph Raz não é apenas um grupo de pessoas ou um líder. É a autoridade do próprio direito, que lhe é intrínseca. Uma crítica que pode ser feita ao conceito de Joseph Raz – para além dos demais, acerca da pluralidade – é o fato de se dificultar a diferenciação da legitimidade da norma ou da regra da autoridade. Tanto ele, quanto John Finnis e Lon L. Fuller vão construir modelos teóricos nos quais existe uma legitimação moral ou social da autoridade do direito. Igualmente, os três autores vão partir de pressupostos liberais para essa legitimação. A diferença de Joseph Raz para os demais é que ele não postula a construção de formas mínimas para basear a legitimação da autoridade. Outra diferenciação notável entre eles é que Raz aceita a moralidade social como um elemento de legitimação dessa autoridade. Assim, ele consegue produzir um argumento relevante sobre a obediência ao direito, sem a necessidade de coerção. Esse ponto de vista auxilia a entender os motivos da adesão em normas e regras morais, sociais e técnicas. Todavia, ele não se dedicou a explorar essas contraposições, mantendo-se no âmbito da teoria do direito.

3.5. *John Finnis e Lon L. Fuller*

Tanto John Finnis, quanto Lon L. Fuller, são mais céticos do que Joseph Raz, ao desenhar modelos nos quais a moralidade possui um papel no conceito de Direito.²⁵ Ambos não rompem com a perspectiva de subjugar a normatividade jurídica em elementos externos, como a vida social, as regras e normas morais e técnicas. Porém, eles definem critérios para que o sistema jurídico possa assim ser considerado.

Uma síntese dos vários autores resenhados pode ser elucidativa. Já deve estar claro que a compreensão dos dilemas normativos do mundo atual exige uma teorização realista ou sociológica do direito. Essa posição é desconfortável para o campo da teoria do direito, já que ela se fundou em contraposição a essa premissa.

²³ Herbert L. A. Hart, *The concept of Law*, 3.^a ed. (Oxford University Press, 2012).

²⁴ Joseph Raz, *The authority of Law*, 2.^a ed. (Oxford University Press, 2009).

²⁵ John Finnis, *Natural Law & natural rights*, 2.^a ed. (Oxford: Oxford University Press, 2011). Lon L. Fuller, *The Law in quest of itself* (New York: The Lawbook Exchange, 2006). Lon L. Fuller, *The morality of Law* (New Haven: Yale University Press, 1969).

4. Os limites dos meios tradicionais de contato entre os sistemas jurídicos e as demais fontes normativas

Já foi escrito por outros autores que o Direito não pode ser entendido apenas em seu aspecto nacional. Todavia, essa visão teórica esbarra com a realidade. A primeira é que a teoria do direito está muito assentada na própria visão social dos juristas e mesmo das pessoas. O direito é visto como um sistema imperativo, externo as pessoas e dotado de notável simbologia. Não é por outro motivo que sociólogos desde Émile Durkheim até Talcott Parsons vão considerar que a vida social é a base do Direito. Para o primeiro, a própria compreensão da sociedade exigiria a análise da moralidade social, a qual somente poderia ser apreendida pela sua concretização no Direito. Para o segundo, o conceito de cultura é normalizado em juridicidade. Nenhum dos dois consegue produzir modelos para entender a pluralidade normativa, como fazia Max Weber.

Porém, mesmo a sociologia compreensiva de Max Weber terá limitações, pois estará restrita a sistemas sociais nacionais. A teoria do direito atual entende o direito internacional privado como ponto de contato normativo entre sistemas jurídicos. Ela também acolhe a cooperação internacional, privada ou pública. Mas, a malha jurídica – ou mescla normativa – só pode ser desembaraçada por uma teoria que aceita o pluralismo normativo como fonte. Há um paradoxo, contudo. Quando se aceita que há outras fontes “*jurídicas*” no mesmo sistema jurídico, isso corrói o próprio conceito de ordenamento. Isso ocorre pelo fato do conceito de sistema jurídico não tolerar antinomias ou lacunas. A solução mais simples seria recorrer aos meios tradicionais de incorporação do direito externo. Ou, ainda, possuir um direito que reconhece regras e normas social, morais e técnicas sem o poder de submissão ao sistema jurídico. Porém, essa solução coloca em risco o conceito de *Rule of Law*.

As soluções possíveis para esse dilema teórico exigem imaginação. Em alguma medida, será entendido que ela já ocorre, no caso das três primeiras. A quarta solução é a inovação desse estudo.

4.1 Sistemas jurídicos abertos e mutuamente influenciáveis

Não é novidade que haja abertura nos sistemas jurídicos nacionais ou regionais para a incorporação de influências. Elas podem vir pelo direito comparado. Elas vinham pelo que, no mundo jurídico luso-brasileiro, se denominou de “*lei da boa razão*.” Há exemplos históricos de normas jurídicas estrangeiras que são aplicadas em detrimento de normas nacionais, pois elas resolveriam com mais acuidade casos concretos. Ainda, há exemplos atuais da influência do direito estrangeiro na produção de normas jurídicas nacionais e exemplos claros de incorporação do direito internacional no direito interno. Ou, também, de modificação do direito interno, em razão da adesão de tratados internacionais. O mesmo ocorre com normas privadas. A arbitragem internacional é uma realidade conhecida e normalizada pelos vários sistemas jurídicos nacionais.

A questão seria o grau de abertura e o grau de influência. Um bom exemplo é o conceito de extraterritorialidade jurídica.²⁶ Para que haja regramento conforme, esse grau precisaria aumentar de forma ampla. Todavia, é sabido que existe uma resistência – consciente, ou não – à abertura e à influência. Ela pode estar baseada

²⁶ Nuno Cunha Rodrigues, ed., *Extraterritoriality of EU economic law: the application of EU economic law outside the territory of the EU* (Cham: Springer Nature, 2021).

em duas premissas. A primeira é a soberania do Estado-nação. O risco de perda desse conceito aumenta, na medida em que o direito externo não passa por filtros nacionais. A segunda é o conceito social de direito. Mesmo que se esteja a tratar de Estados ditos plurinacionais, a abertura e a influência majorada poderia ser um risco teórico para a autodeterminação dos povos.

O fato é que essa abertura e influência já existem. A aceitação dessa situação é que merece clarificação. O direito da União Europeia é um bom exemplo. O papel do Tribunal de Justiça da União Europeia é crucial para efetivar a abertura e a influência, sem corroer a soberania dos Estados-Membros. O direito internacional apresenta exemplos contraditórios. Alguns organismos internacionais possuem bastante ou razoável força normativa em suas decisões, como o Conselho da Europa e o Tribunal Europeu de Direitos Humanos. No caso de outros, esse poder é menos acentuado.

A vantagem do caminho da abertura e da influência é que ele pode ser previsto normativamente nos sistemas jurídicos nacionais. A desvantagem é que alguns Estados-nação com menos poder na seara internacional poderão caminhar para uma situação de se transformar em “*satélites jurídicos*” de Estados-nação fortes. Todavia, essa situação já é uma realidade econômica. Há vários países, cujas economias são “*dolarizadas*”, por exemplo. Os fatos se impõem às teorias. O conceito jurídico e político de soberania poderia ser uníssono. Contudo, a realidade do exercício das soberanias nacionais é muito diversa, como será tratado no próximo tópico.

4.2. Globalização e direito: harmonização

A expressão “*harmonização*” também não é nova. O exemplo mais evidente dela é a UNCITRAL, um órgão da Organização das Nações Unidas que se dedica à produção de textos-modelo para incorporação pelos diversos países.²⁷ As motivações da UNCITRAL são econômicas. O objetivo é que os países possuam maior grau de compatibilidade em seus direitos nacionais para que isso facilite as trocas comerciais. Porém, o fenômeno da globalização é social e cultural. A adesão das sociedades para padrões de consumo e de interação é evidente, ainda que isso – paradoxalmente – reforce as lutas locais em defesa das especificidades. Alguns autores denominam esse fenômeno como o Global-Local.²⁸

4.3. Pluralismo jurídico e sua versão internacional

O pluralismo é uma base para debater fenômenos culturais e jurídicos.²⁹ Ela envolve desde estudos clássicos, que identificam a existência de ordens normativas concorrentes e paralelas, até debates contemporâneos sobre a globalização e seus efeitos jurídicos. O melhor exemplo jurídico para um pluralismo com a intenção de compreender fenômenos tecnológicos é a existência de regras privadas estrangeiras e seu uso generalizado em outras sociedades, mesmo quando o Estado-nação as negam juridicidade. Chris Reed e Andrew D. Murray avançam nessa seara ampliando os conceitos de comunitarismo de rede.³⁰ O primeiro autor também explora o tema com

²⁷ Rishi Gulati, Thomas John, e Ben Köhler, eds., *The Elgar Companion to UNCITRAL* (Chettenham: Edward Elgar Publishing, 2023).

²⁸ Victor Roudometof, “The glocal and global studies”, *Globalizations*, v. 12, no. 5, (2015): 774-787.

²⁹ David Nelken and Johannes Feest, eds., *Adapting legal cultures* (Oxford: Hart Pub., 2001). Paul Schiff-Berman, *Global legal pluralism* (Cambridge: Cambridge University Press, 2012).

³⁰ Chris Reed and Andrew D. Murray, *Rethinking the jurisprudence of cyberspace* (Chettenham: Edward Elgar Pub., 2018).

aplicabilidade, ao propor o modelo de regulação simbiótica.³¹ Ainda, existem diversos exemplos de aplicações de Internet com regras violadoras de direitos nacionais e que são usadas diariamente. O outro exemplo jurídico é a globalização da jurisdição. Uma parte pode escolher litigar em outro país em prol de uma jurisdição mais favorável. Ou, ainda, pode haver uma litigância transnacional, na qual a empresa sofre ações similares em diversas jurisdições, com resultados contraditórios.

4.4. Híbridos culturais e jurídicos

O último conceito é derivado de Néstor García Canclini e Peter Burke: híbrido cultural ou hibridismo cultural. Ele foi construído pelos dois autores em obras diferentes. Mas, a sua origem é similar: a América Latina. Um exemplo é o sincretismo religioso – catolicismo e religiões afro-brasileiras. A postulação dessa pesquisa segue Néstor García Canclini, que está preocupado com as novas tecnologias da informação e da comunicação. Mas, antes, cabe um alerta. O conceito de hibridismo pode ser criticado, em razão de derivar da biologia. Nesse sentido, para Néstor García Canclini, é importante ter uma definição: “*processos sociais e culturais com estruturas e práticas distintas, previamente em formas apartadas, combinadas para gerar novas estruturas, objetos e práticas.*”³² Os exemplos podem alcançar produtos culturais usuais como a música e a arquitetura. Para reconhecer a possibilidade de híbridos jurídicos, é imperativo reconhecer o pluralismo dos direitos, bem como das demais normas e regras (sociais, técnicas e morais). Assim, é necessário entender que os sistemas jurídicos dos Estados-nação possuem limitações – que variarão de acordo com sua força, claro – em fazer valer suas regras. A solução de reconhecer legitimidade e uso em outras fontes normativas é um risco. Porém, ela também apresenta uma virtude: a potencialidade de mudança dos sistemas jurídicos em prol da sua maior adequação em relação à legitimidade social das normas e das regras que organizam as sociedades. Ainda, ela permite – se instrumentos houver – aferir o grau de adesão social às normas e regras jurídicas, por contraste.

5. Discussão e conclusões

Esse estudo apresenta uma solução teórica para lidar com a pluralidade de normas e de regras que são aplicáveis às novas tecnologias da informação e da comunicação. Não obstante, é importante discutir seus riscos, antes de produzir a conclusão de que os híbridos culturais e jurídicos são a melhor solução para tratar da regulação do mundo de conexão radical.

O primeiro risco envolve um conceito importante para a teoria do direito: *Rule of Law*. Ao aceitar a validade de normas e regras não filtradas por um sistema jurídico, isso pode induzir a erosão de vários postulados liberais. Não é por outro motivo que os filósofos do direito da atualidade são céticos ou preocupados. Mesmo aqueles que aceitam a existência de normatividades não-jurídicas, como a moral, estarão preocupados com a manutenção de valores, como a democracia, a liberdade e outros.

O segundo risco envolve um problema típico da sociologia, como disciplina que tem origens na modernidade: a fragmentação social. Ao aceitar a pluralidade normativa, há um risco de fragmentação do Estado-nação em múltiplos grupos com

³¹ Andrew D. Murray, “Symbiotic regulation”, *John Marshall Journal of Computer and Information Law*, v. 26, no. 2 (2009): 207-228.

³² Néstor García Canclini, *Hybrid cultures: strategies for entering and leaving modernity* (Minneapolis: University of Minnesota Press, 2006).

diversas ordens normativas. Em última instância, a dissolução do próprio conceito de sociedade se coloca em risco. A fragmentação social pode ocasionar a disfunção política em alto grau, em especial nos países democráticos.

O terceiro risco é um problema de filosofia política. A perda ou corrosão de um consenso mínimo – no Estado-nação – sobre as normas e regras aplicáveis pode abrir espaço para a normatividade prevalente ser derivada de um processo de um novo tipo de “colonização.” Essa nova “colonização” pode advir de grandes empresas transnacionais, por exemplo; não somente de outros Estados-nação, como no passado. As decisões sobre a vida social são trazidas de outro local, sem que haja interveniência de uma associação política com força para definir seu próprio destino.

Os três riscos precisam de salvaguardas para evitar a corrosão da vida social. Eles precisam ser colocados em conta, para imaginar modelos teóricos que os mitiguem. Mas, tendo ciência das limitações atuais do conceito de Estado-nação.

Apesar dos riscos, do ponto de vista cultural, a criação de híbridos jurídicos já é um processo em curso. Evidentemente, normas e regras jurídicas transitam pelo mundo e pelos Estados-nação, tendo origens diferentes. Porém, os Estados-nação ainda atuam com a força possível – alguns com mais; outros com menos – para reinterpretar, nulificar ou adaptar essas normas e regras exógenas. Um bom exemplo é a influência da União Europeia na área de proteção de dados pessoais³³ e nos campos social e econômico.³⁴ O processo de hibridização jurídica deriva exatamente desse processo de tradução cultural, como já foi aferido em pesquisas de campo. Normas e regras jurídicas podem possuir um significado que, em princípio, remete à identidade. Seria a mesma regra, transplantada. Porém, o fato da norma ou regra advir de um contexto social e jurídico diverso faz com que haja uma tradução. A “*letra da lei*” pode ser igual. O significado dela pode ser diferente. O grau de diferença só pode ser aferido empiricamente, ou seja, a partir do exame de práticas e objetos.

³³ Alexandre Veronese *et al.*, “The influence of European Union personal data protection standards in Latin America from the perspective of social actors and Latin American authorities”, *UNIO - EU Law Journal*, v. 9, no. 2 (2023): 118-138.

³⁴ Elaine Fahey, *The global reach of EU Law* (Abington: Routledge, 2017). Anu Bradford, *The Brussels effect: how the European Union rules the world* (Oxford: Oxford University Press, 2010).

A regulação dos serviços intermediários como garantia da liberdade e pluralismo dos meios de comunicação social numa sociedade digital plataformizada

Inês Neves*

1. Introdução

No seu último Relatório anual sobre o Estado de Direito na União Europeia, a Comissão Europeia recorda que um “*ambiente mediático livre e pluralista é essencial para o Estado de direito, com meios de comunicação social livres e independentes a desempenharem um papel importante enquanto guardiões da democracia e responsabilizadores do poder.*”¹ Por outras palavras, a proteção da liberdade e do pluralismo dos meios de comunicação social, na Internet e fora dela, é, e continua sendo, padrão, critério e pilar essencial do Estado de Direito.

A compreensão do Estado de Direito, como Estado de democracia e como Estado de direitos fundamentais, remonta-nos para uma caracterização básica da liberdade e do pluralismo dos meios de comunicação social como mais do que uma questão de interesse público. Além de relevarem como tal, está-se, também, num domínio de jusfundamentalidade, que se reflete a vários níveis.

Em primeiro lugar, no plano da titularidade, não restam dúvidas de que os meios de comunicação social, seja os jornalistas individualmente considerados, seja os prestadores de serviços de comunicação social – pessoas singulares ou coletivas – são titulares de direitos subjetivos cuja jusfundamentalidade é reconhecida, quer nas Constituições e catálogos de direitos nacionais, quer em instrumentos de proteção regionais e supranacionais, com o particular relevo, entre outros, da Carta dos Direitos Fundamentais da União Europeia (‘CDF’), da Convenção Europeia dos Direitos Humanos (‘CEDH’) e da Declaração Universal dos Direitos Humanos (‘DUDH’). Repare-se que, inclusive admitindo a existência de querelas quanto ao fundamento e alcance da titularidade de direitos fundamentais por pessoas coletivas, ninguém arriscará negar aos *media* a titularidade das liberdades de opinião, expressão e informação, seja como faculdades da liberdade de expressão em geral, seja como dimensões da liberdade de imprensa como *species*.

Em segundo lugar, importa não esquecer que, além da titularidade de direitos fundamentais próprios, os meios de comunicação social são, também, veículos da garantia e efetivação de direitos alheios, nomeadamente, das liberdades de procura, acesso, transmissão e divulgação de informações, surgindo, pois, como instrumentos

* Professora da Faculdade de Direito da Universidade do Porto. Investigadora Integrada do CIJ – Centro de Investigação Interdisciplinar em Justiça.

¹ Comissão Europeia, “Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões. Relatório de 2024 sobre o Estado de Direito – Situação na União Europeia”, (COM(2024) 800 draft, Bruxelas, 24 de julho, 2024), 28.

essenciais para a realização dos direitos dos vários sujeitos da comunidade político-jurídica.

Finalmente, e por inerência, a garantia da liberdade, da independência e do pluralismo dos *media* surge, também, como condição de efetivação da democracia, como regime e como ideia. Isto porque, e recordando o Relatório *supra*, os meios de comunicação social surgem – enquanto veículos do livre fluxo de informações – como verdadeiros contrapoderes e responsabilizadores do poder.

A ligação umbilical e incindível entre os meios de comunicação social e os direitos fundamentais, reforçada e continuada pela recondução destes últimos à tríade simbiótica *Estado de Direito, democracia e direitos fundamentais*, justifica repensar os desafios e, em particular, as ameaças à respetiva independência, liberdade e pluralismo, no contexto digital, e, em particular, num momento em que a centralidade, o poder e a disrupção provocada pela entrada em cena de prestadores de serviços intermediários, com particular destaque para as (grandes) plataformas em linha,² não oferece já dúvidas. Recorde-se, com a doutrina, que os grandes prestadores de serviços digitais *“have transcended their roles as mere content hosts to become active shapers of public discourse and gatekeepers of information access. This transformation has significant implications for the democratic process and the exercise of fundamental rights, particularly in the realms of free speech and privacy.”*³ Sem prejuízo da ubiquidade do seu impacto, não deixa de ser verdade a particular refração nos meios de comunicação social e, por consequência, na constelação de direitos fundamentais e interesses públicos em si personificados.

Com efeito, é hoje inegável a particular vulnerabilidade dos meios de comunicação social no ambiente em linha. As causas são múltiplas. Por um lado, estão as interfaces e a arquitetura digital das plataformas, a automatização e, enfim, toda a lógica própria de atuação dos prestadores de serviços intermediários – privilegiando os conteúdos sensacionalistas ou virais sobre os demais, e optando pelas respostas e abordagens mais eficazes, com os inerentes riscos de silenciamento e *overblocking*. Por outro lado, está a própria mutação social, que redundava numa sociedade polarizada, e pouco receptiva à aceitação dos opostos. Este cenário depressa evolui para a profusão de cenários de assédio e perseguição em linha (afetando, sobretudo, jornalistas mulheres), frequentemente espoletados por denúncias e notificações infundadas,

² As plataformas em linha, ou, mais precisamente, os fornecedores de plataformas em linha são apenas uma categoria de entre os vários serviços da sociedade da informação qualificáveis como serviços intermediários. No 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, de que se tratará em texto, as plataformas em linha são definidas como *“um serviço de alojamento virtual que, a pedido de um destinatário do serviço, armazene e difunda informações ao público, a menos que essa atividade seja um elemento menor e meramente acessório de outro serviço ou uma funcionalidade menor do serviço principal e que, por razões objetivas e técnicas, não possa ser utilizado sem esse outro serviço, e que a integração desse elemento ou dessa funcionalidade no outro serviço não constitua uma forma de contornar a aplicabilidade do presente regulamento”*, cf. artigo 3.º, i) do referido Regulamento. Atenta a sua centralidade para o tema em apreço, conexa com a atual premissa das redes sociais para a atuação dos meios de comunicação social, o texto dirigir-se-á, sobretudo, às (grandes) plataformas em linha, sem prejuízo de as considerações aqui tecidas, ora poderem valer para outros prestadores de serviços intermediários, ora se poderem cingir às plataformas em linha de muito grande dimensão. Nos termos do artigo 33.º do referido Regulamento, estas últimas incluem as plataformas com um número médio mensal de destinatários ativos do serviço na União igual ou superior a 45 milhões, e que são objeto de uma decisão de designação pela Comissão Europeia.

³ Cf. Christophe Geiger e Giancarlo Frosio, *“Towards a digital constitution. How the Digital Services Act shapes the future of online governance”*, in *From the DMCA to the DSA: A transatlantic dialogue on online platform regulation and copyright*, ed. João Pedro Quintais (Berlim: Verfassungsbooks, 2024), e *SSRN Electronic Journal*, 17 de junho, 2024, 46, <https://ssrn.com/abstract=4860225> ou <http://dx.doi.org/10.2139/ssrn.4860225>.

na origem de limitações-restrições à visibilidade de conteúdos disponibilizados por jornalistas, que poderão ir a ponto de incluir a remoção de conteúdo editorial e a suspensão de contas empresariais.

À complexidade da realidade factual acrescem os desafios de um contexto normativo-regulatório em constante construção e evolução, e que, ainda quando não visando os *media* em particular, não deixa de (poder) impactar, positiva e negativamente, na sua independência, liberdade e pluralismo.

Bebendo de todas estas preocupações, procura-se, com esta comunicação, tratar de uma questão de estudo particular: aferir se e de que forma a regulação dos serviços intermediários e, em particular, das (grandes) plataformas em linha, através de atos normativos como o Regulamento Serviços Digitais⁴ contribui ou poderá também contribuir para garantir a liberdade e o pluralismo dos meios de comunicação social no ambiente em linha.

Como se cuidará aqui de assinalar, a disrupção provocada pelo digital confere às plataformas em linha um poder infraestrutural que afeta os meios de comunicação social, e, em particular, a sua liberdade, independência e pluralismo, direta e indiretamente. Diretamente, por força da sua dependência e particular vulnerabilidade em relação às primeiras, que emergem em sociedade como verdadeiras *gatekeepers* de informação e titulares de infraestruturas essenciais de cujo acesso os *media* dependem para chegar à sociedade. Indiretamente, em razão da forma como aquelas (plataformas) desenham as respetivas interfaces, aplicam os respetivos termos e condições e procedem à moderação de conteúdos, atuação que, atentos os padrões atuais do consumo de informação, se repercute, naturalmente, não só na diversidade de vozes e na pluralidade informativa, como, e bem assim, na forma como os *media* e os produtos do jornalismo são perspectivados.

É perante e por causa desta transformação que se considera importante compreender de que forma a regulação das plataformas em linha, pese embora horizontal e com uma intenção de proteção não dirigida, em particular, aos meios de comunicação social, poderá contribuir para assegurar e preservar o papel primordial dos *media* no ambiente em linha. Aproveitando o mote, e sem prejuízo das valias inegáveis do Regulamento Serviços Digitais como *garantia indireta*, nos termos adiante explanados, concluir-se-á no sentido da necessidade de articulação entre diferentes atos normativos – ora dirigidos à regulação dos serviços e dos mercados digitais, ora especificamente orientados para os meios de comunicação social – todos eles, peças do *puzzle* heterogêneo e crescente que caracteriza a legislação digital.

Apontar-se-ão, a final, alguns dos desafios futuros. Retomando, é certo, questões e dúvidas transversais, que há muito alimentam tensões conhecidas – entre a regulação e a inovação, e entre a proteção e a censura – está-se perante desafios que não deixam de surgir particularmente adensados, *in casu*, pelas idiosincrasias e transformação na atividade, na cadeia de valor e no modelo de negócio dos meios de comunicação social, no contexto digital.

Independentemente deste singelo contributo, e retomando o princípio, dir-se-á que aos Estados e à União Europeia caberá garantir que o futuro da liberdade, da independência e do pluralismo dos *media* na era digital continue sendo gizado,

⁴ 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) JO L 277 de 27.10.2022, 1-102. ELI: <http://data.europa.eu/eli/reg/2022/2065/oj>.

norteado, e balizado pela mesma ideia justificativa da sua importância – o Estado de Direito, como Estado democrático, e como Estado de direitos fundamentais.

2. Repensar a cadeia de valor e as situações de perigo para os meios de comunicação social no contexto digital: em particular, do impacto das plataformas em linha no pluralismo e independência dos *media*

Entre os diferentes setores, segmentos e esferas da sociedade particularmente afetados pela transição digital e, em particular, mais recentemente, pela Inteligência Artificial ('IA') generativa, descobrem-se, sem dificuldade, a recolha, a produção, a distribuição e o consumo de notícias. Em suma, as diferentes faces do *modus vivendi* e da *essentia* dos meios de comunicação social.

Sendo certo que as primeiras ameaças aos modelos tradicionais de organização e atuação dos *media* surgem logo aquando do surgimento e do desenvolvimento da Internet e das redes descentralizadas de agregação e distribuição de informação, hoje, os atores da sociedade algorítmica não se resumem já ao simples armazenamento e distribuição de informação. Pelo contrário, além da intensificação do controlo dos conteúdos e, por conseguinte, do inegável papel e influência que desempenham na formação da opinião pública, as (grandes) plataformas em linha surgem, também e já, a criar informação, a direcionar essa e outra informação, e a financiar projetos de inovação e jornalismo.⁵ Tudo isto no *plano da oferta*. No *plano da procura*, e não em contra-harmonia, assiste-se, por seu turno, a uma mudança disruptiva dos hábitos de consumo da informação, que deixa de se fazer através dos canais de *media* tradicionais, para se deslocar para a sociedade digital e, em particular, para as plataformas em linha e os motores de pesquisa em linha.⁶ O fenómeno justifica as referências a uma "*attention-based economy*."⁷

É neste particular contexto que importa repensar os riscos específicos deste ambiente em linha e das novas sociedades plataformizadas para os *media*. Sem prejuízo do mérito relativo das classificações, parece-nos útil aludir à presença de riscos com uma dimensão absoluta e riscos de índole relativa.

Começando pelos absolutos, é inegável o surgimento de novos contextos de perigo,⁸ que independem da identificação de uma relação intersubjetiva entre uma plataforma em linha e um ator dos *media*, e que se afiguram justificativos da

⁵ Seguimos de perto Theresa Josephine Seipp, Natali Helberger, Claes de Vreese, e Jef Ausloos, "Between the cracks: blind spots in regulating media concentration and platform dependence in the EU", *Internet Policy Review* 13, no. 4 (2014): 11. DOI: 10.14763/2024.4.1813, <https://policyreview.info/articles/analysis/regulating-media-concentration-and-platform-dependence>.

⁶ Sobre a substituição do jornalismo profissional como decorrência da plataformização da esfera pública, cf. Matteo Monti, "Why online public discourse needs a media privilege: in defence of Article 18 of the EMFA", *EUI Centre for Media Pluralism and Media Freedom*, 1 de novembro, 2024, <https://cmpf.eui.eu/in-defence-of-article-18-of-the-emfa/>. Sobre a disrupção dos hábitos e consumo, cf. Elda Brogi *et al.* - study requested by the Committee on Civil Liberties, Justice and Home Affairs (European Parliament), "The European Media Freedom Act: media freedom, freedom of expression and pluralism" (Bruxelas, julho 2023), 9, [https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2023\)747930](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)747930).

⁷ Sobre o termo, cf. Marta Cantero Gamito, "Consistent regulatory and self-regulatory mechanisms for media freedom in the Digital Single Market. The European Media Freedom Act (EMFA) as meta-regulation", *RSC Working Paper 2022/42 Robert Schuman Centre for Advanced Studies Centre for Media Pluralism and Media Freedom*, e *SSRN Electronic Journal*, 1 de janeiro, 2022, 1, <https://doi.org/10.2139/ssrn.4148474>.

⁸ A prevalência do assédio em linha, em particular contra jornalistas mulheres, é exemplo patente da necessidade de proteção acrescida.

atuação de deveres de proteção por parte do Estado e – hoje também ou talvez mais – pela União Europeia.⁹ A ambos – Estados e União Europeia –, e dependendo da concreta repartição de competências, caberá adotar medidas suscetíveis de assegurar um ambiente em linha favorável e seguro, no qual todos e todas – e, em particular, os *media* – possam participar sem medo.

Numa dimensão relativa, surgem os perigos associados, em particular, à forte dependência dos meios de comunicação social em relação a novos protagonistas e *atores principais* da cena digital, entre os quais se destacam as plataformas em linha. Estas – titulares de poderes sistémicos que, em resultado do seu particular posicionamento económico, algorítmico, tecnológico, relacional e infraestrutural, se reforçam reciprocamente¹⁰ – depressa relegam os *media* para figurantes sem voz, num enredo heteronomamente ditado.

Sem prejuízo do relevo de ambas as dimensões, à presente comunicação interessa, sobretudo, esta segunda dimensão de perigo, dita relativa. Porque assim é, importa compreendê-la em maior detalhe. Em que medida as plataformas em linha e a respetiva atuação no espaço digital constituem um perigo para os meios de comunicação social tradicionais?

A título prévio, cumpre salientar a natureza das plataformas em linha como *pathfinders* essenciais, ou, noutros termos, como *gatekeepers* ou controladoras do acesso a informação. Em particular, as (grandes) plataformas em linha surgem, hoje, a exercer um papel editorial de facto, intermediando os fluxos informacionais, e participando ou influenciando, expressa ou silenciosamente, nos processos de formação da vontade e da opinião, individual e pública.¹¹ As plataformas adquirem, em suma, a titularidade do já designado “*opinion power*.”¹²

Em particular, pese embora não sendo já novas, realidades como as *filter bubbles*, que nos colocam em contacto com conteúdos restritos e limitados de informação; as *echo chambers*, que nos sujeitam a um diálogo em circuito fechado e homogéneo (reduzindo, pois, a “*exposure diversity*”), e os próprios algoritmos de recomendação e personalização,¹³ atestam o poder decisório das plataformas e respetivos modelos de negócio. Todas estas realidades desvelam como as plataformas surgem hoje a decidir sobre o “*se*” (*se um conteúdo particular de informação é visível*), o “*como*” (*como e com que alcance esse conteúdo se torna visível ou até mesmo viral*), e o “*a/com quem*” (*a/com quem é que esse conteúdo é partilhado ou disponibilizado*). Todas estas realidades provam, pois, o inegável potencial das plataformas para influenciar e distorcer o fluxo informativo, e para marginalizar e inclusive censurar particulares conteúdos e vozes. Enfim, o seu inegável potencial para enfraquecer o pluralismo e minar a democracia.

⁹ Sobre as obrigações positivas que fluem da Convenção Europeia dos Direitos Humanos a este propósito, cf., *inter alia*, “Report on workshop – Online journalism: Digital Services Act and European Media Freedom Act, 23 February 2023”, *DSA Observatory*, 13 de abril, 2023, <https://dsa-observatory.eu/2023/04/13/report-on-workshop-online-journalism-digital-services-act-and-european-media-freedom-act-23-february-0/>.

¹⁰ Sobre este, cf. Seipp, Helberger, de Vreese, e Ausloos, “Between the cracks: blind spots in regulating media concentration and platform dependence in the EU”, 3 e ss.

¹¹ Neste sentido, cf. Oreste Pollicino, e Federica Paolucci, “Unveiling the digital side of journalism: exploring the European Media Freedom Act’s opportunities and challenges”, *La Revue des Juristes de Sciences Po*, no. 1 (2024) e *SSRN Electronic Journal*, 13 de março, 2024, <https://ssrn.com/abstract=4760025>, 1.

¹² Sobre este, cf. Seipp, Helberger, de Vreese, e Ausloos, “Between the cracks: blind spots in regulating media concentration and platform dependence in the EU”, 4.

¹³ Sobre estas realidades, em particular, Brogi *et al.*, “The European Media Freedom Act: media freedom, freedom of expression and pluralism”, 11 e ss.

As mesmas realidades atestam outras dimensões de poder, porém. Entre elas, descobre-se um poder relacional ou mediador,¹⁴ que se compreende como produto da natureza das plataformas como *intermediárias*. Com efeito, entre os meios de comunicação social e as audiências, as plataformas em linha assumem hoje uma intervenção que é fonte de perigos particulares, quer para os conteúdos em circulação, quer para os polos da comunicação (emissor e destinatário da informação) que daquelas dependem para comunicar. Em resultado, antes dos perigos conexos com o conteúdo da informação em circulação e, em particular, com o risco da interferência de um terceiro numa particular cadeia comunicacional, assumem preponderância as situações de perigo relativas ao próprio acesso, com o particular risco de bloqueios, de restrições e de recusas de acesso, por exemplo, de particulares jornalistas ou meios de comunicação social a plataformas em linha – as novas *ágoras digitais*.

Aos poderes decisório e relacional-mediador acabados de descrever soma-se, por fim, um poder por muitos já apelidado de político. Político, não apenas por se sobrepor aos Estados, através de uma atuação e influência transnacional que escapa às respetivas fronteiras físicas. Político, não apenas por mimetizar os poderes estaduais, com faculdades prototípicas suas, como as de elaborar e ditar as próprias leis (termos e condições), executá-las e adjudicá-las direitos. Político, também em razão do seu impacto nos processos democráticos e de formação da vontade.

Com efeito, se nos seus primórdios as plataformas em linha eram aplaudidas como veículos promotores da democracia, garantes da disseminação da informação, da democratização da comunicação e da amplificação do pluralismo,¹⁵ essa imagem idílica depressa se transformaria no seu oposto. Sem aderir, em termos fechados, a qualquer dos descritivos – pois que fazê-lo sempre corresponderia a enveredar na falácia da polarização, devendo a qualificação manter-se uma questão de concreto(s) e de contexto(s) –, certo é que as plataformas em linha são hoje sobretudo perspetivadas como ameaças à democracia. Ora enquanto palcos de disseminação de desinformação, *misinformation*¹⁶ e *malinformation*,¹⁷ discurso de ódio e conteúdos ilegais, ora em razão do seu poder para determinar o (des)favorecimento de conteúdos, a consequente marginalização e até censura (não raras vezes automatizada) de vozes dissidentes ou minoritárias, a atuação das plataformas em linha dá origem a dimensões de perigo, com repercussões (in) diretas nos *media*. Particularmente exemplificativa é a crescente desconfiança na comunidade epistémica, e as evidentes ameaças a uma cidadania informada.¹⁸

Recentemente, somam-se, ainda, os riscos particulares da IA generativa, que, nomeadamente com o desenvolvimento de serviços de notícias assentes em

¹⁴ Sobre este, cf. Seipp, Helberger, de Vreese, e Ausloos, “Between the cracks: blind spots in regulating media concentration and platform dependence in the EU”, 6 e ss.

¹⁵ Cf. Mateo Monti, “The missing piece in the DSA puzzle? Article 18 of the EMFA and the media privilege”, *Rivista Italiana Di Informatica E Diritto* 6, no. 2 (2024): 197, <https://doi.org/10.32091/RIID0173>.

¹⁶ Definida como informação que não é verdadeira, mas que não é disseminada com a intenção de causar dano.

¹⁷ Entendida como informação que é factualmente verdadeira, mas que é partilhada com a intenção de causar dano. Sobre as noções, com referências, cf. Brogi *et al.*, “The European Media Freedom Act: media freedom, freedom of expression and pluralism”, 29.

¹⁸ Sobre esta desconfiança, e a necessidade de ter em conta a perspetiva do utilizador (público e cidadãos) na garantia do pluralismo dos *media*, também para efeitos da sua reabilitação perante os cidadãos, cf. Ivana Stamenković, e Tatjana Đukić Živadinović, “Media pluralism in the digital environment from the users’ point of view”, *Media Studies and Applied Ethics* 4, no. 1 (2023), <https://msae.rs/index.php/home/article/view/68>.

inteligência artificial, desloca a fonte jurígena dos problemas do plano da circulação e intermediação da informação para o próprio estágio da produção de informação,¹⁹ no qual as plataformas em linha evidenciam vantagens inegáveis decorrentes do acesso privilegiado a *inputs* essenciais e estratégicos, como dados, poder computacional e trabalhadores especializados.

Todas estas dimensões de perigo contribuem e adensam evidentes assimetrias de poder, desestabilizam os modelos de negócio tradicionais de jornalistas e meios de comunicação social,²⁰ e impactam inarredavelmente no pluralismo e na independência dos *media* em linha. Fala-se hoje, e por isso, numa *infrastructural capture*, que se soma ao velho problema da *regulatory capture*.²¹

A *captura infraestrutural* a que se faz referência decorre da situação de dependência dos meios de comunicação social *vis-à-vis* as plataformas em linha, que atuam como controladoras de acesso, organizadoras e curadoras de conteúdos em linha. Pese embora a existência de canais alternativos de disseminação da informação, as plataformas em linha emergem, de facto, como pontos de acesso crítico para os meios de comunicação social, convertendo-se, por isso, em verdadeiros serviços essenciais para a distribuição de conteúdos. Em resultado do *status* de dependência em que os meios de comunicação social tradicionais, sobretudo locais ou regionais se encontram em relação às plataformas em linha, cobra, em nosso ver, particular sentido a convocação da ideia de *vulnerabilidade* e de *sujeitos vulneráveis*.

Esta relação de dependência relativa assume uma outra dimensão, porém. Com efeito, importa não negligenciar a circunstância de as plataformas em linha serem também, e agora em relação de concorrência, causas do esgotamento das fontes de rendimento e das estratégias de monetização de que os *media* tradicionais durante muito tempo dependeram para operar de forma sustentável.²² Em particular, a presença das plataformas em linha nos mercados publicitários e a apropriação de lucros decorrentes da distribuição de conteúdo jornalístico – sem compensação equitativa e sem o reconhecimento do papel do jornalismo de qualidade – são fatores que afetam não apenas a igualdade de oportunidades de comunicação (*“kommunikative Chancengleichheit”*)²³ em razão do favorecimento dos conteúdos majoritários e do consequente risco de manipulação e censura, como, e bem assim, a própria sustentabilidade e viabilidade dos meios de comunicação tradicionais no mercado.

Compreendidas, em síntese, as principais dimensões de perigo com as quais os meios de comunicação social se deparam no ambiente em linha, é agora tempo de questionar se a sua liberdade, independência e pluralismo poderão então, como objetivos de interesse público que são, ser assegurados pela regulação das plataformas em linha. Desta questão trata o próximo ponto.

¹⁹ Neste sentido, com referências, cf. Seipp, Helberger, de Vreese, e Ausloos, “Between the cracks: blind spots in regulating media concentration and platform dependence in the EU”, 19-20.

²⁰ Neste sentido, Iva Nenadić, “Policy in practice: The interplay of the Digital Services Act and the European Media Freedom Act”, *EUI Centre for Media Pluralism and Media Freedom*, 18 de outubro, 2024, <https://cmpf.eui.eu/digital-services-act-and-european-media-freedom-act/>.

²¹ Cf. Seipp, Helberger, de Vreese, e Ausloos, “Between the cracks: blind spots in regulating media concentration and platform dependence in the EU”, 6.

²² Sobre a questão, cf. Seipp, Helberger, de Vreese, e Ausloos, “Between the cracks: blind spots in regulating media concentration and platform dependence in the EU”, 10-11.

²³ Cf. Wolfgang Schulz, *Gewährleistung kommunikativer Chancengleichheit als Freiheitsverwirklichung* (Nomos, 1998).

3. A resposta normativa da União Europeia a um ambiente digital em transformação

A resposta normativo-regulatória europeia aos desafios da transição digital caracteriza-se por uma pluralidade e heterogeneidade que somente como conjunto se compreende e revela eficaz. Para essa tessitura contribuem tensões várias, na origem de compromissos nem sempre fáceis de estabelecer e, acima de tudo, de firmar-positivar em lei geral e abstrata. Em primeiro lugar – e numa dialética muito simplificada que não pretende ignorar a presença de outros direitos e interesses constitucionalmente protegidos – está a tensão entre o combate à difusão de conteúdos ilegais e ofensivos em linha, por um lado, e a garantia da liberdade de expressão e de informação, por outro. Um segundo plano, mais abstrato, aponta, por seu turno, para a tensão entre os diferentes direitos fundamentais e objetivos de interesse público justificativos da atuação dos Estados e da União Europeia, nomeadamente na concretização de deveres de proteção (através da lei), por um lado, e a inovação e liberdade de empresa, por outro, esta última uma liberdade jusfundamental particularmente fragilizada, seja pela responsabilização dos privados por funções tipicamente públicas, seja pela imposição de um conjunto de deveres e de obrigações que mimetizam, de igual modo, funções paraestaduais.

Independentemente da complexidade das tensões e da forma como resolvidas pelo legislador, certo é que, no ordenamento jurídico da União Europeia, é hoje possível descobrir vários laços de comunicação entre os diferentes atos normativos e os objetivos de garantia e efetivação da liberdade, independência e pluralismo dos *media*.

Adere-se, quanto ao *quomodo*, a uma distinção-categorização essencial.²⁴ Em primeiro lugar, surgem os atos normativos dirigidos, direta e especificamente, aos meios de comunicação social e respetiva atuação-organização. É o caso da Diretiva Serviços de Comunicação Social Audiovisual.²⁵ Em segundo lugar, aqui chamados de *garantes indiretos*, estão os atos que impactam na liberdade e no pluralismo dos *media*, não já diretamente, mas por força da regulação, seja de atores da cena digital, como as plataformas em linha, seja de aspetos específicos da atividade e da prestação de serviços em linha. A título meramente exemplificativo, cumpre mencionar a Diretiva sobre o comércio eletrónico;²⁶ o Regulamento Serviços Digitais; a Diretiva (UE) 2019/790 relativa aos direitos de autor e direitos conexos no mercado único digital;²⁷ o Regulamento (UE) 2019/1150 também conhecido

²⁴ Seguimos de perto, Brogi *et al.*, “The European Media Freedom Act: media freedom, freedom of expression and pluralism”, 32 e ss.

²⁵ Diretiva 2010/13/UE do Parlamento Europeu e do Conselho, de 10 de março de 2010, relativa à coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à oferta de serviços de comunicação social audiovisual (Diretiva Serviços de Comunicação Social Audiovisual) JO L 95 de 15.04.2010, 1-24 (versão codificada), ELI: <http://data.europa.eu/eli/dir/2010/13/2018-12-18>.

²⁶ Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (Diretiva sobre comércio eletrónico) JO L 178 de 17.7.2000, 1-16 (versão codificada)*, ELI: <http://data.europa.eu/eli/dir/2000/31/2024-02-17>.

²⁷ Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE, JO L 130 de 17.5.2019, 92-125, ELI: <http://data.europa.eu/eli/dir/2019/790/oj>.

como Regulamento P2B – *Platform 2 Business*;²⁸ o Regulamento Mercados Digitais;²⁹ ou, ainda, o Regulamento (UE) 2024/900 sobre a transparência e o direcionamento da propaganda política,³⁰ entre outros. Finalmente, importa não esquecer, também, o contributo de regras horizontais (tradicionais), de que são exemplo a política da concorrência, que, ora através do controlo de operações de concentração,³¹ ora pelo regime dos auxílios de Estado,³² desvela, também, o seu potencial para contribuir para o pluralismo e a independência dos *media*.

3.1. O Regulamento Serviços Digitais como garante indireto de liberdade e pluralismo dos media: oportunidades, riscos e insuficiências

O Regulamento Serviços Digitais (‘DSA’) é um ato normativo da União Europeia, diretamente aplicável em todos os seus Estados-Membros (sem prejuízo da necessidade de legislação nacional de execução-implementação).³³ Este Regulamento atualiza a Diretiva sobre o comércio eletrónico a uma evolução entretanto sofrida no espaço digital, e que deita por terra a crença na suficiência do paradigma do *free marketplace of ideas*.³⁴ Em sua substituição, emerge a era do constitucionalismo digital.³⁵

Além da atualização do regime de isenções condicionais de responsabilidade já consagradas na referida Diretiva, o DSA introduz um conjunto de obrigações de devida diligência que vinculam – de forma escalonada e, portanto, proporcional ao respetivo tipo e dimensão – os diferentes prestadores de serviços intermediários

²⁸ Regulamento (UE) 2019/1150 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha JO L 186 de 11.7.2019, 57-79, ELI: <http://data.europa.eu/eli/reg/2019/1150/oj>.

²⁹ 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) JO L 265 de 12.10.2022, 1-66, ELI: <http://data.europa.eu/eli/reg/2022/1925/oj>.

³⁰ 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 JO L, 2024/900, 20.3.2024, ELI: <http://data.europa.eu/eli/reg/2024/900/oj>.

³¹ Para uma relação entre o pluralismo dos *media* e o controlo de concentrações, *vd.*, *inter alia*, Valeria Caforio, “Media pluralism and competition in the media sector: the Italian experience”, in (eds.) Małgorzata Kozak, e Marta Sznajder, *Yearbook of Antitrust and Regulatory Studies* 17, no. 30 (2024), <https://press.wz.uw.edu.pl/yars/>.

³² Para uma nova abordagem da questão, *cf.*, em particular, Dionysios Pelekis, e Małgorzata Kozak, “Public value and the compatibility of state aid to public service broadcasters – the hot potato for the European Commission”, in Małgorzata Kozak, e Marta Sznajder (eds.), *Yearbook of Antitrust and Regulatory Studies* 17, no. 30 (2024), <https://press.wz.uw.edu.pl/yars/>.

³³ Sobre o DSA, *vd.*, em particular, Martin Husovec, *Principles of the Digital Services Act* (Oxford University Press, 2024). Para uma caracterização, *vd.*, também, Inês Neves, “A reading of the digital markets act in the Light of Fundamental Rights”, in (eds.) Annegret Engel, Xavier Groussot, e Gunnar Thor Petrusson, *New directions in digitalisation. Perspectives from EU Competition Law and the Charter of Fundamental Rights* (European Union and its Neighbours in a Globalized World, vol 13. Springer, Cham, 2025), https://doi.org/10.1007/978-3-031-65381-0_8, e, bem assim, Inês Neves, “From the Digital Services package to the Digital Markets Act: the road to a (more) secure, open, and fundamental rights-friendly digital space”, *UNIO - EU Law Journal, Official Blog* (blog), 4 de maio, 2023, <https://officialblogofunio.com/2023/05/04/from-the-digital-services-package-to-the-digital-markets-act-the-road-to-a-more-secure-open-and-fundamental-rights-friendly-digital-space/>.

³⁴ Sobre a evolução do paradigma, *cf.* Pollicino, e Paolucci, “Unveiling the digital side of journalism”, 4 e ss.

³⁵ Neste sentido, Giancarlo Frosio, “From the E-Commerce Directive to the Digital Services Act”, in *Digital Services Act Commentary*, eds. Christian Twigg-Flesner, e Lorna Woods (Edward Elgar, forthcoming 2025), *SSRN Electronic Journal*, 19 de agosto, 2024, <https://ssrn.com/abstract=4914816> ou <http://dx.doi.org/10.2139/ssrn.4914816>.

abrangidos (desde redes sociais a motores de pesquisa em linha, mercados em linha e outras plataformas de distribuição de conteúdos e prestação de serviços em linha).

Da conjugação destas duas dimensões principais do DSA resulta possível descobrir a sua proximidade e potencial contributo para acomodar os riscos e os perigos enfrentados pelos meios de comunicação social no ambiente em linha, nomeadamente através das normas dirigidas à remoção de conteúdos ilegais e à garantia de transparência (em matéria de recomendação e publicidade) e, bem assim, à consagração de direitos processuais. Isso mesmo ficou particularmente evidenciado aquando da adoção e da entrada em vigor do Regulamento Serviços Digitais, que várias associações representativas do setor e da atividade dos *media* então aplaudiram e acolheram como um marco essencial na proteção da liberdade de imprensa e na garantia da segurança dos jornalistas em linha.³⁶

Antes de desenvolver em maior medida um tal contributo, importa, porém, abrir um breve parêntese para aludir a uma outra dimensão relacional entre o DSA e os *media*. Com efeito, pese embora o cerne desta comunicação se dirija à questão de saber de que forma a regulação das plataformas em linha – como sujeitos diferentes ou oponíveis aos *media* – contribui ou é garantia (ainda que indireta) da liberdade, independência e pluralismo dos segundos, importa não ignorar a possibilidade de prestadores de serviços de comunicação social se verem, também eles, sujeitos às obrigações e ao regime do DSA, enquanto prestadores de serviços intermediários abrangidos. Efetivamente, e apesar de nem sempre os meios de comunicação social apresentarem um modelo de negócio plataformizado, a sua qualificação como prestadores de serviços intermediários não resulta determinantemente afastada, antes sendo perfeitamente possível, desde logo por referência a meios de comunicação social que se apresentem titulares de uma página *web* própria, na qual haja lugar à circulação de conteúdo de terceiros (os leitores, por exemplo), o que se afigura possível, ora em razão da presença de uma secção de comentários, de classificações (*reviews*), ou, ainda, de *chats*.³⁷

Em resultado, se é certo que o DSA reserva a noção de *plataformas em linha* para os cenários em que há disseminação de informação ao público, afastando, portanto, e em particular, elementos menores e ancilares como a secção de comentários de um jornal em linha,³⁸ esta exclusão não afasta a eventual qualificação de *media* como serviço(s) intermediários de outra natureza, por exemplo, de simples alojamento virtual ou *hosting*.³⁹ O parêntese – que não se justifica pela centralidade que assume nesta comunicação – serve, porém, para assinalar que a perspetivação dos meios

³⁶ “Press freedom in the digital age: the impact of the Digital Services Act”, *Free Press Unlimited* (blog), 25 de agosto, 2023, <https://www.freepressunlimited.org/en/current/press-freedom-digital-age-impact-digital-services-act>.

³⁷ Sobre a questão, Philipp Koehler e Thomas Walter, “A snapshot of the DSA’s impact on media companies”, *Taylor Wessing*, 12 de junho, 2023, <https://www.taylorwessing.com/en/interface/2023/media-update-2023/a-snapshot-of-the-dsas-impact-on-media-companies>.

³⁸ Cf. artigo 3.º, i), e, em particular, considerando 13, DSA.

³⁹ Nos termos do artigo 3.º, g), um serviço intermediário é “um dos seguintes serviços da sociedade da informação: i) um serviço de «simples transporte», que consiste na transmissão, através de uma rede de comunicações, de informações prestadas por um destinatário do serviço ou na concessão de acesso a uma rede de comunicações, ii) um serviço de «armazenagem temporária» que consiste na transmissão, através de uma rede de comunicações, de informações prestadas por um destinatário do serviço, que envolve a armazenagem automática, intermédia e temporária dessas informações efetuada apenas com o objetivo de tornar mais eficaz a transmissão posterior das informações a outros destinatários, a pedido destes, iii) um serviço de «alojamento virtual» que consiste na armazenagem de informações prestadas por um destinatário do serviço e a pedido do mesmo”, sendo as plataformas em linha um tipo específico de serviço de alojamento virtual.

de comunicação social que doravante se assumirá – como beneficiários eventuais das obrigações impostas pelo DSA a (grandes) plataformas em linha –, não afasta, por confusão, a sua eventual sujeição, também, a obrigações impostas pelo próprio DSA (ainda que mais leves). Esta mesma ideia resulta, aliás, de forma clara, do *European Media Freedom Act*,⁴⁰ cujo considerando 11 expressamente reconhece que: “[n]o mercado digital dos meios de comunicação social, os fornecedores de plataformas de partilha de vídeos ou os fornecedores de plataformas em linha de muito grande dimensão poderão ser abrangidos pela definição de prestador de serviços de comunicação social. [...] sempre que exerçam controlo editorial sobre uma ou várias secções dos seus serviços, esses fornecedores poderão ser considerados tanto fornecedores de plataformas de partilha de vídeos como fornecedores de plataformas em linha de muito grande dimensão e prestadores de serviços de comunicação social.”

Com este esclarecimento em mente, importa agora retomar a questão de estudo – aferir de que forma as obrigações impostas às (grandes) plataformas em linha pelo DSA contribuem para assegurar a independência e o pluralismo dos meios de comunicação social – e, com ela, concretizar como poderá o Regulamento Serviços Digitais atuar como garantia indireta dos *media* no espaço digital.

3.1.1. Os meios de comunicação social como beneficiários do Regulamento Serviços Digitais

Seja através da promoção da segurança e da proteção dos jornalistas individualmente considerados, seja através da efetivação e garantia da liberdade de expressão e da liberdade de imprensa em linha, considera-se que o DSA é ou pode atuar, de facto, como garantia indireta dos *media*.

Começando pelas evidências textuais, resulta desde logo do n.º 4 do artigo 14.º do DSA que “[o]s prestadores de serviços intermediários agem de forma diligente, objetiva e proporcionada na aplicação e execução das restrições referidas no n.º 1, tendo devidamente em conta os direitos e interesses legítimos de todas as partes envolvidas, incluindo os direitos fundamentais dos destinatários do serviço, como a liberdade de expressão, a liberdade e o pluralismo dos meios de comunicação social e outros direitos e liberdades fundamentais, tal como consagrados na Carta.” Com esta nota, reiterada no considerando 47 por referência aos fornecedores de plataformas em linha de muito grande dimensão, o legislador europeu assinala a necessidade de as plataformas em linha prestarem particular atenção ao impacto que eventuais restrições à utilização dos seus serviços⁴¹ poderão ter em direitos e em interesses públicos particularmente relevantes para os meios de comunicação social.

Já no conjunto de obrigações impostas (apenas) aos fornecedores de plataformas em linha de muito grande dimensão e aos motores de pesquisa em linha de muito grande dimensão, descobre-se, na alínea b) do n.º 1 do artigo 34.º do DSA, uma segunda referência à liberdade e ao pluralismo dos meios de comunicação social, a par da liberdade de expressão e de informação consagradas no artigo 11.º da CDF, desta feita a propósito da avaliação (e consequente dever de atenuação) de riscos

⁴⁰ Regulamento (UE) 2024/1083 do Parlamento Europeu e do Conselho, de 11 de abril de 2024, que cria um regime comum para os serviços de comunicação social no mercado interno e que altera a Diretiva 2010/13/UE (Regulamento Europeu relativo à Liberdade dos Meios de Comunicação Social) JO L, 2024/1083, 17.4.2024, ELI: <http://data.europa.eu/eli/reg/2024/1083/oj>.

⁴¹ São exemplos dessas restrições, a supressão, a desativação do acesso, a despromoção de conteúdos, e, ainda, a suspensão ou a cessação (total ou parcial) da prestação do serviço e/ou o encerramento da conta dos destinatários.

sistémicos. Os referidos direitos e interesses públicos surgem aqui reconduzidos a uma das categorias de risco sistémico cuja avaliação aprofundada é exigida aos fornecedores de plataformas em linha, e que, como o legislador europeu assinala no considerando 81, podem decorrer “*da conceção dos sistemas algorítmicos utilizados [...] ou da utilização abusiva do seu serviço através da apresentação de notificações abusivas ou de outros métodos para silenciar o discurso ou dificultar a concorrência.*”

As referências expressas em texto não fazem *jus* ao potencial do DSA a este propósito, que se estende a outros domínios.⁴² Começando pela moderação de conteúdos – considerada o verdadeiro coração do DSA – não restarão dúvidas sobre o impacto positivo da procedimentalização e da introdução de garantias de *due process* na efetivação dos direitos fundamentais dos *media* no ambiente em linha. Em particular, além de uma aplicação transparente e não discriminatória dos respetivos termos e condições, as plataformas em linha ficam obrigadas a dedicar particular atenção aos direitos fundamentais dos jornalistas e dos meios de comunicação social, atenção que poderá contribuir para evitar ou mitigar o impacto de notificações abusivas,⁴³ estratégias de perseguição e de assédio em linha, e, bem assim, (tentativas de) silenciamento, intimidação e censura de jornalistas (de que o *doxxing* é exemplo),⁴⁴ e que afetam desproporcionalmente as mulheres.⁴⁵

Segue-se o inegável contributo do crescendo de obrigações de transparência, materializadas na elaboração de relatórios anuais e na sujeição a auditorias independentes,⁴⁶ às quais se somam deveres de transparência específicos quanto à publicidade em linha⁴⁷ e aos sistemas de recomendação.⁴⁸ A disponibilização de informação sobre as ações tomadas para o combate à desinformação, e, bem assim, sobre um conjunto de elementos e parâmetros decisivos para a promoção da autonomia e da (liberdade de) escolha do utilizador,⁴⁹ contribui, de forma inegável, para reequilibrar os polos de poder nas plataformas em linha, contribuindo para que os *media* se logrem destacar pela prestação de informação fiável e confiável no ambiente em linha.

Retomando o périplo, e já a propósito das plataformas em linha de muito grande dimensão, adquirem particular importância, como se antecipou, as obrigações conexas com a avaliação periódica e a gestão-mitigação de riscos sistémicos (atuais

⁴² Sobre a relação entre o DSA e a garantia do pluralismo e da liberdade dos *media*, cf. Nenadić, “Policy in Practice: The interplay of the Digital Services Act and the European Media Freedom Act”.

⁴³ Cf. artigo 14.º, n.º 4, DSA.

⁴⁴ Para uma abordagem global da segurança e das diferentes formas de violência contra os jornalistas, cf. Vera Slavtcheva-Petkova *et al.*, “Conceptualizing journalists’ safety around the globe”, in *Journalism and Safety*, ed. Oscar Westlund, Roy Krøvel, e Kristin Skare Orgeret (Routledge, 2024).

⁴⁵ “Press freedom in the digital age: the impact of the Digital Services Act”. Sobre a questão, cf. “Safeguarding women journalists in the digital age”, *European Centre for Press & Media Freedom*, 8 de março, 2024, <https://www.ecpmf.eu/safeguarding-women-journalists-in-the-digital-age/>.

⁴⁶ Cf. artigos 15.º, 24.º, 37.º e 42.º do DSA e, em particular, Regulamento Delegado (UE) 2024/436 da Comissão, de 20 de outubro de 2023, que completa o Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho estabelecendo regras relativas à realização de auditorias das plataformas em linha de muito grande dimensão e dos motores de pesquisa em linha de muito grande dimensão C/2023/6807, JO L, 2024/436, 2.2.2024, ELI: http://data.europa.eu/eli/reg_del/2024/436/oj.

⁴⁷ Cf. artigo 26.º, DSA.

⁴⁸ Cf. artigo 27.º, DSA. Sobre as limitações do preceito, cf. Paddy Leerssen, “An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation”, *Computer Law & Security Review* 48, 105790, 2023, 10-11, <https://doi.org/10.1016/j.clsr.2023.105790>.

⁴⁹ Sobre as diferentes vias e, em particular, a diferença entre abordagens mais paternalistas e liberais, na garantia da autonomia dos utilizadores em relação a conteúdos recomendados, cf., Judith Vermeulen, “To nudge or not to nudge: news recommendation as a tool to achieve online media pluralism”, *Digital Journalism* 10, no. 10 (2022), <https://doi.org/10.1080/21670811.2022.2026796>.

ou potenciais) decorrentes do *design*, operação e uso dos respetivos serviços.⁵⁰ Perante tais riscos sistémicos, os fornecedores de plataformas em linha de muito grande dimensão ficam obrigados a adotar *medidas de atenuação razoáveis, proporcionadas e eficazes*, e que poderão incluir a adaptação das respetivas interfaces em linha, dos processos de moderação de conteúdos e, bem assim, dos sistemas de recomendação.

Conjugando o texto do Regulamento com os considerandos 94 e 95, logra-se extrair uma preocupação particular para com a desinformação. Com efeito, esta surge reconduzida a uma categoria de risco sistémico que exige dos fornecedores especial atenção, nomeadamente quando a “*a amplificação algorítmica das informações contribua para os riscos sistémicos*” ou, ainda, quando tal risco decorra, em particular, da “*utilização não autêntica do serviço, como a criação de contas falsas, a utilização de robôs digitais ou a utilização enganosa de um serviço, e de outros comportamentos automatizados ou parcialmente automatizados.*”⁵¹ Ora, sendo o combate à desinformação uma das vias garantes do acesso a informação fidedigna e de qualidade, também por aqui se descobre o potencial positivo da imposição de medidas de gestão de risco, como a rapidez do tratamento de notificações e da supressão de conteúdos notificados,⁵² a sensibilização dos destinatários do serviço e a prestação de mais informação,⁵³ em particular no que se refere a *deep fakes*.⁵⁴

Finalmente, importa também salientar a preocupação do legislador europeu para com a introdução de garantias (desde logo, de fundamentação e contraditório)⁵⁵ e de vias de reclamação, resolução extrajudicial de litígios, recurso (judicial) e reparação,⁵⁶ que de igual modo contribuem para um ambiente em linha mais seguro, também em favor dos meios de comunicação social.

O breve périplo serve para atestar como o Regulamento Serviços Digitais – pese embora desprovido de uma intenção de proteção talhada e especialmente dirigida aos meios de comunicação social – se apresenta, ainda assim, como um garante indireto do respetivo pluralismo e independência. Visando as plataformas em linha como suas destinatárias, e reconhecendo-as como entidades com um poder infraestrutural impactante na esfera pública,⁵⁷ o legislador europeu adota um enquadramento normativo que beneficia, de igual modo, os meios de comunicação social, como destinatários especiais e prototípicos dos serviços daquelas.

⁵⁰ Cf. artigos 34.º e 35.º, DSA. Acresce, ainda como relevante, o mecanismo de resposta em caso de crise, consagrado no artigo 36.º do DSA. Sobre este, cf., Baskaran Balasingham, e Sofia Minichováin, “The DSA’s crisis response mechanism and the indispensability of social media networks”, in *Yearbook of Antitrust and Regulatory Studies*, ed. Małgorzata Koza e Marta Sznajder, 17, no. 30 (2024), <https://press.wz.uw.edu.pl/yars/>.

⁵¹ Cf. considerandos 84 e 85, DSA.

⁵² Cf. artigo 35.º, n.º 1, al. c), DSA.

⁵³ Cf. artigo 35.º, n.º 1, al. i), DSA.

⁵⁴ As *deep fakes* podem ser definidas como elementos de informação “*quer se trate de uma imagem, de áudio ou de um vídeo gerados ou manipulados que se assemelham sensivelmente a pessoas, objetos, lugares ou a outras entidades ou acontecimentos existentes e que pareçam falsamente a uma pessoa serem autênticos ou verdadeiros*”. O DSA impõe a sua distinguibilidade “*através de marcações visíveis*” e, bem assim, a disponibilização de uma funcionalidade que permita a sua sinalização pelos destinatários do serviço - cf. artigo 35.º, n.º 1, al. k), DSA.

⁵⁵ Cf. artigo 17.º, DSA.

⁵⁶ Cf. artigos 20.º, 21.º, 23.º e 54.º, DSA.

⁵⁷ Cf. Seipp, Helberger, de Vreese, e Ausloos, “Between the cracks: blind spots in regulating media concentration and platform dependence in the EU”, 9.

3.1.2. *Dos riscos às insuficiências do DSA na garantia dos meios de comunicação social em linha*

Não obstante o potencial do Regulamento Serviços Digitais como garante indireto dos meios de comunicação social em linha, importa não ignorar alguns dos riscos que lhe vão associados.

Ab initio, estão os perigos e as incertezas associadas ao papel de *intermediário regulatório* reconhecido a operadores privados.⁵⁸ Com efeito, pese embora o inegável contributo que o DSA vem aportar para a procedimentalização e a introdução de balizas no que antes se poderia considerar um *Velho Oeste*, não deixa de ser verdade que as suas regras carecem de uma implementação prática, atuada por operadores privados cujo modelo de negócio e lógica de atuação se norteiam por objetivos, interesses e valores que, pese embora igualmente dignos de tutela, são em muito distantes ou dissonantes dos objetivos de interesse público que norteiam o Regulamento. Em particular, e naturalmente sem que se lhes possa condenar, não suscitará surpresa o recurso, por tais operadores, a princípios e a mecanismos de automatização, que permitam a operacionalização eficaz das respetivas interfaces, também e sobretudo no que à moderação de conteúdos se refere.⁵⁹

Não sendo *per se* problemática, à automatização somam-se elementos que a associam a um risco particular de censura.

Em primeiro lugar, o enquadramento normativo aplicável que, pese embora refletindo velhos *safe harbours*,⁶⁰ não deixa de responsabilizar as plataformas pelo conhecimento (presumido), na sequência de uma notificação de informação por um destinatário do serviço.⁶¹ Repare-se que, não obstante ciente do risco (da frequência) de notificações ou reclamações manifestamente infundadas,⁶² o legislador europeu não deixar de aceitar e verdadeiramente chancelar a delegação da gestão destes conflitos em privados, numa confiança que ignora a complexidade e as dificuldades dos juízos de ponderação concretos.

Em segundo lugar, a crescente pressão, vigilância (“*civic vigilantism*”), e sujeição a ações coletivas, não raramente ilegítimas, infundadas, e empregues como estratégias de ameaça (“*reverse strategic litigations*”). Ambos os fatores promovem uma leitura e aplicação particularmente cautelosas das obrigações de devida diligência do DSA. Em suma, uma atitude precaucionista que, uma vez conjugada com eventuais erros no processo de moderação de conteúdos, poderá facilmente redundar na remoção por defeito (*overblocking*) e, a final, na “*deplatformization*”⁶³ de meios de comunicação social,

⁵⁸ Sobre este, cf. Gamito, “Consistent regulatory and self-regulatory mechanisms for media freedom in the digital single market”, 2.

⁵⁹ No sentido de que “*algorithmic moderation has become necessary to manage growing public expectations for increased platform responsibility, safety and security on the global stage*”, e procedendo a uma análise dos respetivos riscos, cf. Robert Gorwa, Reuben Binns, e Christian Katzenbach, “Algorithmic content moderation: Technical and political challenges in the automation of platform governance”, *Big Data&Society* 7, no. 1 (2020), <https://doi.org/10.1177/2053951719897945>.

⁶⁰ Referimo-nos às isenções de responsabilidade dos artigos 4.º, 5.º e 6.º, a que se somam os artigos 7.º e 8.º do DSA.

⁶¹ Nos termos do artigo 16.º, n.º 3 do DSA, “*Considera-se que as notificações referidas no presente artigo dão lugar a um conhecimento efetivo ou a um alerta para efeitos do artigo 6.o relativamente ao elemento específico de informação em causa quando permitem a um prestador diligente de alojamento virtual identificar a ilegalidade da atividade ou das informações em causa sem um exame jurídico pormenorizado.*”

⁶² Cf. artigo 23.º, DSA, em particular n.º 2.

⁶³ Sobre a capacidade de as plataformas procederem a esta ‘*deplatformization*’, *vd.*, “The Digital Services Act (DSA): could it impact public media?”, *Public Media Alliance*, 28 de janeiro, 2022, <https://www.publicmediaalliance.org/the-digital-services-act-dsa-could-it-impact-public-media/>. Considerando que, pese embora a ausência de dados, são inegáveis as interferências das plataformas em meios de comunicação

i) seja pela incompatibilidade fundamental entre a automatização e a análise exigida por nuances da linguagem, diferentes intenções (dos autores), e contextos culturais e sociopolíticos heterogêneos,⁶⁴ *ii)* seja pela maior sujeição dos conteúdos jornalísticos – sobretudo críticos, minoritários ou controversos – à notificação por destinatários do serviço. Tudo isto, sem que as garantias de recurso e de eventual reparação se apresentem remédios eficazes, atenta a presença de conteúdos cuja relevância temporal é limitada ou circunscrita. Afinal, não haverá exemplo mais evidente de bem perecível.

Além de riscos, o DSA apresenta, também, insuficiências não despidiendas. Seguindo de perto a doutrina, três merecem particular destaque. Em primeiro lugar, e sem prejuízo dos benefícios indiretos da regulação das plataformas em linha para os meios de comunicação tradicionais, não deixa de ser certo que o Regulamento não visa os *media* diretamente, nem sequer cuida de aspetos relevantes da sua independência e pluralismo (inclusive, em relação às próprias plataformas em linha).⁶⁵ A segunda insuficiência foi já tratada a propósito dos riscos. Referimo-nos à margem de conformação reconhecida às plataformas que – uma vez conjugada com um ambiente de incerteza regulatória, e com as particularidades e dificuldades ínsitas à ponderação de direitos e interesses conflitantes e colidentes na era digital – se poderá sobrepor às vantagens da procedimentalização e das garantias tentativamente introduzidas no DSA. E com isto se chega à terceira insuficiência, contendente com o grau de determinação logrado pelo DSA. Com efeito, apesar da introdução de balizas procedimentais antes inexistentes no que se refere aos mecanismos de notificação e ação, descobrem-se soluções que, podendo satisfazer os direitos e interesses dos demais destinatários dos serviços intermediários, poderão, na prática, não alcançar idêntico grau de suficiência em relação aos meios de comunicação social e tipo de atividade em linha. A título meramente exemplificativo, se é certo que o artigo 17.º do DSA impõe uma exposição de motivos subsequente à adoção de uma medida de restrição (ex.: a remoção de um conteúdo específico de informação), as plataformas em linha não se veem obrigadas a um qualquer dever de informação a ser exercido em momento prévio a essa atuação. Por seu turno, se é também verdade que o artigo 16.º do DSA exige que as plataformas atuem “*sem demora injustificada*” na sequência de uma notificação por um destinatário do serviço, o preceito não prevê um prazo específico de atuação, imprecisão que, pese embora compreensível pelo casuismo ínsito à apreciação, poderá aportar consequências muito danosas para os meios de comunicação social e, em particular, para os jornalistas individualmente considerados, em razão do potencial de disseminação de um conteúdo ou comentário lesivo ou danoso.⁶⁶

social e os casos de recusa de acesso de jornalistas a plataformas em linha, cf. “Report on workshop – Online journalism: Digital Services Act and European Media Freedom Act, 23 February 2023”, *DSA Observatory*, 13 de abril, 2023, <https://dsa-observatory.eu/2023/04/13/report-on-workshop-online-journalism-digital-services-act-and-european-media-freedom-act-23-february-0/>.

⁶⁴ Sobre os problemas da moderação de conteúdos decorrentes da presença de juízos de valor complexos, cf. Elizabeth Stewart, “Detecting fake news: two problems for content moderation”, *Philosophy & Technology* 34 (2021), <https://doi.org/10.1007/s13347-021-00442-x>.

⁶⁵ Neste sentido, cf. Seipp, Helberger, de Vreese, e Ausloos, “Between the cracks: blind spots in regulating media concentration and platform dependence in the EU”, 9-10. De idêntica insuficiência padece o Regulamento Mercados Digitais, que, contribuindo, é certo, para a liberdade de entrada no mercado de utilizadores profissionais, ignora as idiossincrasias dos meios de comunicação social como utilizadores “*diferentes*.” O que se acaba de assinalar é sobremaneira relevante, dado apontar para uma idiossincrasia dos *media* nos mercados digitais. Em particular, considera-se que os meios de comunicação social nem são utilizadores profissionais comuns, do tipo empresas, prestadoras de um serviço como qualquer outro, nem são, por seu turno, consumidores ou utilizadores finais comuns.

⁶⁶ Cf. “Press freedom in the digital age: the impact of the Digital Services Act.”

Estes riscos e insuficiências atestam a necessidade de valorar o Regulamento Serviços Digitais por aquilo que ele é – garante indireto e parcial dos *media* –, e que importa conjugar com outros atos normativos. Em particular, dar-se-á nota de como o âmbito e o regime da moderação de conteúdos do Regulamento Serviços Digitais se veem hoje particularmente exauridos, na sequência da adoção Regulamento Europeu relativo à Liberdade dos Meios de Comunicação Social. Desse ato, e da controversa questão do tratamento a votar aos meios de comunicação social *vis-à-vis* as plataformas em linha, se tratará agora.

4. Do DSA ao *European Media Freedom Act*: diferentes caminhos para a proteção da liberdade e pluralismo dos *media* no ambiente em linha

Como se assinalou, o Regulamento Serviços Digitais é apenas uma peça num *puzzle* normativo-regulatório maior, e que inclui outros atos normativos, todos eles podendo aportar contributos não despidiendos para acomodar as insuficiências assinaladas ao primeiro. A título meramente exemplificativo, importa assinalar o disposto no artigo 4.º do Regulamento (UE) 2019/1150 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha, nos termos do qual se exige aos prestadores de serviços de intermediação em linha um dever de fundamentação, que, em contraste com o previsto no artigo 17.º do DSA, deverá ser transmitida “*antes ou no momento em que a restrição ou suspensão produza efeitos, a fundamentação da sua decisão num suporte duradouro*”, e, inclusive, pelo menos no caso de cessação da prestação de todos os serviços de intermediação em linha a um determinado utilizador profissional, “*pelo menos trinta dias antes da cessação produzir efeitos.*”

Mais recentemente, o legislador europeu viria a adotar o Regulamento Europeu relativo à Liberdade dos Meios de Comunicação Social (*European Media Freedom Act* ou ‘EMFA’ como mais comumente conhecido) que, pese embora preservando a aplicabilidade do DSA como *lex generalis* supletiva, não deixa – pelo menos no que às plataformas em linha de muito grande dimensão se refere – de lhe retirar centralidade no domínio da moderação de conteúdos, respeitante a meios de comunicação social.

Em causa está uma meta-regulação que, ao contrário do DSA, visa diretamente os meios de comunicação social, e que tem por objetivos *i)* proteger a independência editorial, nomeadamente evitando a interferência indevida de Estados e grupos privados na produção de conteúdo jornalístico; *ii)* combater a concentração excessiva dos *media*; *iii)* assegurar a transparência da respetiva estrutura de propriedade e, com tudo isto, *iv)* salvaguardar o funcionamento independente dos meios de comunicação social.⁶⁷

Em particular no que se refere à atuação dos *media* em linha, reconhece o legislador, nos considerandos do EMFA, que *i)* “[o]s prestadores de serviços de comunicação

⁶⁷ Apesar da sua adoção recente, a preocupação da União Europeia para com a garantia de liberdade, independência e pluralismo dos *media* não deve ser encarada como novidade. Querelas quanto à divisão de competências e, em particular, quanto à possibilidade de a União Europeia adotar legislação vinculativa na matéria obstaram, segundo se afirma, a uma posição anterior. Neste sentido, Elda Brogi *et al.*, “The European Media Freedom Act: media freedom, freedom of expression and pluralism”, 9 e ss. No mesmo sentido, Christina Holtz-Bacha, “Freedom of the media, pluralism, and transparency. European media policy on new paths?”, *European Journal of Communication* 39, no. 1 (2024), <https://doi.org/10.1177/02673231231176966>.

social que exercem a responsabilidade editorial pelos seus conteúdos desempenham um papel essencial na distribuição de informações e no exercício do direito de receber e transmitir informação em linha”, e que ii) “[a]s plataformas em linha de muito grande dimensão funcionam, para muitos utilizadores, como uma porta de acesso a conteúdos mediáticos e a serviços de comunicação social.” Partindo de ambas as assunções, e ciente do impacto positivo de uma proteção particular dos *media* na liberdade de prestação de serviços, na liberdade de expressão, e no direito dos utilizadores de receberem e transmitirem informação, o legislador europeu considera importante garantir que “os prestadores de serviços de comunicação social atuem com diligência e forneçam informações fiáveis e respeitadoras dos direitos fundamentais, em consonância com os requisitos regulamentares ou os mecanismos de correção ou de autorregulação a que estão sujeitos nos Estados-Membros.”⁶⁸

Laborando sobre estes pressupostos, o legislador europeu introduz, no *European Media Freedom Act*, um verdadeiro regime especial em favor dos serviços de comunicação social que se autodeclarem como tal,⁶⁹ e que preencham determinados requisitos de independência editorial (face a Estados-Membros, partidos políticos, países terceiros e entidades por estes controladas ou financiadas) e sujeição a requisitos regulamentares, e ou a mecanismos de correção ou de autorregulação, impondo obrigações de transparência e regras profissionais e éticas.⁷⁰

Vinculados a este regime e ao conjunto de deveres de devida diligência especiais constantes do texto do Regulamento⁷¹ ficam os fornecedores de plataformas em

⁶⁸ Cf. considerando 50, EMFA, também para as citações anteriores.

⁶⁹ Nos termos do considerando 53 do EMFA, “os fornecedores de plataformas em linha de muito grande dimensão que facultam acesso a conteúdos mediáticos deverão disponibilizar uma funcionalidade nas suas interfaces em linha que permita aos prestadores de serviços de comunicação social declarar que cumprem determinados requisitos, mantendo simultaneamente a possibilidade de rejeitarem essa autodeclaração, caso considerem que as referidas condições não são cumpridas. Quando um prestador de serviços de comunicação social declarar que cumpre os requisitos regulamentares ou que aplica um mecanismo de correção ou autorregulação, deverá poder facultar os dados de contacto da autoridade ou entidade reguladora nacional competente ou dos representantes do mecanismo de correção ou autorregulação, incluindo os dados de contacto fornecidos por associações profissionais amplamente reconhecidas que representem um determinado subsector e operem a nível da União ou a nível nacional. Em caso de dúvidas razoáveis, essa informação permitirá ao fornecedor de uma plataforma em linha de muito grande dimensão confirmar junto dessas autoridades ou entidades se o prestador de serviços de comunicação social está sujeito a tais requisitos ou mecanismos. Se for caso disso, os fornecedores de plataformas em linha de muito grande dimensão deverão recorrer a informações relativas ao cumprimento destes requisitos, como a norma de leitura por máquina da Journalism Trust Initiative (Iniciativa Jornalismo de Confiança), desenvolvida sob a égide do Comité Europeu de Normalização, ou outros códigos de conduta pertinentes. As organizações da sociedade civil reconhecidas, as organizações de verificação de factos e outras organizações profissionais pertinentes que reconheçam a integridade das fontes dos meios de comunicação social com base em normas acordadas com o setor dos meios de comunicação social deverão também ter a possibilidade de assinalar aos fornecedores de plataformas em linha de muito grande dimensão qualquer potencial problema relativo ao incumprimento, por parte dos prestadores de serviços de comunicação social, dos requisitos pertinentes para a autodeclaração. As orientações emitidas pela Comissão serão fundamentais para facilitar uma aplicação eficaz dessa funcionalidade. Essas orientações deverão contribuir para minimizar o risco de potencial abuso da funcionalidade, em especial por parte dos prestadores de serviços de comunicação social que se dedicam sistematicamente à desinformação, à manipulação da informação e à ingerência, incluindo os controlados por determinados países terceiros, tendo em conta os critérios a desenvolver pelo Comité relativamente aos prestadores de serviços de comunicação social fora da União. Para o efeito, essas orientações poderão abranger disposições relacionadas com a participação de organizações da sociedade civil reconhecidas, incluindo organizações de verificação de factos, na análise das declarações, ou com a consulta a autoridades ou entidades reguladoras nacionais ou a organismos de correção ou autorregulação.” Sobre o âmbito de aplicação subjetivo do “*media privilege*”, cf. Monti, “The missing piece in the DSA puzzle?”, 197 e ss.

⁷⁰ Cf. artigo 18.º e considerando 50 e ss., EMFA. Além disso, o artigo 18.º, n.º 1, e), EMFA exige, ainda, que o potencial prestador de serviços de comunicação social declare que não fornece conteúdos gerados por sistemas de inteligência artificial sem os submeter a análise humana ou a um controlo editorial.

⁷¹ O texto do EMFA revela-se, na sua versão final, um tanto distante da proposta original, então sujeita a críticas várias. Neste sentido, cf. Monti, “The missing piece in the DSA puzzle?”, 197.

linha de muito grande dimensão⁷² que, além da atenção ao impacto da moderação de conteúdos na liberdade e pluralismo dos meios de comunicação social, e em acréscimo aos deveres de fundamentação já resultantes do DSA e do Regulamento (UE) 2019/1150, atos normativos que em nada ficam prejudicados, ficam agora cumulativamente vinculados às obrigações resultantes do EMFA.

Em particular, o *European Media Freedom Act* impõe às plataformas em linha de muito grande dimensão *i)* a disponibilização e gestão de uma funcionalidade de autodeclaração; *ii)* a apresentação de uma fundamentação prévia à produção de efeitos de uma suspensão ou restrição da visibilidade (com o consequente atraso na moderação de conteúdos);⁷³ *iii)* a garantia de contraditório (resposta à fundamentação) ao prestador de serviços de comunicação social afetado, no prazo de 24 horas (ou mais curto, em caso de crise); e, na sequência dessa resposta ou ausência dela, *iv)* o subsequente dever de informação ao prestador de serviços de comunicação social afetado, da intenção de proceder à suspensão do serviço ou à restrição da visibilidade do conteúdo. Já em contexto de reclamação, o Regulamento impõe, ainda, *iv)* o tratamento prioritário e sem demora injustificada das reclamações apresentadas por prestadores de serviços de comunicação social.

Em paralelo, o legislador europeu prevê, ainda, a organização, pelo Comité Europeu dos Serviços de Comunicação Social,⁷⁴ de pelo menos um diálogo estruturado por ano, “*entre fornecedores de plataformas em linha de muito grande dimensão, representantes de prestadores de serviços de comunicação social e representantes da sociedade civil, a fim de promover o acesso a ofertas diversificadas de meios de comunicação social independentes em plataformas em linha de muito grande dimensão, debater experiências e boas práticas relacionadas com a aplicação das disposições pertinentes do presente regulamento, nomeadamente no que diz respeito aos processos de moderação por parte das plataformas em linha de muito grande dimensão, e acompanhar a adesão a iniciativas de autorregulação que visem proteger os utilizadores contra conteúdos nocivos, incluindo as destinadas a combater a desinformação.*”⁷⁵ Com esta figura, o Regulamento preceitua a obrigatoriedade de os fornecedores de plataformas em linha de muito grande dimensão participarem em diálogos com os prestadores de serviços de comunicação social que respeitem normas de credibilidade e transparência, nomeadamente quando estes considerem que os referidos fornecedores aplicam e impõem repetidamente restrições ou suspensões injustificadas.⁷⁶

Finalmente, e pese embora se não refira, já, a uma garantia em favor dos *media*, importa não ignorar o direito de personalização da oferta reconhecido, no artigo 20.º do EMFA, aos destinatários de serviços de comunicação social, e que lhes permite escolher efetivamente os conteúdos que pretendem ver ou ouvir, de acordo com os seus interesses ou preferências, nos limites do Direito aplicável.⁷⁷

⁷² A definição de fornecedor de plataforma em linha de muito grande dimensão resulta, por remissão, do DSA – cf. artigo 2.º, 10), EMFA.

⁷³ Saliente-se que, tal como consagrado no seu artigo 17.º, o DSA não exige um dever de fundamentação prévio à atuação da plataforma, sem prejuízo das garantias de reclamação, resolução extrajudicial de litígios e demais vias de recurso.

⁷⁴ O Comité Europeu dos Serviços de Comunicação Social (*European Board for Media Services*) é criado na qualidade-condição de organismo consultivo independente a nível da União que reúne as autoridades ou entidades reguladoras nacionais e coordena as suas ações, sucedendo ao Grupo de Reguladores Europeus dos Serviços de Comunicação Social Audiovisual (*European Regulators Group for Audiovisual Media Services*, ERGA).

⁷⁵ Cf. considerando 56, EMFA.

⁷⁶ Cf. artigo 19.º, EMFA.

⁷⁷ *Vd.*, também, considerando 57, EMFA.

Não obstante a sua importância e significado inegáveis, o Regulamento Europeu relativo à Liberdade dos Meios de Comunicação Social afigura-se suscetível de críticas a vários níveis. Se parte delas são comuns e transversais a outros atos normativos europeus no domínio do digital,⁷⁸ outras respeitam, em particular, a insuficiências e a problemas suscitados pelo EMFA em particular. Entre estas últimas, contam-se questões de articulação institucional (entre diferentes autoridades competentes) e normativa (entre enquadramentos normativos nacionais-estaduais e o ordenamento jurídico da União Europeia e, dentro deste, entre o EMFA como *lex specialis*⁷⁹ e as soluções consagradas noutros diplomas, cujas disposições se poderão afirmar de igual modo pertinentes para a compreensão do regime da moderação de conteúdos implicando os *media*.⁸⁰ Ambas as dimensões problemáticas suscitam, por seu turno, desafios à efetividade do Regulamento e respetiva implementação prática.

A estes desafios somam-se as críticas em torno do respetivo alcance subjetivo e substantivo. Em primeiro lugar, o enfoque nos meios de comunicação tradicionais poderá esquecer a importância crescente de jornalistas independentes e de *freelancers*, a que acrescem outras figuras porventura reconduzíveis a uma noção lata de *media*, e cuja precarização poderá justificar idêntica ou até maior proteção.⁸¹ Em segundo lugar, a ausência de mecanismos específicos de proteção dos jornalistas perante os riscos de violência em linha e fora de linha, e, bem assim, em relação a ações estratégicas, justifica repensar os objetivos do EMFA sob o prisma do princípio da proibição da insuficiência.⁸² Em terceiro lugar, não poderá deixar de se assinalar que, pese embora o enquadramento particularmente garantístico ora introduzido em matéria de moderação de conteúdos pelas grandes plataformas em linha, este apenas se aplica a conteúdos violadores dos termos e condições da plataforma, não afetando, pois, a moderação e, por conseguinte, a adoção de medidas restritivas em relação a conteúdos ilegais ou cujo tratamento seja exigido pelo DSA ou pela Diretiva Serviços de Comunicação Social Audiovisual.⁸³

⁷⁸ A atuação da União Europeia em domínios em relação aos quais a sua competência é contestada vem assentando no artigo 114.º do Tratado sobre o Funcionamento da União Europeia como *corredor normativo*, e, em particular, no objetivo de assegurar o bom funcionamento do mercado interno. A favor da particular necessidade de intervenção europeia nesta matéria poderá avançar-se o contexto de *democratic backsliding* em alguns Estados-Membros, como a Polónia e a Hungria, porventura configurando uma atuação em *estado de necessidade*, justificativo da flexibilização das regras de competência (questão orgânica). Sobre esta dimensão em particular, cf. Gamito, “Consistent regulatory and self-regulatory mechanisms for media freedom in the digital single market”, 10 e ss.

⁷⁹ Cf. Seipp, Helberger, de Vreese, e Ausloos, “Between the cracks: blind spots in regulating media concentration and platform dependence in the EU”, 3.

⁸⁰ Destacam-se, em particular, o DSA e o Regulamento n.º 2019/1150. Sobre a articulação deste último com o EMFA, cf. Doris Buijs, “Article 17 Media Freedom Act & the Digital Services Act: aligned or alienated?”, *DSA Observatory*, <https://dsa-observatory.eu/2022/11/25/article-17-media-freedom-act-the-digital-services-act-aligned-or-alienated/>.

⁸¹ Com particulares objeções à definição tradicional acolhida pelo EMFA, cf., *inter alia*, Theresa Seipp, Ronan Ó Fathaigh, e Max van Drunen, “Defining the ‘media’ in Europe: pitfalls of the proposed European Media Freedom Act”, *Journal of Media Law* 15, no. 1 (2023), <https://doi.org/10.1080/17577632.2023.2240998>.

⁸² Sobre as *Strategic Lawsuits against public participation* (‘SLAPPs’), cf. Brogi *et al.*, “The European Media Freedom Act: media freedom, freedom of expression and pluralism”, 30.

⁸³ Nos termos do n.º 4 do artigo 18.º, EMFA, a obrigação de comunicação prévia e garantia de contraditório não se aplicam “se os fornecedores de plataformas em linha de muito grande dimensão suspenderem a prestação dos seus serviços em relação aos conteúdos disponibilizados por um prestador de serviços de comunicação social ou restringirem a visibilidade desses conteúdos em conformidade com as obrigações que lhes incumbem por força dos artigos 28.o, 34.o e 35.o do Regulamento (UE) 2022/2065 e do artigo 28.o-B da Diretiva 2010/13/UE ou com as obrigações relacionadas com conteúdos ilegais nos termos do direito da União.”

As críticas que se podem dirigir a este Regulamento, a par das insuficiências já apontadas ao DSA, no que se refere à garantia e efetivação da liberdade, independência e pluralismo dos meios de comunicação social em linha, não são de molde a privar estes atos normativos do respetivo mérito. Pelo contrário, cada um deles desvela, no respetivo âmbito e contexto aplicativo, um potencial inegável de proteção dos *media*, e que, portanto, não poderá deixar de ser mobilizado neste e com este sentido. Ainda assim, e sem prejuízo, está-se perante insuficiências a que importa votar particular atenção, sendo muitos os desafios futuros, e grande, portanto, a responsabilidade do intérprete, dos *enforcers* e de toda a comunidade de *stakeholders*. O capítulo subsequente visa, apenas e tão-somente, ilustrar alguns desses desafios, atestando a necessidade de uma leitura e aplicação devidamente articuladas do conjunto de atos normativos relevantes para assegurar a liberdade, a independência e o pluralismo dos meios de comunicação social numa sociedade digital plataformizada.

5. Desafios futuros para a liberdade, a independência e o pluralismo dos meios de comunicação social numa sociedade digital plataformizada

A questão de saber como deverá o legislador (europeu) efetivar os deveres de proteção que para si decorrem da liberdade de expressão e da liberdade de imprensa é interrogação que extravasa o objeto desta comunicação, e que se reconduz ainda, às diferentes teorias da democracia.

Duas principais vias logram, porém, identificar-se, e às mesmas subjazem posições de princípio de certo modo antagonísticas quanto à melhor forma de assegurar e promover a liberdade, a independência e o pluralismo dos *media*. Por um lado, é possível defender a adoção de um enquadramento normativo especial, adequado às particularidades e às idiossincrasias dos meios de comunicação social como destinatários *especiais* dos serviços de plataforma, e talhado com respostas específicas às ameaças que os afetam. Por outro lado, e em contraste, é também sustentável um enquadramento normativo geral, que, assumindo como objetivo o combate à desinformação, permita aos *media* reconquistar(em) a sua posição na nova *sociedade da informação*, destacando-se pela prestação de informações sérias e confiáveis.⁸⁴

O binómio ora apresentado animou, em verdade, a particular discussão em torno da “*media exemption*”, que esteve em cima da mesa aquando da elaboração e da negociação do texto final do Regulamento Serviços Digitais.⁸⁵ Em particular, na sequência de propostas apresentadas por um conjunto de deputados do Parlamento Europeu, discutiu-se se seria de prever, no texto do DSA, salvaguardas especiais (como a previsão de uma notificação e do direito ao contraditório, prévios à adoção de uma medida restritiva) em favor dos *media*, ou se se deveria, inclusive, excluir, ou até mesmo proibir a realização de qualquer tipo de moderação de conteúdos em relação aos meios de comunicação social (impedindo, pois, a remoção e/ou suspensão de acesso aos respetivos conteúdos ou contas).

A favor da proteção-diferenciação positiva, posicionaram-se, sobretudo, as editoras, apelando ao papel fundamental dos meios de comunicação social tradicionais na disponibilização de notícias e de análises verificadas e ao respetivo contributo

⁸⁴ Sobre a questão, “The Digital Services Act (DSA): could it impact public media?”, *Public Media Alliance*, 28 de janeiro, 2022, <https://www.publicmediaalliance.org/the-digital-services-act-dsa-could-it-impact-public-media/>.

⁸⁵ Sobre a questão, cf. Monti, “The missing piece in the DSA puzzle?”, 202 e ss.

para a formação da opinião pública e a educação política dos cidadãos. Em suma, recordando os *media* como guardiões principais da democracia. Laborando sobre o princípio de priorização de informações pertinentes, autênticas e fidedignas, tal como propugnado no Código de Conduta sobre Desinformação de 2018⁸⁶ e respetiva versão reforçada de 2022,⁸⁷ e sublinhando a maior responsabilidade ética e jurídica, e, bem assim, a sujeição a requisitos vários, no que se refere à verificação de factos, à imparcialidade e à transparência, os militantes deste enquadramento especial defendiam, assim, a necessidade de um regime especial, nomeadamente mais protetor dos meios de comunicação social tradicionais, os quais particularmente vulneráveis às plataformas e às preferências da respetiva gestão algorítmica, em favor de conteúdo sensacionalista, polarizado e, portanto, mais monetizável. Como se viu, seria este regime especial e de favor dos *media*, aquele que, falhando no DSA, viria a ser introduzido no Regulamento Europeu relativo à Liberdade dos Meios de Comunicação Social, ato normativo que, segundo alguns autores, codifica assim o *privilégio dos media*, alinhando com o Código de Práticas de 2018 e a respetiva versão reforçada de 2022.⁸⁸

Contra a diferenciação, posição que acabou por encontrar respaldo no regime do DSA, posicionaram-se, desde logo, comunidades envolvidas na verificação de factos (os sinalizadores de confiança)⁸⁹ e, bem assim, entidades dedicadas ao estudo da desinformação em linha. Em particular, eram por estas sinalizados os riscos de um tratamento especial dos *media*, no contexto de uma sociedade sensacionalista, na qual também aqueles surgem a concorrer pela atenção, e, portanto, como potenciais canais de desinformação.⁹⁰ O tratamento mais favorável dos meios de comunicação tradicionais era, ainda, qualificado de ilegítimo, atenta a crescente produção de conteúdos por pessoas singulares que, pese embora não preenchendo a totalidade dos critérios e indicadores qualificativos dos *media* tradicionais, não deixam de, materialmente, se aproximar daqueles, merecendo, portanto, igual tratamento. Isto, seja por força do princípio da igualdade e da proibição da discriminação, seja, e sobretudo, em linha com a abordagem gradual defendida pelo Conselho da Europa,⁹¹ relativamente à noção de meios de comunicação social.

Reconhecendo o mérito de ambas as posições, considera-se, para os presentes efeitos, que a complexidade do desafio só logrará devida resposta através de uma abordagem integrada e multidimensional,⁹² que, além da inclusão de enquadramentos

⁸⁶ “Código de Conduta da UE sobre Desinformação” (Bruxelas, setembro 2018), último acesso em 30 de dezembro de 2024, <https://digital-strategy.ec.europa.eu/pt/library/2018-code-practice-disinformation>.

⁸⁷ “Código de Conduta da UE sobre Desinformação reforçado” (Bruxelas, junho 2022), último acesso em 30 de dezembro de 2024, <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>.

⁸⁸ Neste sentido, Monti, “The missing piece in the DSA puzzle?”, 196 e 202.

⁸⁹ Nos termos dos considerandos 61 e 62 e do artigo 22.º do DSA, os fornecedores de plataformas em linha devem adotar medidas para priorizar as notificações apresentadas por sinalizadores de confiança, estatuto concedido a entidades “*que tenham demonstrado, nomeadamente, que possuem conhecimentos especializados e competências específicas para combater os conteúdos ilegais e que trabalham de uma forma diligente, rigorosa e objetiva.*”

⁹⁰ No mesmo sentido, Gamito, “Consistent regulatory and self-regulatory mechanisms for media freedom in the digital single market”, 10.

⁹¹ Cf. Conselho da Europa, *Recommendation CM/Rec(2011)7 of the Committee of Ministers to member States on a new notion of media* (21 September, 2011), último acesso em 30 de dezembro de 2024, <https://edoc.coe.int/en/media/8019-recommendation-cmrec20117-on-a-new-notion-of-media.html>.

⁹² Neste sentido, também, Pier Luigi Parcu, “New digital threats to media pluralism in the information age. Competition and Regulation”, *Network Industries* 21, no. 2 (2020), <https://doi.org/10.1177/1783591719886101>.

com uma intenção de proteção particular e especial para com os meios de comunicação tradicionais e a sua particular vulnerabilidade no espaço digital, não poderá deixar de buscar, também, a adoção de medidas de apoio ao jornalismo independente e de qualidade e, bem assim, iniciativas de promoção da literacia e de sensibilização da sociedade para os riscos da desinformação, estas últimas em favor de todos aqueles que se possam qualificar como *novos media*.

Repare-se que, não obstante a presença de atos normativos refletindo as diferentes posições do referido binómio, a garantia da liberdade, independência e pluralismo dos meios de comunicação social deparar-se-á, no futuro, e independentemente da evolução da sociedade e do Direito, nacional e europeu, com desafios a vários níveis

Num primeiro plano, situam-se os desafios concetuais, contendentes com a própria noção e/ou alcance dos meios de comunicação social, que se consideram justificativos ou merecedores de um tratamento especial ou dedicado.⁹³ A este propósito, adere-se a uma constatação dilemática essencial: se o princípio da igualdade poderá, em alguns casos, exigir a equiparação e o alargamento da proteção a indivíduos, organizações não governamentais e à nova realidade do jornalismo cidadão,⁹⁴ a segurança jurídica aconselhará, na maioria deles, a manutenção de critérios precisos e determinados, por forma a evitar situações de abuso e de proteção injustificada. Esta tensão, que caracteriza o Direito como ciência, nunca obsteu à sua aplicação e atuação práticas. Se o Direito com ela conviveu até aqui, confia-se que não encontrará, aqui, (nova) causa de autodestruição. Não se interprete, porém, a mensagem como um qualquer atestado de sossego.

Pelo contrário, considera-se que os riscos de fragmentação concetual que, como aqui exposto, contendem, logo, com a definição mesma de sujeito ou objeto protegido, exigem repensar o fundamento constitucional justificativo de uma proteção diferenciada dos meios de comunicação social tradicionais. Está-se perante questão que, como se sabe, não logra ser tratada em agnosticismo para com a matriz constitucional relevante.

Com efeito, se na família norteamericana vigora um princípio de igualdade epistémica, subjacente à equiparação entre a *Press Clause* e a *Speech Clause*,⁹⁵ no contexto europeu, e sem que a realidade da moderação de conteúdos em linha pareça negá-la, continuará sendo inegável a especial valoração, seja dos meios de comunicação social como mais do que simples prestadores de um serviço no mercado, seja dos produtos do jornalismo como mais do que bens ou serviços consumíveis. Como se começou por assinalar, à atuação dos *media* estão subjacentes valores jusconstitucionalmente protegidos que sinalizam o seu duplo papel e, portanto, uma matriz axiológica particularmente densa e pronunciada. Além de titulares de liberdades fundamentais, no exercício das quais exercem a respetiva atividade, os meios de comunicação social devem ser valorados e protegidos, também pela sua importância funcional ou instrumental, isto é, como veículos garantes da efetivação e do exercício de direitos fundamentais, pelos sujeitos da comunidade político-jurídica, contribuindo, também, desde logo pela sua qualidade-condição de contrapoderes ativos no escrutínio do poder, para a realização da democracia, como regime e como ideal de participação cívica e política.⁹⁶

⁹³ Sobre a fragmentação concetual, cf. Gamito, “Consistent regulatory and self-regulatory mechanisms for media freedom in the digital single market”, 4 e ss.

⁹⁴ Neste sentido, Monti, “Why online public discourse needs a media privilege: in defence of Article 18 of the EMFA”.

⁹⁵ Neste sentido, Monti, “The missing piece in the DSA puzzle?”, 196.

⁹⁶ Erguendo o pluralismo dos *media* a característica e pilar essencial das sociedades democráticas

O que se acaba de referir a propósito da existência de fundamento constitucional para um tratamento positivo dos meios de comunicação social *vis-à-vis* outros destinatários de serviços de plataforma e, portanto, como uma categoria de utilizadores especiais, diferentes dos comuns utilizadores finais e/ou profissionais, é questão (e resposta) que importa não confundir com uma outra, subsequente, já contendente, por seu turno, com o alcance desse tratamento ou regime favorável. Por outras palavras, a questão de saber que entidades devem poder beneficiar desse enquadramento especial.

É sobretudo neste segundo plano que o crescente fosso entre o alcance dos enquadramentos especiais e dedicados, e a evolução da noção *de meios de comunicação social* suscita questões mais complexas. E é sobretudo em relação a estas que os particulares riscos de proteção por defeito e por excesso surgem mais adensados. Começando pela primeira – proteção por defeito – é comum a alusão, por alguns Autores, a um paradoxo do privilégio.⁹⁷ Consideram estes que a adoção e perpetuação de uma noção estrita de *media* poderá deixar desprotegidos novos atores, como indivíduos, *influencers* e *bloggers*,⁹⁸ quando são precisamente estes que carecem de maior proteção. Em contraste, a proteção por excesso decorreria, segundo outras vozes, da inclusão, nas referidas soluções especiais (o caso do artigo 18.º do EMFA) de meios de comunicação social (tradicionais) cuja sujeição à supervisão de autoridades reguladoras ou a obediência a requisitos e standards determinados pelos Estados-Membros poderá – sobretudo em contextos de *democratic backsliding*, de parca ou inexistente independência e credibilidade das autoridades reguladoras – ocultar verdadeiros megafones de propaganda política, veículos e agentes e desinformação e de teorias da conspiração populistas,⁹⁹ cujo tratamento preferencial configurará, pois, um privilégio injustificado e lesivo de princípios fundamentais dos ordenamentos jurídicos nacionais e europeu. A problemática é, em nosso ver, particularmente adensada pela circunstância de os cenários acabados de descrever – de insuficiência por excesso e por defeito – não lograrem ser definitivamente resolvidos pelo legislador. Pelo contrário, é precisamente a adoção de soluções gerais e abstratas a causa do problema. E porque assim é, considera-se que a questão só logrará ser devidamente ultrapassada com uma discussão renovada sobre a noção relevante de meios de comunicação social, procurando um consenso que, podendo não fundar, ainda, uma certeza suscetível de positivação em norma geral e abstrata, deverá, ainda assim, permitir ao intérprete e aplicador da lei, proceder – sem usurpação de poderes – a uma aplicação teleologicamente fundada das normas, assente, nomeadamente, em resultados interpretativos decorrentes de uma interpretação restritiva e/ou extensiva da lei, consoante os casos.

Também subsequente à questão primeira, relativa ao eventual fundamento para um tratamento diferente dos *media*, e à qual já se respondeu positivamente, estão importantes questões de política pública, desde logo contendentes com o *se* e o

contemporâneas, cf. Brogi *et al.*, “The European Media Freedom Act: media freedom, freedom of expression and pluralism”, 11. Anteriormente, também, Elda Brogi, “The Media Pluralism Monitor: Conceptualizing Media Pluralism for the Online Environment”, *Profesional De La información* 29, no. 5 (2020), <https://doi.org/10.3145/epi.2020.sep.29>.

⁹⁷ Sobre a questão, com referências, cf. Seipp, Helberger, de Vreese, e Ausloos, “Between the cracks: blind spots in regulating media concentration and platform dependence in the EU”, 16.

⁹⁸ Recomendando a inclusão de novas formas de jornalismo profissional na definição de prestador de serviços de comunicação social, e respetiva proteção, cf. Brogi *et al.*, “The European Media Freedom Act: media freedom, freedom of expression and pluralism”, 74.

⁹⁹ Neste sentido, Monti, “The missing piece in the DSA puzzle?”, 208 e 209.

como da proteção, e entre as quais se poderá avançar, como relevante, a opção entre *i)* uma abordagem tecnologicamente neutra – inclusiva dos meios de comunicação tradicionais e de novos atores que atuam em linha e através das plataformas –, e *ii)* um regime diferenciado. Seguem-se as dúvidas atinentes à concreta forma de assegurar os objetivos de interesse público em presença, e que surge particularmente relevante no contexto da querela em torno da melhor forma de garantir o financiamento e a sustentabilidade dos *media* tradicionais e do jornalismo local, nomeadamente, através *i)* da imposição de pagamentos às plataformas, através *ii)* da concessão de subsídios, ou, ainda, *iii)* da criação de um fundo financiado através de contribuições decorrentes de um imposto digital,¹⁰⁰ a que se soma a questão subsequente quanto à forma de garantir a respetiva canalização e aplicação em termos consonantes com os objetivos de interesse público subjacentes.¹⁰¹

Um desafio subsequente logo surge como decorrência automática desta primeira dimensão concetual. Com efeito, não deverá merecer espanto a circunstância de toda a incerteza e divergência concetual assinalada se refletirem ou poderem refletir em fragmentação regulatória,¹⁰² esta por seu turno adensada por dificuldades ínsitas à articulação *i)* horizontal – entre diferentes atos normativos potencialmente pertinentes para a compreensão da atividade dos meios de comunicação social (em linha) – e *ii)* vertical – entre o ordenamento jurídico da União Europeia e as legislações nacionais, estas últimas produto de contextos político-jurídicos marcados pela diversidade.¹⁰³ A sobreposição de objetivos e a interação multinível entre estes atos normativos suscitarão inegáveis desafios, não apenas ao intérprete, mas, e sobretudo, aos vinculados e aos beneficiários da legislação, circunstância que votará particular relevo e importância a mecanismos de cooperação (desde logo, entre diferentes autoridades competentes) e de diálogo interinstitucional (de que é exemplo o reenvio prejudicial,¹⁰⁴ no contexto da União Europeia).

A todos estes desafios, somam-se, sem que possam ser esquecidos, os desafios de aplicação e implementação de um Direito que, pese embora pautado pela maior procedimentalização¹⁰⁵ e o abandono do *laissez-faire* típico dos primórdios da regulação do digital, não logra abandonar, antes reforça, a delegação de funções paraestaduais em privados, ou, noutras palavras, o *outsourcing* de deveres de proteção de direitos fundamentais em agentes económicos.¹⁰⁶ Trata-se de uma problemática particularmente

¹⁰⁰ Sobre o impacto de um imposto digital nos incentivos das plataformas em contexto de moderação de conteúdos, cf. Leonardo Madio, e Martin Quinn, “Content moderation and advertising in social media platforms”, *Journal of Economics & Management Strategy* (2024), <https://doi.org/10.1111/jems.12602>.

¹⁰¹ Sobre a questão, com referências, cf. Theresa Josephine Seipp, Natali Helberger, Claes de Vreese, e Jef Ausloos, “Between the cracks: blind spots in regulating media concentration and platform dependence in the EU”, *Internet Policy Review* 13, no. 4 (2014), DOI: 10.14763/2024.4.1813, <https://policyreview.info/articles/analysis/regulating-media-concentration-and-platform-dependence>, 16-17.

¹⁰² Sobre esta, Gamito, “Consistent regulatory and self-regulatory mechanisms for media freedom in the digital single market”, 5 e ss.

¹⁰³ Sobre a fragmentação decorrente de diferentes enquadramentos normativos domésticos e a necessidade de articulação horizontal e vertical, cf. Gamito, “Consistent Regulatory and Self-Regulatory Mechanisms for Media Freedom in the Digital Single Market”, 2-3.

¹⁰⁴ Cf. artigo 267.º, Tratado sobre o Funcionamento da União Europeia.

¹⁰⁵ Sobre a dimensão processual-procedimental do constitucionalismo digital, cf. Oreste Pollicino, “The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism”, *European Law Journal* 29, no. 1-2 (2023), <https://doi.org/10.1111/eulj.12472>.

¹⁰⁶ Neste sentido, Martin Senftleben, “Human rights outsourcing and reliance on user activism in the DSA”, in (ed.) João Pedro Quintais, *From the DMCA to the DSA: A Transatlantic Dialogue on Online Platform Regulation and Copyright* (Verfassungsbooks, 2024), e *SSRN Electronic Journal*, 17 de junho, 2024, <https://ssrn.com/abstract=4860225> ou <http://dx.doi.org/10.2139/ssrn.4860225>.

agravada pelo incremento da responsabilidade das plataformas num contexto em que uma diversidade de fatores – entre os quais, o incremento dos conteúdos sujeitos a moderação, a consequente e inevitável necessidade de automatização, a incerteza regulatória, e a sujeição a vigilância constante – se conjuga num resultado porventura inimigo das liberdades. Assume centralidade a *remoção por default* e, no caso dos meios de comunicação social, poderá vir a assumi-la o paradigma contrário da *manutenção por excesso*, nomeadamente pleo receio da responsabilização pela moderação de conteúdos “*protegidos*.” Coloca-se, em suma, o problema da delegação, em privados, de juízos de concordância e da resolução de tensões que nem o legislador soberano logra resolver. Afinal, e na descrição expressiva da doutrina, “[c]ontent moderation of online speech is a moral minefield, especially when two key values come into conflict: upholding freedom of expression and preventing harm caused by misinformation.”¹⁰⁷

Todos estes desafios exigem soluções que se não poderão encontrar em lógicas como aquela que pontua a sociedade polarizada em que vivemos. Pelo contrário, e em contraste, as diferentes dimensões de perigo e as variadas e heterogéneas frentes de ameaça que se erguem à sustentabilidade do jornalismo tradicional (e a propósito das quais importará, também, distinguir a hipervulnerabilidade do jornalismo local) justificam uma atenção reforçada para com a necessidade de articular e coordenar as diferentes peças de um *puzzle* normativo de complexidade inultrapassável, e de cuja globalidade depende a busca de soluções para a crescente fragilização dos meios de comunicação social *vis-à-vis* os poderes político, económico, tecnológico e, enfim, infraestrutural, das (grandes) plataformas em linha.

A variabilidade dos desafios e das interrogações exige que, em conjugação com os novos atos, se aproveite o potencial dos velhos instrumentos, atuando-os, se necessário, à luz de uma interpretação conforme com a mudança de paradigma e com as novas questões. Novos e velhos instrumentos deverão ser articulados, nenhum podendo ser lido em isolamento, mas, e antes, como peça de um *puzzle* que dele depende, mas que com ele se não basta.¹⁰⁸ Eis o caminho para assegurar a liberdade, a independência, e o pluralismo dos *media*, também *online*, e também em relação a *novos poderes*.

¹⁰⁷ Cf. Anastasia Kozyreva *et al.*, “Resolving content moderation dilemmas between free speech and harmful misinformation”, *Proceedings of the National Academy of Sciences (PNAS) USA* 120, no. 7 (2023): 1, <https://doi.org/10.1073/pnas.2210666120>.

¹⁰⁸ Referindo-se em particular ao EMFA, cf. Brogi *et al.*, “The European Media Freedom Act: media freedom, freedom of expression and pluralism”, 7.

PAINEL II

**ENQUADRAMENTO E MECANISMOS DE
COMBATE À CORRUPÇÃO – DESAFIOS AO ESTADO
DE DIREITO DIANTE DA TRANSIÇÃO DIGITAL**

PAINEL II

Enquadramento e mecanismos de combate à corrupção – desafios ao Estado de direito diante da transição digital

Manuel Protásio *

Maria Inês Costa **

No seu relatório de 24 de julho de 2024 sobre o Estado de direito, a Comissão Europeia reiterou o compromisso da União Europeia (UE) no combate à corrupção, através do apoio a reformas de ordem jurídica e política para a criação de instituições que atuem nesse sentido, de organismos de supervisão e do reforço da vigilância desempenhada por uma série de atores relevantes,¹ seguindo a lógica do investimento tanto em medidas de prevenção como de repressão para uma ação mais eficaz.² De facto, o estabelecimento de quadros anticorrupção constitui um dos quatro pilares do relatório em causa, na medida em que as práticas corruptivas – de que são exemplo os subornos, fluxos financeiros ilícitos, branqueamento de capitais, nepotismo, clientelismo, abuso de funções e tráfico de influências³ – apresentam um conjunto de consequências corrosivas em diferentes âmbitos das democracias modernas: tanto as impacta a nível económico, como no que tange à própria legitimação do Estado de direito.

Como sublinha Maria Teresa Santos *et al.*, a corrupção é um “*fenómeno crítico para a sustentação dos Estados, para a confiança das democracias constitucionais, para a credibilidade e legitimação dos regimes políticos, para o desenvolvimento económico e para a justiça social, para a igualdade e para a defesa dos direitos fundamentais.*”⁴ Serve esta pertinente observação para frisar a importância do estabelecimento de uma cultura anticorruptiva, objetivo a que a UE atribui enorme relevância, com o desenvolvimento uma série de instrumentos e boas práticas para esse fim, assim como na elaboração de recomendações para os Estados-Membros nesse âmbito de atuação. Neste contexto, cumpre salientar, tal como indicado pela Comissão Europeia, que as áreas que tendem a demonstrar alto risco de ocorrência de corrupção são as de gestão de fundos públicos significativos, como os contratos públicos, ou o acesso a serviços

* Bolseiro da Fundação para a Ciência e Tecnologia (FCT), com referência UI/BD/152801/2022, <https://doi.org/10.54499/UI/BD/152801/2022>, e estudante de doutoramento em Ciências Jurídicas Públicas na Escola de Direito da Universidade do Minho.

** Bolseira da Fundação para a Ciência e Tecnologia (FCT), com referência UI/BD/154522/2023, <https://doi.org/10.54499/UI/BD/154522/2023>, e estudante de doutoramento em Ciências Jurídicas Públicas na Escola de Direito da Universidade do Minho.

¹ Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, *Relatório de 2024 sobre o Estado de direito – situação na União Europeia*, Bruxelas, 24.7.2024 COM(2024) 800 draft, 10. Disponível em [27db4143-58b4-4b61-a021-a215940e19d0_pt](https://doi.org/10.54499/UI/BD/154522/2023).

² Comunicação da Comissão, *Relatório de 2024 sobre o Estado de direito – situação na União Europeia*, 19.

³ United Nations (UN) Development Programme, *New technologies for sustainable development: perspectives on integrity, trust and anti-corruption*, 2021, 11. Disponível em [UNDP-New-Technologies-for-Sustainable-Development-Perspectives-on-integrity-Trust-and-Anti-Corruption.pdf](https://www.un.org/development/dp/dp-ntsd/perspectives-on-integrity-trust-and-anti-corruption.pdf).

⁴ Maria Teresa Santos, Nuno Coelho e José Mouraz Lopes, “Corrupção, Estado de direito e cooperação: a experiência de um instrumento de cooperação internacional (PACED)”, *Julgar*, no. 39 (2019): 80.

essenciais – nessa medida, os setores da saúde, da energia, do planeamento urbano e da administração regional e local foram identificados como vulneráveis.⁵

Releva ainda ter presente que a urgência deste repto de mitigação da corrupção se acentua perante a mudança de paradigma introduzida pelo desenvolvimento e utilização das novas tecnologias que, a uma velocidade avassaladora, potenciam o fenómeno corruptivo e respetivas consequências numa escala sem precedentes. Simultaneamente, as soluções que apresentam maior capacidade para garantir transparência e integridade e, nessa medida, para fazer face à corrupção no século XXI, integram tecnologias emergentes, de que são exemplo a Inteligência Artificial (IA), a tecnologia de *blockchain* e *big data analytics*.⁶ Atualmente, tanto os desafios como as soluções em torno do fenómeno corruptivo apresentam uma dimensão tecnológica emergente que não pode ser descurada.

Considerando as reflexões anteriormente delineadas, o Congresso cujo segundo painel agora apresentamos, procurou debater problemas e soluções práticas no combate à corrupção, tendo em conta tanto a legislação europeia como a realidade concretamente vivida nos tribunais e instituições públicas. Visando a obtenção de uma perspetiva privilegiada sobre o modo como os vários intervenientes encaram a aplicação das normas, o papel das novas tecnologias, bem como as implicações culturais que atravessam o fenómeno da corrupção, foram formuladas questões e produzidas reflexões que se apresentam e contextualizam a seguir.

Assim, a primeira vaga de questões dirigidas aos oradores sublinhou questões fundamentais: a proteção de denunciantes (*whistleblowers*) e a relevância dos canais de denúncia eletrónicos, que ainda enfrentam desafios de confidencialidade e segurança.⁷ Foi ainda feita referência ao Mecanismo Anticorrupção (MENAC),⁸ em Portugal, cuja operacionalização depende de um canal eletrónico – “*MENAC+! Transparente*” – que, na prática, enfrentou uma série de dificuldades aquando da sua criação.^{9/10} Tal canal, à luz da diretiva europeia relativa à proteção de denunciantes de infrações [Diretiva (UE) 2019/1937, vulgo “*Diretiva do Denunciante*”],¹¹ deveria assegurar mecanismos claros e eficientes de confidencialidade para encorajar denúncias. O “*Relatório Cibersegurança em Portugal*”, produzido pelo Centro Nacional de Cibersegurança (CNCS) no ano de 2024, revela que o princípio de informação

⁵ Comunicação da Comissão, *Relatório de 2024 sobre o Estado de direito – situação na União Europeia*, 24.

⁶ United Nations (UN) Development Programme, *New technologies for sustainable development: perspectives on integrity, trust and anti-corruption*, 2021, 13.

⁷ Ver *Relatório da Comissão ao Parlamento Europeu e ao Conselho sobre a transposição e a aplicação da Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho de 23 de outubro de 2019 relativa à proteção das pessoas que denunciam violações do direito da União*, Bruxelas, 3.7.2024, COM(2024) 269 final, 6-7: “(...) O artigo 11.º estabelece a obrigação de criar canais de denúncia externa e de dar seguimento às denúncias. Algumas destas obrigações foram transpostas incorretamente. Um Estado-Membro exclui o seguimento de denúncias de violações cometidas há mais de dois anos, uma limitação temporal que compromete a eficácia da diretiva em termos de reforço do controlo da aplicação do direito da UE. Alguns Estados-Membros não garantem a segurança jurídica necessária quanto às autoridades competentes designadas. O artigo 11.º, n.º 6, estabelece obrigações específicas para as autoridades que recebem denúncias, mas não têm competência para resolvê-las. Cerca de metade dos Estados-Membros transpuseram-nas incorretamente. É o que acontece, por exemplo, quando impõem estas obrigações apenas a determinadas autoridades, quando omitem a obrigação de transmitir as denúncias às autoridades competentes num prazo razoável e de forma segura ou omitem a obrigação de informar prontamente o denunciante (...).”

⁸ Para mais informações, visitar <https://mec-anticorruptcao.pt/>.

⁹ Público, “Anticorrupção: novo organismo ainda não tem plataforma para denúncias nem quadro de pessoal completo”, 8 de setembro de 2023, <https://www.publico.pt/2023/09/08/politica/noticia/anticorruptcao-novo-organismo-nao-plataforma-denuncias-quadro-pessoal-completo-2062639>.

¹⁰ Transparência Internacional Portugal, “MENAC sem motor de arranque”, 14 de setembro de 2023, <https://transparencia.pt/menac-sem-motor-de-arranque/>.

¹¹ Transporta para o regime jurídico português pela Lei n.º 93/2021, de 20 de dezembro.

com mais comprometimentos notificados à Comissão Nacional de Proteção de Dados (CNPd) foi o da confidencialidade,¹² levantando dúvidas sobre a segurança digital daqueles sistemas.

Ainda neste âmbito, foram dirigidas ao painel um conjunto de interrogações sobre a interoperabilidade entre diferentes agências e bases de dados no contexto da UE, que releva brevemente situar. De acordo com Relatório sobre o Estado de direito, alguns Estados-Membros, como a Malta, Croácia e Grécia, continuam a enfrentar desafios de longa data no que respeita à eficácia dos sistemas de justiça, sendo que em Portugal se observa um padrão semelhante, agravado pela inadequação da legislação processual penal para lidar eficazmente com processos penais intrincados.¹³ Em Portugal, “apesar de a corrupção ser o crime principal que surge associado ao maior número de procedimentos criminais”, na sua maioria, tais procedimentos acabam arquivados.¹⁴ Perante estes dados que espelham uma tendência preocupante, ganha uma importância acrescida a linha de ação prevista na Agenda Anticorrupção:¹⁵ a de tornar mais ágil “a obtenção de informação processualmente relevante junto de outras entidades públicas, através da interoperabilidade entre autoridades judiciais, órgãos de polícia criminal e outras entidades públicas, para potenciar a eficácia e a celeridade da investigação.”¹⁶ Por outro lado, a interoperabilidade acarreta desafios ao nível da proteção de dados, podendo colidir com os direitos fundamentais dos cidadãos, sobretudo se implementada sem salvaguardas robustas. Neste âmbito, foi também referida a utilização de IA e o receio de vigilância excessiva, exemplificada por episódios como o uso do *spyware* “Pegasus”^{17/18} em determinados Estados-Membros. Impera, assim, a questão: como se garante um diálogo eficaz entre especialistas em cibersegurança, legisladores e o ramo judiciário para garantir soluções integradas, atualizadas e que protejam as liberdades, direitos e garantias?

Ainda no âmbito das questões formuladas, relevamos a seguinte: apesar de haver cada vez mais normas contra a corrupção, estaremos, de facto, a prestar a atenção devida às lacunas (*loopholes*) já existentes na regulamentação atual que, porventura, facilitam práticas corruptas, sobretudo na interação entre grupos de interesse e o poder legislativo? A dúvida gira, portanto, em torno da pegada legislativa: não estaremos a criar mais legislação em vez de rever eficazmente o que já existe? Como alerta a literatura jurídica crítica, a sobreprodução normativa pode ter o efeito paradoxal de obscurecer responsabilidades e criar zonas cinzentas de atuação. De acordo com especialistas como Alina Mungiu-Pippidi, o excesso de normas não eleva necessariamente o combate a corrupção, podendo mesmo ser instrumentalizado

¹² Centro Nacional de Cibersegurança, *Relatório Cibersegurança em Portugal – riscos & conflitos*, julho de 2024, 16. Disponível em rel-riscosconflitos2024-obcibercncs.pdf.

¹³ Comunicação da Comissão, *Relatório de 2024 sobre o Estado de direito – situação na União Europeia*, 16.

¹⁴ Mecanismo Nacional Anticorrupção (MENAC), *Relatório anual 2023*, Lisboa, 2024, 42. Disponível em: <https://mec-anticorruptao.pt/wp-content/uploads/2024/05/relatorio-menac-2023.pdf>.

¹⁵ XXIV Governo português, Agenda Anticorrupção aprovada no Conselho de Ministros e apresentada pelo Primeiro-Ministro e pela Ministra da Justiça. Disponível em <https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDEyNwcAGD1%2fKgUAAAA%3d>.

¹⁶ XXIV Governo português, Agenda Anticorrupção (sumário executivo), ponto 23. Disponível em: <https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDEyNwMAjg14XQUAAAA%3d>.

¹⁷ Drumbava Costica, “Investigation of the use of Pegasus and equivalent surveillance spyware”, *European Parliament – Think Thank, At a Glance*, EPRS | European Parliamentary Research Service, 7 June 2023. Disponível em: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA\(2023\)747923](https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2023)747923).

¹⁸ Comunicação da Comissão, *Relatório de 2024 sobre o Estado de direito – situação na União Europeia*, 34.

por atores maliciosos para legitimar práticas desviantes sob a capa da legalidade.¹⁹ Assim, torna-se urgente mapear e rever normas contraditórias, pouco fiscalizadas ou desatualizadas, promovendo uma racionalização legislativa que privilegie a clareza, a aplicabilidade e a coerência sistémica.

Adicionalmente, foi debatida a questão sobre a possível dimensão cultural do fenómeno da corrupção. Estudos recentes, como os promovidos pelo GRECO (Grupo de Estados contra a Corrupção), reforçam a tese de que sistemas judiciais eficazes, liberdade de imprensa, e participação cidadã ativa são mais determinantes na prevenção da corrupção do que fatores culturais *per se*. A cultura, neste sentido, deve ser entendida não como uma predisposição estática dos povos, mas como um reflexo institucional dinâmico, moldado por incentivos legais, mecanismos de responsabilização e práticas quotidianas de transparência.²⁰ Embora alguns índices internacionais apontem para níveis diferentes de corrupção nos Estados do norte e do sul da Europa,²¹ vários especialistas na conferência refutaram a ideia de que a corrupção seja inata a determinada cultura, sublinhando antes a importância de fatores como transparência, tradição jurídica e aplicação real das medidas anticorrupção.

Em resposta às questões formuladas, Susana Figueiredo, Procuradora Europeia Delegada, ilustrou o desfasamento entre o discurso político e as condições reais em tribunais e procuradorias. Apesar das várias “*agendas anticorrupção*”, na prática faltam meios e laboratórios tecnológicos para analisar prova digital, ferramentas de cooperação e até equipamentos básicos. Além disso, a oradora sublinha que o canal de denúncias do MENAC não está efetivamente funcional. Isso reflete a realidade de muitos Estados-Membros, onde, apesar de estarem dotados de programas ambiciosos, há barreiras logísticas, tecnológicas e orçamentais.

Vários oradores, como Valentina Faggiani e Pedro Jacob Morais, assinalaram que o sucesso das diretivas europeias (por exemplo, a do “*Denunciante*”) depende da consciencialização cívica. Em muitos países, uma boa lei não surte efeito se o cidadão não sabe que tem direitos ou, por receio de represálias, evita denunciar. Este ponto relaciona-se diretamente com a cultura de transparência, que vai além de formalismos legais e requer educação e mudança de mentalidades.

No que respeita às soluções tecnológicas, Valentina Faggiani destacou a agência eu-LISA, criada para gerir sistemas informáticos de grande escala no Espaço de Liberdade, Segurança e Justiça da UE, como exemplo de interoperabilidade. Todavia, há riscos de violação de direitos, dada a circulação transfronteiriça de dados sensíveis. O desafio, de acordo com o painel, é encontrar um equilíbrio entre eficácia na investigação criminal e proteção dos direitos fundamentais, consagrado em instrumentos como o Regulamento Geral de Proteção de Dados (RGPD) e a Carta dos Direitos Fundamentais da UE.

De facto, a conferência evidenciou a existência de “*dois mundos*”: o mundo das “*boas intenções legislativas*” e o mundo prático, onde persistem carências e burocracias

¹⁹ Alina Mungiu-Pippidi, “Anti-corruption policies revisited. Global trends and European responses to the challenge of corruption”, Title of deliverable: “D3.4.1 the good, the bad and the ugly: controlling corruption in the European Union”, EU Grant Agreement number: 290529, Project acronym: ANTICORRP, Hertie School of Governance, 2016. Disponível em: <https://anticorrrp.eu/wp-content/uploads/2016/04/D3.4.1-The-Good-The-Bad-The-Ugly.pdf>.

²⁰ Grupo de Estados contra a Corrupção (GRECO), 24.º Relatório Geral de Atividades (2023), Conselho da Europa, Estrasburgo, 2024. Disponível em: <https://rm.coe.int/general-activity-report-2023-greco-060424-gbr-web/1680afd7f2>.

²¹ Transparency International, *Corruption Perceptions Index 2024*, relatório anual, 2024. Disponível em: <https://www.transparency.org/en/cpi/2024>

que atrasam a efetividade do combate à corrupção. A nível europeu, a harmonização de normas e a digitalização de processos surgem como soluções promissoras, mas que ainda enfrentam resistência cultural e administrativa. A proposta de um canal de denúncias fiável e anónimo, prevista na “*Diretiva do Denunciante*”, aponta para um caminho de maior responsabilização e participação cidadã, mas a sua eficácia depende de infraestruturas tecnológicas adequadas, formação dos profissionais e cultura de transparência.

Em suma, a conferência deixou claro que o combate à corrupção não se esgota em leis ou ferramentas tecnológicas avançadas. Exige-se uma mudança holística, que inclua o diálogo constante entre o meio jurídico, os especialistas em cibersegurança, as instituições públicas e a sociedade civil. Só assim se poderá caminhar para uma aplicação real das normas europeias e para a consolidação de uma cultura de integridade, onde os mecanismos de denúncia, de interoperabilidade e de responsabilização sejam efetivamente funcionais e respeitem, em simultâneo, os direitos fundamentais de todos os cidadãos.

Transição digital e corrupção

Susana Figueiredo *

É já um lugar-comum afirmar que a luta contra a corrupção é uma das travesmestras da construção do Estado de Direito. Tal luta, enquanto houver Estado de Direito Democrático, constituirá, a nosso ver, um trabalho contínuo, uma tarefa *in fieri*, um perpétuo “*work in progress*”, pois é conatural ao exercício dos poderes e *munus* públicos a sua potencial desvirtuação ou instrumentalização para atingir fins outros que não o do interesse público, devendo tal tarefa ser humildemente encarada como um contrapeso rotineiro e necessário, uma repetida e doméstica tarefa de Sísifo, um ato de quotidiana higiene democrática.

Com efeito, não obstante uma leitura simplista dos factos que atente na mera perceção pública da corrupção (CPI)¹ nos poder fazer crer que existem sociedades (por regra as mais económica e socialmente evoluídas) onde o fenómeno corruptivo se encontra quase erradicado, uma leitura mais fina como aquela potenciada por um alternativo “*índice desagregado da corrupção*” (UCPI)² permitir-nos-á concluir que a corrupção que, para efeitos de distinção da baixa-corrupção (corrupção para acesso a serviços ou para agilização dos mesmos), designaremos de topo ou de alto perfil é transversal aos diversos Estados independentemente do seu grau relativo de evolução socioeconómica. Estados que, por definição, levam sempre acopladas estruturas de poder (ainda que democráticas) e, por inerência, a potencialidade da respetiva instrumentalização. Sem qualquer pendor catastrofista, sempre se afirmará aquilo que nos parece um truísmo: lá onde houver poder sempre haverá potencialmente corrupção. Com efeito, e no que respeita às possíveis leituras enviesadas potenciadas pelos chamados índices de perceção de corrupção, basta atentar que não raro, nos países de menor pendor democrático, onde a prática corruptiva (apesar de endémica) se centraliza num grupo de elite mais restrito, são obviamente menores os índices de perceção pública da corrupção, desde logo porque inexistem contrapoderes (nomeadamente poder judicial independente e imprensa livre) que permitam revelar e dar a conhecer à população os casos corruptivos.

* Procuradora Europeia Delegada.

¹ Ver Transparência Internacional, <https://transparencia.pt/indice-de-percecao-da-corrupcao-2023/>. O Índice de Perceção da Corrupção (CPI) foi criado pela “Transparency International” em 1995 e é, desde então, uma referência na análise do fenómeno da corrupção, a partir da perceção de especialistas e executivos de negócios sobre os níveis de corrupção no setor público. É um índice composto, ou seja, resulta da combinação de fontes de análise de corrupção desenvolvidas por outras organizações independentes, e classifica de 0 (percecionado como muito corrupto) a 100 (muito transparente) 180 países e territórios.

² Yuen Yuen Ang, *China’s gilded age: the paradox of economic boom and vast corruption* (United States: Cambridge University Press, 2020); Yuen Yuen Ang, “Unbundling corruption: why it matters and how to do it”, OECD – *Development matters*, 25 June 2020, <https://oecd-development-matters.org/2020/06/25/unbundling-corruption-why-it-matters-and-how-to-do-it/>.

Esta afirmação, aparentemente encerrando em si mesma uma platitude, é hoje, num contexto histórico de acelerado recrudescimento de populismos demagógicos, um credo a recitar diariamente por parte daqueles que, muitas vezes em estado de desânimo, protagonizam, nas suas funções profissionais, tarefas de luta contra o fenómeno corruptivo. Vê-lo como uma praga anómala suscetível de ser definitivamente exterminada ou alvo de panaceia miraculosa convocará apetites por soluções e protagonistas providenciais para o debelar. Ora, após quase duas décadas a trabalhar nesta área, alimentamos a convicção pessoal de que lidar com o fenómeno corruptivo será sempre, em estado de normalidade democrática, uma tarefa a visitar quotidiana e rotineiramente, a qual convoca uma contínua ação de vigilância preventiva, investigatória e repressiva por forma a reinstalar a convicção da comunidade na integridade e realidade dos valores democráticos formalmente consagrados nas constituições nacionais.

Com efeito, o fenómeno corruptivo³ acarreta uma conjunto de efeitos nefastos para as sociedades democráticas e para o Estado do Direito em que assentam, nomeadamente: *i)* a distorção das políticas públicas, seja na fase da sua adoção, seja na fase da sua execução e implementação; *ii)* a promoção da desigualdade social e económica, na medida em que favorecendo os agentes corruptores ou os grupos de interesses e pessoas por estes indicados, exacerba as desigualdades sociais e económicas, desviando muitos dos recursos que deveriam destinar-se à prestação de bens e serviços públicos essenciais (como saúde e educação) com prejuízo dos cidadãos mais vulneráveis ou de dados grupos económicos; *iii)* a redução da qualidade dos serviços públicos e a eliminação da equanimidade no acesso aos mesmos uma vez que, por um lado, quando os recursos são desviados, a qualidade dos serviços públicos diminui, e, por outro, passam a ser afetados ou usufruídos, preferencialmente, por quem tenha capacidade corruptiva ou, ao invés, por quem não tenha acesso a serviços privados de qualidade, e não por todos os cidadãos de forma igualitária; *iv)* aumento da pobreza, na medida em que constitui um entrave à mobilidade social ao impedir que os recursos públicos cheguem igualmente a todos os cidadãos, potencialmente afastando aqueles com maior capacidade pessoal para os rentabilizar individual e coletivamente, perpetuando, assim, ciclos de pobreza e impactando negativamente no desenvolvimento económico e social; *v)* afetação da livre concorrência e da iniciativa privada ao favorecer determinados operadores económicos em detrimento de outros sem qualquer critério de razoabilidade económica com prejuízo não só da propriedade privada como do setor público que contrata a prestação de serviços ou a aquisição de bens ao sector privado.

Tais efeitos indesejáveis, por sua vez, e na medida em que não sejam eficazmente combatidos, constituem fatores de erosão da confiança colectiva nas instituições públicas e no sistema político, na medida em que uma perceção de corrupção generalizada mina a confiança da população no sistema democrático e nas instituições em que assenta.

A resiliência das nossas democracias, incluindo o grau de confiança no Estado de Direito, depende, pois, da capacidade do sistema de justiça de responder adequadamente às necessidades dos cidadãos, entre as quais aquelas que radicam na

³ Salientado que, quando aqui usamos o termo corrupção, o estamos a fazer num sentido lato, de pendor criminológico, que abarca a multitudine de práticas criminosas em torno dos exercícios dos poderes públicos e políticos, assim como a prática corruptiva no setor privado e no comércio internacional, conceito lato que integra tipos de crime distintos, ainda que adjacentes, ao tipo legal de crime de corrupção em sentido estrito.

necessária crença de que o Estado de Direito Democrático, assente em ideais matriciais de respeito pela pessoa humana e de igualdade e liberdade, bem como nos direitos fundamentais, é, ainda, o *meio ambiente cultural e político* no qual o ser humano, em condições de igualdade, encontrará a melhor base para o desenvolvimento comunitário de todo o seu potencial existencial. Tal crença fundadora encontrará, todavia, obstáculos onde a prossecução do interesse público – que sempre deverá nortear a ação pública – seja substituída pela prossecução desigualitária e ilegítima de interesses particulares ou de determinados grupos económicos ou sociais em detrimento de outros.

A concretização dos valores do Estado de Direito Democrático e a sua reafirmação perante a comunidade encontram-se, na prática, associadas a uma pletora de ideias-satélite que orbitarão em torno da prossecução do interesse público, quais sejam as de celeridade, eficácia, eficiência, proximidade, acessibilidade, facilidade, transparência e sindicabilidade da ação pública.

Tais ideias ou metas-ideais encontram nas ferramentas das Tecnologias de Informação e Comunicação (TIC) um poderoso aliado e catalisador. Sendo a transição digital, que hoje aqui nos ocupa, precisamente, uma das ferramentas cruciais, e atualmente, indispensáveis para empreender tal tarefa.

Existe, ao dia de hoje, um reconhecimento político unânime e consensual da relevância das TIC para o exercício da Justiça, em geral, reconhecida nos chavões da “*E-Justice*” e no princípio do “*digital por defeito*”, bem como, em particular, no *combate*⁴ à corrupção, abrangendo as suas diversas etapas: prevenção, investigação e julgamento, falando-se hoje de uma *tecnologia da integridade (integrity tech)*.

Tal reconhecimento foi consabidamente acelerado e potenciado pela experiência – limite proporcionado pela pandemia de COVID-19, a qual destacou as fragilidades dos sistemas menos desenvolvidos tecnologicamente, sublinhando a necessidade de os Estados investirem em TIC.

Vários são os documentos, programas e ações políticas, a nível nacional e internacional, que atestam tal aguda e hodierna consciencialização. Assim, e a mero título de exemplo:

- A Estratégia da Justiça Electrónica para 2019-2023, Conselho Europeu;⁵
- O Compêndio Sobre Boas Práticas na Publicação e Utilização de Dados Abertos para o Combate à Corrupção (OCDE, 2017);⁶
- A Agenda Digital 2022-2025. *Protecting human rights, democracy and the rule of law in the digital environment* (2022), do Conselho da Europa;⁷
- Índice de Transformação Digital e Integridade, da Transparência Internacional, Brasil;⁸

⁴ Jargão este, à custa de tanta repetição, difícil de abandonar – apesar de preferirmos uma ideia de higiene diária democrática às tarefas epopeicas associadas a atos heroicos de “*luta*” ou “*combate*.”

⁵ Estratégia de justiça eletrónica para 2019-2023, (2019/C 96/04), 13.3.2019, [https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52019XG0313\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52019XG0313(01)&from=EN).

⁶ OCDE, “OCDE: Compendium of good practices on the publication and reuse of open data for Anti-corruption across G20 countries”, 2017, <https://www.all4integrity.org/tech4integrity/knowledge-center/relatorio-compedium-of-good-practices-on-the-publication-and-reuse-of-open-data-for-anti-corruption-across-g20-countries/>.

⁷ Conselho da Europa, “Digital Agenda 2022-2025 – Accompanying digital transition”, <https://www.coe.int/en/web/digital-governance/strategy>.

⁸ Ver Transparência Internacional – Brasil, “Índice de Transformação Digital e Integridade”, dezembro de 2021, <https://transparenciainternacional.org.br/publicacoes/indice-de-transformacao-digital-e-integridade/>.

- Relatório de 2024 sobre o Estado de Direito, União Europeia;⁹
- Conferência de Alto Nível Para uma Justiça Eletrónica Centrada nas Pessoas (E-Justice) (Ministério da Justiça, 2021, XXII Governo Constitucional);¹⁰
- Estratégia Nacional Anticorrupção 2020-2024, XXII Governo Constitucional;¹¹
- Agenda Anticorrupção, XXIV Governo Constitucional;¹²
- Plano de Recuperação e Resiliência (PRR) e a Transição Digital (componentes 18 e 19).¹³

Vejam, de seguida, com mais pormenor, em que medida as TIC poderão contribuir, nas diversas fases (prevenção, investigação, julgamento), para o tratamento do fenómeno corruptivo, assim como os desafios e obstáculos que as mesmas convocam e que podem constituir outros tantos óbices ao cabal desempenho de tal tarefa.

Com efeito, da mesma forma que não somos portadores de uma visão catastrofista do fenómeno corruptivo, também, *et pour cause*, não nos deixamos iludir com qualquer visão cândida acerca da existência de uma qualquer panaceia – no caso as TIC – para “*acabar de vez com a corrupção*”, como se seguida se procurará demonstrar.

Assim, **no plano preventivo**, destacamos, de forma esquemática, alguns aspetos nos quais as TIC podem contribuir de forma significativa. Assim:

- O uso de TIC pode contribuir para a promoção da desburocratização através do reforço da “*e-Governança*”, desmaterializando e automatizando os procedimentos e eliminando contextos humanos que potenciem a corrupção, promovendo a agilidade da administração, eliminando aquilo que pode integrar a mercadoria transacionada pelo funcionário corrupto no seio de sistemas pesadamente burocratizados (“*criar dificuldades para vender facilidades*”; *speed money* para “*olear o sistema*”, a “*gasosa*” para o fazer funcionar, etc);
- O uso de tecnologias como *Distributed Ledger Technologies* (DLTs) e *blockchain* para a promoção de registos íntegros, imutáveis e sindicáveis.¹⁴ Comporta um grande potencial na prevenção, designadamente dadas as suas especiais características de:
 - **Transparência e Imutabilidade:** os registos num *ledger* distribuído são transparentes e imutáveis. Isso significa que uma vez que uma transação é registada, ela não pode ser alterada ou apagada, tornando difícil para qualquer pessoa manipular dados;
 - **Desintermediação:** DLT elimina a necessidade de intermediários em muitas transações, fator de redução das oportunidades corruptivas;
 - **Auditabilidade:** todas as transações registadas por via da tecnologia *blockchain* são auditáveis, facilitando a rastreabilidade e a verificação

⁹ Comissão Europeia, Relatório de 2024 sobre o Estado de direito – Comunicação e capítulos sobre cada país, https://commission.europa.eu/publications/2024-rule-law-report-communication-and-country-chapters_pt?prefLang=pt.

¹⁰ Ministério da Justiça, Conferência de Alto Nível – Para uma justiça eletrónica centrada nas pessoas – E-justice, <https://eu2021.justica.gov.pt/Portals/0/Ficheiros/Organismos/JUSTICA/eBook%20Conferencia%20eJustice%202021-PT.pdf?ver=nzVG9Qa2B83cfM9ej5w9mA%3d%25>.

¹¹ Estratégia Nacional Anticorrupção 2020-2024, <https://justica.gov.pt/Estrategia-Nacional-Anticorruptao-2020-2024>.

¹² Agenda Anticorrupção aprovada no Conselho de Ministros e apresentada pelo Primeiro-Ministro e pela Ministra da Justiça, <https://www.portugal.gov.pt/pt/gc24/comunicacao/documento?i=agenda-anticorruptao>.

¹³ RECUPERARPORTUGAL, Transição digital – Investimento na capacitação digital, <https://recuperarportugal.gov.pt/transicao-digital/>.

¹⁴ OCDE, Recommendation of the Council on Blockchain and Other Distributed Ledger Technologies, OECD/LEGAL/0470, 2024, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0470>.

- de transações, permitindo que auditores e reguladores identifiquem rapidamente quaisquer atividades suspeitas;
- **Segurança:** a natureza descentralizada e criptografada do *blockchain* torna-o altamente seguro contra fraudes e ataques cibernéticos, protegendo os dados contra adulterações e acessos não autorizados;
 - **Eficiência:** as DLT podem automatizar muitos processos através, por exemplo, de contratos inteligentes que são programas autoexecutáveis com os termos do acordo diretamente escritos no código, o que não só aumenta a eficiência como cria desintermediação humana;
 - **Administração e Governo Abertos:** TIC revelam-se instrumentos da promoção da transparência da governação e da participação pública dos cidadãos.
- O exemplo nacional do Portal + Transparência;¹⁵
 - A organização “*Open Data Charter*”¹⁶ e a identificação de 30 conjuntos de dados tidos como essenciais em termos de acesso público para efeitos de luta anticorrupção;
 - O registo e acesso, por via de TIC, da “*pegada legislativa*”, como fatores de incremento da sindicabilidade e da responsabilização no exercício do poder legislativo;
 - A divulgação pública de planos de cumprimento normativo, códigos de conduta e planos de prevenção de riscos (vide legislação que instituiu o Mecanismo Nacional Anticorrupção (MENAC) e o Regime Geral de Prevenção da Corrupção aprovado pelo DL 109-E/2021 de 09-12);¹⁷
 - A criação de plataformas eletrónicas para declaração de interesses de determinadas categorias de agentes públicos com maior exposição ao risco corruptivo;¹⁸
 - A criação de plataformas eletrónicas para registos das contas e dos financiamentos dos partidos políticos;¹⁹
 - A criação de plataformas informáticas de registo obrigatório e público de interesses legítimos (regulamentação da atividade de lóbi):
 - registo da identidade dos representantes e representados;
 - código de conduta para lobistas e entidades públicas que com os mesmos interajam;
 - registo de agenda pública de interações.
 - A criação de plataformas digitais completas de aquisições públicas de bens e serviços (contratação pública) (por exemplo, Portal Base)²⁰ e a utilização de *smart contracts*;

¹⁵ Ver Portal “Mais transparência”, <https://transparencia.gov.pt/pt/>.

¹⁶ Ver “Open Data Charter”, <https://opendatacharter.org/who-we-are/>.

¹⁷ Ver Mecanismo Nacional Anticorrupção, <https://mec-anticorruptao.pt/>.

¹⁸ Entre nós, o caso das plataformas da Entidade para a Transparência, criada em 2019, e em funcionamento desde 6 de março de 2024, na qual foi criticamente assinalada a falta de interoperabilidade com o Banco de Portugal e a necessidade de verificação manual das informações aí introduzidas. Foi recomendada uma ampliação dos seus conteúdos e um aumento da sua interconexão com outros sistemas informáticos de entidades públicas, como a AR e o IRN, com reconhecimento de que tal implica um especial equilíbrio entre o princípio da administração aberta e a proteção de dados (v. III, IV, V Recomendação do Relatório GRECO 2024 e Agenda Anticorrupção do XXIV Governo).

¹⁹ O caso da plataforma nacional da Entidade das Contas e Financiamentos Políticos, https://www.tribunalconstitucional.pt/tc/contas_portal_recomendacoes.html.

²⁰ Ver Portal “Base”, <https://www.base.gov.pt/base4>.

- Plataformas digitais de leilões públicos nas vendas em processos executivos e processos de insolvência (por exemplo, e-Leilões);²¹
- Criação de bases de dados compreensivas das decisões judiciais através de instrumentos TI de anonimização (v. Recomendação X do Relatório GRECO 2024 ante a lacuna existente entre nós quanto à 1ª instância);²²
- IA e *data analytics*: utilização de instrumentos de inteligência artificial (IA) por atores de integridade dentro e fora do Estado para identificação de padrões suspeitos, anomalias e sinais de alerta em grandes conjuntos de dados (*big data*) auxiliando na deteção de condutas ilícitas enquanto método ancilar de estudos e auditorias (INTEGRITY-TECH);
- Promoção de formação em linha e plataformas eletrónicas de formação em matéria de corrupção para operadores judiciais e cidadãos (por exemplo, cursos HELP do Conselho da Europa);
- Plataformas para distribuição automática de processos nas fases judiciais (garantia do juiz natural).²³

Também na fase de investigação muitas são as ferramentas de TIC suscetíveis de contribuir para o aumento da qualidade da investigação e da celeridade da mesma. Assim, e sem pretensão de exaustividade:

- A criação de canais informáticos internos e externos de denúncia (cf. Regime Geral de Proteção dos Denunciantes, Lei n.º 93/2021,²⁴ de 20/12 e Diretiva (UE) 2019/1937, Regime Geral de Proteção de Denunciantes; DCIAP-PGR,²⁵ PJ,²⁶ EPPO);²⁷
- A utilização de sistemas informáticos de tramitação e gestão de processos na fase de inquérito;²⁸
- A criação de canais eletrónicos seguros de comunicação entre autoridades judiciais e outras instituições com funções no domínio da investigação ou na sua coadjuvação;
- A utilização de ferramentas TI para descriptação de comunicações eletrónicas;
- A utilização de *software* para a realização de pesquisas informáticas *online* ou remotas;
- Ferramentas de reconhecimento e conversão de voz em texto (especial relevo para a redução a auto dos depoimentos produzidos com a recolha de prova oral);
- Ferramentas de indexação, pesquisa e gestão da prova;

²¹ Ver “E-Leilões”, <https://www.e-leiloes.pt/index.aspx>.

²² Conselho da Europa, Quinto ciclo de avaliação - Prevenir a corrupção e promover a integridade em governos centrais (funções executivas de topo) e forças e serviços de segurança, Relatório de avaliação - Portugal, GrecoEval5Rep(2022)3, <https://rm.coe.int/grecoeval5rep-2022-3-final-pt-evaluation-report-portugal-public-2780-0/1680ac2293>.

²³ Diário da República, Portaria n.º 86/2023, de 27 de março – procede à alteração das regras relativas à distribuição, por meios eletrónicos, dos processos nos tribunais judiciais e nos tribunais administrativos e fiscais, <https://diariodarepublica.pt/dr/detalhe/portaria/86-2023-210982935>.

²⁴ Diário da República, Lei n.º 93/2021, de 20 de dezembro - estabelece o regime geral de proteção de denunciante de infrações, transpondo a Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União, <https://diariodarepublica.pt/dr/detalhe/lei/93-2021-176147929>.

²⁵ Ministério Público (Portugal), Denúncia de actos de corrupção e fraudes, <https://simp.pgr.pt/dciap/denuncias/index2.php>.

²⁶ Polícia Judiciária, Denúncia anónima, <https://www.policiajudiciaria.pt/denuncia-anonima/>.

²⁷ The independent public prosecution office of the EU, “Comunicar um crime à Procuradoria Europeia”, <https://www.eppo.europa.eu/pt/comunicar-um-crime-procuradoria-europeia>.

²⁸ Justiça.gov, “Plataformas tecnológicas Magistratus e MP Codex avançam nos tribunais”, 4 de fevereiro de 2022, <https://justica.gov.pt/Noticias/Plataformas-tecnologicas-Magistratus-e-MP-Codex-avancam-nos-tribunais>.

- Comunicações eletrónicas e videoconferência com sujeitos e intervenientes processuais (arguidos, assistentes, testemunhas, peritos);
- Ferramentas TI de descriptação de comunicações eletrónicas;
- Utilização de IA na pesquisa e análise de prova digital ou digitalizada (ex. análise de fluxos bancários entre elevado número e contas bancárias identificadas);
- Transmissão eletrónica segura de instrumentos de cooperação judiciária e de prova (a questão da interoperabilidade de sistemas entre os Estados Membros e Agências Europeias como a Eurojust e a Europol; Projeto e-CODEX²⁹ e as DEI; EPPO Case Manager System; projeto E-EDES³⁰ para a transmissão da prova digital).

Também na fase de julgamento, a utilização de ferramentas TIC poderá contribuir para agilizar e facilitar, conferindo maior eficácia, o processo de produção de prova, assim como o processo decisório. Assim:

- Sistemas de tramitação eletrónica de processos (projeto *Magistratus*);³¹
- Sistema de digitalização, gestão, organização, associação e produção de prova em julgamento (por exemplo, a aplicação SIIP);³²
- O uso de IA no processo judicial pode promover a igualdade e harmonização na aplicação da pena. Com efeito, se certamente ninguém quer ser julgado por algoritmos, não será de descartar o contributo que a IA pode ter para o processo decisório e na própria preparação das estratégias de acusação e defesa, nomeadamente através do uso de tecnologia preditiva de decisões judiciais a partir de bases compreensivas de dados a partir de casos históricos anteriores para situações similares;
- O uso de IA também poderá facilitar o processo decisório ao nível de tarefas que se reconduzam a operações de cálculo, pesquisa de fontes, despiste de contradições lógicas na fundamentação de facto e de direito e na procura de precedentes;
- Utilização de IA para prever probabilidades de reincidência e de aplicação de penas (por exemplo, software norte-americano *COMPAS: Correctional Offender Management Profiling For Alternative Sanctions*).³³

A transição digital, todavia, como o próprio mundo digital, integra uma realidade binária, podendo ser percecionada não apenas como um instrumento de luta contra a corrupção, mas também como autora da corrupção, ou seja, uma nova oportunidade para as velhas práticas corruptivas, ou seja, *um não tão admirável mundo novo*.

Programas como o Europa Digital (€7.5 biliões), *Horizon Europe* (€95.5 biliões), Fundos Estruturais (€21.4 biliões) e o PRR alocaram fundos europeus à digitalização (2021-2027) em montantes sem precedentes.

²⁹ Ver “EVIDENCE2e-CODEX”, <https://evidence2e-codex.eu/>.

³⁰ European e-Justice, “e-Evidence Digital Exchange System”, https://e-justice.europa.eu/37138/EN/eevidence_digital_exchange_system.

³¹ Justiça.gov, “Plataformas tecnológicas Magistratus e MP Codex avançam nos tribunais”, 4 de fevereiro de 2022, <https://justica.gov.pt/Noticias/Plataformas-tecnologicas-Magistratus-e-MP-Codex-avancam-nos-tribunais>.

³² Ministério Público (Portugal), Protocolo de cedência gratuita da aplicação SIIP, [protocolo_aplicacao_siip_0.pdf](https://www.mpsp.gov.pt/pt/protocolo-aplicacao-siip-0.pdf); Conselho Superior da Magistratura, “Protocolo para a utilização do Serviço Integrado de Informação Processual foi assinado, entre o CSM e os autores da aplicação”, <https://csm.org.pt/protocolo-para-a-utilizacao-do-servico-integrado-de-informacao-processual-foi-assinado-ontem-entre-o-csm-e-os-autores-da-aplicacao/>.

³³ Dominique Ferreira, “A utilização e os efeitos do software COMPAS”, Jusbrasil, <https://www.jusbrasil.com.br/artigos/a-utilizacao-e-os-efeitos-do-software-compas/837747472>.

Uma percentagem significativa dos casos alocados à EPPO e relativos a *Expenditure Fraud* (fraude na despesa) encontra-se relacionada com a política europeia de transformação e transição digital.

Esforços tem vindo a ser realizados com vista a padronizar condutas e identificar sinais de alerta no âmbito da fraude na contratação para aquisição de bens e serviços, como sejam os casos de aquisição de equipamentos e *software* já em uso, de conflito de interesses, de inflacionamento de preços, de consultoria fictícia, de sobrefaturação e ocultação do real fornecedor.

Por outro lado, a transição digital na justiça, para além de convocadora de negócios avultados e de novas oportunidades corruptivas, convoca ainda, e de arrasto, um conjunto complexo de novos riscos e desafios.

De entre tais tiscos avulta a matéria da proteção dos dados. Preocupação que sempre haverá de acompanhar qualquer política inovadora em matéria de digitalização da justiça e que se depara, a nível nacional, com a lacuna verificada em matéria do tratamento de dados nos processos criminais ante a não cabal transposição, até à presente data, da Diretiva (EU) 2016/680 [cf. considerando 19 do Regulamento Geral da Proteção de Dados (RGPD), Lei 58/2029, de 08/08, a Lei 59/2029, de 08/08 (tratamento de dados e OPCs); Proposta Lei 126/XIII/3, visando alterar a Lei 34/2009, de 14/07 e veto presidencial].

Também a matéria da propriedade, domínio, gestão e manutenção das plataformas e aplicações digitais levanta sensíveis questões sobre a separação de poderes, independência judicial e acesso pelo executivo aos dados judiciais, mormente na fase de inquérito coberto por segredo de justiça.

Outro perigo real poderá consistir naquilo que cunharemos de *deslumbre pela tecnologia* que poderá conduzir a descartar, de forma incauta, meios tradicionais de investigação ou o risco da “*inibição da arte de pensar*”,³⁴ especialmente na investigação, onde a eficiência pode ser priorizada em detrimento da qualidade. Um dos principais resultados da digitalização é a eficiência, não necessariamente a qualidade.

O uso de instrumentos de indexação de prova e motores de pesquisa na produção de prova em julgamento pode, ainda, levar à incompletude da sua apreensão global, desvalorizando a necessária compreensão humana.

Também o uso de algoritmos na investigação pode levar à discriminação, privilegiando-se uma dada tese ou hipótese em detrimento de outra igualmente válida, substituindo-se hipóteses metodológicas por um viés tecnológico na apreensão da matéria de facto assim fazendo perigar os deveres de objetividade e legalidade que norteiam a ação do Ministério Público o qual, estatutária e constitucionalmente, se encontra vinculado a um dever de investigar “à charge *et à décharge*” (ou seja, quer contra, quer a favor do arguido).

Perigos de intrusão e sabotagem assomam, outrossim, como perigos reais a não descurar, aumentando as exigências em ética digital, cibersegurança e identidade digital.

A possibilidade de rápida obsolescência das TI pode comportar, ainda, um risco de contaminação da prova, levantando especiais cautelas na preservação e na custódia da mesma.

³⁴ Cunha Rodrigues, “Transição digital da justiça: ganhos e perdas”, 14, <https://justica.gov.pt/Portals/0/Ficheiros/Organismos/JUSTICA/eBook%20Conferencia%20eJustice%202021-PT.pdf?ver=nzVG9Qa2B83cfM9ej5w9mA%3d%3d>.

Também a matéria conexa da preservação da prova armazenada na *cloud* e a proteção de dados quando dispersos por jurisdições diversas se revelam matéria crucial e a demandar redobrada atenção.

Poderá ainda, ante o elevado custo e/ou dificuldade de acesso a determinadas TIC, ser colocado um especial desafio ao princípio da igualdade de armas entre a “*acusação*” e a defesa, criando-se disparidades no acesso a tais tecnologias (v.g. TI de pesquisa de prova digital ou digitalizada usada na investigação a que poderão pretender aceder, em condições de igualdade, as diversas defesas) e hipotética afetação do direito a um processo equitativo e das garantias de defesa.

Riscos previsíveis se podem ainda divisar no uso da *jurimetria* e da tecnologia preditiva de decisões judiciais, que podem violar a separação de poderes e a independência judiciária (questão de propriedade e responsabilidade pela organização e seleção das decisões que integram as bases de dados usada), perpetuar erros e sobrevalorizar precedentes em detrimento da avaliação do caso concreto. Tais riscos podem conduzir à violação de direitos fundamentais na medida em que promovam a discriminação e atentem contra garantias de defesa e ao direito a um processo justo e equitativo.

Ciente dos riscos em tal matéria, a Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente (CoE, 2018)³⁵ estabeleceu um conjunto de princípios que regem o seu uso, designadamente os princípios de respeito dos direitos fundamentais, de não discriminação, da qualidade e segurança, da transparência, da imparcialidade e equidade.

Também o Regulamento (UE) 2024/1689³⁶ classifica os sistemas de IA na administração da justiça como sendo de risco elevado.

Também os custos das tecnologias usadas e os seus impactos ambientais (o caso das DLTs) serão desafios não despendendo colocados na fase de avaliação, adoção e implementação de ferramentas TIC no seio da justiça.

Em suma, encontramos-nos num momento histórico no qual o uso de TIC se revela uma realidade inescapável, designadamente em matéria do exercício da atividade judicial e, em especial, em matéria de execução da justiça criminal. Tais tecnologias, sendo, em simultâneo, uma necessidade e uma inevitabilidade, encerram em si mesmas grandes potencialidades e mais-valias que não podem deixar de ser aproveitadas a fim de conferir maior celeridade, eficácia e eficiência ao sistema judicial, designadamente na investigação de realidades criminais complexas e organizadas como o são, via de regra, aquelas associadas à comissão dos crimes de corrupção. Eficiência, eficácia e celeridade – estas que, por sua vez, contribuirão para o reforço da confiança comunitária no Estado de Direito Democrático.

Todavia, a sua adoção, implementação, execução e resultados não se revelam neutros ou isentos de riscos e de especiais desafios que urge de antemão encarar. Cientes de tais riscos importa, quanto antes, sedimentar na prática judiciária um conjunto de princípios, regras e metodologias no uso das referidas TIC,

³⁵ Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente, adoptada pela CEPEJ na sua 31.ª reunião plenária (Estrasburgo, 3 e 4 de dezembro de 2018), <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>.

³⁶ 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), <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689>.

designadamente através da tipificação de tais riscos e dos respetivos meios de os prevenir, com vista à criação de instrumentos que norteiem jurídica, prática e eticamente o respetivo uso.

Consideraciones sobre la aplicación de las nuevas tecnologías a la lucha contra el crimen organizado

Francisco Javier Garrido Carillo *

1. Introducción

La globalización de nuestra sociedad y de la economía ha supuesto, de forma paralela, la globalización del crimen, y, por lo tanto, la lucha contra las redes criminales y otras formas graves de delincuencia requiere y exige de los Estados una respuesta penal común. Por consiguiente, es preciso poner en marcha instrumentos y sistemas verdaderamente eficaces.¹ En esta globalización ha sido clave el desarrollo de las nuevas tecnologías, y la digitalización de todos los sectores de nuestra civilización.

En este marco, el fenómeno de la corrupción se puede entender como estructural en el crecimiento y expansión de la criminalidad organizada transfronteriza, por lo que ha tenido su correspondiente reflejo en la adopción de medidas esenciales adoptadas en instrumentos internacionales.² Muestra de ello, entre otras,³ tenemos la Convención de las Naciones Unidas contra la corrupción de 31 de octubre de 2003, que ya en su prefacio señala que *“La corrupción es una plaga insidiosa que tiene un amplio espectro de consecuencias corrosivas para la sociedad. Socava la democracia y el Estado de Derecho, da pie a violaciones de los derechos humanos, distorsiona los mercados,*

* Professor de Derecho Procesal en la Facultad de Derecho de la Universidad de Granada. Este trabajo ha sido realizado en el ámbito de los Proyectos: Módulo Jean Monnet “Challenges and strategic profiles of the EU in the fight against organised crime” Erasmus-Jean Monnet 2023-2026 Module. (Ref. 101127315); Módulo Jean Monnet, «Challenges to justice in the EU: perspectives for reform», Erasmus-Jean Monnet 2022-2025 Module, (Ref. 101085462); Proyecto de investigación I+D+ i “Proceso Penal y Espacio de Libertad, Seguridad y Justicia: Garantías, Cooperación Transfronteriza y Digitalización”, PID2023-152074NB-I00; y Red de Cooperación internacional y de excelencia científica de estudio y análisis “Justicia, Derecho, Constitución y Proceso.”

¹ Sobre este tema, cf. Francisco Javier Garrido Carillo, *Instrumentos contra el crimen organizado. Cuestiones pendientes para que el delito no resulte provechoso* (Madrid: Aranzadi, 2024).

² Como señala Nicolás Rodríguez García, *El decomiso de activos ilícitos* (Navarra: Aranzadi, 2017), 28, *“Ante un escenario de globalización de la economía se ha favorecido indirectamente una globalización de la delincuencia, que exige de los Estados una globalización de la respuesta penal”*; Sobre la misma cuestión, cf. Michael Levi, “Crimes of globalization: some measurement issues”, in *New types of crime. Proceedings of the International Seminar held in connection With HEUNI’s thirtieth anniversary*, ed. Matti Joutsen, (Helsinki: European Institute for Crime Prevention and Control, 2011), 107 y ss.

³ Entre la multiplicidad de medidas e instrumentos internacionales existentes podemos mencionar las siguientes; el artículo 5 del Convenio de Naciones Unidas firmado en Viena de 1988, contra el tráfico ilícito de estupefacientes y sustancias sicotrópicas, y junto a esta medida en la lucha contra la criminalidad organizada destacamos también el Convenio de las Naciones Unidas de 1961 sobre estupefacientes (artículo 37); el Convenio de Viena de 21 de febrero de 1971, sobre psicotrópicos (artículo 22.3); el Convenio para la represión de la financiación del Terrorismo hecho en Nueva York el 9 de diciembre de 1999; la Convención de la ONU sobre Delincuencia organizada transnacional de 15 de noviembre de 2000; y la Convención de las Naciones Unidas contra la corrupción de Nueva York, de 31 de octubre de 2003.

*menoscaba la calidad de vida y permite el florecimiento de la delincuencia organizada, el terrorismo y otras amenazas a la seguridad humana.”*⁴

Y es que la corrupción, privada y pública, camuflándose, adaptándose y mimetizándose con estructuras legales, se imbrica en los Estados, ocupando y parasitando sus instituciones, debilitando las sociedades democráticas, devaluando y vaciando de contenidos los derechos básicos y los sistemas normativos, dando lugar a crisis irreversibles y a estados fallidos.

Ante esta realidad, y como cuestión previa, hemos de ser conscientes de la dimensión del problema, por cuanto que el Crimen Organizado y la Delincuencia Grave avanza y se desarrolla hacia nuevas perspectivas más sofisticadas y difíciles de perseguir, que se caracterizan por la diversificación de sus estructuras y métodos, y por la proliferación de grupos itinerantes.⁵

Así mismo, en esta tipología criminal destacan cuestiones emergentes, y factores externos, como: el imparable uso de las nuevas tecnologías; las vinculaciones entre crimen organizado y terrorismo; los nuevos modelos de negocio criminal; las amenazas híbridas; o los cambios demográficos. Por lo tanto, podemos concluir que el crimen organizado es una amenaza de naturaleza transnacional, flexible y opaca, “*con una enorme capacidad desestabilizadora, que contribuye a debilitar el Estado y mina la buena gobernanza económica.*”⁶

2. Perfiles estratégicos en la lucha contra el crimen organizado

La dimensión del problema, junto a su globalización y su transversalidad exige el diseño de perfiles estratégicos (que no tácticos), con el objeto de articular esta lucha contra el Crimen Organizado. Perfiles que, deben concretarse en una respuesta institucional y normativa, a la vez que coherente, eficaz.⁷

Ahora bien, la búsqueda de esta eficacia no puede convertirse en una excusa para tensionar la arquitectura jurídica básica de nuestros sistemas de justicia penal, poniendo en riesgo o excepcionando los derechos y garantías básicas de las partes, pues estos mecanismos de garantías no sólo son respuesta a la necesidad de dotarse de sistemas jurisdiccionales propios de un Estado de Derecho, respetuoso con los derechos humanos, sino que legitiman, a su vez, la acción de dicho Estado en la persecución del delito y en el ejercicio del *ius puniendi*.

Por otro lado, la búsqueda de la eficacia en la respuesta institucional y normativa de los distintos Estados debe permitir coordinar las políticas criminales sobre una base jurídica integrada, completa, transversal y eficiente, que facilite a los operadores jurídicos actuar con seguridad y dinamismo.⁸

⁴ Dedicando dicha Convención internacional, su capítulo V (Artículos 51-59), a la recuperación de activos.

⁵ En este sentido, cf. la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave para 2019-2023 (actualmente en renovación). *Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023. La seguridad es un proyecto común*, Madrid, junio, 2019, 26.

⁶ *Estrategia de Seguridad Nacional 2017*, BOE 309, 21 diciembre de 2017, 125983.

⁷ Obsérvese que no es lo mismo eficacia que eficiencia, por cuanto la eficacia es “*la capacidad de lograr el efecto o deseo que se espera*”, mientras que la eficiencia es “*la capacidad de lograr los resultados deseados con el mínimo posible de recursos.*” Por eso aquí hablo de eficacia que no de eficiencia.

⁸ Ante la situación del crimen organizado en la UE, hemos de tratar la respuesta institucional del sistema de derecho penal de la UE, y sus límites, deteniéndonos especialmente en la Fiscalía Europea y Eurojust, y apostando, para la profundización en el ELSJ, por una ampliación de competencias de la mencionada Fiscalía, o por una mayor evolución de Eurojust. En mi opinión si la UE quiere dar una respuesta eficiente a los desafíos planteados por el crimen organizado y transfronterizo, se enfrenta a un dilema; o bien se encamina a un sistema federal, y amplía las competencias de la Fiscalía Europea; o bien opta por mejorar los mecanismos de coordinación existentes, ampliando las prerrogativas

Entre los posibles perfiles estratégicos, es oportuno detenerse en cuatro: en el análisis de la relación “*Globalización y Crimen organizado*”; en los instrumentos y órganos especializados en la lucha contra la delincuencia organizada; en el decomiso, y en las experiencias en la recuperación y gestión de activos derivados del crimen; y por último en el impacto de las nuevas tecnologías.

2.1. La relación “*globalización y crimen y organizado*”⁹

La criminalidad organizada es hoy “*un sistema*” que ha evolucionado con los tiempos y ha alcanzado una dimensión supranacional, como ponen de relieve, entre otros informes, el “*Global Risk Report*” promovido por el *World Economic Forum*, en el que se señala que las redes criminales generan un negocio de más de 3 billones de euros,¹⁰ sin que se alcance en la UE el 1 % en la confiscación de estos bienes.¹¹

Y en concreto, atendiendo a los datos del Museo Nacional de Crimen Organizado y Cumplimiento de la Ley de Las Vegas, (Nevada)¹² en 2021 los ingresos totales de los grupos de delincuencia organizada transnacional se acercaron a los 2 billones de dólares al año. Y, podemos comprobar el impacto de las tecnologías, destacando, que el cibercrimen mueve casi el doble de dinero que el tráfico de drogas, armas y trata de personas juntos, alcanzando su valor casi el 1,5% del PIB mundial.¹³

de Eurojust de acuerdo con las posibilidades que ofrece el artículo 85 del TFUE, y mejorando el proceso de armonización a nuevos ámbitos del derecho penal. Estas cuestiones, sin duda, se habrán de dilucidar en los próximos años y marcarán la proyección de futuro de la Unión Europea.

⁹ Este análisis, nos permite disponer de un marco de actuación y de una perspectiva de trabajo. En el diseño de una estrategia adecuada, el punto de partida es poner en relación, en el ámbito sustantivo y procesal, el concepto de “*globalización*” y “*delincuencia organizada*.” Tener una medida real de esta simbiosis y una conciencia clara de su impacto y de sus efectos negativos sobre las respuestas nacionales e internacionales, nos permite concretar, y reclamar con urgencia, la necesidad de un marco jurídico sólido, que sea apoyo firme y abierto a las diferentes coyunturas que muestra este tipo de delincuencia, y no sólo desde la variable de su internacionalización, sino desde los derechos sustantivos nacionales. Y es que, el crimen organizado trasciende las fronteras de los Estados, ya no caben únicamente respuestas nacionales, aunque se planteen de forma coordinada, pues esto en definitiva es trasladar los problemas de un país a otro. Lo que hay que hacer es plantear una respuesta internacional y global ante este conflicto, y este camino ya lo inició Naciones Unidas en torno al concepto de “*grupo delictivo organizado*”, y no en torno a comportamiento delictivos definidos o intereses separados a proteger. El concepto de “*grupo delictivo organizado*”, que se recoge en el artículo 2 de la Convención de Palermo, ha ido ampliándose y matizando sucesivamente, tanto en instrumentos normativos, como por la doctrina, y ha puesto de relieve la dificultad y la confusión que existe al intentar acotar un concepto unívoco de crimen organizado tanto en el orden internacional como en el ámbito nacional. Partiendo de esta situación tenemos que incorporar al concepto de delincuencia organizada la dimensión globalizadora pues, aprovechando esta globalización, las organizaciones criminales, cada vez más, utilizan métodos sofisticados tanto para ocultar sus actividades delictivas como el producto de sus delitos. Y, si bien esta inter-relación entre globalización y delincuencia organizada genera nuevos espacios para esta última, también debe proyectarse sobre la necesaria adecuación de la respuesta del derecho penal a este fenómeno criminal.

¹⁰ Para una mejor comprensión de estas cifras hemos de tener en cuenta que el PIB mundial en 2023, alcanzó los 96’5 billones de euros, conforme a las proyecciones del Fondo Monetario Internacional (FMI) en su Informe sobre Perspectivas de la Economía Mundial de octubre de 2023. Y por su parte el PIB de la UE, en 2021 ascendió a 14.5 billones de Euros.

¹¹ Asimismo, los informes SOCTA de Europol constatan la amenaza del Crimen organizado en la Unión (*European Organised Crime Threat Assessment*), siendo posible trazar un mapa de la “*mala-Europa*” y de su economía paralela. Consultar: <https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021> (último acceso 10/10/2024).

¹² *National Museum of Organized Crime and Law Enforcement*, de Las Vegas, Nevada. Consultar <https://www.themobmuseum.org> (último acceso 11/09/2024).

¹³ Consultar <https://www.itdigitalsecurity.es/actualidad/2023/06/el-valor-del-cibercrimen-se-aproxima-al-15-del-pib-mundial> (último acceso 10/02/2024).

Por otro lado, en la actualidad, Europol ha identificado 821 redes criminales¹⁴ (con más de 25.000 integrantes, que están activas en áreas delictivas como el tráfico de drogas, el tráfico ilícito de personas migrantes y delitos contra la Propiedad),¹⁵ dedicándose más del 70% de las mismas a la corrupción para facilitar la actividad delictiva o impedir la aplicación de la ley.

En definitiva, estamos en un nuevo mundo y hemos llegado a un punto de “no retorno”, en el que se ha superado el binomio tradicional “*crimen organizado-transnacional*”, para concretarse un trinomio de extraordinaria gravedad “*crimen organizado-transnacional-digital*.” Y es que los grupos delictivos en la UE se caracterizan por tener una alta capacidad de adaptación; por la posibilidad de actualizar constantemente sus habilidades tecnológicas; y por tener múltiples “*objetos sociales*”

¹⁴ Estos datos se recogen en el informe publicado por Europol con el título “*Decodificando las redes criminales más amenazantes de la UE*” (2024), donde se analizan las principales redes criminales a nivel europeo. En su elaboración han participado todos los Estados miembros de la UE y 17 países socios de Europol. Y en el mismo se ha visto que las redes dirigidas por españoles se dedican principalmente al tráfico de drogas. Para elaborar el listado de redes criminales se tuvieron en cuenta cuatro criterios: agilidad, operaciones transfronterizas, control de estas redes y capacidad de destrucción. Y Europol ha llegado a la conclusión de que “*la amenaza que plantean estas redes es generalizada y compleja*», por lo que «*es necesaria -subrayan- una respuesta coordinada, sostenida, multilateral y conjunta*.”

¹⁵ El informe de Europol constata que, a día de hoy, estas redes criminales son multidisciplinarias, y se dedican a más de un tipo de delito. Por ello Europol, con la contribución de los Estados miembros ha creado “*mapas de calor*” para identificar zonas y el tipo de actividad más agresiva. Lo que ha revelado la concentración de estos grupos criminales en la zona de los puertos. El informe, considera que las 821 redes criminales identificadas como amenazantes y de alto riesgo, lo son porque tienen en común cuatro características principales: a) En primer lugar, su agilidad o facilidad para ir adaptando sus operaciones delictivas a los nuevos desafíos que les plantean las fuerzas y cuerpos de seguridad. De hecho, en el informe se hace constar que estas redes tienen capacidad para infiltrarse hasta tal punto que se aprovechan de las estructuras comerciales que operan legalmente. Eso les permite que su entramado criminal prospere, porque son capaces de blanquear sus beneficios y evitar su detección por parte de las fuerzas policiales. El 86% de las redes criminales identificadas recurren a este tipo de estructuras empresariales legales (la mayoría de las cuales están dentro de la UE); b) En segundo lugar, son organizaciones criminales transfronterizas, es decir, que operan simultáneamente en diferentes países y su estructura organizativa es internacional, con miembros que actúan tanto dentro como desde fuera de Europa. De hecho, en el informe se han identificado un total de 112 nacionalidades y se ha llegado a la conclusión de que un 68 % de estas redes están integradas por criminales de múltiples nacionalidades. Sin embargo, también se observa que la mayoría de las redes mantiene un mismo entorno geográfico; c) En tercer lugar, hay que referirse al Control. Las redes criminales de mayor riesgo ejercen, según recoge el informe, un fuerte control sobre sus operaciones criminales. Es decir, que cada una tiende a especializarse en un negocio criminal concreto. De hecho, se hace constar que las redes ‘poli-criminales’ son la excepción, y no la norma. Por otra parte, también se refleja que los líderes del 82% de estas redes se encuentra en el país principal objeto de su actividad criminal, o en el país de origen de esos miembros clave para la organización; d) Y, en cuarto lugar, hay que hablar de la Capacidad destructiva. En el informe se asevera que las actividades delictivas y las prácticas corruptas de las redes delictivas más amenazantes están infligiendo un daño significativo a la seguridad interior, al estado de derecho y a la economía de la UE. La mitad de estas redes están involucradas en el tráfico de drogas como principal actividad delictiva. Más del 70% de las redes se dedican a la corrupción para facilitar la actividad delictiva u obstruir la aplicación de la ley o los procedimientos judiciales. Y el 68% de las redes utilizan la violencia y la intimidación como una característica inherente a su modus operandi. Por lo que se refiere a las redes con líderes españoles, la mayoría se dedican al tráfico de drogas y operan en casi 50 países (principalmente en Bélgica, China, Colombia, Francia, Alemania, Italia, Marruecos, Países Bajos, Portugal y España). En el informe se detallan tanto la procedencia de los miembros de estas organizaciones criminales, como las principales actividades delictivas que desarrollan. Y, en el caso de España, las redes criminales cuyos líderes principales son españoles están integradas por miembros de múltiples nacionalidades, que cooperan y establecen contactos con redes de 48 nacionalidades diferentes. Estas redes criminales se dedican principalmente al tráfico de drogas (cocaína y cannabis), a la delincuencia medioambiental, al fraude contra los intereses públicos de la UE y al blanqueo de capitales. Y por añadir algún dato más a este marco del crimen organizado en España, señalar que, a día de hoy, el CITCO (*Centro de Inteligencia contra el Terrorismo y el Crimen Organizado*) mantiene abiertas 12.000 investigaciones en el ámbito del crimen organizado y alrededor de 1.300 están relacionadas con el terrorismo.

(más del 45% de estos grupos están implicados en más de una actividad ilegal); contando, además, con el uso de factores “*facilitadores*”, y así, por ejemplo, casi el 70% de los grupos criminales denunciados participan, en actividades de corrupción, y el 86% utilizan estructuras empresariales legales.

2.2. Instrumentos y órganos especializados en la lucha contra el crimen organizado

El segundo perfil estratégico se centra en los instrumentos y órganos especializados en la lucha contra la delincuencia organizada, poniendo en valor los avances y profunda transformación, que ha sufrido la fiscalía y otros órganos en el desarrollo de sus capacidades para enfrentarse a este fenómeno criminal. Y es que, como ha dejado escrito, y de forma muy acertada, Jiménez-Villarejo: “*cualquier estrategia eficaz de lucha contra el crimen organizado, necesita, junto con la imprescindible arquitectura normativa sustantiva y procesal, que prevea tipos penales adecuados y nos proporcione herramientas eficaces de investigación en un entorno cambiante, de la creación y permanente remodelación, reforzamiento e impulso de estructuras institucionales, oficinas o unidades multidisciplinarias, desde las que se pueda asegurar la aplicación de los instrumentos legales existentes contra la delincuencia organizada de la manera más eficaz.*”¹⁶

Actualmente, las políticas criminales y las estrategias de seguridad vienen poniendo el foco de atención en las autoridades policiales, en un claro desequilibrio con las autoridades judiciales y con la denominada dimensión judicial en la lucha contra la criminalidad organizada.

Por otro lado, no hay que olvidar que un enfoque integral de la lucha contra la corrupción y el crimen organizado¹⁷ debe sustentarse en una combinación de medidas preventivas y represivas, lo que exige sistemas judiciales independientes (y un Ministerio Público también independiente), que garanticen con eficacia el cumplimiento de la legislación mediante investigaciones y juicios imparciales, con sanciones efectivas, proporcionadas y disuasorias, y con la recuperación de activos.

Hoy en día, sin duda alguna, el Fiscal tiene un protagonismo destacado, en concreto en dos de los cuatro ejes de actuación señalados por la COM en su comunicación sobre la estrategia de la UE frente al Crimen organizado 2021-2025,¹⁸ tanto en la recuperación de activos, como en la cooperación judicial internacional, razón por la cual esta Institución está llamada a desempeñar un papel central como oficina judicial especializada en la respuesta penal ante la criminalidad organizada. En este sentido, la Fiscalía Europea es ya un referente, aunque limita su ámbito de actuación a la investigación y acusación sólo por delitos que afecten a los intereses financieros de la Unión. Y es que, su estructura institucional integrada y sus procesos de toma de decisiones colegiados son sin duda una importante ventaja en la lucha contra el crimen organizado. En este sentido, se debe valorar y avanzar en la vía que abre el artículo 86.4 del TFUE, con la perspectiva de ampliar las competencias de la Fiscalía Europea con el objeto de incluir “*delitos graves que tengan una dimensión transfronteriza.*”

¹⁶ Cf. Francisco Jiménez-Villarejo Fernández, “La Fiscalía ante el crimen organizado. Referencias a la fiscalía especial contra la corrupción y la criminalidad organizada”, in *Respuesta institucional y normativa al crimen organizado. Perfiles estratégicos para una lucha eficaz*, ed. Francisco Javier Garrido Carillo (Pamplona: Aranzadi, 2022), 169, 171.

¹⁷ Documento COM(2020) 580 final.

¹⁸ Documento de 14 de abril de 2021 COM(2021) 170 final.

2.3. Decomiso y experiencias en la recuperación y gestión de activos derivados del crimen

Un tercer perfil estratégico sería el dedicado al decomiso,¹⁹ y a las experiencias en la recuperación y gestión de activos derivados del crimen. No es necesario insistir en que éste es el “*talón de Aquiles*” de las estructuras criminales: actuar sobre su capacidad económica y sus beneficios. Por lo tanto, las experiencias de recuperación de activos derivados del delito, que supongan un avance en “*que el delito no resulte provechoso*”,²⁰ son un elemento central en el diseño y articulación de cualquier política-criminal contra el crimen organizado. En definitiva, las actuaciones dirigidas al decomiso, a la recuperación de activos del delito, al control de los flujos financieros y al reforzamiento de las medidas de investigación, se enmarcan en la creación y desarrollo de una política criminal de la UE dirigida a asfixiar económicamente a las organizaciones criminales mediante la expropiación de las ganancias proporcionadas por sus actividades delictivas. Y a todo ello hemos de sumar el valor añadido que supone la posibilidad de poner los recursos y activos decomisados a las redes criminales, al servicio del Estado de Derecho aumentando sus medios para combatir a esta delincuencia organizada y transfronteriza.

Las medidas e instrumentos adoptados hasta la fecha han supuesto grandes avances en la dirección correcta, pero hay que reconocer, como hace la Comisión Europea, que siguen siendo insuficientes e ineficientes. Por lo tanto, hay que trabajar y profundizar en los marcos jurídicos disponibles y en la conformación de mecanismos y sistemas de cooperación, coordinación e intervención en la recuperación y gestión de activos derivados del delito. En este ámbito se hacen esenciales las políticas e instrumentos de decomiso y embargo, las medidas de control de los flujos financieros de los colectivos criminales,²¹ la adopción de medios de investigación y análisis tecnológicos, la adaptación de otros medios clásicos, y la adecuada actuación y coordinación de instituciones como la Fiscalía Europea, Europol, Eurojust y la Oficina Europea de Lucha contra el Fraude (OLAF). Todo ello exige el diseño y adaptación de instrumentos e instituciones penales y procesales, que han de operar en el marco de nuestro proceso penal, respetando los derechos y garantías básicas del mismo.

Dos instrumentos hay que destacar en este apartado, por un lado la Directiva (UE) 2024/1260 del Parlamento Europeo y del Consejo sobre recuperación y decomiso de activos de 24 de abril de 2024, que intenta dar respuesta a la necesidad de reforma de la institución, de la que era consciente las distintas instituciones europeas desde hace tiempo, pues era y sigue siendo necesario complementar un conjunto de instrumentos legislativos que armonizan la definición de los delitos y las sanciones de las actividades delictivas, así como otros instrumentos destinados a prevenir o combatir actividades ilícitas relacionadas con aquellos.

¹⁹ Sobre el decomiso cf. Francisco Javier Garrido Carillo, *El decomiso. Innovaciones, deficiencias y limitaciones en su regulación sustantiva y procesal* (Madrid: Dykinson, 2019).

²⁰ Comunicado de la Comisión al Parlamento Europeo y al Consejo, de 20 de noviembre de 2008, Productos de la delincuencia organizada: garantizar que “*el delito no resulte provechoso*”, COM (2008) 766 final – no publicado en el Diario oficial.

²¹ Sobre el control de los flujos económicos y financiero cf. María Ángeles Pérez Marín, “El control de las vías financieras frente a la delincuencia organizada en el Espacio de libertad, seguridad y justicia: los avances hacia la persecución de nuevas amenazas”, in *Retos en la lucha contra la delincuencia organizada: Un estudio multidisciplinar: garantías, instrumentos y control de los beneficios económicos*, ed. Francisco Javier Garrido Carillo (Aranzadi, 2021), 85.

La directiva va en la buena dirección, solventa muchas de las deficiencias de la regulación anterior de 2014²² y establece unas normas mínimas sobre las distintas medidas y las correspondientes garantías, con el objeto de que haya una interpretación común y unas bases homogéneas para el seguimiento e identificación y para el embargo, decomiso y gestión de activos en los distintos Estados miembros. Por otro lado, la adopción de estas normas mínimas no impide a los Estados miembros, otorgar competencias más amplias a los organismos de recuperación de activos, o a los organismos de gestión de activos, ni establecer garantías adicionales a través de la legislación nacional, siempre y cuando dichas medidas y disposiciones nacionales no vayan en detrimento del objetivo de la propuesta de Directiva. Sin duda alguna, la actual Directiva (UE) 2024/1260 va a dar respuesta y solución a muchas de las deficiencias ya detectadas, ahora bien, también incorpora innovaciones y modificaciones que suponen transformaciones en profundidad en la materia, y que pueden dar lugar a los mismos problemas que se pretenden solventar y a nuevas dificultades, por lo que habrá que estar muy atentos al desarrollo de esta norma por los distintos Estados miembros, y a su impacto en la práctica diaria.

Y, en segundo lugar, en relación a los instrumentos en la lucha contra el crimen organizado, es ineludible ocuparse de las Oficinas de Recuperación y Gestión de Activos (ORGA's),²³ que en España se ha conformado como un órgano instrumental, centralizado y especializado, que, en relación principalmente con procedimientos e investigaciones de delincuencia organizada, auxilia a las Fiscalías y órganos judiciales en la localización, administración, gestión y realización de activos derivados del delito. Estas oficinas, como elemento central en la realización de efectos judiciales, exigen un análisis de su deficiente regulación, pues los problemas prácticos que la misma ha planteado desde el primer momento han querido ser solventados por el legislador con la reforma operada por la LO 1/2015 de 30 de mayo de modificación de la Ley Orgánica 10/1995 del Código Penal, que ha supuesto una transformación en profundidad de la regulación vigente, que ha sido desarrollada reglamentariamente en el Real Decreto 948/2015 de 23 de octubre por el que se regula la mencionada Oficina de Recuperación y Gestión de Activos.²⁴ Por último, este Real Decreto 948/2015²⁵ fue modificado posteriormente por el Real Decreto 93/2018, de 2 de marzo.²⁶

²² Sobre esta cuestión, cf. Francisco Javier Garrido Carillo, "Cuestiones pendientes sobre el decomiso ocho años después. La propuesta de Directiva del Parlamento Europeo y del Consejo sobre recuperación y decomiso de activos", *Revista de Estudios Europeos*, n.º extraordinario monográfico 1 (2023), 311.

²³ Directiva 2014/42/UE del Parlamento Europeo y del Consejo de 3 de abril sobre el embargo y el decomiso de instrumentos y del producto del delito en la Unión Europea.

²⁴ Cf. Francisco Javier Garrido Carillo, "Instrumentos en la lucha contra el crimen organizado. La Oficina de Recuperación y Gestión de Activos en España", *Revista Peruana de Ciencias Penales*, no. 34 (2020), 107.

²⁵ El Real Decreto 948/2015 fue modificado posteriormente por el Real Decreto número 93/2018 de 2 de marzo, y a este desarrollo Reglamentario hay que añadir el Plan de Acción aprobado el 10 de febrero de 2016, que ha sido complementado con la Orden JUS/188/2016 de 18 de febrero del Ministerio de Justicia por la que se determina el ámbito de actuación y la entrada en funcionamiento operativo de la oficina de Recuperación y Gestión de Activos y la apertura de su cuenta de depósitos y consignaciones (BOE núm. 44 de 20 de febrero de 2016), así como por la Resolución de la Secretaría de Estado de Justicia, de 16 de septiembre de 2016, por la que se desarrolla el procedimiento de gestión de activos por la Oficina de Recuperación y Gestión de Activos y su régimen económico, y por último la Resolución de 5 de abril de 2018 de la Secretaría de Estado de Justicia por la que se publica el Convenio con el Consejo General del Poder Judicial en materia de colaboración y apoyo al funcionamiento de la Oficina de Recuperación y Gestión de Activos.

²⁶ Publicado en el BOE de 13 de marzo de 2018, y que afectó a los artículos 1, 3, 5, 6, 9 y 11 a 13, se añadió el capítulo VI y la disposición Adicional tercera. El objetivo de reforma es "configurar el marco

2.4. El impacto de las nuevas tecnologías

Y el cuarto perfil estratégico que exige nuestra atención, no es otro que el impacto de las nuevas tecnologías en la lucha contra el crimen organizado. Con especial referencia a la realidad de la inteligencia artificial (IA) y la necesaria protección de datos. Pues, en esta batalla desigual, el crimen organizado se adapta en tiempo real a los avances tecnológicos, modificando sus pautas de actuación y ocupando los espacios de impunidad que la falta de regulación y de agilidad del legislador, le permite.

La irrupción de las nuevas tecnologías en nuestro “*ecosistema judicial*”, normativamente hablando, tiene ya una trayectoria de más de veinticinco años, y a veces parece una cinta de *moebius*, pues da la impresión que, avanzando, siempre estamos en el mismo punto de partida. Y es que, llevamos más de dos décadas, con la informatización de la oficina judicial, la incorporación de la tecnología a la justicia, y con la digitalización judicial, es decir, se ha trasladado a la sociedad en general y a los operadores jurídicos en especial. Esto va a tener lugar un antes y un después, estando inmersos en una nueva dinámica, que supone una transformación estructural, profunda y constante, que afecta transversalmente a nuestra sociedad y a la forma, que hemos tenido hasta ahora, de relacionarnos. En el fondo, es una auténtica “*revolución*”, pues, las nuevas tecnologías, suponen un cambio en nuestra civilización, poniendo en discusión la centralidad del ser humano.

La aplicación de la IA – de la que no existe una definición única y pacífica²⁷ – en la justicia penal, pone de relieve los riesgos para un adecuado respeto de los derechos fundamentales, y es que el algoritmo puede constituir un instrumento de prevención y lucha contra el crimen organizado, pero al mismo tiempo ser un arma al servicio de la criminalidad.

Y es que, el carácter polifacético de la IA da lugar no solo a ventajas sino también a graves riesgos, en especial para los sectores más sensibles de la seguridad y la estabilidad de la democracia, por lo que, como ya afirmaba la Comisión Europea en el Libro Blanco de 2020, es necesario adoptar un enfoque antropocéntrico, ético, sostenible, y respetuoso de los derechos y valores fundamentales. Es por ello, que, el uso de la IA en la fase de investigación penal ha de llevarse a cabo desde el máximo respeto a los derechos fundamentales de sospechosos, acusados y víctimas, evitando sesgos, discriminaciones y desviaciones indeseables o intrusivas en la vida privada y en la intimidad personal, y evitando, asimismo, poner en riesgo la presunción de inocencia.

normativo de la actuación de la oficina adecuándolo a los principios de seguridad jurídica, transparencia, eficacia y eficiencia”, pues al tratarse la Oficina de un órgano de la administración General del Estado de nueva creación y con la peculiaridad de ser auxiliar de la administración de justicia, surge la necesidad de desarrollar su régimen de funcionamiento regulando los procedimientos que seguirá la Oficina para el desarrollo de la función de gestión de los bienes encomendados por la autoridad judicial (Parágrafo II del preámbulo de RD 93/2018 de 2 de marzo), puesto que no existía una regulación de los procedimientos de gestión de activos por la Oficina con el rango normativo adecuado para surtir efectos jurídicos frente a terceros.

²⁷ La inteligencia artificial no sería una sola cosa, sino un conjunto de tecnologías conexas, desarrolladas para igualar o sustituir la inteligencia humana. Sobre el tema, cf. Yanqing Duan, John S. Edwards y Yogesh K., Dwivedi, “Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda”, *International Journal of Information Management*, v. 48 (2019), 63. Disponible en <https://doi.org/10.1016/j.ijinfomgt.2019.01.021>; Toby Walsh *et al.*, *Closer to the Machine: Technical, Social, and Legal Aspects of AI* (Office of the Victorian Information Commissioner, 2019). Disponible en <https://ovic.vic.gov.au/wp-content/uploads/2019/08/closer-to-themachine-web.pdf>.

A esto hay que añadir que los sistemas de IA son capaces, a través de “*juicios de la máquina*” (la artificialización) de adquirir y aplicar soluciones a los problemas, y paralelamente, de aprender de la experiencia, pudiendo desarrollar, hasta cierto punto, algunas funciones cognitivas relacionadas con la memoria, el lenguaje y la planificación,²⁸ se trata de un fenómeno de “*desresponsabilización del hombre*” y “*responsabilización de la máquina*.”²⁹ En definitiva, la IA avanza y evoluciona, integrando artificialmente funciones cognitivas, especialmente en el ámbito militar y de seguridad, siendo su uso cada vez más creciente en nuestra sociedad, bajo la idea de una supuesta neutralidad, eficiencia, exactitud y precisión absoluta.

Ahora bien, la IA ha venido para quedarse en todos los ámbitos de la sociedad actual y también en el judicial, por lo que es necesario afrontar este reto, desde el máximo respeto de los derechos y libertades fundamentales que se consagran en los Estados democráticos, y esto hace necesario intervenir desde la ley, promoviendo una regulación armonizada entre los distintos Estados miembros, con unos mínimos indiscutibles, haciendo de la IA un recurso y una herramienta para una mejor respuesta judicial, pero sin que ello suponga la sustitución del juez ni la implementación de sistemas de riesgo para los derechos de los ciudadanos.

Para evitar los riesgos que los sistemas de IA puede conllevar para la democracia,³⁰ y para proteger los derechos fundamentales de los afectados, es necesario establecer una serie de exigencias a los sistemas de IA que, además de modos de consentimiento nuevos, más seguros y legítimos, también cumplan con una serie de requisitos entre los que podemos destacar: la explicabilidad (XAI),³¹ la inteligibilidad; la interpretabilidad; la auditabilidad (que se pueda conocer una traza de todas las acciones que permitan averiguar lo que ocurrió); la transparencia;³² la reversibilidad; la imputabilidad; la responsabilidad; y la protección de los datos personales, especialmente los llamados sensibles.

2.4.1. Situación normativa actual

Ahora bien, la situación normativa existente hasta ahora la podríamos definir como un “*compost*” normativo, una amalgama de normas de *soft law*,³³ que ha cambiado radicalmente en este año 2024, con la aprobación del Convenio Marco del

²⁸ Eduardo Magrani, *A internet das coisas* (Rio de Janeiro: FGV Editora, 2018), 42-43.

²⁹ Sobre esta cuestión cf. Fabio Basile, “Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine”, *Diritto Penale e Uomo* (2019), 1, pp. 28-29 y Adam Liptak, “Sent to prison by a software program’s secret algorithms”, *The New York Times*, May 1 2017.

³⁰ Valentina Faggiani, “El derecho a un proceso con todas las garantías ante los cambios de paradigma de la IA”, *Teoría y Realidad Constitucional (TRC)*, no. 50 (2022): 518.

³¹ Es decir, que los resultados de la explicación puedan ser entendidos por humanos expertos.

³² [El efecto *Black Box* (caja negra) impide conocer, por la opacidad de estos sistemas, los códigos desde los que se deduce el algoritmo y sus efectos en la decisión, violando el derecho de la persona afectada a ser informado de forma clara e inteligible].

³³ Podemos señalar entre otras normas las siguientes: El Establecimiento de la Oficina Europea de IA (European AI Office) por Decisión de la Comisión Europea de 24 de enero [C(2024) 390 final]; Comunicación de la Comisión “Artificial Intelligence in the European Commission (AI@EC)” [C(2024)380 final], por la que establece su visión estratégica para impulsar el desarrollo legal, seguro y confiable de los sistemas de IA; La Declaración Europea sobre los Derechos y principios Digitales para la era Digital (2023/C 23/01) adoptada el 15 de diciembre de 2022; la Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la Inteligencia Artificial en la era digital [2020/2266(INI)]; La Comunicación de la Comisión, Una estrategia europea para los datos, (Bruselas, 19.2.2020, COM/2020/66 final); Comunicación de la Comisión, “Crear confianza en la inteligencia artificial antropocéntrica”, 8.4.2019, (COM (2019) 168 final); Carta Europea de Ética sobre el Uso de la Inteligencia Artificial en 2018; la Comunicación de la Comisión de 6 de abril de 2016 titulada “Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad.”

Consejo de Europa sobre Inteligencia Artificial y derechos humanos, democracia y Estado de derecho, que es el primer tratado internacional jurídicamente vinculante destinado a garantizar el respeto de estos derechos, de los propios Estados de derecho y de las normas jurídicas democráticas en el uso de los sistemas de IA,³⁴ y con la aprobación del Reglamento (UE) 2024/1689 de Inteligencia Artificial el pasado 13 de junio de 2024,³⁵ por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican distintos instrumentos normativos de la UE. Este Reglamento, está llamado a tener, desde la perspectiva procesal, una repercusión indiscutible en la efectividad de la cooperación transfronteriza en el Espacio de Libertad, Seguridad y Justicia (ELSJ) de la UE.

El Reglamento, que cuenta con 113 artículos, y 180 considerandos, precisa de un análisis exhaustivo y profundo, aunque solo fuera de las 68 definiciones que incorpora en su artículo 3, pero dicha labor supera los objetivos de este trabajo. No obstante, dejemos dicho, que el considerando n.º 61 clasifica como de alto riesgo *los “... sistemas de IA destinados a la administración de justicia y los procesos democráticos, dado que pueden tener efectos potencialmente importantes para la democracia, el Estado de Derecho, las libertades individuales y el derecho a la tutela judicial efectiva y a un juez imparcial.*

En particular, a fin de hacer frente al riesgo de posibles sesgos, errores y opacidades, procede clasificar como de alto riesgo aquellos sistemas de IA destinados a ser utilizados por una autoridad judicial o en su nombre para ayudar a las autoridades judiciales a investigar e interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos (...).”

Y, en el mismo Considerando señala que *“La utilización de herramientas de IA puede apoyar el poder de decisión de los jueces o la independencia judicial, pero no debe sustituirlas: la toma de decisiones finales debe seguir siendo una actividad humana.”*

Y es que, entre otras cuestiones, *“los sistemas de IA pueden constituir una fuente de prueba y, eventualmente, ser aportados al proceso como medios de prueba”*, y, asimismo toda esa ingente cantidad de información y datos sobre un gran número de individuos, y sobre usuarios concretos permite *“construir perfiles, segmentando por comportamientos y finalmente por individuos, de tal manera que, después de hacer un seguimiento acerca de cómo cada uno de ellos interactúa con esos dispositivos, es capaz de determinar, y por tanto de predecir, pautas de conducta o necesidades de una persona concreta.”*

Por consiguiente, el problema se encuentra en la utilización en el proceso penal de estos elementos cognoscitivos de gran impacto de tal manera que la denominada *“Eficiencia tecnológica”*, *“acabe siendo un criterio autosuficiente sobre la fiabilidad de la prueba, reemplazando así el juicio humano y dejando prácticamente sin efecto la presunción de inocencia”*, a lo que habría que añadir que la *“igualdad de armas”* también se vería afectada.

Ante esta situación, hay que mantener con contundencia que el uso de sistemas de IA en la fase de valoración de los medios de prueba no podrá reemplazar al juez-persona, por cuanto esta tarea de valoración libre, conjunta y racional de toda la prueba lícita practicada en la causa por el juez competente para el enjuiciamiento, es un función estrictamente jurisdiccional e indelegable.³⁶ De la misma forma hay

³⁴ CM (2024)52-addfinal Mayo 17 2024, Estrasburgo, *Council of Europe Treaty Series* – no. 225.

³⁵ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828.

³⁶ Sobre esta cuestión, cf. la referencia del artículo 14 de la LO 7/2021 de 26 de mayo de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

que mantener que en el marco del proceso penal, los informes, herramientas o instrumentos que tengan incidencia sobre los derechos del sospechoso o acusado, han de ser evaluados y asumidos por el juez, sin que quepa la automatización de los mismos.

2.4.2. *El compromiso y responsabilidad de la UE en la buena gobernanza de los sistemas de IA*

Ante esta situación, la Unión Europea ha intentado avanzar en su compromiso con la buena gobernanza de los sistemas de IA, en dos líneas de actuación: en los sistemas de gestión de riesgos y en la gobernanza de datos.

Con respecto al sistema de gestión de riesgos, la referencia básica o el elemento central que encontramos en el Reglamento de Inteligencia Artificial (RIA), exige que *“los sistemas de IA sean precisos, no discriminatorios y transparentes, a fin de garantizar que se respeten los derechos fundamentales de las personas afectadas y, en particular, sus derechos a la libre circulación, la no discriminación, la intimidad personal y la protección de los datos personales, la protección internacional y la buena administración”* (considerando n.º 60). Esta referencia está en la línea de perseguir una deseada *“neutralidad tecnológica.”*³⁷

Este *“sistema de gestión de riesgos”* para el uso de tecnología de IA, consistirá en un *“proceso iterativo continuo que se llevará a cabo durante todo el ciclo de vida de un sistema de IA de alto riesgo”*, y requerirá de actualizaciones sistemáticas periódicas (artículo 9 RIA).³⁸

Junto al *“Sistema de gestión de riesgos”*, el Reglamento se ocupa de la Gobernanza de datos en su artículo 10, que sería la segunda línea de actuación de la UE, exigiendo, que el conjunto de datos de entrenamiento, validación y prueba, cumplan con unos criterios de calidad (recogidos en los apartados 2 a 5 del precepto), con lo que se quiere examinar la existencia de *“posibles sesgos”*, y/o detectar *“posibles lagunas o deficiencias en los datos y la forma de subsanarlas”* [artículo 10.2 f) y g) Reglamento IA].³⁹

³⁷ Además, estos sistemas, se considerarán de *“Alto riesgo”* cuando los utilicen en determinados supuestos, por lo que, ahora que está aprobado el Reglamento de IA, están condicionados al cumplimiento de los requisitos y garantías previstos para este tipo de productos, que deberán ser evaluados, para comprobar esta conformidad (artículo 43 RIA). Como señala el Considerando n.º 61 del RIA los sistemas de IA de estas características pueden tener efectos *“potencialmente importantes para la democracia, el Estado de Derecho, las libertades individuales...”*, por lo que deben aplicarse a estos sistemas, como señala el considerando n.º 66 del mencionado RIA, requisitos que afectan; a la calidad de los conjuntos de datos utilizados, a la documentación técnica y el registro, a la transparencia y la comunicación de información a los usuarios, a la vigilancia humana, a la solidez, la precisión y la ciberseguridad, pues de esta manera se mitigan los riesgos para la salud, la seguridad y los derechos fundamentales.

³⁸ Este proceso iterativo, constará de cuatro etapas; a) en la primera se identificará y analizarán los riesgos conocidos y previsibles vinculados a cada sistema de IA de alto riesgo; b) en la segunda se estimarán y evaluarán los riesgos que podrían surgir cuando el sistema de IA de alto riesgo en cuestión se utilice conforme a su finalidad prevista y cuando se le dé un uso indebido razonablemente previsible; c) en la tercera se evaluarán otros riesgos que podrán surgir a partir del análisis de los datos recogidos con el sistema de seguimiento posterior a la comercialización; d) y en la cuarta etapa se adoptarán las medidas oportunas de gestión de riesgos con arreglo a lo dispuesto en las etapas anteriores.

³⁹ En esta línea marcada por la UE, y normativizada en el RIA, podemos encuadrar la referencia que el legislador español ha incorporado en el artículo 23 de la Ley Integral de Igualdad de Trato y no discriminación (Ley 15/2022 de 12 de julio) sobre *“inteligencia artificial y sistemas automatizados de toma de decisiones”*, con la que persigue que las Administraciones que usen estos sistemas tengan en cuenta criterios de minimización de sesgos, transparencia y responsabilidad. En concreto la disposición española establece que:

- Las administraciones públicas favorecerán la implantación de mecanismos que permitan que los algoritmos utilizados en dichas administraciones tengan en cuenta criterios de minimización de sesgos, transparencia y responsabilidad, siempre que sea técnicamente posible.
- La ley también exige que en estos mecanismos se incluyan su diseño y datos de entrenamiento, y

En definitiva, el Reglamento establece un conjunto de garantías y salvaguardas que, de cumplirse escrupulosamente, permitirían que los dispositivos de IA, y los algoritmos de última generación desarrollen su función con eficacia, puesto que se respetarían y protegerían de forma efectiva los derechos de los afectados, que es lo que legitimaría el uso de estos dispositivos.

3. Aplicaciones de las nuevas tecnologías en el proceso penal: potencialidades y límites

3.1. Las nuevas tecnologías como herramienta de auxilio a la decisión judicial

Llegados a este punto, y antes de abordar algunas aplicaciones de las nuevas tecnologías en el proceso penal, tanto en el ámbito de la investigación como de la decisión jurisdiccional, es oportuno que nos detengamos en algunos aspectos conceptuales.

En primer lugar, en relación a la denominada “*justicia predictiva*”, es decir a la posibilidad de predecir la actividad jurisdiccional, y en definitiva la decisión de órganos jurisdiccionales y tribunales (utilizando para ello la estadística) mediante el desarrollo de algoritmos específicos, que permite analizar ingentes cantidades de datos con una extraordinaria eficacia y supuesta neutralidad, es algo que merece una reflexión profunda y que pone en crisis el concepto de justicia que hasta ahora se ha manejado. Un primer problema sería la eliminación de la innovación jurisprudencial, y con ello la evolución del sistema legal.⁴⁰

Parte de la doctrina mantiene que la aplicación de algoritmos de predicción, para auxiliar y/o complementar las decisiones jurisdiccionales, supone una mejora

abordarán su potencial impacto discriminatorio que pueda surgir de su uso.

- Por otro lado, prevé la activación de evaluaciones de impacto para identificar posibles sesgos discriminatorios.

- Y por último recoge, el deber de las administraciones públicas de priorizar la garantía de transparencia en el diseño e implantación de los dispositivos de toma de decisiones automatizadas, así como la capacidad de interpretar las decisiones adoptadas por los mismos (artículo 23, párrafo. 2º Ley 15/2022 de 12 de julio).

Asimismo, hay que tener en cuenta la incidencia, en la cooperación penal internacional, de la Ley Orgánica 7/2021 de protección de datos personales en el proceso penal. Esta LO transpone -tarde- la Directiva 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. En este ámbito, recordemos que la petición y la prestación de cualquier auxilio judicial internacional penal por parte de las autoridades judiciales lleva consigo la cesión y el tratamiento de datos personales recabados con ocasión del proceso penal que requiere tal asistencia internacional, y, por lo tanto, la nueva regulación europea sobre la protección mínima, de datos personales en el proceso penal, incide de manera decisiva en esta materia, desde dos frentes; por un lado, favoreciendo la libre circulación del dato dentro de la UE; y por otro lado, concretando unas limitaciones y exigencias para que la transmisión de ese dato personal a un tercer Estado sea conforme a Derecho. En definitiva, por una parte, se regula un alto nivel de protección nacional de los datos de carácter personal, y por otra, se facilita la libre circulación de esos datos entre las autoridades de la UE. En este marco son múltiples las dudas y cuestiones que surgen para el operador jurídico nacional que necesite solicitar o prestar una asistencia judicial internacional con ocasión de un proceso penal. Y estas dudas no sólo surgen respecto de terceros países que no han adecuado su legislación a los dispuesto por la UE, o porque el Estado Miembro tenga un nivel de protección más alto y garantista del dato personal que el fijado en la Directiva, sino también de aquellos otros con los que España tiene convenios vigentes, pero dichos convenios no contengan cláusulas de protección de datos personales que respeten el mínimo fijado en la normativa de la UE.

⁴⁰ Aleš Završnik, “Algorithmic justice: algorithms and big data in criminal justice settings”, *European Journal of Criminology* (2019): 623, DOI: <https://doi.org/10.1177/1477370819876762>.

en la referida actividad jurisdiccional,⁴¹ lo que no deja de causar asombro, por cuanto que la “*eficacia*”, la rapidez, la capacidad en el manejo de ingente de datos, no supone “*a priori*” una mejora de la actividad jurisdiccional. La capacidad de trabajo o de desarrollar más trabajo, o de ser más rápido, no conlleva la mejora de los resultados de dicho trabajo. Por otro lado, la eficacia no supone neutralidad, y así mismo, en la actividad de juzgar y ejecutar lo juzgado, la tecnología no puede sustituir al ser humano, sino que ha de ser un instrumento de dicho ser humano.

En este marco, cuando se habla de “*justicia predictiva*” en un sentido amplio, se refiere tanto a herramientas de auxilio a la decisión, así como a tecnologías de revisión y sistemas de gestión administrativa y procesal, pero esto ha de tener una limitación en lo que se refiere a las actividades propiamente jurisdiccionales, es decir de decisiones del órgano jurisdiccional, o de la administración pública correspondiente que afecten a derechos y garantías básicas del afectado, pues a modo de ejemplo, una cosa es la ordenación, acceso, y visualización de expedientes, informes periciales, resoluciones judiciales, incorporando criterios de interés para esta actuación y otra muy distintas adoptar decisiones que afecten a la persona.⁴²

Por otro lado, hemos de señalar que la “*justicia predictiva*”, no se puede confundir con lo que se conoce como “*jurimetría*.”⁴³ Sobre esta cuestión, y con carácter previo, hay de recordar que, a día de hoy, el valor de la jurisprudencia en los distintos ordenamientos, así como la distinción tradicional entre los sistemas de precedentes y los fundamentados en la ley escrita, no tiene ningún valor descriptivo.⁴⁴ Dicha situación, sumada a la expansión del *Legaltech* entendida como la tecnología que se incorpora a los operadores jurídicos⁴⁵ y en el entorno judicial, nos lleva a que la jurimetría, entendida como el análisis estadístico de la jurisprudencia, se confunda con la “*justicia predictiva*.”⁴⁶

⁴¹ Jean-Pierre Buyle y Adrien Van Den Branden, “La robotisation de la justice”, in *L'intelligence artificielle et le droit*, ed. Hervé Jacquemin y Alexandre de Streel (Bruselas: Larcier, 2017), 270.

⁴² Dicho de otra manera, una cosa es la administración judicial, y otra muy distinta la administración de justicia, por cuanto que la primera es la actividad administrativa que sirve y se organiza para permitir que se pueda desarrollar la segunda, que es la actividad puramente jurisdiccional.

⁴³ Un concepto que no incorpora la Real Academia de la Lengua (RAE), pero al que se refieren las grandes plataformas jurídicas como La ley que la define como “*la herramienta de analítica jurisprudencial más innovadora del mercado que permite definir la estrategia procesal más idónea para el éxito del caso, a través de indicadores gráficos interactivos, basados en el análisis cognitivo de millones de decisiones judiciales.*” C.f. <https://jurimetria.laleynext.es/content/Inicio.aspx>.

⁴⁴ Como señala Taruffo “*en los sistemas de civil law se hace verdaderamente un amplio uso de la jurisprudencia, mientras que en los sistemas de common law se hace un amplio uso de la ley escrita, y áreas enteras de estos ordenamientos -desde el derecho comercial al derecho procesal- son en realidad ‘codificadas’.*” Cf. Michele Taruffo, “Precedente y jurisprudencia”, *Precedente Revista Jurídica* (2007): 86, DOI: <https://doi.org/10.18046/prec.v0.1434>. <https://www.icesi.edu.co/revistas/index.php/precedente/article/view/1434/1831>.

⁴⁵ Más en concreto, *legaltech*, no se centra en las tecnologías en sí mismas, sino en cómo dichas tecnologías se incorporan en la prestación de los servicios. No se trata de *blockchain*, inteligencia artificial, o automatización robótica de procesos (RPAs), sino de analizar cómo se aplican esas tecnologías para aumentar la productividad de los profesionales y para sistematizar y *productivizar* lo servicios legales. En definitiva, se refiere al conjunto de tecnologías y soluciones digitales que se utilizan para transformar y mejorar la prestación de servicios legales y la gestión de asuntos jurídicos.

⁴⁶ La jurimetría no tiene que tener como objetivo hacer predicciones de sentencias futuras, es más en sus inicios tenía un fin distinto y mucho más teórico, pues lo que se pretendía es articular un sistema para realizar análisis. Cf. David Robertson, “Judicial ideology in the House of Lords: A jurimetric analysis”, *British Journal of Political Science*, v. 12, no. 1 (1982): 1. La jurimetría como modelo de análisis estadístico, puede ser de utilidad para la previsión de sentencias judiciales futuras, pero esto no significa que se trate de “*justicia predictiva*” pues son conceptos autónomos e independientes. En relación a su carácter de conceptos autónomos e independientes. Cf. Morris H. DeGroot, *Optimal statistical decisions* (Wiley: Interscience, 2005). Por último, hemos de distinguir entre previsión y predicción, pues, siguiendo

Por lo tanto, y a la vista de lo expuesto podríamos definir la justicia predictiva como la herramienta en la que el algoritmo, tras valorar distintos factores facilita información a un juez de un riesgo que se puede dar en un futuro, como que un individuo se sustraiga a la acción de la justicia, sea un riesgo para la sociedad, o cometa hechos delictivos.

Y, en el marco de la justicia predictiva, hemos de distinguir la justicia predictiva de riesgos,⁴⁷ del análisis predictivo del impacto de normas,⁴⁸ de la anticipación del contenido de sentencias por programas generado por IA,⁴⁹ y por último de aquellas actuaciones de policía predictiva que no se someten a la valoración del juez.⁵⁰

Y es que no podemos incluir dentro del concepto de “*justicia predictiva*”, aquellos informes, que, aunque basados en sistemas de automatización y mecanismos de predicción de riesgos, no son judiciales hasta que un órgano jurisdiccional los acepta. Tampoco, han de ser entendidos como mecanismos de apoyo a la decisión de los jueces y magistrados, si son empleados por peritos y expertos del entorno judicial pero no por el juez. Tampoco, se pueden incluir en el ámbito de la “*justicia predictiva*”, las actuaciones policiales que se dan en el ámbito policial, aunque ofrezcan usos de sus resultados en el ámbito de la instrucción penal. Y así mismo, tampoco cabría incorporar a la justicia predictiva, técnicas o herramientas, que aun aplicándose al entorno judicial tiene en cuenta factores no jurídicos como los sociales o los factores del entorno.

Como vemos se hace necesario un mecanismo, una transición, una incorporación de estos informes, herramientas o resultados al ámbito jurisdiccional, pues el juzgador los ha de hacer suyos en el desarrollo de su actividad jurisdiccional, y en este “*viaje de transformación*”, dichos informes, herramientas o resultados, han de salvar todas las exigencias que el sistema de derechos y garantías procesales de nuestro proceso penal dispone.⁵¹ De tal manera que, si no pasa dicha criba, queda fuera del ámbito judicial, se trata en definitiva de una “*transfiguración para la legitimación*.”

3.2. Algunas herramientas de predicción de riesgos

Entre los sistemas de predicción de riesgos, mal llamados “*sistemas de justicia predictiva*”, hemos de mencionar en España el sistema *VioGen*, y el sistema *RisCanvi*. El primero de ellos (sistema *VioGen*) consiste en un algoritmo desarrollado para

a Battelli, la justicia predictiva, no se trata, de la adquisición preventiva del resultado (de una justicia anticipada), sino de la expectativa razonable de alcanzarlo, es decir, del resultado razonable de un proceso. Cf. Ettore Battelli, “La decisión robótica: Algoritmos, interpretación y justicia predictiva”, *Revista de Derecho Privado*, no. 38 (2020): 74-75. Este autor define la justicia predictiva como la posibilidad de utilizar los métodos de la ciencia exacta en el ámbito jurídico para predecir eventos futuros.

⁴⁷ Como dice Humeric, la justicia predictiva de riesgos utiliza “*probabilidades estadísticas basadas en factores como la edad, el historial laboral y los antecedentes penales*”, para predecir la probabilidad de reincidencia de un acusado. Cf. Jacob Humeric, “Reprogramming fairness: Affirmative action in algorithmic criminal sentencing”, *Columbia Human Right Law Review* (2020): 219.

⁴⁸ Que supone valorar como se va a interpretar una norma. Cf. Eugene Volokh, “Chief justice robots”, *Duke Law Journal*, no. 68 (2019): 1182.

⁴⁹ Sobre esta cuestión ver entre otros a Juan Gustavo Corvalán, “La primera inteligencia artificial predictiva al servicio de la justicia: Prometea”, *La Ley. Revista Jurídica Argentina*, (2017), online, y a Nuria Belloso Martín, “Inteligencia artificial en la resolución de asuntos judiciales. Reflexiones desde el paradigma de la justicia predictiva”, *Cuadernos Digitales de Formación, CGPJ*, no. 3 (2021): 4-5.

⁵⁰ Se trataría de programas predictivos que diseñan mapas de calor que delimitan zonas y espacios geográficos, en los que tienen lugar más delitos o un tipo de delito concreto y que por la tanto exigen que se envíen más efectivos policiales.

⁵¹ Comenzando por el principio de legalidad y continuando con el respecto de la independencia judicial, el derecho de defensa, el derecho al recurso, a la transparencia, etcétera.

evaluar los riesgos de las mujeres víctimas de violencia de género.⁵² Esta plataforma reúne toda la información de un caso o de una víctima, lo que incluye declaraciones de víctimas y de testigos, de registros oficiales, de antecedentes policiales y registros accesibles para la policía, y así mismo incorpora los propios hechos objeto de la investigación, y todo ello con el objetivo final de determinar o valorar el nivel de riesgo de sufrir nuevas agresiones, o de determinar la gravedad o la frecuencia de las mismas. El algoritmo trabaja con los datos que se le incorporan, puntuando cada uno de los riesgos, y concreta una valoración en una escala de cinco niveles “No Apreciado”, “Bajo”, “Medio”, “Alto” y “Extremo”, que se comunica al Juzgado de Violencia sobre la Mujer y a la Fiscalía.⁵³

Los resultados de este algoritmo se incorporan al debate jurídico, por ejemplo, a la hora de confirmar o revocar medidas de alejamiento o dispositivos de control,⁵⁴ lo que no quita que sea objeto de severas críticas, por ser un sistema automatizado con mínima intervención humana, o por su insuficiencia para comprender correctamente la situación de la mujer víctima de violencia.⁵⁵

Otra herramienta de predicción de riesgos es el sistema *RisCanvi*,⁵⁶ que se aplica a personas adultas sólo en Cataluña, y que predice un riesgo asociado a la peligrosidad

⁵² El AAP de Madrid, secc. 27.^a, 145/2024 de 25 de enero señala que es un sistema de seguimiento integral en los casos de violencia de género. La base normativa de *VioGen* es el artículo 282 LECrim, a través del “Protocolo para la valoración de riesgos de violencia de género” (LO 1/2004 de 28 de diciembre), y “de gestión de la seguridad de las víctimas”, aprobado mediante la Instrucción n.º 7/2016 de la Secretaría de Seguridad.

⁵³ Se parte de un primer cuestionario denominado VPR (Valoración Policial del Riesgo) y tiene la función de cuantificar el grado de probabilidad de que la persona pueda seguir siendo objeto de acoso. El formulario incluye 39 indicadores de riesgo de reincidencia, agrupados en cuatro áreas temáticas (relacionadas con la gravedad del incidente denunciado, los datos del presunto agresor, las características de la víctima y la percepción de la situación por parte del agresor), y permite clasificar el peligro como inexistente, bajo, medio, alto o extremo. Esta clasificación va seguida de la adopción de medidas de protección que, en los supuestos más graves, pueden suponer la elaboración de un plan de seguridad personalizado, sugerido por el propio *VioGén*. Y existe un segundo formulario, VPER (Valoración Policial de Evolución del Riesgo) que se realiza de forma general un año después del primero, una vez celebrado el juicio e independientemente de la sentencia que se dicte. Este segundo formulario consta de 34 indicadores de riesgo de reincidencia y 9 factores de protección. Y lo que persigue es reevaluar la peligrosidad estimada inicialmente, y, por lo tanto, permite ajustar las medidas adoptadas, reforzándolas o flexibilizándolas. Cf. Jordi Gimeno Beviá, “Instrumentos actuales de Policía y justicia predictiva en el proceso penal español: Análisis crítico y reflexiones de *lege ferenda* ante aplicaciones futuras”, *Estudios penales y criminológicos*, no. 44 (2023): 2-3.

⁵⁴ E incluso se ha valorado como un elemento indiciario para acreditar un delito de abuso sexual, cf. la SAP de Salamanca, secc. 1.^a, n.º 200/2023 de 29 de noviembre, que une al reconocimiento de los hechos por el acusado, el informe de *VioGen*.

⁵⁵ En este sentido la Fundación Éticas, en un informe de auditoría externa al Sistema *VioGen*, señaló que en la práctica “es un sistema automatizado con una supervisión humana mínima e inconsciente...”, Informe Fundación Éticas, 2022, 35-36. Accesible en <https://eticasfoundation.org/es/la-fundacion-eticas-realiza-una-auditoria-externa-e-independiente-del-sistema-viogen/>. Así mismo, la Sentencia de la Audiencia Nacional de 30 de septiembre de 2020, cuestionó la efectividad de *VioGén*. Esta resolución judicial condenó al Ministerio del Interior español por falta de protección a una víctima de violencia de género con resultado de muerte, pues la herramienta *VioGén* estimó el riesgo de la víctima como bajo y el Juzgado correspondiente denegó la orden de protección, y todo ello parece derivarse, atendiendo a la resolución judicial, de la insuficiencia de la respuesta del sistema de *VioGén* para una correcta comprensión de la situación de la mujer víctima de violencia.

⁵⁶ Sobre *RisCanvi*, cf. Lorena Alemán Aróstegui, “El uso de RISCANVI en la toma de decisiones penitenciarias”, *Estudios penales y criminológicos XXXI*, no. 44 (2023), on-line; Antonio Madrid Pérez, “El uso de sistemas predictivos automatizables en la actividad decisional de las autoridades públicas: aportaciones para un análisis iusfilosófico sobre la digitalización del proceso decisonal”, *Anuario de Filosofía del Derecho*, no. 40 (2024): 226; María Arranz et al., “Factores de riesgo de quebrantamiento de medidas privativas de libertad en jóvenes infractores”, *Revista Española de Investigación Criminológica*, no. 21 (2023), on-line.

del individuo una vez que es condenado.⁵⁷ Lo importante aquí, no es solo la función predictiva de la herramienta, sino que la misma se inserta en el proceso que lleva a la toma de una decisión jurídicamente vinculante, puesto que la herramienta se dirige a prever cuatro posibilidades: el quebrantamiento de condena, la violencia dentro de la prisión, la reincidencia violenta y la violencia autodirigida (suicidio, intento de suicidio, autolesiones), y puede influir en las decisiones que determinan la clasificación inicial del interno, la progresión de grado, la concesión de permisos y la libertad condicional.

Pero esta herramienta tampoco está exenta de crítica, pues por un lado es limitada y no alcanza a valorar la compleja conducta humana, no es incuestionable,⁵⁸ da lugar a falsos negativos, y sus resultados son inferiores al 50 %, ⁵⁹ y por otro lado no es una herramienta neutra, puesto que emplea factores como la nacionalidad o la etnia de pertenencia del sujeto, que sirven como predictores del riesgo y esto puede tener efectos discriminatorios.

Ya, fuera de nuestro país, es inevitable citar el caso de EEUU en donde los sistemas de predicción de riesgos, son muy utilizados, en especial antes del juicio como alternativa a la prisión provisional, o como guía para la supervisión penitenciaria y también, de forma excepcional, para el incremento de la pena.⁶⁰ El programa más conocido es COMPAS (*Correctional Offender Management Profiling for Alternative Sanction*),⁶¹ que se trata de una herramienta algorítmica de carácter privado de evaluación de riesgos que se presenta en forma de gráfico de barras, con un abanico de puntuaciones del uno al diez que determina el riesgo de reincidencia antes del juicio, el riesgo de reincidencia general y el riesgo de reincidencia violenta.⁶²

Recordemos que la herramienta COMPAS pertenece a una entidad privada, y que su falta de transparencia ya fue objeto de debate, resolviéndose, por el Tribunal Supremo de Wisconsin en *State v. Loomis* del año 2016, la validez del sistema de COMPAS,⁶³ permitiendo que los Tribunales sentenciadores puedan utilizar el sistema COMPAS para la determinación de la pena, pero impidiendo que puedan utilizar las puntuaciones de riesgo de las mismas para determinar si un delincuente debe ser encarcelado.

⁵⁷ Este sistema no aplica IA en sentido estricto, y funciona en base a dos protocolos. El primero, el *RisCarvi screening*, se aplica a la entrada del penado al centro penitenciario, consta de 10 ítems distintos y puede concretar un riesgo bajo o alto de violencia. El segundo protocolo, el *RisCarvi complet*, dispone de 43 variables que concreta una puntuación de riesgo bajo, medio o alto. Estos protocolos tienen un carácter meramente orientador, como señala el AAP de Barcelona, secc. 21.ª n.º 938/2019 de 30 de mayo.

⁵⁸ Y así lo constata la AAP Girona secc. 3.ª, 17/2024 de 10 de enero.

⁵⁹ Lucía Martínez Garay, “Errores conceptuales en la estimación del riesgo de reincidencia”, *Revista Española de Investigación Criminológica*, no. 14 (2016): 9.

⁶⁰ Cf., entre otros, a Michael Brenner *et al.*, “Constitutional Dimensions of Predictive Algorithms in Criminal Justice”, *Harvard Civil Rights-Civil Liberties Law Review*, no. 55 (2020), 270; Vincent M. Southerland, “The intersection of race and algorithmic tools, in the criminal legal system”, *Maryland Law Review*, no. 80 (2021), 497.

⁶¹ El *Compas* se utiliza en Florida, Wisconsin, Indiana, Michigan, en la mayoría de los condados de Nueva York, en los de mayor población de Nuevo México, California usa el *Static Risk Assessment Instrument* (CSRAI), Connecticut el *Salient Factor Score* (SFS), Montana el *Montana Offender and Reentry Risk Assessment Tool* (MORRA) y Texas el *Risk Assessment System* (TRAS).

⁶² Las puntuaciones del COMPAS se fundamentan en los antecedentes penales y en una entrevista que se hace al individuo. Se utilizan 137 parámetros. El sujeto responde a un cuestionario (que incluye preguntas como cuantos de sus amigos han sido arrestados alguna vez; cuantas veces ha cambiado de residencia en el último año, con qué frecuencia está sin dinero o se siente desmotivado, etcétera). Este cuestionario se envía a la empresa propietaria del programa, que devuelve una puntuación de riesgo y una puntuación de necesidades.

⁶³ *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).

Esta resolución judicial fue objeto de duras críticas puesto que no sólo el acusado y el abogado no podían conocer las razones y fundamentos del COMPAS para emitir su evaluación de riesgos, sino que tampoco el propio juez podía conocer si el algoritmo de propiedad privada utilizaba variables legalmente aceptadas, y carentes de sesgos para responder al propósito legítimo que se le supone.⁶⁴ Y, por otro lado, como acreditó la organización de periodismo de investigación sin ánimo de lucro *ProPublica*,⁶⁵ el algoritmo de COMPAS tenía un sesgo racial contra los acusados negros, pues tras el análisis de más de 10.000 datos de presos, se comprobó que, dichos acusados negros, tenían casi el doble de probabilidades de ser clasificados por el algoritmo como de alto riesgo en comparación con los acusados blancos en sus mismas condiciones.

Como se puede comprobar estas herramientas de predicción de riesgos presentan graves deficiencias, en especial cuando sus resultados se encuentren entre los factores que conforman decisiones judiciales que se proyectan sobre situación personales de sospechosos, acusados o penados, como podrían ser por ejemplo a la hora de adoptar medidas cautelares de protección de la víctima.⁶⁶ Pues una cosa es contar con un elemento más a la hora de valorar y evaluar riesgos relativos a la presencia del sospechoso o acusado en el juicio, o a la posibilidad de su reincidencia; y otra muy distinta adoptar decisiones que pueden afectar y lesionar derechos básicos del justiciable como su presunción de inocencia, o su derecho de defensa.⁶⁷

3.3. Otros sistemas inteligentes: el sistema de “frontera inteligente” Entry/Exit (EES)

Otros sistemas inteligentes a tener en cuenta en la lucha contra el Crimen organizado, y al margen de lo que podríamos llamar propiamente actividad jurisdiccional, salvo cuando sus informes y resultados se incorporen a la actividad investigadora del juez de instrucción, con ocasión, por ejemplo, de la investigación de delitos de terrorismo, son por ejemplo los diseñados para el control de fronteras.⁶⁸

En este ámbito un último sistema que merece ser analizado es el sistema inteligente de la compañía THALES⁶⁹ que se está implantando en la frontera de

⁶⁴ Cf. Andrea Nishi, “Privatizing sentencing: a delegation framework for recidivism risk assessment”, *Columbia Law Review*, no. 6 (2019): 1704; Carolyn McKay, “Predicting risk in criminal procedure: actuarial tools algorithms AI and judicial decision-making”, *Legal Research Studies Paper Series*, no. 67 (2019), on-line; Willem Gravett, «Jailed by a “black box.” The impact of opaque algorithms on the right to a fair trial in the United States of America», *University of Pretoria* (2021): 305-312; Caoimhe Anderson, “The impact of algorithms in criminal sentencing on due process rights”, (PhD diss., Queen’s University, 2019), 103-105.

⁶⁵ <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (<https://perma.cc/GY-DJRX>).

⁶⁶ Lo que sin duda genera graves problemas. Sobre esta cuestión, cf. Fernando Gascón Inchausti, “Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial”, in *La justicia digital en España y la Unión Europea: situación actual y perspectivas de futuro*, ed. Jesús Conde Fuentes *et al.* (Atelier, 2019).

⁶⁷ En este sentido, y como ya advertía De Hoyos Sancho, aunque las herramientas de justicia predictiva pueden ser de ayuda y apoyo a la decisión de judicial, por cuanto disponen de muchísimos más datos que el propio juzgador, han de contar con la debida transparencia, evitando actuaciones discriminatorias. Cf. Montserrat de Hoyos Sancho, “El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea”, *Revista General de Derecho Procesal*, no. 55 (2021).

⁶⁸ Sobre esta cuestión ya me ocupé en otro trabajo titulado “La Inteligencia Artificial en el control de los flujos migratorios en la Unión Europea. La necesidad de un marco normativo garantista de los derechos fundamentales”, publicado en la *Revista General de Derecho Europeo (RGDE)* no. 60 (2023): 1-39.

⁶⁹ La Compañía Thales desarrolla tecnologías biométricas y sistemas de control de fronteras desde

El Tarajal y en otros países europeos. Se trata del sistema de “*frontera inteligente*” denominado “*Entry/Exit*” (EES) para agilizar las entradas y salidas de personas y vehículos. Se trata de un sistema de información unificado que gestiona los datos de entrada y salida de los nacionales de terceros países que viajan a la zona Schengen para estancias cortas (no más de 90 días en cualquier período de 180 días),⁷⁰ y, que está basado en sistemas biométricos⁷¹ (reconocimiento facial, huellas dactilares, o el iris), que a buen seguro traerá problemas tanto por la cantidad como por las características de los datos personales recolectados y almacenados, así como por el uso que se haga de ellos.⁷²

En este sentido va a ser de interés, en relación al uso de estos sistemas biométricos,⁷³ por un lado, como se va a desarrollar la arquitectura centralizada gestionada por la agencia eu-LISA (que es la encargada del desarrollo y la implementación del sistema central y de las interfaces nacionales en cada estado miembro); y, por otro lado, como cada país miembro de la UE implementa su propia Interfaz Nacional Uniforme (NUI) para conectar sus sistemas nacionales con el sistema inteligente “*Entry/Exit*” (EES) central.

Consciente de la cantidad de datos personales recolectados y almacenados, así como de la importancia de los mismos, el sistema incluye en su diseño medidas avanzadas de seguridad cibernética o ciberseguridad para asegurar la privacidad y seguridad de los mismos. Y es que no podemos olvidar que el estudio de los rasgos físicos o de conducta que permiten identificar de forma exclusiva y excluyente a una determinada persona puede conllevar restricciones de sus derechos fundamentales, lo que se puede agravar, si incorporamos el uso de la IA al tratamiento de estos datos biométricos, lo que puede dar lugar a algún sesgo o error.⁷⁴

hace más de 30 años. El desarrollo específico del sistema EES comienza en 2013, cuando la Comisión Europea introduce el concepto de Fronteras Inteligentes. Consultar <https://eur-lex.europa.eu/ES/legal-content/glossary/border-checks.html>.

⁷⁰ Este sistema reemplaza el método manual de estampado de pasaportes con un registro electrónico centralizado que incluye información biométrica como huellas dactilares y fotografías faciales. El Sistema EES automatiza los controles en las fronteras exteriores, y pretende la mejora de la seguridad y eficiencia de los controles migratorios, facilitando con ello la lucha contra la migración irregular y el terrorismo. El sistema en cuestión se está implantando en todos los países que forman parte del espacio Schengen, que incluye 26 Estados miembros.

⁷¹ Las tecnologías utilizadas en el sistema están basadas en sistemas biométricos, que utilizan el reconocimiento facial y toma de huellas dactilares (mediante escáneres biométricos y cámaras de alta resolución) para verificar la identidad de los viajeros. Cada uno de los atributos o características físicas (reconocimiento facial, huella dactilar o el iris) que identifica o autentifica a la persona en cuestión, se utiliza para servicios específicos. La biometría ofrece confianza, transparencia y agiliza los procesos de verificación.

⁷² Recordemos que en España ya funciona el sistema de reconocimiento facial ABIS (*Automated Biometric Identification Systems*) cuyo objeto exclusivo es la identificación de culpables y sospechosos de delitos. El sistema permite identificar en segundos, a una persona que aparezca en una grabación de cámara, ya sea pública y privada, facilitando su identidad, si está en las bases de datos de la Policía y la Guardia Civil. El ministerio del Interior mantiene que el sistema ABIS opera en el marco del fichero número 15 SAID (Sistema Automático de Identificación Dactilar) autorizado por la Agencia Española de Protección de Datos, cumpliendo con la Ley Orgánica de Protección de datos personas para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales.

⁷³ Sobre esta cuestión, cf. Mercedes Llorente Sánchez-Arjona, “Datos biométricos y su aplicación al proceso penal”, in *Next Generation Justice: Digitalización e Inteligencia Artificial*, ed. Sonia Calaza López y Ixusko Odeñana Gezuraga (Madrid: La ley, 2024), 1307-1385.

⁷⁴ Cf. José Francisco Etxeberria Guridi, “Sistemas biométricos (el reconocimiento facial en particular) y sus aplicaciones”, in *Inteligencia artificial legal y administración de justicia*, ed. Sonia Calaza López, Mercedes Llorente Sánchez-Arjona (Aranzadi, 2022), 152.

Los objetivos del sistema son: a) la automatización de los controles de entrada y salida, reemplazando los sellos manuales en los pasaportes por registros electrónicos; b) la creación de una base de datos centralizada que registra todos los movimientos transfronterizos de los visitantes, permitiendo un seguimiento preciso y eficiente; c) el refuerzo de la seguridad nacional y la lucha contra el terrorismo y el crimen grave, facilitando la identificación de individuos que exceden su estancia permitida; d) y el aumento de la eficiencia de los controles fronterizos, reduciendo tiempos de espera y mejorando la experiencia del viajero, al tiempo que mantiene altos estándares de seguridad.

Por otro lado, este sistema, como todos aquellos de sus características, adopta tecnologías avanzadas que facilitan controles más rápidos y precisos, ayuda a prevenir y detectar el fraude de identidad y otros delitos, facilita la detección temprana de actividades ilegales y la vigilancia de individuos con antecedentes criminales, y permite a los funcionarios (a los agentes de frontera) centrarse más en casos de sospechosos, optimizando el uso de recursos y mejorando la gestión de fronteras. A todo ello habría que añadir que el sistema está diseñado para ser flexible y escalable, permitiendo la incorporación de nuevas tecnologías en el futuro, lo que significa que puede incorporar mejoras en los sistemas de biometría (avances en tecnologías de reconocimiento facial y huellas dactilares, como algoritmos más precisos y rápidos); puede incorporar e integrar soluciones de automatización avanzada y sistemas de control más inteligentes (como robots y kioscos de auto-registro); desarrollar nuevas medidas de ciberseguridad para proteger la integridad y la privacidad de los datos, y por último integrar tecnologías emergentes como IA, *big data* y análisis predictivo para mejorar la eficiencia y la efectividad del sistema.

Pero estas supuestas ventajas o avances pueden suponer a la vez involución, pues, en muchas ocasiones, dan lugar a violaciones de derechos fundamentales⁷⁵ y actuaciones discriminatorias. La falta de transparencia y la presencia de sesgos en los algoritmos y sistemas de IA justifican una preocupación generalizada en todos los ámbitos, y en especial en el judicial. Pues no sólo pueden codificar las discriminaciones humanas, sino que además pueden amplificarlas y esto podría conducir a la institucionalización y sistematización de las mismas y, a la larga, a la exclusión de personas sobre la base de características protegidas, como la raza y la etnia.

Por otro lado, el uso generalizado y sistemático de dispositivos basados en la IA exige preparar un marco normativo adecuado, en el que su uso alcance un equilibrio entre la eficiencia perseguida y la eficacia en la protección de los derechos y garantías de los ciudadanos. El camino para lograr este objetivo es la convivencia, integración e inter-relación, por un lado, de normas específicas que regulan usos y espacios concretos de estas tecnologías, y por otro lado, de normativas orgánicas y generales (Reglamentos en el caso de la UE), que diseñen un marco de estándares, principios, requisitos y garantías de obligado cumplimiento para todas las administraciones, autoridades competentes e instituciones privadas que opten por esta tecnología basada en la IA.

Las tecnologías, y entre ellas también las que se basan en sistemas de IA, han de ser un instrumento al servicio de la sociedad, y no un fin en sí mismas, por lo que deben ayudar a dar respuesta a los problemas del ser humano, pero no sustituirlo.

⁷⁵ Como por ejemplo la protección de datos de carácter personal, la privacidad, el honor, la intimidad y la propia imagen. Sobre esta cuestión, cf. Francisco Pérez de los Cobos Orihuel, *El Derecho al respeto de la vida privada: los retos digitales, una perspectiva de derecho comparado* (Consejo de Europa, 2018).

Por último, hemos de ser conscientes que la denominada tecnología “*inteligente*” puede ser utilizada para intereses políticos y económicos particulares, sin que existan sobre este uso sistemas de control y de respeto a unos mínimos estándares de protección de los derechos humanos reconocidos en las normas internacionales sobre la materia, esto, no es solo una posibilidad, sino que se trata de una realidad que hay que prevenir y revertir. Los sistemas de IA con sesgos que proyectan sobre decisiones automatizadas en los distintos ámbitos afectan a los derechos fundamentales de los ciudadanos, y también de los migrantes, y es contrario al avance tecnológico guiado por la ética y la defensa de los derechos humanos, en el sentido que concretó la Carta ética europea sobre el uso de la inteligencia artificial en 2018 en Estrasburgo,⁷⁶ que es el primer texto en el que se enuncian los “*principios sustanciales y metodológicos*”,⁷⁷ que están llamados a convertirse en el centro de la ciber-justicia europea.

⁷⁶ Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno adoptado por el CEPEJ (Comisión Europea para la Eficiencia de la Justicia), durante su 31.ª Reunión Plenaria en Estrasburgo, 3-4 de diciembre de 2018. CEPEJJ (2018), 14. Accesible en <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> (último acceso 30.10.2022). En línea con la Carta ética europea, en diciembre de 2020, el CAHAI, el Comité ad hoc sobre la IA del Consejo de Europa, adoptó por unanimidad el estudio de viabilidad de un marco normativo sobre el diseño, el desarrollo y la aplicación de la IA, con un enfoque basado en los derechos humanos, centrando la atención en los riesgos para la democracia y el Estado de Derecho.

⁷⁷ Clementina Barbaro, “Uso dell’intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?”, *Quistione Giustizia*, no. 4 (2018): 189. Accesible en www.questionegiustizia.it y Serena Quattrococo, “Intelligenza artificiale e giustizia: nella cornice della carta etica europea, gli spunti per un’urgente discussione tra scienze penali e informatiche”, *La Legislazione Penale*, 18 diciembre, 2018, www.la legislazione penale.eu.

La estrategia europea de lucha contra la corrupción: entre cooperación judicial y digitalización

Valentina Faggiani*

1. Multidimensionalidad y carácter transnacional de la corrupción

La corrupción es un fenómeno delictivo tan antiguo como el ser humano, siendo inherente a su naturaleza. Con eso, no se pretende justificar estos comportamientos, normalizándolos; todo lo contrario, se quiere más bien entender cómo funcionan para intentar limitarlos – pues erradicarlos es imposible – y elaborar una respuesta eficaz. Por todo ello, el objetivo de esta contribución es elaborar un cuadro de la estrategia de lucha de la Unión Europea (UE), la cual se basa en el refuerzo y la digitalización de la cooperación judicial en materia penal y de la cooperación policial, y en la adopción por parte de las autoridades nacionales de *law enforcement* y de la administración pública de sistemas para luchar contra este crimen y sus principales manifestaciones.

El trabajo se estructurará en tres partes: en la primera parte, de carácter más bien introductorio, se analizarán las características y dimensiones, que la corrupción ha asumido en la sociedad actual y su impacto en nuestros sistemas, haciendo hincapié en su afectación al Estado de derecho, a la economía y a la seguridad. Esto es muy importante para luchar contra esta forma de criminalidad organizada.

La segunda parte tendrá por objeto las medidas en materia de cooperación judicial para favorecer la elaboración de una respuesta común a través tanto de la armonización normativa [artículo 83 del Tratado de Funcionamiento de la Unión Europea (TFUE)] así como, en general, de la actuación de las autoridades involucradas en este ámbito. Y, por último, la tercera parte se centrará en la digitalización de la respuesta a este crimen en la UE y en algunos de los Estados miembros, a fin de conocer el estado de la cuestión, para deducir los avances, pero también los límites persistentes y lo que se podría hacer para mejorar.

En la doctrina se han formulado muchas definiciones de corrupción. Parece acertado concebirla como una desviación de la gestión del poder delegado por la sociedad en las autoridades públicas¹ para conseguir intereses particulares de carácter

* Profesora de Derecho Constitucional en la Facultad de Derecho de la Universidad de Granada. Este trabajo se enmarca en los siguientes proyectos: Módulo Jean Monnet, “*Challenges to justice in the EU: perspectives for reform*”, 2022-2025, ref. 101085462; Módulo Jean Monnet: “Desafíos y perfiles estratégicos de la UE en la lucha contra el crimen organizado” (RUECO) 2023-2026, ref. 101127315; y Proyecto de investigación I+D+ i “Proceso Penal y Espacio de Libertad, Seguridad y Justicia: Garantías, Cooperación Transfronteriza y Digitalización”, PID2023-152074NB-I00.

¹ Cf. V. Musacchio, “Corruzione politica e criminalità organizzata: le connivenze pericolose”, *Rivista giuridica del Mezzogiorno*, a. XXVII (2013): 1-2, 187-193. Según Musacchio, “La corruzione politica attualmente rappresenta lo strumento più efficace e potente che i criminali possono utilizzare, in quanto, permette di influenzare la burocrazia, le forze dell’ordine, la magistratura nonché, in alcuni casi, l’economia e le forze sociali” (p. 187).

económico en perjuicio de la *res pública*.² Esta extralimitación en el uso del poder deriva de un “contrato”³ entre un sujeto público y un actor privado, que produce una disfunción en la gestión del interés público, que se ve instrumentalizado para la persecución de finalidades personales.

Dicha noción podría ser a su vez integrada, reenviando a Vannucci, según quien la corrupción es el “*pacto de hierro entre corruptos y corruptores, que a ninguno de los participantes conviene denunciar*”,⁴ porque nos permite entender cómo este fenómeno delictivo se mueve y su peligrosidad. Se trata de un crimen muy insidioso porque en muchas ocasiones no se consigue percibirlo, pues no se manifiesta de forma evidente, quedándose escondido. Además, es un crimen sin víctimas, puesto que las partes no suelen denunciarlo, pues no les interesa. Tampoco, suelen denunciar las personas, que llegan a tener conocimiento de ese crimen, por miedo a las repercusiones.

Esta característica contribuye a rodearlo de un halo de impunidad. De hecho, el que no se denuncie es solo un reflejo de las demás dificultades, que la corrupción plantea. En general es muy difícil recabar pruebas y por lo tanto llevar a cabo las investigaciones, poner en marcha los juicios y que estos terminen con una sentencia de condena. Todo ello contribuye a desarrollar una sensación de impotencia en la ciudadanía, que acaba perjudicando de forma inevitable la confianza en las instituciones.

Además, en la sociedad actual globalizada, la corrupción no es solo un fenómeno universal muy complejo con un carácter sistémico,⁵ pues siempre ha habido corrupción en todos los países, ninguno ha estado exento; en las últimas décadas sus manifestaciones y el *modus operandi* han adquirido un plus de gravedad, por su carácter multidimensional y transnacional. De hecho, se puede fácilmente observar que esta lacra afecta a todos los niveles de gobierno y por lo tanto a la sociedad en su conjunto, pues ya no existe corrupción solo a nivel local, sino que también se han destapado casos muy graves en las instituciones europeas y también en las organizaciones internacionales. Además, este crimen suele interrelacionarse con las demás formas de criminalidad organizada (terrorismo, tráfico de seres humanos, cibercrimen), que se caracterizan por la presencia de elementos de extraterritorialidad.⁶ Todo ello proyecta la corrupción más allá del Estado, puesto que estos esquemas criminales suelen involucrar a más Estados juntos. Y, por último, no se puede soslayar la digitalización, que permite romper las barreras espacio-temporales, favoreciendo la comisión de crímenes a gran escala.

² J. M^a. Terradillos Basoco, “Corrupción política: Consideraciones político-criminales”, *Revista Electrónica de Estudios Penales y de la Seguridad: REEPS*, no. 1 (2017).

³ R. Cantone, E. Carloni, *Corruzione e anticorruzione: Dieci lezioni* (Milano: Feltrinelli, 2018).

⁴ A. Vannucci, “Un nuovo paradigma contro la corruzione”, *il Mulino*, Fasc. 3, maggio-giugno (2012): 422-430, sobre el punto cf. p. 425.

⁵ D. Della Porta, A. Vannucci, *La corruzione come sistema. Meccanismi, dinamiche, attori* (Bologna: Il Mulino, 2021), 240, según quienes: “È evidente la somiglianza tra il liquido gelatinoso in cui sono immersi gli attori coinvolti nel reticolo corruttivo e la cosiddetta area grigia – in questo specifico caso priva di una connotazione mafiosa – da intendersi come metafora utile a descrivere lo spazio opaco in cui «prendono forma relazioni di collusione e complicità», che coinvolgono «un’ampia varietà di attori, diversi per competenze, risorse, interessi e ruoli sociali», in un contesto nel quale «sono diventati molto più opachi e porosi i confini tra mercati legali ed illegali: non si tratta di una mera estensione dell’area dell’illecito nel lecito quanto di una commistione tra le due aree.”

⁶ L. Zúñiga Rodríguez, “Redes internacionales y criminalidad: a propósito del modelo de participación en organización criminal”, in *El derecho penal ante la globalización*, coord. L. Zúñiga Rodríguez, C. Méndez Rodríguez, M^a. Rosario Diego Díaz-Santos (Barcelona: Colex, 2002), 51-72.

2. El impacto de la corrupción en el Estado de derecho, la economía y la seguridad

La corrupción, como ha quedado dicho, es muy peligrosa, y lo es no solo por cómo se desenvuelve sino también por su afectación de forma simultánea a elementos esenciales para el mantenimiento de los sistemas democráticos y el bienestar de los ciudadanos: al Estado de derecho, tal y como lo entendemos *ex vi* artículo 2 Tratado de la Unión Europea (TUE), a la economía y a la seguridad.

Desde el primer punto de vista, la corrupción menoscaba la esencia del *Rule of Law* (ROL), penetrando en sus instituciones y también en las empresas privadas, capturándolas. Por ello, la doctrina política ha definido a la corrupción en los sistemas democráticos como “*microgolpes de Estado*”⁷ o “*criminalidad del poder*.”⁸ En cuanto a su incidencia en la economía, es suficiente confrontar los datos.⁹ Todo ello contribuye a dejar las democracias más vulnerables y favorece el desarrollo de espacios de impunidad y de formas de delincuencia grave, sin dejar a un lado las influencias desde fuera procedentes de terceros países no precisamente democráticos.

Si bien los resultados del Índice de Percepción de la Corrupción (IPC) muestran que más de la mitad de los 20 países mejor clasificados a escala internacional, es decir más virtuosos, son Estados miembros de la UE, según el último informe de transparencia internacional, la corrupción en la UE está empeorando, y es la primera vez que empeora en más de una década.¹⁰ Por otra parte, también se constata que existen fuertes diferencias entre los Estados, que han articulado políticas diferentes para responder a este fenómeno. Al respecto, se considera que los países menos corruptos del mundo son Dinamarca, Finlandia y Noruega, mientras que los peor clasificados son Hungría, Rumanía y Bulgaria, los países centro-orientales de la UE, los cuales siguen caracterizándose por importantes deficiencias. También los países de los Balcanes occidentales, los candidatos para el ingreso en la UE, se sitúan por debajo de la media, pudiéndose definir todavía como “*hot countries*.”¹¹

Ahora bien, la lucha contra la corrupción representa un elemento de salvaguarda del Estado de derecho. De hecho, ha inspirado el conjunto de medidas adoptadas

⁷ M. Alcaraz Ramos, “Corrupción política, derechos fundamentales y opinión pública”, in *¿Corrupción pública, prueba y delito: cuestiones de libertad e intimidad*, dir. A. Jareño Leal, A. Doval Pais (Cizur menor: Aranzadi, 2015), 20 s.

⁸ L. Ferrajoli, “Criminalidad y globalización”, *Boletín Mexicano de Derecho Comparado*, no. 115 (2006): 301-316, según quien “*La criminalidad que hoy en día atenta contra los derechos y los bienes fundamentales no es ya la vieja criminalidad de subsistencia, ejecutada por sujetos individuales, prevalentemente marginados. La criminalidad que amenaza más gravemente los derechos, la democracia, la paz y el futuro mismo de nuestro planeta es seguramente la criminalidad del poder: un fenómeno no marginal ni excepcional como la criminalidad tradicional, sino inserto en el funcionamiento normal de nuestras sociedades.*”, 303.

⁹ Transparency International Italia, “L’Unione europea aumenterà i suoi standard anticorruzione? Will the EU act decisively and raise its anti-corruption standards?”, <https://www.transparency.it/informati/blog/unione-europea-standard-direttiva-anticorruzione>; Rand, Press Room, News Releases, The Cost of Corruption in Europe – Up to €990 Billion (£781.64 Billion) Lost Annually, For Release, Tuesday, March 22, 2016. [The Cost of Corruption in Europe – Up to €990 Billion \(£781.64 Billion\) Lost Annually | RAND](https://www.rand.org/pubs/press_room/20160322/cost_of_corruption_in_europe.html). Al respecto, vid. también European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2024, Rule of Law Report, The rule of law situation in the European Union, Brussels, 24.7.2024, COM(2024) 800 final, 17 ss.

¹⁰ Transparency International, 2023 Corruption Perceptions Index: Weak checks & balances undermining anti-corruption efforts in Western Europe & EU, Region’s first CPI score drop in almost a decade, 30 January 2024, <https://www.transparency.org/en/press/2023-corruption-perceptions-index-weak-checks-balances-undermining-anti-corruption-efforts-in-western-europe-eu>.

¹¹ Transparency International, 2023 Corruption Perceptions Index: Weak checks & balances undermining anti-corruption efforts in Western Europe & EU.

por la UE para la defensa del ROL.¹² En efecto, lucha contra la corrupción e independencia judicial están estrictamente conectadas, siendo uno de los principales indicadores del “*estado de salud*” de nuestras democracias.¹³ Esto significa que la *conditio sine qua non* para que la estrategia en materia de lucha contra la corrupción pueda funcionar es la existencia de un marco institucional sólido y robusto, que permita llevar a cabo investigaciones y juicios efectivos e impulse una política clara, que contribuya a educar a la ciudadanía, siendo necesario contar con sistemas de justicia independientes, imparciales y eficientes, dotados de medios financieros suficientes y de recursos humanos adecuados.

Sin embargo, también es cierto que, si bien la existencia de un proceso de involución democrática o de transición constitucional sean terrenos fértiles, que facilitan el desarrollo de la criminalidad, la corrupción es un fenómeno mucho más complejo, endémico, que constituye parte integrante del sistema, puesto que tampoco los demás Estados ni las mismas instituciones de la UE están exentos. Por lo tanto, independientemente de la existencia de una situación de involución, la investigación y el procesamiento de los casos de corrupción son de por sí complicados también en los Estados “*democráticamente más fuertes*”, puesto que a menudo involucran a altos cargos o personas que revisten roles destacados en la sociedad.

Es suficiente pensar al respecto en el asunto del Qatargate. Este caso ha sido muy impactante por varias razones: en primer lugar, por su carácter simbólico, puesto que ha mostrado la existencia de una “*crisis del Estado de derecho de la UE y en la UE*”, al afectar a la institución de la Unión por definición más democrática, es decir el Parlamento Europeo, la casa de los pueblos de Europa. En segundo lugar, se trata de un caso de criminalidad “*capilar y reticulado*”,¹⁴ de extrema gravedad, pues no es un simple supuesto de corrupción y soborno de carácter local y “*bajo nivel*”, sino que se ha manejado mucho dinero, integrando un caso de “*corrupción de elite*.” Además, podría constituir la ocasión para destapar otros asuntos, que involucran también a otras instituciones de la UE con la colaboración de los grupos de interés (lobbies). Y, por último, ha mostrado cómo las injerencias de Terceros Estados pueden perjudicar la estructura democrática de la UE, interfiriendo en sus procesos decisorios, que se ven determinados desde fuera.

¹² Una confirmación en este sentido se puede encontrar en las medidas adoptadas por la UE para la defensa del ROL, pues todas se basan en el binomio lucha contra la corrupción/independencia judicial, como bases para el mantenimiento de los sistemas democráticos: desde el mecanismo de cooperación y verificación (MCV), instituido en 2006 para supervisar el cumplimiento de las reformas requeridas a Rumanía y Bulgaria para adaptarse a los estándares europeos, facilitando el proceso de integración (Decisión 2006/929/CE, DO L 354 de 14.12.2006), a la solicitud de aplicación del artículo 7, par. 1, TUE a Hungría y Polonia, que en este último caso se cerró en junio de 2024, tras el cambio de gobierno, a la adopción del Reglamento de condicionalidad horizontal, 2020/2092 para la protección del presupuesto de la UE (DO L 433I de 22.12.2020). Este último es muy interesante porque supedita el acceso a la financiación de la UE al respeto del Estado de derecho, siendo la existencia de sistemas de justicia corruptos, como ocurrió en el caso de Hungría, unos de los supuestos que legitimaría su aplicación. Además, este contexto de deterioro democrático, fomentado por la existencia de élites de poder corruptas, ha sido criticado duramente en los últimos años también por el TEDH y el TJUE. Ambos han mostrado el nexo entre la presencia de déficits sistémicos en los sistemas judiciales y administrativos de estos países y su mayor exposición a fenómenos de corrupción y en general de delincuencia organizada porque facilitan la creación de espacios de impunidad.

¹³ V. Faggiani, “La lucha contra la criminalidad organizada como cuestión de Estado de derecho”, in *Planificación, estrategias y medios en la lucha contra el crimen organizado y en la recuperación de activos*, dir. F.J. Garrido Carrillo, coord. V. Faggiani (Cizur Menor: Aranzadi, 2023), 27-52.

¹⁴ E. Vasques, “I possibili effetti devastanti del Qatargate sull’Ue”, www.rivistailmulino.it/a/i-possibili-effetti-devastanti-del-qatargate-sull-unione-europea, 19.12.2022.

Las distintas manifestaciones de la corrupción se suelen interrelacionar con otras formas de criminalidad, incluso organizada, agravando su impacto. De esta forma, los ordenamientos devienen más vulnerables. Por ello, la lucha contra este género de delitos se ha convertido en una prioridad para la *EU Security Union Strategy* (2020-2025),¹⁵ en coordinación con la *EU Strategy to tackle Organised Crime*,¹⁶ en la que se proponen medidas específicas, para combatir la corrupción como motor de la delincuencia organizada. La vinculación con las principales manifestaciones de esta forma de criminalidad grave, como el tráfico de droga (*EU Roadmap to step up the fight against drug trafficking*),¹⁷ la trata de personas o los delitos contra el medio ambiente, la dotan de un carácter transnacional, convirtiéndola en una amenaza para el mantenimiento de la seguridad y del orden público en la UE (EU SOCTA 2021)¹⁸ y, en definitiva, la supervivencia del Estado de derecho.

La conexión entre redes delictivas y corrupción ha sido puesta de relieve también por Europol en el último informe de 5 de abril de 2024 “*Decoding the EU’s most threatening criminal networks in the EU*”, según el cual alrededor del 71% de las redes criminales recurren a alguna forma de corrupción, y alrededor del 28% lo hace de forma proactiva y sistemática, tanto en el sector público como en el privado.¹⁹ Por todo ello, habida cuenta de la dimensión transnacional de este crimen, se considera necesario desarrollar una estrategia coherente, que cuente con un marco común. Esta estrategia, que requiere de una actuación tanto desde los Estados miembros como desde la UE, deberá basarse en dos pilares: el refuerzo de la cooperación judicial en materia penal y de la cooperación policial y la digitalización de estos ámbitos.

3. La necesidad de un marco normativo común

La adquirida dimensión transnacional de la corrupción impone instituir un marco común. Para ello, la cooperación judicial en materia penal y la cooperación policial pueden jugar un rol determinante. Dicha cooperación se desarrolla tanto en el plano normativo, a través de la armonización, como en el plano procesal y operativo, mediante la actividad de los jueces, de los fiscales y de las autoridades de policía de los Estados miembros, y de la colaboración con las agencias involucradas en estos ámbitos.

Lamentablemente, en la UE falta una estrategia coherente: las normas anticorrupción no son completas ni capaces de prevenir y contrarrestar de forma eficaz este crimen y no existe un marco común en lo que se refiere a los delitos de corrupción y cómo perseguirlos. En este sentido, es necesario ir más allá de la Convención de las Naciones Unidas contra la corrupción (UNCAC, 2003),²⁰ el único instrumento jurídicamente vinculante a nivel internacional del que es parte también la UE, que ofrece definiciones sobre las diferentes manifestaciones de la corrupción.

¹⁵ Comunicación, de 24 de julio de 2020, sobre la Estrategia de la UE para una Unión de la Seguridad [COM(2020) 605 final].

¹⁶ Comunicación, de 14 de abril de 2021, sobre la Estrategia de la UE contra la Delincuencia Organizada 2021-2025 [COM(2021) 170 final].

¹⁷ European Commission, Communication to the European Parliament and the Council on the EU roadmap to fight drug trafficking and organised crime, COM/2023/641 final.

¹⁸ Europol, SOCTA 2021, *Serious and organised crimes threat assessment. A corrupting influence: the infiltration and undermining of Europe’s economy and society by organised crime*.

¹⁹ Europol, *Decoding the EU’s most threatening criminal networks*, Publications Office of the European Union, Luxembourg, 2024.

²⁰ Convención de las Naciones Unidas contra la corrupción, hecha en Nueva York el 31 de octubre de 2003.

Por ello, precisamente a raíz del Qatargate, la UE, para intentar recuperar la confianza de los ciudadanos, ha elaborado un paquete de medidas, entre las que destaca la propuesta de Directiva sobre la corrupción, que está pendiente de ser adoptada.²¹ Aunque es muy difícil atacar estas redes criminales, la medida es sin duda oportuna, puesto que no existe una noción única de corrupción, que puede abarcar todas sus distintas manifestaciones (cohecho y soborno, la malversación y la apropiación indebida, el tráfico de influencias, la revelación de información privilegiada, el abuso en el ejercicio de funciones y el enriquecimiento ilícito).

Además, la corrupción es un tipo penal, que se interrelaciona de forma inevitable con las otras actividades propias de la delincuencia organizada, como la trata de seres humanos, el contrabando y el terrorismo, siendo parte integrante de su *modus operandi*. Esto conlleva la necesidad de indagar los nexos con otros tipos de delincuencia.

La propuesta de Directiva sobre la lucha contra la corrupción,²² cuyas bases jurídicas se encuentran en los artículos 325, 82 y 83 TFUE, representa un importante paso adelante en la lucha contra esta forma de criminalidad tanto en el sector público como privado, obligando a los Estados de la UE a tipificar como delitos los mismos actos de corrupción y a definirlos de la misma manera y a imponer sanciones proporcionadas, efectivas y disuasorias.

Además, la armonización normativa tendría efectos positivos en el desarrollo de una cultura común. En efecto, como es sabido, la percepción del desvalor de la corrupción en los distintos países de la UE y, especialmente, en los países terceros difiere mucho de un Estado al otro. La adopción de normas mínimas incentivaría la formación de los operadores jurídicos, de los funcionarios públicos, de los cuerpos y fuerzas de seguridad. Asimismo, dicha normativa contribuiría a mejorar la colaboración y cooperación de todos los actores llamados a la lucha contra la corrupción (OLAF, Europol, Eurojust, Fiscalía Europea).

Y, por último, no se puede soslayar la importancia de la aplicación conjunta de la Directiva sobre corrupción con el corpus normativo en materia de lucha contra la criminalidad transnacional grave y cooperación judicial, en el intento de crear un marco legal de respuesta. Piénsese, por ejemplo, en la importancia de la Directiva (UE) 2024/1640, de 31 de mayo de 2024,²³ relativa a los mecanismos que deben establecer los Estados miembros a efectos de la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y la nueva Directiva (UE) 2024/1260 sobre recuperación y decomiso de activos,²⁴ pues esta última “*equiparía a las autoridades con mejores herramientas para privar a los grupos*

²¹ *Vid.* también la Propuesta del Alto representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad al Consejo de Decisión del Consejo relativa a la adopción de medidas restrictivas contra los actos graves de corrupción [HR(2023)108] para evitar las interferencias extranjeras.

²² Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la corrupción, por la que se sustituyen la Decisión Marco 2003/568/JAI del Consejo y el Convenio relativo a la lucha contra los actos de corrupción en los que estén implicados funcionarios de las Comunidades Europeas o de los Estados miembros de la Unión Europea, y por la que se modifica la Directiva (UE) 2017/1371 del Parlamento Europeo y del Consejo. Propuesta de 3.05.2023 COM (2023) 234 final. Al respecto, cf. L. Salazar y F. Clementucci, “Per una nuova anti corruzione europea: EU-RBI et orbi”, *Sistema penale*, 7-8 (2023); M. Gambardella, “La “proposta di direttiva in materia di lotta alla corruzione” al vaglio del parlamento: qualche riflessione sui reati di abuso d’ufficio e traffico di influenze”, *Sistema penale*, 27.7.2023.

²³ DO L 2024/1640, 19.6.2024.

²⁴ DO L 2024/1260, 2.5.2024.

*de delincuencia organizada de los medios financieros necesarios para seguir delinquir y cometiendo actos de corrupción.”*²⁵

Y finalmente, en este marco, no se puede soslayar la importancia de la correcta aplicación de la Directiva (UE) 2019/1937,²⁶ que regula la posición de los denunciantes (*whistleblowers*), es decir de las personas que informen sobre infracciones del derecho de la UE, y del Reglamento (UE) 2024/1083,²⁷ por el que se establece un marco común para los servicios de medios de comunicación en el mercado interior (Reglamento Europeo sobre la Libertad de los Medios de Comunicación) para proteger a periodistas y medios de comunicación europeos de interferencias políticas o económicas y la Directiva (UE) 2024/1069, relativa a la protección de las personas que se implican en la participación pública frente a pretensiones manifiestamente infundadas o acciones judiciales abusivas (“*demandas estratégicas contra la participación pública*”, SLAPP) y su *chilling effect*, permitiéndoles defenderse.

La aplicación conjunta de todas estas medidas por las que se pretende crear un marco legal para “la nueva *governance*” de la corrupción podría representar un avance importante. En efecto, es necesario alcanzar la “*progresiva osmosis*”²⁸ entre la lucha contra la criminalidad organizada y la corrupción,²⁹ para estudiar a medio plazo la eficiencia y la efectividad de las medidas represivas y preventivas existentes.³⁰ Estos actos a su vez tienen que ser leídos juntos a todas las medidas adoptadas por la UE en el marco del sistema de cooperación judicial y de cooperación policial.

4. La digitalización de la cooperación judicial en materia penal y de la cooperación policial

A la digitalización del crimen es necesario responder a través de la digitalización de los instrumentos de *law enforcement*, de la cooperación judicial y, en general, de la justicia.³¹ Desde este punto de vista, es importante considerar que la tecnología y especialmente los mecanismos de Inteligencia artificial (IA) tienen un carácter bifronte, puesto que pueden constituir no solo un arma contra el crimen sino también un instrumento de la criminalidad.

En la UE se está desarrollando una estrategia en este sentido para luchar contra las formas de criminalidad grave transnacional (artículo 83 TFUE). El centro neurálgico de la gestión operativa de los sistemas informáticos de gran magnitud en el Espacio Europeo de Libertad, Seguridad y Justicia (EELSJ) – tanto en materia de inmigración y asilo como de cooperación judicial y policial – se encuentra en EU-LISA.³² Dicha Agencia es competente para llevar a cabo “*todas las funciones necesarias*

²⁵ *Ibidem*, exposición de motivos. F. J. Garrido Carrillo, “Cuestiones pendientes sobre el decomiso ocho años después. La Propuesta de Directiva del Parlamento Europeo y del Consejo sobre recuperación y decomiso de activos”, *Revista de Estudios Europeos*, Extra 1 (2023): 311-348 (Ejemplar dedicado a: Consolidación del Espacio Europeo de Libertad, Seguridad y Justicia en materia penal).

²⁶ DO L 305 de 26.11.2019.

²⁷ DO L 2024/1083 de 17.4.2024.

²⁸ V. Mongillo, “La legge ‘spazzacorrotti’: ultimo approdo del diritto penale emergenziale nel cantiere permanente dell’anticorruzione”, *Diritto Penale Contemporaneo*, no. 5 (2019): 231-311, sobre el punto p. 247 ss.

²⁹ A. La Spina, F. Roberti, “Il contrasto alla mafia e alla corruzione: una panoramica sugli sviluppi recenti”, *Rivista economica del Mezzogiorno*, Fasc. 3/settembre (2018): 441-470.

³⁰ R. Cantone, E. Carloni, *Corruzione e anticorruzione: Dieci lezioni*, cit.

³¹ V. Faggiani, “La Estrategia europea sobre la justicia penal en Red: avances en la aplicación de la Inteligencia Artificial”, *Derecho Digital e Innovación. Digital Law and Innovation Review*, no. 19 (2024).

³² DO L 2024/1069, 16.4.2024. Sobre Eu-LISA, cf. V. Faggiani, “La cooperación de EU-LISA con Eurojust y Europol: entre extraordinarias potencialidades y persistente opacidad en la digitalización

para el mantenimiento del funcionamiento de estos sistemas informáticos”, con la inclusión de la responsabilidad de las infraestructuras de comunicación, que utilicen,³³ con el objetivo de asegurar la interoperabilidad,³⁴ es decir un mejor acceso a la información almacenada en distintos sistemas de información de la UE y la gestión de la identidad a escala de la UE.

Entre 2023 y 2024 se han adoptado interesantes medidas al respecto, que ven a EU-LISA de protagonista y suponen un avance en la lucha contra la delincuencia organizada transnacional. Piénsese, por ejemplo, en el Reglamento (UE) 2023/969 por el que se ha instituido la plataforma informática de colaboración para los equipos conjuntos de investigación (ECI),³⁵ cuyo fin es facilitar el intercambio de datos e información estructurada y realizar la comunicación, indicando el *modus procedendi*, la cual estará alojada en EU-LISA. Los miembros de los ECI, Eurojust, Europol, la OLAF y otros órganos y organismos competentes de la Unión o representantes de una autoridad judicial internacional, que participe en un ECI, podrán acceder a dicha plataforma de colaboración como “usuarios.”³⁶

Y por lo que se refiere a la cooperación policial, además de potenciar el rol de Europol, en marzo de 2024, se ha adoptado el Reglamento de Prüm [Reglamento (UE) 2024/982],³⁷ cuyo objetivo es responder a la circulación de los delincuentes mediante la circulación de los datos. De esta forma, por un lado, los Estados miembros podrán comprobar automáticamente los datos biométricos procedentes de terceros países conservados por Europol y ponerlos a disposición de las autoridades policiales. Por otro, Europol, que será parte integrante del marco de Prüm, podrá cotejar los datos procedentes de terceros países sobre delincuentes y terroristas, con la inclusión de los que se encuentran en las bases de datos nacionales de los Estados miembros, estableciendo vínculos.³⁸

de la justicia penal en la UE”, in *Avances en el desarrollo de la Inteligencia Artificial. Principios éticos y democráticos, concreciones normativas en la Unión Europea, y límites para las Administraciones públicas*, dir. V. Faggiani y F. J. Garrido Carrillo (Cizur Menor: Aranzadi 2025), 147-174; M. Illamola Dausà, “EU-LISA, el nuevo modelo de gestión operativa de las distintas bases de datos de la UE”, *Revista CIDOB d’afers internacionals*, no. 111 (2015): 105-126; F. Tassinari, “La institucionalización de la competencia operativa de la Unión Europea para la gestión y la interoperabilidad de los sistemas informáticos de gran magnitud del Espacio de Libertad, Seguridad y Justicia: eu-LISA”, *La Ley Unión Europea*, no. 111 (2023).

³³ Tales sistemas son: SIS II, el Sistema de Información de Schengen de segunda generación; VIS, Sistema de Información de Visados; EURODAC, el Sistema Europeo de Comparación de Impresiones Dactilares de los solicitantes de asilo; EES, el Sistema de Entrada/Salida; DubliNet, para la transmisión de las solicitudes de asilo en la UE; ETIAS, el Sistema Europeo de Autorización de Viajes; ECRIS-TCN y la aplicación de referencia ECRIS, el Sistema Europeo de Información de Antecedentes Penales - Nacionales de Terceros Países; e-CODEX, el sistema informatizado para el intercambio electrónico transfronterizo de datos en el ámbito de la cooperación judicial en materia civil y penal; la plataforma de colaboración de los equipos conjuntos de investigación (ECI); y el enrutador Prüm II.

³⁴ F. Tassinari, “La interoperabilidad de los sistemas de información de gran magnitud de la Unión Europea y la detección de identidades múltiples: garantías y responsabilidades”, in *Lucha contra la criminalidad organizada y cooperación judicial en la UE: instrumentos, límites y perspectivas en la era digital*, dir. F.J. Garrido Carrillo, coord. V. Faggiani (Thomson Reuters Aranzadi, 2022), 291-338.

³⁵ OJ L 132, 17.5.2023.

³⁶ Artículo 3.5 del Reglamento (UE) 2023/969.

³⁷ DO L 2024/982, 5.4.2024. EDPS, Opinion on the Commission’s Proposal for the Regulation on automated data exchange for police cooperation (“Prüm II”), www.edps.europa.eu/system/files/2022-03/22-03-07_opinion-4-2022_prum_en.pdf, 2.3.2022. EDRI, “Automated data exchange in Prüm II: The EU’s securitisation mindset keeps encroaching on our fundamental rights”, 6.2.2024.

³⁸ Considerando n.º 8 del Reglamento (UE) 2024/982.

Más en concreto, se regulan los “*procedimientos de búsqueda automatizada de perfiles de ADN, datos dactiloscópicos, determinados datos de matriculación de vehículos, imágenes faciales y antecedentes policiales*”,³⁹ para permitir el intercambio de información entre las autoridades de *law enforcement* sobre personas involucradas en el proceso penal en cuanto sospechosas y acusadas y o incluso desaparecidas en el contexto de investigaciones penales o por motivos humanitarios y la identificación de restos humanos.

En este sentido, la cooperación entre Europol y las autoridades nacionales es básica. Recientemente, por ejemplo, en el ámbito de una operación llevada a cabo por Albania, Bélgica, Francia e Italia, con la ayuda de Europol, el 25 de noviembre de 2024, se dismanteló una red de corrupción integrada entre otros por un exjuez, un abogado, un agente de policía y dos periodistas de investigación, relacionada con una organización delictiva violenta, que opera en torno a un clan familiar, que se dedicaba a importar cocaína de Sudamérica a Europa.

La operación se puso en marcha gracias a los resultados de las comunicaciones cifradas de la plataforma SKY ECC, que mostraron pruebas de prácticas de corrupción. El producto de estas actividades delictivas se blanqueaba en Albania. El exjuez y el exabogado están acusados de manipular procedimientos judiciales para favorecer la organización delictiva, mientras que el agente de policía es sospechoso de filtrar información operativa sensible. Se cree que dos periodistas aprovecharon su posición para difundir desinformación, influir en la opinión pública y socavar las investigaciones sobre la red delictiva.⁴⁰

El asunto de que se trata muestra algunos aspectos fundamentales tanto del *modus operandi* de los criminales como de la estrategia de la UE. Con respecto a la forma de actuación de la delincuencia organizada, se observa la existencia de una red, con estructura jerárquica, que cuenta con el apoyo de autoridades públicas, que han sido corrompidas, para obstaculizar las investigaciones y el desarrollo de los procedimientos judiciales. Y desde el segundo perfil, reafirma la necesidad de responder a las redes criminales a través de más cooperación, potenciando el desarrollo de *networks* entre los actores de *law enforcement*, y la importancia de los instrumentos digitales en la lucha contra la criminalidad organizada.

5. Intentos de los Estados miembros de aplicación de herramientas basadas en mecanismos automatizados para luchar contra la corrupción

A diferencia de la UE, cuya actuación está siendo incisiva, puesto que se han movilizado importantes recursos para el desarrollo de proyectos muy ambiciosos, sobre todo en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, en los Estados miembros se pueden observar algunos “*intentos*” de aplicación de las nuevas tecnologías tanto a la fase preventiva como represiva para responder a la corrupción, y las demás formas de criminalidad a esta conectadas, especialmente en el ámbito de la pública administración.

³⁹ Considerando n.º 8 del Reglamento (UE) 2024/982.

⁴⁰ Europol, Media & Press, Violent Albanian criminal group linked to corruption disrupted via SKY ECC analysis, www.europol.europa.eu/media-press/newsroom/news/violent-albanian-criminal-group-linked-to-corruption-disrupted-sky-ecc-analysis, 26.11.2024.

La digitalización de los mecanismos de control y detección del riesgo y de la comisión del delito⁴¹ es sin duda necesaria para dotar a las fuerzas del orden y a las autoridades competentes de los instrumentos para descubrir esquemas de corrupción por su capacidad de procesar ingentes cantidades de datos e identificar patrones ocultos. Esto puede contribuir sin duda a transformar la estrategia de lucha. No obstante, además de ser limitada, su implementación no está exenta de riesgos y dificultades desde el respeto de los principios fundamentales del ordenamiento, especialmente desde el punto de vista del respeto al derecho a la protección de datos personales, del derecho a un proceso equitativo y del principio de igualdad.

El desarrollo de una actuación preventiva, a través de la identificación de indicadores de riesgo, “anomalías” o “anormalidades”,⁴² permite medir la corrupción, configurándose como “*parámetros de referencia para estrategias descentralizadas*”, que requieren una respuesta diferenciada, más específica y, por lo tanto, adaptada al contexto territorial de referencia.⁴³ En este sentido, medir la corrupción tiene que permitir comprender de dónde viene, supervisar cómo evoluciona y facilitar la adopción de acciones de respuestas, que permitan contrastar el fenómeno.

Sin embargo, tenemos que ser conscientes de que, como afirma Sbicca, si bien la corrupción representa uno de los principales obstáculos al desarrollo económico, político y social, es un fenómeno latente y por lo tanto difícil de medir.⁴⁴ Por ello, en su opinión, se puede comparar a un “iceberg”, del que solo es visible la punta, es decir los asuntos sobre los que los tribunales han llegado a pronunciarse con sentencia judicial. La parte sumergida, de la que no tenemos conocimiento porque no conseguimos percibir, es mucho mayor de lo que parece. Esto evidentemente dificulta la lucha contra el crimen.

En cuanto a las distintas experiencias nacionales, por ejemplo, en los Países Bajos, en términos generales, la corrupción se considera, en gran medida, vinculada a los intereses de la “*delincuencia organizada subversiva*”⁴⁵ por su efecto disruptivo dirigido a “*subvertir*” la integridad del Gobierno y de los sectores público y privado, menoscabando los valores y las normas.

En el marco de la prevención y lucha contra el fraude fiscal y la seguridad social, hace algunos años en los Países Bajos se adoptó el sistema SyRI (*Systeem Risico Indicatie* (*SyRI* o *SyRI i*)).⁴⁶ Syri se basaba en el uso masivo de datos personales interrelacionados

⁴¹ Pone de relieve la necesidad de centrarse en la estrategia de contraste y respuesta: E. Carloni, “Misurare la corruzione? Indicatori di corruzione e politiche di prevenzione”, *Politica del diritto*, no. 3 (2018): 445-466.

⁴² R. Cantone, E. Carloni, “Corruzione e anticorruzione: dieci lezioni, Milano, Feltrinelli”, *Misurare la corruzione? Indicatori di corruzione e politiche di prevenzione* Ibidem, 456.

⁴³ R. Cantone, E. Carloni, “Corruzione e anticorruzione: dieci lezioni, Milano, Feltrinelli”, *Misurare la corruzione? Indicatori di corruzione e politiche di prevenzione* Ibidem, 450.

⁴⁴ F. Sbicca, “Artificial Intelligence and Anti-Corruption”, <https://ceur-ws.org/Vol-3762/481.pdf>.

⁴⁵ Cf. European Commission, 2024 Rule of Law Report, Country Chapter on the rule of law situation in the Netherlands, Brussels, 24.7.2024, SWD(2024) 819 final, 12. En el informe se considera que “*Subversive crime*” links to all forms of severe organised crime that include meddling in the bona fide structures of society. It refers to forms of crime that subvert the integrity of Government, public and private sector and have a degrading effect on values and norms.”»

⁴⁶ *Rechtbank Den Haag*, sent. del 5 de febrero 2020, SyRI, ECLI:NL:RBDHA:2020:865 (<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878>). Vid. J. Gesley, “Netherlands: court prohibits government’s use of AI software to detect welfare fraud”, *Global Legal Monitor*, 13.5.2020; Y. F. Ng, M. O’Sullivan, M. Paterson y N. Witzleb, “Revitalising public law in a technological era: rights, transparency and administrative justice”, *University of New South Wales Law Journal*, vol. 43, no. 3 (2020): 1-37; L. Cotino Hueso, “Hacia la transparencia 4.0: el uso de la inteligencia artificial y big data para la lucha contra el fraude y la corrupción y las (muchas) exigencias constitucionales”,

entre ellos. La *Hague District Court*, en la sentencia de 5 de febrero de 2020, consideró que este mecanismo vulnera el respeto de la vida privada [artículo 8, par. 2, Convención Europea de Derechos Humanos (CEDH)], constituyendo un sistema desproporcionado, no necesario en una sociedad democrática, opaco y no verificable.⁴⁷

El Tribunal de la Haya, sirviéndose de un enfoque multinivel, estimó que el Estado no hizo públicos, ni reveló a los interesados el modelo de riesgo y los indicadores de los que se compone o puede estar compuesto, en definitiva, cómo funciona, y el procedimiento decisorio, y que no proporcionó al tribunal información objetivamente verificable para evitar que los ciudadanos encuentren la manera para eludir este programa.⁴⁸

Un sistema de este tipo, además de ser contrario al artículo 22 del Reglamento (UE) 2016/679 de protección de datos personales (RGPD), que establece con carácter general y salvo determinadas excepciones la prohibición de adoptar decisiones individuales de forma automatizada, incluida la elaboración de perfiles, viola el principio de transparencia y con esto las garantías procesales más elementales. El particular no puede verificar ni cómo se genera el árbol de decisión, ni cómo se ha llegado a una determinada decisión, ni cómo la persona interesada, cuyos datos fueron procesados en SyRI, pero que no dieron como resultado un informe de riesgo, puede ser consciente de que sus datos fueron procesados por motivos correctos.

En esta línea, en Letonia, se ha adoptado un sistema electrónico de declaración de bienes. Se trata de una herramienta de procesamiento automatizado, que identifica posibles riesgos de infracción de la Ley de Prevención de Conflictos de Intereses en las Actividades de los Funcionarios Públicos, a partir de la información facilitada en las bases de datos disponibles.⁴⁹ Un mecanismo parecido para verificar las declaraciones de bienes debería estar operativo en 2025 en Estonia.⁵⁰

Por su parte, Italia, para enfrentarse también a los últimos escándalos derivados de la gestión de fondos del *Piano Nazionale di Ripresa e Resilienza* (PNRR) y en de los contratos para la transición verde,⁵¹ ha procedido a la digitalización del procedimiento para la adjudicación de los contratos públicos, para que pueda aportar más transparencia. El procedimiento digital, que ha entrado en vigor desde el 1º de enero de 2024 (nuevo Código de los contratos públicos, atendiendo al decreto legislativo n.º 36/2023),⁵² ha previsto la puesta en marcha de ANAC,⁵³ la plataforma de los contratos públicos (PCP), que en virtud del principio de interoperabilidad interactúa con las demás plataformas digitales de contratación. La plataforma permite

in *Repensando la Administración digital y la innovación pública*, coord. C. Ramío (Instituto Nacional de Administración Pública, 2021), 169-196.

⁴⁷ El Tribunal de Distrito de la Haya declara en esta sentencia que el artículo 65 de la Ley SUWI y el Capítulo 5a del Decreto SUWI no tienen efecto vinculante, siendo contrarios al artículo 8.2 del CEDH.

⁴⁸ Tribunal de Distrito de la Haya, asunto *SyRI*, ap. 6.49.

⁴⁹ European Commission, Commission Staff Working Document 2024, Rule of Law Report, Country Chapter on the rule of law situation in Latvia, Brussels, SWD (2024) 814 final, 24.7.2024, 13 y 14.

⁵⁰ European Commission, 2024 Rule of Law Report, Country Chapter on the rule of law situation in Estonia, Brussels, 24.7.2024, SWD (2024) 806 final, 11.

⁵¹ Commissione Europea, Relazione sullo Stato di diritto 2024, Capitolo sulla situazione dello Stato di diritto in Italia, Bruxelles, 24.7.2024, SWD (2024) 812 final, La EPPO y la “Guardia di Finanza” están llevando la investigación “Resilient Crime”, 19-20.

⁵² Decreto legislativo 31 marzo 2023, n. 36, Codice dei contratti pubblici in attuazione dell’articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici, G.U. n.º 77 del 31 marzo 2023 - S.O. no. 12.

⁵³ El Data base Nacional de los Contratos Públicos, gestionado por ANAC, recoge datos de distintas bases de datos y permite un enfoque unificado sobre el proceso de licitación.

la publicidad de las bases de las licitaciones en un único portal digital, que puede ser consultado por todos de forma unificada y conectada a nivel europeo con la oficina de publicaciones de la UE. A través del fascículo virtual del operador económico se puede acceder a los documentos que permiten constatar los requisitos para que se pueda ser destinatarios de los contratos públicos.

El artículo 30 del Código de los contratos públicos promueve no solo la automatización de los procedimientos de concesión de los contratos mediante la adopción de soluciones tecnológicas, con la inclusión de la IA,⁵⁴ sino que en su tercer apartado establece los requisitos, que tienen que reunir las decisiones asumidas mediante automatización. Tales decisiones tienen que respetar los principios de: cognoscibilidad y comprensibilidad, en virtud de los que los operadores económicos tienen derecho a conocer la existencia de procesos automatizados de toma de decisiones que les conciernan y, en caso afirmativo, a recibir información significativa sobre la lógica utilizada; no exclusividad de la decisión algorítmica, atendiendo al que tiene que haber una aportación humana en el proceso decisorio capaz de controlar, validar o refutar la decisión automatizada; y no discriminación algorítmica, por la el que el responsable del tratamiento aplica medidas técnicas y organizativas adecuadas para evitar efectos discriminatorios contra los operadores sesgos.

Asimismo, se reconoce el derecho a que las entidades adjudicadoras adopten todo tipo de medida técnica y organizativa para asegurar que se rectifiquen los factores que comportan inexactitudes de los datos y minimicen el riesgo de errores, y a impedir los efectos discriminatorios por razones de nacionalidad, origen étnico, opiniones políticas, religión, convicciones personales, afiliación a un sindicato, caracteres somáticos, status genético, estado de salud, género y orientación sexual.

Si bien tanto la recepción de la dimensión digital-algorítmica como el reconocimiento de un conjunto de principios fundamentales, que tienen que regir la actuación de la administración pública, sean sin duda interesantes para proteger al ciudadano de posibles injerencias indebidas en sus derechos fundamentales, adaptando así mismo la administración pública a los nuevos desafíos, que esta dimensión plantea, no podemos no fijarnos en que la automatización de estas actividades, mediante el recurso a *“soluciones tecnológicas, con la inclusión de la inteligencia artificial y de las tecnologías de registración distribuidas, tiene que respetar las específicas disposiciones en materia ‘ove possibile’”*, es decir en la medida de lo posible (apartado primero). En otros términos, no estamos ante una imposición, como afirma Buoso *“absoluta”*, sino que se podría definir meramente relativa,⁵⁵ lo cual contribuye sin duda a limitar su eficacia y también a incrementar las posibilidades de intrusiones excesivas en los derechos fundamentales.

Y, por último, resulta interesante también la experiencia de Francia. El Consejo Constitucional,⁵⁶ en 2019, se pronunció sobre el recurso, que tenía por objeto la Ley de

⁵⁴ Atendiendo al artículo 30.2 del Código de los contratos públicos: *“Nell’acquisto o sviluppo delle soluzioni di cui al comma 1 le stazioni appaltanti e gli enti concedenti: a. assicurano la disponibilità del codice sorgente, della relativa documentazione, nonché di ogni altro elemento utile a comprenderne le logiche di funzionamento; b. introducono negli atti di indizione delle gare clausole volte ad assicurare le prestazioni di assistenza e manutenzione necessarie alla correzione degli errori e degli effetti indesiderati derivanti dall’automazione.”*

⁵⁵ Al respecto, cf. E. Buoso, *“Disruptive technologies and public administration: rethinking administrative law for the brave new world?”*, in *Avances en el desarrollo de la Inteligencia Artificial*. Principios éticos y democráticos, concreciones normativas en la Unión Europea, y límites para las Administraciones públicas, dir. Valentina Faggiani Francisco, Javier Garrido Carrillo (Aranzadi, 2025), cit., 225-241.

⁵⁶ Cf. apartados 84 y 85 de la sentencia del Conseil Constitutionnel n.º 2019-796 DC, 27.12.2019. En <https://www.conseil-constitutionnel.fr/decision/2019/2019796DC.htm>.

presupuestos para 2020,⁵⁷ declarando la conformidad de la herramienta, que permite a las autoridades tributarias y aduaneras recopilar y utilizar de forma automatizada, durante un plazo de tres años, los contenidos de acceso público, que encuentren en redes sociales y sitios de internet de usuarios de plataformas *web*.

De tal forma, se pretendía facilitar la investigación y detección de infracciones y delitos fiscales y aduaneros, permitiendo revisar perfiles, publicaciones y fotos accesibles online para encontrar pruebas de ingresos no declarados o de inconsistencias en sus declaraciones de aduanas o de impuestos. Los demandantes lamentaban que dicha normativa, en concreto el artículo 154, además de exceder las competencias de la ley de presupuestos, establecía un dispositivo de vigilancia informática, que violaba el derecho a la vida privada y la protección de datos personales y, en el caso de autocensura de los usuarios de internet, a la libertad de expresión.

El Consejo Constitucional, si bien declaró la conformidad de este mecanismo, estableció algunos límites. En su opinión, le corresponde al legislador alcanzar el equilibrio entre el objetivo de la lucha contra el fraude, que tiene un valor constitucional, y la evasión fiscal, por un lado, y el derecho al respeto de la vida privada, a la comunicación libre y la libertad de hablar, escribir y publicar, por otro, estableciendo las garantías para que el ciudadano pueda ejercer tales derechos. En todo ello, no obstante, no hay que perder de vista que la libertad de expresión representa una condición indispensable de la democracia y la garantía del respeto de otros derechos y libertades. Las limitaciones al ejercicio de esta libertad deben ser necesarias, apropiadas y proporcionales con el objetivo perseguido.

Ahora bien, aunque es cierto que la normativa en cuestión incidía en el derecho a la protección de datos personales y también en la libertad de expresión, desalentando el uso de servicios de comunicación en línea o, en todo caso, limitándolo, en el supuesto de que se trata se constató que se habían adoptado las garantías oportunas, puesto que el objetivo era razonable, pues el contenido de la información tenía que ser de libre acceso en un servicio de comunicación en línea abierto al público. No se pueden difundir contenidos que revelen datos especialmente sensibles. Además de haber aceptado divulgar las informaciones que les conciernen, los usuarios tienen derecho al acceso, rectificación y eliminación de los datos, así como a la limitación del procesamiento de la información. Para que la medida fuera proporcional, era necesario asegurar, y el juez tenía que comprobar que los algoritmos empleados solo permitieran la recopilación y el almacenamiento de los datos estrictamente necesarios.

El Consejo Constitucional llegó, por lo tanto, a la conclusión de que la medida impugnada era constitucional, puesto que establecía las garantías oportunas para asegurar una conciliación equilibrada entre el derecho al respeto de la vida privada y el objetivo de valor constitucional de combatir el fraude y la evasión fiscal. Por consiguiente, la limitación de la libertad de expresión y del derecho a la comunicación era necesaria, apropiada y proporcional con los objetivos perseguidos. Esta estrategia ha sido reforzada por la Ley de finanzas para 2024, que autoriza a los funcionarios de Hacienda a crear cuentas falsas e intercambiar información en las redes sociales, utilizando seudónimos, lo cual potencia considerablemente los poderes de investigación de la administración fiscal en Internet.⁵⁸

⁵⁷ Article 154 de la loi n.º 2019-1 479 du 28 décembre 2019 de finances pour 2020.

⁵⁸ J. Briot-Hadar – V. Drezet, “Le recours à l’Intelligence artificielle pour lutter contre la fraude fiscale”, <https://institut-rousseau.fr/intelligence-artificielle-fraude-fiscale/>, 11.10.2024. Cf. Article 112 de la loi n.º 2023-1 322 du 29 décembre 2023 de finances pour 2024.

6. Conclusiones

Si bien somos conscientes de que la corrupción no se puede erradicar, siendo parte integrante de la gestión de los esquemas de poder, pues cuanto más poder haya en juego, más el hombre, sobre todo si débil, es corruptible, se considera que precisamente por ello, tanto los Estados como la UE tienen el deber de intervenir para intentar limitar este fenómeno delictivo y su adquirida dimensión transnacional en la medida de lo posible.

Al respecto, hay que reconocer que la UE en los últimos años ha apostado por la digitalización de la cooperación judicial y de la cooperación policial para enfrentarse a las formas de criminalidad grave transnacional, las cuales acaban conectándose inevitablemente con las distintas manifestaciones de la corrupción. En cambio, los Estados miembros se han centrado en la digitalización de la administración pública para reforzar las distintas áreas en las que pueden producirse fenómenos de esta tipología.

En este sentido, la IA puede ser utilizada en las diferentes áreas de la administración pública, como en la contratación, para controlar los concursos públicos, detectando patrones anómalos, en las auditorías públicas para examinar los gastos, para controlar subvenciones y ayudas públicas en la gestión de recursos humanos y servicios públicos, para detectar irregularidades en procesos selectivos, como promociones internas y bolsas, y para proteger datos sensibles, alertando sobre accesos no autorizados o manipulaciones en bases de datos por parte de los mismos funcionarios y para facilitar las investigaciones de posibles casos de fraude. No obstante, la sensación es que dichos instrumentos parecen capaces solo de detectar “*los peces más pequeños*”, careciendo de real eficacia para descubrir las tramas criminales más complejas y articuladas.

En definitiva, la estrategia de lucha tiene que basarse en el refuerzo de la digitalización de la cooperación judicial en materia penal⁵⁹ y de la cooperación policial y en la adopción por parte de las autoridades nacionales de *law enforcement* y de la administración pública de sistemas para luchar contra este crimen y sus principales manifestaciones. El fortalecimiento de estos ámbitos puede contribuir a desarrollar una conciencia y percepción común de la gravedad de este crimen. En todo esto, no obstante, es muy importante tener en cuenta los aspectos positivos y negativos de las nuevas tecnologías, en particular su impacto en los derechos fundamentales. A tal fin, se identifican cuatro necesidades en las que es necesario conveniente trabajar.

En primer lugar, hace falta adoptar un enfoque ético y transparente, con una perspectiva antropocéntrica, que conciba la IA como un complemento y no como un sustituto. Al respecto, es fundamental la supervisión humana, puesto que la máquina no puede sustituir al hombre, especialmente en los mecanismos automatizados, que inciden en el ámbito procesal penal y sancionador administrativo.⁶⁰

En segundo lugar, hay que promover la formación, incentivando programas de training y capacitación para los profesionales y los funcionarios de las administraciones públicas, no solo para que adquieran conciencia de las dimensiones de la corrupción y de sus distintas manifestaciones, sino también para que aprendan a conocer y manejar los mecanismos digitales, con la inclusión de los sistemas automatizados.

⁵⁹ Council, Strategy 2019-2023 on European e-Justice (2019/C 96/04).

⁶⁰ V. Faggiani, “El derecho a un proceso con todas las garantías ante los cambios de paradigma de la inteligencia artificial”, *Teoría y realidad constitucional*, no. 50 (2022): 517-546 (ejemplar dedicado a: Poder Judicial).

En tercer lugar, para gestionar las nuevas tecnologías y hacer un buen uso de ellas, es imprescindible conocer sus potencialidades y el impacto disruptivo que pueden tener en los derechos fundamentales, en particular en la privacidad del individuo, en la protección de sus datos personales y en el principio de igualdad por lo sesgos, que suelen caracterizar las configuraciones algorítmicas, siendo al respecto necesaria la adopción de protocolos para la corrección rápida de errores. Y, finalmente, como cuarta necesidad de trabajo, no se puede dejar a un lado la importancia, tanto para las autoridades de *law enforcement* como para la administración pública, de dotarse de las necesarias infraestructuras tecnológicas, lo cual evidentemente requiere ingentes inversiones.

Corrupção e transição digital

*Pedro Jacob Morais**

1. Digitalização

O termo “*digitalização*” remete-nos imediatamente para o ciberespaço ou, melhor, remete-nos para a representação física do ciberespaço, para o ecrã ou monitor que nos permite aceder ao binarismo autorreferencial do sistema operativo. No entanto, observado com atenção, o signo “*digital*” desvela-se polissémico ao indicar simultaneamente algarismos inteiros ou decimais e dados. Encontra-se igualmente ligado com estreiteza à escrita, ao ato de digitar, redigir ou datilografar.

A digitalização possui uma clara dimensão construtivista, como demonstrou histórica e semiologicamente a transição do tempo analógico para o tempo digital. O tempo analógico referia-se à mensuração horária anterior ao surgimento dos relógios mecânicos e coetânea aos relógios solares, às ampulhetas, às clepsidras, ao incenso e restantes equivalentes funcionais. Aquele tempo firmava a relação do ser humano com o ambiente, uma relação de imediação a firmar a sobreposição entre o mundo natural e o mundo social e humano. Em certa medida, o tempo analógico surgia ainda como um produto da natureza ainda distante da intervenção ordenadora humana. Dito com clareza, o ser humano servia-se dos elementos naturais nessa agrimensura pretérita do tempo.

Foi com o advento dos relógios mecânicos que assistimos ao dealbar do tempo digital. Submetido ao império dos dígitos, o tempo deixava de ser relativo e relacional, passando a ser intelectualizado numa configuração sistémica, ou seja, em horas precisas, meias horas, minutos e segundos. O tempo reconfigurava-se enquanto obra humana, obra autónoma em relação ao ambiente circunstancial. Dito de modo diverso, sob o ascendente dos dígitos, o tempo afastou-se do sincronismo do ambiente em favor do diacronismo,¹ da possibilidade de ser perspectivado como produto e referente do sistema social, fechado ao ambiente no curto-circuito das rodas dentadas, massas oscilantes e escapes da máquina-relógio.²

Um segundo momento essencial à digitalização ocorreu com a invenção da imprensa ou tipografia mecânica. Uma vez mais, o signo, desta feita a palavra, reconfigurou-se e adquiriu uma dimensão sistémica, ou seja, a imprensa autonomizou a palavra, libertando-a ou deixando-a livre para interferir, para alterar o mundo. A prensa tipográfica inscreveu a palavra no mundo, alterando-o. Para nos servirmos da

* Professor da Escola de Direito da Universidade do Minho.

¹ Sobre a precipitação do tempo digital no presente, cf. Byung-Chul Han, *O aroma do tempo* (Lisboa: Relógio D'água, 2016), 9 e ss.

² A propósito das vicissitudes da mensuração do tempo, cf. David S. Landes, *A revolução no tempo* (Lisboa: Gradiva, 2009), 87 e ss.

expressão de Heidegger,³ a digitalização apresenta-se como “*formadora de mundo*” ou, pelo menos, compreende um sério desafio às estruturas sociais.

Como terceiro e decisivo momento do processo de digitalização, encontramos o surgimento dos computadores e respetivos sistemas de interação computacional, momento que vem conhecendo o seu zénite no expansionismo totalizante das redes sociais e com o desenvolvimento das *performances* algorítmicas e da inteligência artificial. Notemos que semelhante e recente estádio do *fatum* digital apenas se afigurou possível pela miniaturização tecnológica vertida na multiplicação dos pontos de acesso às redes cibernéticas. É neste terceiro momento da digitalização que pensamos quotidianamente e que subsumimos semiologicamente ao inescapável fosso dos ecrãs.

2. Conspirações

Vejam agora um curioso, funesto e tristemente atual exemplo dos desafios da digitalização. No final do séc. XIX, começou a circular pelo leste e centro da Europa um panfleto intitulado “*Os Protocolos dos Sábios de Sião*”, que talvez tenha constituído a primeira teoria da conspiração pós-moderna. Panfleto que assegurava que uma elite judaica se preparava para dominar o espaço geopolítico europeu, depondo as fronteiras, a independência bancária, as moedas nacionais, entre outros condimentos do *requiem* antissemita. Esta teoria da conspiração viria a reforçar Estados autocráticos e totalitários, a multiplicar o ódio e a respetiva perseguição aos judeus.⁴ Serviria igualmente de inspiração a diversas teorias conspirativas que continuam a crescer e a recrudescer. Ora, como elemento comum a diversas teorias da conspiração encontramos a ideia de que o Estado é permeável a pressões externas, à inflação de determinados grupos de interesses. A ideia de que o Estado pode ser feito refém por determinados agentes.

3. Corrupção

As teorias da conspiração fantasiam preconceituosamente um problema real. Trata-se do problema da corrupção ou, se quisermos referir o bem jurídico mais amplamente indicado pela doutrina, do problema da perda da autonomia intencional do Estado.⁵ A corrupção coloca em causa as atribuições do sistema estatal e dos seus diversos subsistemas. Neste sentido, degrada e deixa por cumprir as finalidades dos sistemas de saúde, de educação, da segurança social, dos sistemas judiciais, entre outros. E se quisermos recorrer a uma expressão dotada de maior plasticidade, o fenómeno corruptivo degrada os Estados de direito em sentido material ou, melhor, degrada a dimensão social do Estado. A ser assim, a prevenção da corrupção e dos crimes conexos⁶ surge particularmente desafiante em duas dimensões fulcrais, a saber:

³ De acordo com Giorgio Agamben, *O aberto: o homem e o animal* (Lisboa: Edições 70, 2013), 72, o «fio condutor da exposição de Heidegger é constituído pela tripla tese: “a pedra não tem mundo [*weltlos*], o animal é pobre de mundo [*weltarm*], o homem é formador de mundo [*weltbildend*]”».

⁴ Como refere Hannah Arendt, *As origens do totalitarismo* (Amadora: 2008), 8 e ss.

⁵ Para uma compreensão aprofundada das diversas possibilidades de declinação do bem jurídico protegido pelo tipo legal da corrupção, cf. António Manuel Costa, *Sobre o crime de corrupção: breve retrospectiva histórica. Corrupção e concussão. Autonomia “típica” das corruptions “activa” e “passiva”. Análise dogmática destes dois delitos: Separata do número especial do Boletim da Faculdade de Direito da Universidade de Coimbra - “Estudos em Homenagem ao Prof. Doutor Eduardo Correia” – 1984* (Coimbra: Universidade de Coimbra, 1987), 81 e ss.

⁶ Num enquadramento preciso das dimensões europeia e internacional da corrupção e respetiva criminalidade conexa, cf. Albuquerque, Paulo Pinto Albuquerque, *Comentário do código penal: à luz da*

na estabilização normativa ou reforço da confiança da comunidade no ordenamento jurídico, que poderá ser igualmente designada como prevenção geral positiva ou de integração; na dimensão da ressocialização do agente, também designada como prevenção especial positiva. Esta segunda dimensão apresenta-se como um domínio que ainda permanece profundamente marcada por uma visão classista e que demanda alternativas de ressocialização para os agentes da corrupção, seja ativa ou passiva. Notemos que a corrupção vem marcando presença entre os crimes de prevenção prioritária e entre os crimes de investigação prioritária em todas as leis de política criminal promulgadas no ordenamento jurídico português e que tiveram início no biênio 2007-2009,⁷ bem como nos diversos Relatórios Anuais de Segurança Interna.

4. Prevenção da corrupção

No que à prevenção da corrupção em sentido amplo diz respeito – entenda-se, a prevenção pré (*ex ante facto*) e pós-delitiva (*ex post facto*) –, Portugal tem registado avanços dignos de nota, *maxime*, o aumento de inquéritos por crimes de corrupção e crimes conexos,⁸ bem como o aperfeiçoamento da estrutura normativa penal e processual penal. Ademais, tem sido avaliado positivamente por organismos internacionais como o Grupo de Ação Financeira Internacional (GAFI) e pelo Grupo de Estados Contra a Corrupção do Conselho da Europa (GRECO).

Em termos político-criminais, encontra-se atualmente a ser implementado – e quase a atingir o seu período de vida útil – a Estratégia Nacional Anticorrupção (2020-2024),⁹ documento orientador que definiu sete prioridades operativas:

- i) Melhorar o conhecimento, a formação e as práticas institucionais em matéria de transparência e integridade;
- ii) Prevenir e detetar os riscos de corrupção na ação pública;
- iii) Comprometer o setor privado na prevenção, deteção e repressão da corrupção;
- iv) Reforçar a articulação entre instituições públicas e privadas;
- v) Garantir uma aplicação mais eficaz e uniforme dos mecanismos legais em matéria de repressão da corrupção, melhorar os tempos de resposta do sistema judicial e assegurar a adequação e efetividade da punição;
- vi) Produzir e divulgar periodicamente informação fiável sobre o fenómeno da corrupção;
- vii) Cooperar no plano internacional no combate à corrupção.

A Estratégia encontra-se em linha com o Plano de Ação para a Transição Digital, aprovado pela Resolução n.º 30/2020, de 21 de abril. De facto, a ideia de transição digital encontra arraigo no Plano, a vários níveis:

- i) No reconhecimento de que a digitalização aumenta os desafios relacionados com a corrupção, *maxime*, no que tange às oportunidades delitivas;

Constituição da República e da Convenção Europeia dos Direitos do Homem (Lisboa: Universidade Católica Editora, 2009), 968 e ss.

⁷ A saber: Lei n.º 51/2007, de 31 de agosto; Lei n.º 38/2009, de 20 de julho; Lei n.º 72/2015, de 20 de julho; Lei n.º 96/2017, de 23 de agosto; Lei n.º 55/2020, de 27 de agosto; e Lei n.º 51/2023, de 28 de agosto.

⁸ Como indicado no Relatório Anual de Segurança Interna (IASI) de 2023, 69.

⁹ Numa aproximação à dimensão pré e pós delitiva da Estratégia, cf. Pedro Jacob Morais, “Estratégia nacional de combate à corrupção. Breves notas sobre o Regime Geral e o Mecanismo de Prevenção da Corrupção”, in *Corrupção em Portugal: avaliação legislativa e proposta de reforma*, org. Paulo Pinto Albuquerque, Rui Cardoso e Sónia Moura (Lisboa: Universidade Católica Editora, 2021), 97 e ss.

ii) Mas que também pode ser um mecanismo ao serviço da prevenção das condutas corruptivas;

iii) Os instrumentos digitais podem ser utilizados nos diversos serviços do Estado de modo a reduzir a sua permeabilidade a condutas corruptivas, a disponibilizar informação junto dos cidadãos e a contribuir para a sua formação para a cidadania, sem esquecer a importância de dotar o Ministério Público dos instrumentos necessários para a investigação em contexto digital.¹⁰

Na planificação da Estratégia notamos a presença recorrente da área governativa da economia e transição digital, área fundamental para a implementação de medidas anticorrupção no contexto da transição digital. Refira-se ainda que da Estratégia resulta:

i) A criação do Mecanismo Nacional Anticorrupção (MENAC), entidade administrativa independente¹¹ que apresenta como escopo a garantia da efetividade das políticas de prevenção da corrupção e dos crimes conexos. Refira-se que o MENAC publicou um guia de apoio aos instrumentos do Regime Geral de Prevenção da Corrupção (Guia n.º 1/2023), e ainda um Plano de Formação para a integridade, a transparência e a prevenção da corrupção (2024-2025), documento que aposta na dimensão digital da prevenção do fenómeno em estudo.

ii) A aprovação do Regime Geral da Prevenção da Corrupção (DL n.º 109-E/2021, de 9 de dezembro), diploma aplicável a entidades públicas e a pessoas coletivas de direito privado e que prevê diversas medidas de prevenção da corrupção.¹² Refira-se, a título de exemplo, os programas de cumprimento normativo;¹³ os planos de prevenção de riscos; os códigos de conduta; os canais de denúncia; e a importância na aposta em formação e comunicação.

Como é bom de observar, a prevenção do fenómeno corruptivo que surge como finalidade do Regime Geral apresenta-se suscetível de ser otimizado através do recurso a instrumentos digitais. Basta pensarmos na efetivação dos canais de denúncia ou na divulgação e disponibilização de códigos de conduta, medidas que dependem, em grande medida, de instrumentos digitais.

Antecipando a Estratégia Nacional Anticorrupção para o período 2025-2028, que se encontra em desenvolvimento, o XXIV Governo da República Portuguesa publicou a Agenda Anticorrupção desenvolvida sobre os eixos da prevenção, da punição, da celeridade processual e da proteção do setor público. Vejamos cada

¹⁰ Como recolha testemunhal das dificuldades técnicas sentidas pela magistratura do Ministério Público nos inquéritos relativos à corrupção, cf. Luís Rosa, *45 anos de combate à corrupção* (Lisboa: Fundação Francisco Manuel dos Santos, 2021), especialmente a página 65 e ss.

¹¹ As entidades administrativas independentes surgem “*como resposta à necessidade de neutralizar certos setores de intervenção pública. (...)*.” Para maiores desenvolvimentos, consultar Rita Ribeiro de Barros, “As agências europeias no Direito Administrativo Europeu” (Tese de mestrado, Universidade do Minho, 2014), 24 e ss.

¹² A enquadrar o Mecanismo, cf. Inês Ferreira Leite, “O Regime Geral de Prevenção da Corrupção na Estratégia Nacional Anticorrupção (2020-2024)”, in *Corrupção em Portugal: avaliação legislativa e proposta de reforma*, org., Paulo Pinto de Albuquerque, Rui Cardoso e Sónia Moura (Lisboa: Universidade Católica Editora, 2021), 79 e ss.

¹³ Para uma reconstituição sumária da história dos programas de cumprimento normativo, ainda que debruçada sobre a sua dimensão empresarial, cf. Anabela Miranda Rodrigues, *Direito penal económico: uma política na era do compliance* (Coimbra: Almedina, 2020), 83 e ss. E sobre os programas de cumprimento normativo no setor público, cf. Flávia Novera Loureiro, “Programas de cumprimento normativo no setor público”, in *Corrupção em Portugal: avaliação legislativa e proposta de reforma*, org. Paulo Pinto de Albuquerque, Rui Cardoso e Sónia Moura (Lisboa: Universidade Católica Editora, 2021), 130 e ss.

um destes eixos com maior detalhe. No âmbito da prevenção, merecem ênfase as seguintes medidas: a intensificação da discussão respeitante à regulação do lóbi; o registo da “*pegada legislativa*”; a importância de potenciar a assessoria jurídica do Estado; a consulta pública dos processos legislativos e regulamentares; o princípio do governo aberto vertido na disponibilização de documentos e dados administrativos; o aperfeiçoamento do portal de contratação pública BASE; e a intenção de generalizar a venda judicial em leilão eletrónico.

A manifestação da transição digital apresenta-se clara nas medidas enunciadas, com particular incidência na transparência do processo legislativo. Em bom rigor, o registo da “*pegada legislativa*”, ou seja, uma maior transparência dos diversos passos da génese normativa, incluindo os agentes consultados e os pareceres colhidos, não se perspetiva exequível sem o envolvimento da sociedade através da consulta pública dos diplomas. Sem esquecer a disponibilização de documentos e dados administrativos, devendo apostar-se numa apresentação dos documentos simples e intuitiva, num “*site*” que seja perceptível para o cidadão médio. O mesmo se diga relativamente aos instrumentos digitais utilizados por profissionais, como os relativos à contratação pública, que devem ser orientados em razão da eficácia e da simplicidade de utilização. Outro elemento digno de nota será a maximização da assessoria jurídica por parte de serviços do Estado, por duas ordens de razão. Em primeiro lugar, pela eficiência económica vertida na desnecessidade de contratar especialistas externos, alocando recursos adicionais aos pareceres jurídicos. Em segundo lugar, pelo reforço da transparência que o recurso a juristas próprios convoca ou, dito de modo diverso, pela redução do sentimento de opacidade da comunidade em relação ao recurso a juristas *extranei*. Serão igualmente razões de celeridade, eficiência económica e eventual transparência ou maior possibilidade de escrutínio que presidirão ao alargamento da venda em leilão eletrónico.

No eixo da punição merecem igualmente destaque, enquanto manifestação da transição digital, as seguintes medidas: a efetivação do mecanismo de perda alargada de bens; a dinamização dos Gabinetes de Recuperação de Ativos e Administração de Bens; a criação de uma “*lista negra*” de fornecedores do Estado, proposta sempre questionável pelo seu potencial estigmatizador ou, quando muito, intimidatório; e a operacionalização de um canal de denúncia comum a todo o Governo. Este último aspeto releva-se de particular importância, quer pela redução da complexidade ínsita na multiplicação de canais de denúncia, quer porque o melhor modo de o concretizar será por via da digitalização.

Relativamente à celeridade processual, destaque-se que as novas tecnologias poderão ser um importante aliado na promoção da celeridade processual, nomeadamente através da aposta em meios digitais para o inquérito. E não resistimos em acrescentar que os tão propalados e mediáticos algoritmos, que mais não são de que formas de concatenação e resolução problemática ou, dito de modo diverso, *performances* sistémicas orientadas à resolução de problemas, apresentar-se-ão, num futuro próximo, capazes de auxiliar o julgador em tarefas marcadas pela repetição e pelo pendor burocrático. Nesta ótica, a implementação de tecnologia algorítmica marcará certamente o panorama processual futuro, contribuindo para a celeridade judicial.

Por fim, o eixo da proteção do setor público reforça a necessidade da transparência nos concursos públicos e não esquece a aposta na formação dos diversos ciclos ou níveis de ensino. O investimento na educação, longe de

constituir um truísmo pedagoga, compreende um dos mais importantes ativos da prevenção pré-delitiva, contribuindo para a sedimentação da consciência axiológica comunitária, desde os níveis de ensino básico, em torno da coisa pública e, como corolário necessário, para uma compreensão mais aprofundada do Estado de direito por parte do cidadão médio. Num sistema de justiça verdadeiramente integrado e comprometido com os direitos, liberdades e garantias dos cidadãos, a agulheta da prevenção delitiva deve ser redirecionada para o momento anterior ao facto.¹⁴

5. O Relatório da Comissão Europeia sobre o Estado de direito

A Comissão Europeia publica anualmente um Relatório sobre o Estado de direito na União Europeia, *rectius*, nos seus Estados-Membros. O Relatório apresenta-se tripartido nas seguintes áreas de análise: sistema judicial; quadro de luta contra a corrupção; pluralismo e a liberdade dos meios de comunicação social. Compreende então três níveis de corte que podemos designar simplisticamente como judicativo, normativo e comunicacional. Partindo da estrutura do Relatório, apercebemo-nos de que a Comissão coloca a corrupção como uma das principais forças degradantes do Estado de direito em sentido material e prescreve como antídoto a prevenção normativa, o bom funcionamento do sistema judicial, sem esquecer o papel dos meios de comunicação social, habitualmente designados como quarto poder, na afirmação ou infirmação das perceções a propósito da corrupção.

Curiosamente, o capítulo do Relatório referente a Portugal parte da perceção dos especialistas e quadros empresariais “*de que os níveis de corrupção no setor público permanecem relativamente baixos.*” Claro que as perceções dos cidadãos constituem um dado volátil – ainda que possa ser objetivado, dependendo o grupo questionado – e que deve ser devidamente apartado da real incidência da corrupção. Ilustremos a variabilidade das perceções sobre a corrupção com dois exemplos. De acordo com o Índice de Perceção da Corrupção da associação Transparência Internacional, Portugal obteve a classificação de 61 pontos em 100, ocupando a 12.^a posição da UE e a 34.^a mundial. Por sua vez, o Eurobarómetro Especial sobre a Corrupção de 2024 atesta que 96% dos inquiridos consideram que a corrupção constitui uma prática generalizada em Portugal, contra os 68% da média da UE. Ademais, refere que 61% dos inquiridos se sentem pessoalmente afetados pela corrupção no seu quotidiano, contra 27% da média das perceções na UE.

De volta ao Relatório sobre Estado de direito, a Comissão sublinha os seguintes elementos:

- i) A falta de relatórios periódicos da Estratégia Nacional Anticorrupção 2020-2024, ausência anquilosante para um diploma que se quer operativo e não meramente teórico;
- ii) O MENAC, apesar de ter assumido a maior parte das suas funções – mais especificamente no âmbito da fiscalização da aplicação do Regime Geral de Prevenção da Corrupção –, ainda não as exerce em determinados domínios, como os estudos setoriais e as recomendações específicas;
- iii) Os casos de corrupção estão a ser investigados com carácter prioritário;

¹⁴ A refletir sobre os contributos do direito penal e da criminologia no horizonte da justiça penal, ver Mário Ferreira Monte, “Relação entre criminologia e justiça penal nas ciências criminais”, in *As palavras necessárias: estudos em comemoração dos 30 anos da Escola de Direito por ocasião do centenário de Francisco Salgado Zenha*, vol. II. (Braga: UMinho Editora, 2023), 133 e ss.

- iv) A legislação referente às “*portas giratórias*” agravou as penas aplicáveis;¹⁵
- v) A criação um código de conduta aplicável aos membros do Governo e a altos funcionários;
- vi) A verificação eficaz das declarações de património de altos funcionários públicos e políticos por parte da Entidade para a Transparência;
- vii) O escrutínio do enquadramento jurídico do financiamento dos partidos;
- viii) O debate em torno da atividade de lóbi.

Como principais recomendações da Comissão, registamos a necessidade de melhorar os recursos de prevenção, investigação e prossecução da corrupção; melhorar o controlo das declarações de património por parte da Entidade para a Transparência; e implementar reformas que aumentem a transparência do processo legislativo.

6. A importância de uma abordagem complexiva

Aqui chegados, devemos notar que a prevenção da corrupção não se reduz a uma dimensão normativa, tal como o Relatório da Comissão não prescreve uma visão unidimensional do Estado de direito. Assim sendo, uma visão da corrupção excessivamente atida à norma ou à perfeitibilidade da sua génese ignoraria a dimensão social-comunitária do fenómeno. Mais especificamente, ignoraria que as perceções comunitárias, podendo residir em concretos défices normativos, não deixam de render homenagem a um conjunto de preconceitos ou, melhor, a um conjunto de ideias pré-estabelecidas. Ideias que residem na desconfiança comunitária em relação aos sistemas de justiça, mais especificamente, à celeridade processual,¹⁶ à efetividade das vias de recurso, à transparência da distribuição dos processos ou à formação dos magistrados.

Podemos assacar às considerações anteriores dois corolários. Em primeiro lugar, a norma deve ser sempre pensada como um módulo de vigência político-criminal, ou seja, carece de realização prática por via do sistema judicial. Para nos servirmos da estrutura do Relatório da Comissão, a prevenção da corrupção não se subsume a um normativismo puro, à génese normativa desgarrada da realidade. Antes pelo contrário, a norma demanda a eficácia da aplicação, *rectius*, da estabilização contrafática das expectativas comunitárias, razão pela qual a norma bem redigida necessita de um sistema de justiça robusto, capaz de a receber e efetivar. Em segundo lugar, e para além das normas bem redigidas e dos sistemas de justiça capazes de as efetivar, a prevenção da corrupção não dispensa o Estado de uma ação comunicativa dirigida aos cidadãos. Uma ação comunicativa capaz de esclarecer, ao nível do cidadão médio, os instrumentos normativos existentes e o funcionamento transparente do sistema de justiça. Uma ação comunicativa, verdadeira comunicação em ciência, que forme os estudantes, nos diversos níveis

¹⁵ Sem nos adentrarmos na ingente questão de saber se o neopunitivismo representa o caminho adequado à prevenção criminal, mas dando nota da perspetiva crítica de Fernando Conde Monteiro, “Os crimes de recebimento indevido de vantagem, de corrupção passiva e ativa no âmbito da Lei n.º 34/87, de 16 de julho, Lei da Responsabilidade dos Titulares de Cargos Políticos: reflexões jurídico-criminais à luz do ideologismo crítico”, in *Corrupção em Portugal: avaliação legislativa e proposta de reforma*, org. Paulo Pinto de Albuquerque, Rui Cardoso e Sónia Moura (Lisboa: Universidade Católica Editora, 2021), 394.

¹⁶ Sobre os desafios convocados pelos processos de elevada complexidade, ver Joana Marques Vidal, «Gestão de “megaprocessos”: reflexões», in *Corrupção em Portugal: avaliação legislativa e proposta de reforma*, org. Paulo Pinto de Albuquerque, Rui Cardoso e Sónia Moura (Lisboa: Universidade Católica Editora, 2021), 441 e ss.

ou ciclos de ensino, e que informe a comunidade, de modo a desmontar ideias pré-estabelecidas e a aplacar os sentimentos de insegurança que eventualmente surjam. Outro elemento apresentado no Relatório como essencial ao Estado de direito e, acrescentamos, à prevenção da corrupção, será o pluralismo e a liberdade dos meios de comunicação. De facto, a veiculação da informação, numa sociedade aberta¹⁷ e pluralista, não deve residir apenas na ação estatal, exigindo a intervenção dos meios de comunicação social, meios estes que, dependendo do modelo editorial escolhido, poderão exponenciar ou desmontar os diversos preconceitos comunitários suprarreferidos. Melhor será que o denominado quarto poder atue como um agente ativo na informação da comunidade, contribuindo para uma cidadania mais esclarecida e conaturalmente mais exigente.

O Relatório que nos ocupa deve então ser analisado no conjunto dos seus elementos, na medida em que o Estado de direito constitui um conceito tão complexo como agregador. Um conceito que demanda a consideração de um sistema de justiça que não seja preenchido apenas pelo direito penal, mas por todas as áreas normativo-jurídicas que contribuam para uma sociedade plural e aberta.

De volta à relação entre a digitalização e o tempo, as novas tecnologias não serão aceites enquanto fechamento sistémico ou curto-circuito informacional que nos afaste das linhas orientadoras do Estado de direito. Dito com clareza, as tecnologias digitais devem ser perspectivadas como um convite à constituição de um *locus* ausente de Estado, uma sede refratária ao Estado de direito em sentido material. Pelo contrário – e mesmo que, por vezes, sirvam de veículo à erosão da dimensão pluralista a que nos referimos, através da disseminação de desinformação, *maxime*, através das teorias da conspiração com que iniciámos o presente excuro – as novas tecnologias constituirão certamente um instrumento imprescindível na prevenção da corrupção e, como corolário, na manutenção do Estado de direito.

¹⁷ A distinguir os conceitos de sociedade aberta e fechada, cf. Karl Popper, *A sociedade aberta e os seus inimigos. Primeiro volume: o sortilégio de Platão* (Lisboa: Edições 70, 2015), 218 e ss.

Estado de direito: notas sobre a corrupção e a transparência

*Pedro Madeira Froufe**

1. A corrupção é um fator de risco para a democracia. Desacredita-a e, de alguma forma, desacreditando-a, atinge os alicerces da legitimidade do poder democrático. Desde logo, o exercício do poder público que tolere ou mesmo, no limite, seja exercido com a corrupção, não será materialmente e por definição, integralmente democrático.

No entanto, a corrupção não é um facto apenas existente e identificável no funcionamento das democracias. Regimes não democráticos são tão ou mais corruptos do que os democráticos. Muitas vezes, a corrupção é intrínseca ao funcionamento de ditaduras; por vezes, as ditaduras têm um impulso genético, assente na corrupção. O que sucede frequentemente é que há mais visibilidade e escrutínio (imprensa livre, liberdade de informação, liberdade de expressão) em regimes democráticos do que em ditaduras. E, sobretudo, há uma cultura anticorrupção que mais facilmente se difunde e é debatida em liberdade. E o respetivo impacto social da corrupção é, inevitavelmente, mais bem percecionado em sociedades livres e “abertas.”

Como é referido por Luís de Sousa, a corrupção ataca a “*essência da democracia e os seus valores fundamentais (de igualdade, transparência, livre concorrência, imparcialidade, legalidade, integridade), valores que não têm o mesmo significado num regime autoritário.*”¹ Por isso, há uma relação quase dialética entre corrupção e democracia. Se aquela fragiliza a democracia, esta, sendo materialmente efetiva, é sempre um antídoto (mais ou menos eficaz) da corrupção. Fatores como a transparência do exercício do poder e a própria participação cidadã impedem sempre a disseminação ou a banalização de práticas corruptivas e reforçam uma cultura anticorrupção.

Luís de Sousa, identificando duas vertentes do problema da corrupção² – a saber, a vertente legal e a vertente ética – ensaia uma noção ampla: a corrupção é geralmente entendida como “*o abuso de funções por parte de eleito, de funcionários públicos ou agentes privados, mediante promessa ou aceitação de vantagem patrimonial ou não patrimonial indevida, para si ou para terceiros, para prática de qualquer ato ou omissão contrários aos deveres, princípios e expectativas que regem o exercício do cargo que ocupam, com o objetivo de transferir rendimentos e bens de natureza decisória, pública ou privada, para um determinado indivíduo ou grupos de indivíduos ligados por quaisquer laços de interesse comum.*”³ Ou seja, sob o prisma relacional, a corrupção é um pacto normalmente oculto, implicando

* Professor da Escola de Direito da Universidade do Minho. Membro do Centro de Excelência Jean Monnet CitDig (Cidadania Digital e Sustentabilidade Tecnológica) da Escola de Direito da Universidade do Minho (Portugal).

¹ Luís de Sousa, *Corrupção* (Lisboa: Fundação Francisco Manuel dos Santos, 2011), 12.

² Desde logo, sublinhe-se, a corrupção é entendida e sentida assumidamente como um problema, em regimes democráticos.

³ Luís de Sousa, *Corrupção*, 17.

uma troca da qual poderá resultar quer um favorecimento *lato sensu* (a que se tem ou não direito) e, por outro lado, um qualquer benefício impróprio ou indevido e intencional, pecuniário ou não pecuniário, atual ou futuro, para as próprias partes contratantes e/ou para terceiros.

2. No ordenamento jurídico português, os artigos 372.º a 374.º-A da versão atual do Código Penal consagram o tipo legal de crime de corrupção no exercício de funções públicas, especificando duas modalidades desse tipo de comportamento desviante, no exercício de funções públicas e/ou com estas conexions: corrupção ativa (artigo 374.º do Código Penal) e corrupção passiva (artigo 373.º do Código Penal). Esses normativos e respetiva tipificação criminal visam a corrupção (ativa ou passiva) no Setor Público. Porém, a corrupção, no enfoque dado pelo Código Penal português, poderá, igualmente, correr no Setor Privado: artigos 379.º e 380.º do mesmo diploma legal. O legislador português pensou esta tipificação tendo em conta e assumindo predominantemente o contexto das relações negociais/comerciais privadas. Em princípio, a ação corruptiva deverá estar relacionada com o exercício de funções que poderão atentar contra a equidade, a lealdade, a sã concorrência, o justo equilíbrio negocial (equilíbrio contratual) nas relações empresariais.

Em última linha, direta ou indiretamente, estará sempre em causa a repercussão negativa desses comportamentos, no bom funcionamento do mercado, para além de tonalidades ético-jurídicas serem atingidas com tais condutas (ou serem, no mínimo, distorcidas ou enfraquecidas). Também nesse universo do Setor Privado, o legislador, nos termos consagrados no Código Penal, distingue entre corrupção ativa (artigo 380.º do Código Penal) e corrupção passiva (artigo 379.º do Código Penal). A Lei 20/2008, de 21 de abril, acaba por concretizar, nomeadamente, nos respetivos artigos 8.º e 9.º (com a redação que lhes foi introduzida pela Lei 30/2015, de 22 de abril), os termos da corrupção passiva e ativa no Setor Privado, respetivamente.

Remetemos – compreendendo-se a *ratio* fundamental da tutela e do combate criminal (também) à corrupção no Setor Privado – para o Acórdão do Tribunal da Relação do Porto, de 6 de março de 2013, proferido no Processo 269/10.2TAMTS.P1 (Relator Castela Rio) e, especialmente, para o seu sumário, onde se lê: “*O bem jurídico tutelado pelos crimes de Corrupção ativa no setor privado e de Corrupção passiva no sector privado, dos artigos 8.º e 9.º da Lei n.º 20/2008, de 21 de abril, é a lealdade e a confiança imprescindíveis para as relações privadas, já que o núcleo do injusto reside na violação dos deveres funcionais por parte do trabalhador do sector privado.*” No fundo, estão em causa comportamentos que se traduzem numa violação de deveres funcionais assumidos ou, no mínimo, objetivamente expectáveis para quem desempenhe uma determinada função que “*afetem a lealdade e a confiança imprescindíveis para as relações privadas.*”⁴

3. O combate à corrupção requer uma abordagem holística, convocando uma dimensão, desde logo, política (vontade política), com um foco, igualmente, pedagógico e cultural. Mais do que ações que incidam imediatamente sobre o fenómeno e/ou fenómenos corruptivos, importa combater todo um ecossistema da corrupção. Ecossistema esse que, com a digitalização acentuada da vida hodierna e com o desenvolvimento intenso dos quadros de vida da sociedade técnica da informação, tem vindo a expandir-se e, de certo modo, a fortalecer-se. A digitalização e a massificação do uso de tecnologias da informação facilitam a

⁴ Disponível em “Acórdãos do Tribunal da Relação do Porto”: Instituto de Gestão Financeira e Equipamentos da Justiça, I.P., acedido em 24 de fevereiro de 2025, <https://www.dgsi.pt/jtrp.nsf/Por+Ano?OpenView>.

difusão de comportamentos desviantes, em termos de ação e de decisão políticas. Num Estado de direito democrático, preservando-se, efetivamente, a liberdade de informação (liberdade de obter informação, de informar e de se ser informado), os meios tecnológicos e a vida digital proporcionam, por um lado, mais vias de conhecimento e de debate (escrutínio), relativamente a comportamentos de corrupção e/ou relativamente a práticas políticas de risco corruptivo.

No entanto, por outro lado, a vida corrente digitalizada e a expansão intensa e rápida do modo de vida característico das sociedades técnicas (ultra técnicas e ultra especializadas) da informação, também acentua a inevitável rapidez da tomada de decisões. Há cada vez mais informação especializada, pois a complexidade dos problemas requer, igualmente, uma especialização e um conhecimento técnico mais aprofundados. A pressão mediática, nomeadamente em termos de atividade política, implica cada vez menos tempo de reflexão e, necessariamente, de decisão. A complexidade dos processos de decisão raramente se casa bem com a falta de tempo. O excesso de informação (relevante e irrelevante) que circula, por exemplo, pela Internet, sobretudo quando há significativas falhas de literacia digital, pode dificultar a apreensão da ocorrência de fenómenos de corrupção. A aparente criação de condições para que haja mais transparência poderá, ao invés e sob a aparência de muita informação, gerar menos transparência ou uma mera ilusão de transparência. O modo como se entende a transparência e a garantia da sua efetividade devem, necessariamente, equacionar esse emergente e cada vez mais intenso, contexto digital.

Tudo isso, simultaneamente, impulsiona também uma espécie de transformação da vida e da atividade políticas, reduzindo-as, por vezes, quase exclusivamente, a confrontos de narrativas. Ou seja, uma cada vez mais evidente “*psicopolítica*” – servindo-nos, aqui, da expressão de Byung-Chul-Han⁵ – que se esgota nas narrativas, independentemente da realidade. *Rectius*: a realidade política é, sobretudo, uma narrativa. O papel da comunicação social (pelo menos, da comunicação social editada) pode ser, nessa perspetiva, decisivo. Poderá não ser apenas a de quem informa e elucida e passar a ser, também, a do “*fazedor*” de políticas (narrativas). Há o risco de a imprensa ser também um ator/interveniente político. A falta de tempo para o tratamento noticioso de processos de decisão – eventualmente, sob a pressão do tempo e das narrativas dominantes – poderá resvalar, cada vez mais, para o critério do senso comum. Senso comum que, desde logo, é um estado de conhecimento frequentemente erróneo, sobretudo em domínios de alguma complexidade técnica. Nesse contexto, caracterizado também pela política – “*psicopolítica*” –, o combate à corrupção passará, no fundo, pela referida abordagem holística que significa criar-se e fortalecer-se um ecossistema anticorrupção.⁵

Inevitavelmente, o impacto que a digitalização tem no que se entenda por transparência, e no modo como tal transparência é operacionalizada e efetivada, repercute-se na preservação do Estado de direito. A redução da atividade política democrática a um predomínio crescente de narrativas fáceis e imediatas, bem como o crescimento do que atrás denominamos “*política-psicopolítica*”, são potenciados pela nossa cada vez mais intensa e dependente relação com o mundo digital. E a própria formação livre e consciente das nossas cosmovisões e opções políticas, enquanto eleitores, é mais facilmente prejudicada e distorcida através da massificação da comunicação “*em rede*”, via Internet – mesmo sem disso nos apercebermos. A mensagem e o debate políticos, desenvolvendo-se, cada vez mais, através de “*chats*”, “*redes sociais*” fechadas,

⁵ Byung-Chul-Han, *Psicopolítica* (Lisboa: Relógio d'Água, 2015).

plataformas digitais de comunicação, etc., apelam intensamente a uma comunicação quase instantânea, através da qual se procura alcançar uma adesão quase epidérmica e sensitiva (não racional) do destinatário (eleitor). A política transforma-se, muitas vezes, quase exclusivamente numa narrativa (independentemente da verificação da realidade), sendo que tal narrativa é, também ela e em grande medida, construída em torno de uma linguagem (“*highlights*”) imediatista e publicitária. A redução da mensagem política e da explicação do que seja, por exemplo, o exercício de funções de Estado, a uma narrativa simples, imediatista e necessariamente incompleta ou errónea, acaba por afetar a transparência – e, por conseguinte, o correto escrutínio da decisão pública! Afeta a democracia e, materialmente, a vigência do Estado de direito. Por outro lado, o reverso dessa medalha – ou seja, um mais fácil escrutínio de certos atos e exercício de funções – será, também, uma vantagem potencial daquele estado de coisas, daquela vertiginosa e intensa digitalização da vida quotidiana – e, por conseguinte, também de parte da decisão e da atividade políticas. Os instrumentos jurídicos disponíveis – nomeadamente, os regimes vigentes que pretendem garantir a transparência, como uma componente do direito fundamental a uma “*boa administração*”⁶ – deverão ser repensados e, por vezes, ajustados a este tipo de nova e crescente “*política-psicopolítica*”, de narrativas cada vez mais digitais.

O combate à corrupção passa, também, por tal exercício de ajustamento de tais instrumentos a essa realidade, moldada pelos efeitos da digitalização e da mediatização.

4. A literatura identifica, habitualmente, vários fatores determinantes da corrupção. Causas incentivadoras de comportamentos de corrupção, por via de regra, no setor público. De um modo sintético, podemos enunciar as seguintes grandes quatro causas ou grupos de causas determinantes de atos de corrupção: teoria das escolhas públicas, teoria do “*salário e/ou da remuneração de eficiência*”, teoria da agência, e a teoria orgânica e contextual.⁷

As causas determinantes e/ou motivacionais da prática de atos de corrupção, ínsitas nestes quatro grupos ou teorias, podem ser de natureza predominantemente institucional, política, social/subjetiva ou económica.⁸ Naturalmente, analisando de *per se* cada uma das possíveis causas determinantes do fenómeno, muitas vezes encontramos, simultaneamente, motivações de natureza diversa, incentivando o mesmo comportamento corruptivo em causa.

A teoria das escolhas públicas incide sobretudo na dimensão subjetiva/pessoal do agente que pratica o ato de corrupção. Trata-se de uma análise que se foca numa perspetiva egoística e de oportunidade do agente. Este pretende (e é motivado pela oportunidade para praticar o respetivo ato) pela maximização dos seus interesses pessoais, à custa de um dano do interesse coletivo ou interesse público. O agente, nesta perspetiva, desenvolve racionalmente uma análise “*custo-benefício*” e avança para a prática do ato de corrupção quando entende que as vantagens, para si, resultantes dessa prática, serão superiores aos eventuais inconvenientes (possibilidade de tal ato ser detetado, possíveis sanções e/ou outras consequências penalizadoras). Pressupõe-se, portanto, nesta teoria, um comportamento racional e volitivo do agente.

⁶ Como é o caso, no ordenamento português, da Lei 26/2016, de 22 de agosto – LADA (Lei de Acesso aos Documentos Administrativos e à Informação Ambiental).

⁷ Jean Oda Cesar e Nadia Smaili, “Écosystème de la lutte contre la corruption: une approche intégrative”, *Éthique Publique - Revue internationale d'Étique Sociétale et Gouvernementale*, v. 23, no. 1 (2021), acedido em 7 de março de 2025, <https://doi.org/10.4000/ethiquepublique.5735>.

⁸ Jean Oda Cesar e Nadia Smaili, “Écosystème de la lutte”, 2.

A teoria do “*salário e/ou da remuneração de eficiência*” assenta num pressuposto ainda económico e também, por conseguinte, racional. Melhores salários conduzem a maior produtividade e a menor incentivo à prática de atos de corrupção. Assim, e no que respeita à prática desses atos, na perspetiva desta teoria, quanto melhor for a remuneração do agente, menos predisposição mental haverá, da parte desse mesmo agente, para a prática de condutas corruptivas. Ao invés, menores salários ou remunerações insuficientes produzirão menos produtividade e maior incentivo para a prática de atos de corrupção. Esta teoria também é utilizada por alguns Autores para explicarem a questão (macroeconómica) do desemprego involuntário. A partir desse foco macroeconómico, segundo alguns, essa teoria do “*salário de eficiência*” estender-se-ia, igualmente com prestabilidade, para a questão da corrupção.⁹

No entanto, a relação direta entre salário e corrupção, sugerida por esta teoria, é rebatida por alguns estudos. Na verdade, tal relação desvalorizaria a importância, mesmo numa ótica de empenho pessoal, da prossecução do interesse público e do cumprimento das obrigações. O brio profissional não seria, de resto, considerado como um elemento motivacional dos comportamentos dos agentes públicos. Por exemplo, de acordo com um estudo publicado já em 2003, sobre os efeitos de uma ação de combate à corrupção, realizada nos hospitais públicos da cidade de Buenos Aires, entre 1996 e 1997 (estudo esse de Rafael Di Tella e Ernesto Schargrodsky),¹⁰ sugere-se que o aumento do salário dos agentes públicos não terá nenhum impacto no nível de corrupção existente, se não se verificar, igualmente, um acréscimo de medidas de controlo.¹¹ Assim, uma remuneração dita “*eficiente*” só o será realmente se, porventura, existirem medidas de deteção e de controle da corrupção adequadas. Em síntese, a crítica que se poderá fazer a esta teoria, aparentemente, será a seguinte: provavelmente, um salário e/ou uma remuneração significativa e aparentemente “*eficiente*” só poderão dissuadir a prática ou a tentativa de prática de atos de corrupção, se forem (salário e/ou remuneração) acompanhados de medidas adequadas de controle, sem as quais o agente público poderá sempre ter a tentação de aproveitar a sua informação privilegiada (assimetria de informação) para benefício (enriquecimento) próprio.

A referida assimetria de informação (a informação privilegiada de que dispõe o funcionário ou agente público) é um dos pressupostos da teoria da agência. Com efeito, a informação de que dispõe o agente público, o seu conhecimento técnico, especializado – ou, simplesmente, a sua familiaridade com circunstâncias que envolvem a sua atividade/missão – dotam-no de uma vantagem operativa em relação ao seu “*mandante*” ou “*principal*.” Esta teoria que assenta nas especificidades ou características dessa relação “*principal/mandante-agente*” nota que o conjunto dos benefícios e dos custos da relação (dessa relação “*principal-agente*”) está, habitualmente, sob controle operativo do agente. O agente dispõe, normalmente, de um relativo poder discricionário que, aliado à assimetria de informação de que beneficia (desde logo, em relação ao seu “*principal*”) pode criar oportunidades para que o agente público possa retirar, para si, benefícios, praticando atos de corrupção.

⁹ Jean Oda Cesar e Nadia Smaili, “Écosystème de la lutte”, 4.

¹⁰ Rafael di Tella e Ernesto Schargrodsky, “The role of wages and auditing during a crackdown on corruption in the city of Buenos Aires”, *The Journal of Law & Economics*, v. 46, no. 1 (2003): 269-292, acedido em 7 de março de 2025), <https://doi.org/10.1086/345578>. Em síntese, e na conclusão do estudo referido, pode ler-se: “*Theory predicts no correlation between wages and corruption when the probability of audit is very low or very high. Including observations with these characteristics will bias the results toward finding no significant effects of wages on corruption.*”

¹¹ Jean Oda Cesar e Nadia Smaili, “Écosystème de la lutte”, 4.

Além disso, essa situação facilitadora da corrupção poderá ser potenciada quando há uma divergência de interesses entre os interesses individuais do agente e os interesses do “*principal*” (novamente, retornando, em parte, à teoria do “*salário de eficiência*”, o caso de o agente perceber a sua retribuição como sendo insuficiente, relativamente aos sacrifícios que deverá suportar para prosseguir a sua função ou, simplesmente, o agente não se rever nos fins prosseguidos pelo seu “*principal*” ou mandante). Uma das críticas mais recorrentes que esta perspectiva da “*teoria da agência*” suscita, prende-se com situações em que todo o sistema funciona, generalizadamente, com atos de corrupção. Na literatura esta crítica é sobretudo direcionada para muitos países em vias de desenvolvimento, nos quais a corrupção não corresponde a um desvio individual em relação ao funcionamento do sistema de decisão e de trabalho, mas em que a corrupção é generalizada e faz parte integrante, ordinariamente, do próprio sistema. Ou seja, a corrupção é que é o sistema e quase todos os agentes e decisores incorrem (em maior ou menor escala) na prática atos de corrupção.

5. Servindo-nos da categorização de Cesar e de Smaili,¹² podemos distinguir entre atos de corrupção de um nível “*micro*”, atos de corrupção que se determinam a um nível intermédio, entre os níveis “*micro*” e “*macro*” (“*més*”, segundo a expressão em língua francesa) e a corrupção determinada a um nível “*macro*.”

“*Micro*” pretende significar que as causas determinantes (entre as quais, as causas motivacionais) da corrupção podem reconduzir-se, sobretudo, à esfera individual, subjetiva, do agente. Por outro lado, neste contexto, “*macro*” significa que tais causas determinantes se encontram principalmente a um nível supra individual, organizativo, institucional e/ou mesmo cultural.

A perspectiva que nos é dada não só pela teoria da agência – mas também pela teoria das escolhas públicas e dos “*salários de eficiência*” – é uma perspectiva de causas determinantes da corrupção a um nível “*micro*” e, de certo modo, também a um nível intermédio (“*més*”).

Numa perspectiva “*macro*”, podemos dar nota de uma teoria “*orgânica*” ou contextual que identifica, principalmente, causas determinantes da corrupção em aspetos do funcionamento e da organização institucional dos sistemas públicos e também em características culturais. Podemos enunciar, como ilustrações dessas causas determinantes da corrupção, fatores como, nomeadamente: alguns aspetos formais e organizacionais do funcionamento institucional, como sejam, por exemplo, a ausência de controlos internos, dissuasores da prática de atos de corrupção, a complexidade de organigramas de serviços públicos, o centralismo decisório que introduz não só ineficiência nos processos de decisão, como ajuda a disseminar uma cultura de desresponsabilização, frequentemente manifestada pelos serviços e agentes fora do perímetro central ou centralizado desses serviços, a própria desvalorização do interesse público (e respetiva priorização dos interesses estritamente pessoais, por parte dos agentes públicos) e, como foi assinalado a propósito das críticas à “*teoria da agência*”, uma cultura e uma habitação à prática de atos de corrupção, inerentes ao funcionamento de certos serviços públicos (a corrupção será o próprio sistema).

6. As visões sobre as causas determinantes da corrupção descritas, decorrentes das teorias atrás identificadas, dão-nos pistas parciais não só sobre tais causas determinantes, como também nos permitem avançar com hipóteses de medidas a adotar para combater a corrupção – no fundo, para se ir construindo um ecossistema anticorrupção. Uma nota salientada por Cesar e Smaili é a da existência de uma

¹² Jean Oda Cesar e Nadia Smaili, “Écosystème de la lutte”.

espécie de “*triângulo*”¹³ das determinantes da corrupção: um agente público poderá envolver-se na prática de atos de corrupção (ativa ou passiva), se *i*) verifica existir essa possibilidade/oportunidade, *ii*) encontra justificações para a prática desses atos (se racionaliza a corrupção), e *iii*) o agente sente pressões e/ou encontra uma motivação pessoal para a prática desses atos de corrupção. Para se construir um ecossistema anticorrupção, dever-se-á atingir, anulando-o, esse “*triângulo*” de determinantes da corrupção.

Ora, é possível – partindo de uma análise global das causas determinantes salientadas por cada uma daquelas teorias – equacionar medidas anticorrupção quer no plano interno do funcionamento dos serviços públicos, quer no plano externo (ou seja, tendencialmente, medidas do contexto envolvente e condicionantes do funcionamento desses serviços). A existência de organigramas dos serviços públicos que sejam simples ou facilmente perceptíveis pelos funcionários e pelos cidadãos é um dos exemplos dessas medidas internas. De igual modo, torna-se fundamental a existência, por via de regra, de mecanismos de auditoria e de controlo internos, adequados e eficazes. Um cuidado na formação e na disseminação de uma cultura anticorrupção, própria de cada serviço e que seja assimilada pelos agentes/funcionários, será outra medida interna necessária. Por outro lado, a existência de uma cultura geral (no plano das relações económicas) de concorrência e de elucidação das vantagens (económicas e de justiça e de igualdade de oportunidades) inerentes à concorrência será um elemento determinante da tomada de consciência coletiva dos danos que a corrupção provoca.

A falta de concorrência ou uma concorrência falseada afetam diretamente o interesse público. Esse ambiente “*amigo*” da concorrência será uma medida externa que integrará, necessariamente, um ecossistema anticorrupção. O próprio sistema legal vigente e as respetivas políticas legislativas prosseguidas formam o contexto externo, não só dos serviços em consideração, como da comunidade. É impensável a criação de um ecossistema anticorrupção, no qual se integre um sistema legal (elemento externo) que não tenha em consideração, explícita ou implicitamente, esse desiderato anticorrupção.

7. Há, contudo, dois fatores que, numa perspectiva holística, são estruturantes, relativamente à edificação de um ecossistema anticorrupção. São elementos de carácter simultaneamente interno e externo à organização e funcionamento dos serviços – sendo, além do mais, catalisadores da disseminação de uma cultura de responsabilidade (sentida individual e coletivamente). Cultura de responsabilidade e dissuasão da corrupção são indissociáveis. Referimo-nos, quanto àqueles dois fatores, à transparência e à prestação de contas. Estes dois fatores acabam por estar, implícita ou explicitamente, subjacentes a todas as medidas parciais, decorrentes e propostas por cada uma das quatro teorias sobre as determinantes da corrupção, atrás enunciadas.

No que respeita aos serviços públicos, a prestação de contas incide, simultaneamente, na respetiva organização interna e no respetivo contexto global (no plano externo). A criação de órgãos e de serviços internos de auditoria – e, por consequência, de justificação e de responsabilização pelo bom ou mau funcionamento dos serviços – é uma medida interna necessária. A discussão sobre modelos de avaliação do desempenho dos agentes e dos próprios serviços insere-se, também, neste *item* da prestação de contas. Igualmente, numa perspectiva externa, a cultura anticorrupção integra, igualmente, uma aceitação generalizada da justificação e explicitação dos

¹³ “*Le triangle de la fraude (corruption)*”, Jean Oda Cesar e Nadia Smaili, “*Écosystème de la lutte*”, 18.

atos praticados – seja individual, seja coletivamente e/ou institucionalmente. Uma sociedade aberta não pode deixar de considerar necessária uma efetiva cultura de prestação de contas – o mesmo é dizer-se, de responsabilidade. Num plano interno, é necessário, em contrapartida, que tais mecanismos de responsabilização e de prestação de contas sejam, também, minimamente eficazes, équos e incentivadores de boas práticas. Naturalmente, quando a organização socioprofissional de uma determinada comunidade é, tendencialmente, pouco recetiva à concorrência – e assenta em lógicas excessivamente corporativas e/ou de grupos de interesse – há mais dificuldade em se encarar como pressuposto de tal organização quer a prestação de contas, quer, por consequência, a vigência de uma cultura de responsabilidade.

A transparência, por outro lado, é um elemento fundamental da boa governação pública, sendo, igualmente, uma forma indireta de abertura à participação cidadã – na medida em que permite um escrutínio amplo e generalizado relativamente às decisões tomadas pelos poderes públicos. Em termos de governação pública, refere-se, desde logo, à abertura e à possibilidade de acesso às informações respeitantes ao governo de todas as entidades públicas, por parte dos cidadãos. Existem, contudo, outras dimensões da transparência que concorrem para um governo justo e eficiente, num contexto democrático. A responsabilidade e a prestação de contas que referíamos anteriormente pressupõem a transparência. Quando as informações relevantes são de fácil acesso, isso promove, facilitando, a prestação de contas. É também um pressuposto da participação cidadã e é entendida como sendo um instrumento necessário para o combate à corrupção. Não é possível conceber-se um ecossistema anticorrupção, sem transparência.

Em Portugal – como, de resto, na União Europeia – existem instrumentos normativos que positivam um regime de acesso aos documentos administrativos, densificando, no que respeita à governação pública, a transparência. A própria Constituição da República Portuguesa, no artigo 268.º, n.º 2, estabelece “o direito de acesso aos arquivos e registos administrativos, sem prejuízo do disposto na lei em matéria relativa à segurança interna e externa, à investigação criminal e à intimidade das pessoas.” Como é salientado por J.J. Canotilho e Vital Moreira, “o artigo 268.º (da Constituição da República Portuguesa) não deve ler-se de forma isolada, mas antes em articulação com o catálogo de direitos, liberdades e garantias de participação política (Parte II, Capítulo III).”¹⁴

Atualmente, a Lei 26/2016, de 22 de agosto – LADA (Lei de Acesso aos Documentos Administrativos e à Informação Ambiental) – consagra o regime vigente em matéria de acesso aos documentos administrativos e à informação administrativa (e sua reutilização) incluindo em matéria ambiental, transpondo para a ordem jurídica interna a Diretiva 2003/4/CE, do Parlamento Europeu e do Conselho, de 28 de janeiro de 2003, relativa ao acesso do público às informações sobre ambiente, e a Diretiva 2003/98/CE, do Parlamento Europeu e do Conselho, de 17 de novembro de 2003, relativa à reutilização de informações do setor público. A própria LADA, no artigo 2.º, invoca a transparência, impondo às entidades públicas um comportamento proativo e de iniciativa própria, promovendo-a, através da divulgação da informação pública relevante.

Assim, nos termos do referido n.º 2, do artigo 2.º, da LADA, “(a) informação pública relevante para garantir a transparência da atividade administrativa, designadamente a relacionada com o funcionamento e controlo da atividade pública, é divulgada ativamente,

¹⁴ J.J. Canotilho e Vital Moreira, “Comentário ao artigo 268.º”, in *Constituição da República Portuguesa anotada*, volume II (Coimbra: Wolter Kluwer Portugal, Coimbra Editora, 2010), 820.

de forma periódica e atualizada, pelos respetivos órgãos e entidades.” Por seu turno, o n.º 3, da mesma regra, explicita que: “Na divulgação de informação e na disponibilização de informação para reutilização através da Internet deve assegurar-se a sua compreensibilidade, o acesso livre e universal, bem como a acessibilidade, a interoperabilidade, a qualidade, a integridade e a autenticidade dos dados publicados e ainda a sua identificação e localização.” Trata-se de uma decorrência necessária do próprio princípio geral, enunciado naquele artigo 2.º da LADA, ou seja, o princípio da “*administração aberta*.”¹⁵ Note-se que apesar do regime em causa, consagrado na LADA, não visar unicamente documentos administrativos gerados e utilizados através da Internet, é, sobretudo, com o advento desta e com a digitalização da atividade administrativa que mais facilmente se efetiva correntemente a “*administração aberta*.” Neste ponto, a crescente digitalização da tomada de decisões administrativas (da própria atuação da administração pública) facilita a transparência e a efetividade do princípio da “*administração aberta*.”

Esse regime consagrado na LADA, com efeito, concretiza a transparência através da disponibilização e da garantia de acesso à informação pública. Tal significa – utilizando a terminologia legal – que aquele acesso tem por objeto os denominados “*documentos administrativos*.” Ora, por “*documento administrativo*” [cf. artigo 3.º, n.º 1, alínea *a*) da LADA] entende-se “*(...) qualquer conteúdo, ou parte desse conteúdo, que esteja na posse ou seja detido em nome dos órgãos e entidades referidas (no artigo 4 da LADA), seja o suporte de informação sob forma escrita, visual, sonora, eletrónica ou outra forma material*”, neles se incluindo, designadamente, aqueles relativos a:

- i*) Procedimentos de emissão de atos e regulamentos administrativos; *ii*) Procedimentos de contratação pública, incluindo os contratos celebrados; *iii*) Gestão orçamental e financeira dos órgãos e entidades; *iv*) Gestão de recursos humanos, nomeadamente os dos procedimentos de recrutamento, avaliação, exercício do poder disciplinar e quaisquer modificações das respetivas relações jurídicas.

As entidades que detêm informação pública relevante – ou seja, documentos administrativos – e, estão, portanto, sujeitas à aplicação do regime em causa, são elencadas no n.º 1, do artigo 4.º da LADA. Esta norma, definindo o âmbito subjetivo de aplicação do regime em consideração, é bastante extensiva, incluindo órgãos quer da administração central, quer da administração pública autárquica, institutos públicos, empresas públicas municipais, intermunicipais, regionais ou locais, associações e fundações públicas, mas igualmente privadas, na medida em que a enunciação abrange, nomeadamente, “*associações ou fundações de direito privado nas quais órgãos ou entidades públicas (os demais órgãos previstos nesse mesmo número 1, do artigo 4) exerçam poderes de controlo, de gestão ou designem, direta ou indiretamente, a maioria dos titulares dos órgãos de administração, de direção ou de fiscalização*” [cf. alínea *g*) do n.º 1, do artigo 4 da LADA].

Há uma consideração material do que seja a atividade administrativa para, a partir de tal atividade, qualificar como informação pública relevante aquela que estiver na posse do órgão que prossiga tal atividade. Nesse sentido, compreende-se

¹⁵ Tal como enunciado pelo Tribunal Constitucional (português), o artigo 268.º da Constituição, “*veio consagrar, no plano constitucional, o princípio da administração aberta ou do arquivo aberto, que permite a qualquer cidadão o acesso a arquivos e registos administrativos. Na raiz do princípio está a pretensão de substituir e superar o princípio da arcana praxis ou o princípio do segredo, característico de um modelo de Administração Pública autoritária, burocrática, fechada sobre si mesmo, que decide em segredo, pelo princípio geral da publicidade ou da transparência, próprio de uma Administração aberta, participada, que age em comunicação com os administrados*.” Cf. Acórdão do Tribunal Constitucional n.º 117/2015, 12 de fevereiro de 2015, Processo 686/12, n.º 11 da respetiva “Fundamentação”, acedido em 19 de março de 2025, <https://files.diariodarepublica.pt/2s/2015/04/067000000/0840308415.pdf>.

a alínea i) do n.º 1, do artigo 4.º da LADA, elencando, ainda, no âmbito subjetivo de aplicação do regime de acesso à informação pública (acesso aos “*documentos administrativos*”), a informação detida por “*outras entidades no exercício de funções materialmente administrativas ou de poderes públicos, nomeadamente as que são titulares de concessões ou de delegações de serviços públicos.*”

8. Estas notas não pretendem analisar o regime instituído pela LADA.¹⁶ No entanto, sem empreender, por agora, essa análise, importa sublinhar a transparência (nomeadamente, a sua concretização através da densificação normativa do “*princípio da administração aberta*”) como fator estruturante da construção e da vigência de um ecossistema anticorrupção, sendo, na perspetiva assinalada, indissociável (no fundo, “*duas faces da mesma moeda*”) da cultura e da prática ordinária de prestação de contas e da responsabilidade, individual e institucional. Fatores externos, cuja respetiva consideração é determinante quer para a conceção, quer para a implementação de uma política pública de combate à corrupção.

A crescente digitalização da atividade administrativa tem, pelo menos, a virtude de permitir um escrutínio mais fácil dessa atividade – nomeadamente, pela via do acesso aos documentos administrativos (aplicação da LADA e de regimes similares àquele que a LADA consagra). Nessa perspetiva, a digitalização pode favorecer a criação do mencionado ecossistema anticorrupção e fortalecer o Estado de direito.

¹⁶ Cf. *Texto de apresentação de Alberto Oliveira, 1993/94 - 2023/24: Três décadas de Lei de Acesso aos Documentos Administrativos (LADA) 30 anos de Comissão de Acesso aos Documentos Administrativos (CADA)*, CADA – Comissão de Acesso aos Documentos Administrativos, acedido em 19 de março de 2025, <https://www.cada.pt/noticias/1993-94-2023-24-tres-decadas-de-lei-de-acesso-aos-documentos-administrativos-lada-30-anos-de-comissao-de-acesso-aos-documentos-administrativos-cada>. Cf., ainda, José Renato Gonçalves, *Acesso à informação das entidades públicas* (Coimbra: Almedina, 2002).

PAINEL III

**FUNCIONAMENTO DO SISTEMA DE JUSTIÇA
E INDEPENDÊNCIA JUDICIAL – DESAFIOS AO
ESTADO DE DIREITO DIANTE DA TRANSIÇÃO
DIGITAL**

PAINEL III

Funcionamento do sistema de justiça e independência judicial – desafios ao Estado de direito diante da transição digital

Ana Cardoso *

Diogo Morgado Rebelo **

O princípio do Estado de direito – decorrente do artigo 2.º da Constituição da República Portuguesa (CRP) e do artigo 2.º do Tratado da União Europeia (TUE) – implica que os cidadãos estejam protegidos contra qualquer poder (do Estado ou de outras “constelações políticas”)¹ e serve como garante da democracia e dos direitos e liberdades dos cidadãos.² O Estado de direito legitima, controla e modera o exercício do poder público, submetendo-o a normas e procedimentos que permitem ao cidadão perscrutar – e, porventura, impugnar – as decisões tomadas pelas autoridades públicas.³

Com a designada transição digital, os sistemas de justiça são chamados a responder consistentemente às alterações substanciais da sociedade – que se vê a braços com desafios tecnológicos cujas consequências ainda são inescrutáveis. O Direito tem um tempo de reação e adaptação lento – que não se compadece com as exigências de uma sociedade eminentemente digitalizada. Mas, ao mesmo tempo, não se pode escusar de a regular.⁴

A introdução de tecnologias digitais na prática diária dos sistemas judiciais tem reconhecidas vantagens identificadas pela doutrina. Estas prendem-se sobretudo com o aumento da eficiência, reduzindo o peso processual e financeiro para o contribuinte. Prendem-se ainda com o acesso à justiça, através dos sistemas de “e-justice”, através de plataformas para a mediação de litígios que facilitem os procedimentos de citação e notificação, assim como a recolha de provas que simplifique a cooperação entre Estados, autoridades judiciais e cidadãos nos litígios transfronteiriços. Designadamente, a doutrina ainda refere que a introdução de algoritmos de Inteligência Artificial (IA) poderia incrementar a imparcialidade nas decisões judiciais, assim como assistir na administração da justiça – por exemplo,

* Estudante de doutoramento em Ciências Jurídicas Públicas na Escola de Direito da Universidade do Minho. Mestre em Direito da União Europeia.

** Bolseiro da Fundação para a Ciência e Tecnologia (FCT), com a referência 2023.01496.BD e estudante de doutoramento em Ciências Jurídicas Privativas na Escola de Direito da Universidade do Minho.

¹ Alessandra Silveira, *Fundamentos jurídico-políticos da integração europeia* (Coimbra: Coimbra Editora, 2024), 110.

² Diário da República, “Estado de direito democrático”, *Lexionário*. Disponível em <https://diariodarepublica.pt/dr/lexionario/termo/estado-direito-democratico>. Comissão Europeia, “O que é o Estado de direito?”. Disponível em https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/what-rule-law_pt.

³ Diário da República, “Estado de direito democrático”, *Lexionário*. Disponível em <https://diariodarepublica.pt/dr/lexionario/termo/estado-direito-democratico>.

⁴ Nuno Coelho (coord.), *Agenda da Reforma da Justiça – uma reflexão aberta e alargada do judiciário* (Coimbra: Almedina, 2023), 266-269.

intervindo nos procedimentos de alocação de casos. Tudo isto conduziria a uma maior abertura e, consequentemente, maior democratização da justiça.⁵

No que toca à IA, especificamente, já é reconhecida como uma ferramenta capaz de organizar e processar informação, reconhecendo padrões em documentos; mas também capaz de aconselhar, podendo ser útil para as partes comporem uma solução que previna disputas em tribunal; é ainda capaz de fazer previsões, o que pode ser perspetivado como uma forma de reduzir o risco e a incerteza.⁶

Contudo, como foi reconhecido na “*Agenda da Reforma da Justiça*” – apresentada em 2023 pela Associação Sindical dos Juizes Portugueses (ASJP) –, a digitalização levanta necessidades de normação que regulem esta nova realidade, uma vez que as categorias jurídicas existentes não são suficientes para lhe fazer face.⁷ Ademais, a crescente utilização de sistemas de IA em atividades judiciais – enquanto ferramentas de apoio à decisão – tem levantado debates profundos sobre a preservação da independência judicial e os riscos associados a potenciais interferências externas.

Diante deste cenário, colocam-se algumas questões. Como se pode conciliar o controlo sobre os sistemas de IA no âmbito judicial, caso sejam desenvolvidos por entidades privadas contratadas pelo Estado, com a necessidade de preservar a independência judicial e evitar a suspeita de interferências do poder executivo e legislativo? A atual regulamentação de IA na UE é suficiente para proteger a independência judicial?⁸ Como se pode garantir que os diversos órgãos de controlo – como sejam, a autoridade notificadora e as autoridades nacionais competentes – operem de forma totalmente independente e livre de influências governamentais ou legislativas em finalidades previstas como a utilização da IA no sistema judiciário?

Uma outra questão relevante neste âmbito prende-se com o enquadramento prático da implementação dos sistemas de IA no sistema de justiça. O Tribunal de Justiça da União Europeia (TJUE) afirmou a independência judicial – uma manifestação do princípio do Estado de direito (artigo 2.º do TUE) e, mais concretamente, do princípio da tutela jurisdicional efetiva (artigo 19.º, n.º 1, segundo parágrafo do TUE) – como uma dimensão essencial para o funcionamento da União Europeia (UE) enquanto União de direito. Sistemas judiciais que não cumpram a independência judicial (segundo os critérios definidos pelo TJUE) violam o princípio do Estado de direito.⁹

A intervenção de juizes independentes para resolver disputas judiciais é essencial para a justiça processual – e contribui para a confiança pública e para a legitimidade dos tribunais e das suas decisões. Os juizes, pela natureza da sua posição, estão particularmente dotados de legitimidade democrática necessária para decidir. Assim,

⁵ Andrii Shabalin *et al.*, “Use of digital technologies in judicial proceedings in some countries of Europe and USA”, *Petita* 9, no. 1 (2024): 3.

⁶ A. D. Reiling, “Courts and artificial intelligence,” *International Journal for Court Administration* 11, no. 2 (2020): 3-5. Disponível em <https://doi.org/10.36745/ijca.343>.

⁷ Coelho, *Agenda da Reforma da Justiça*, 271.

⁸ 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 diversos regulamentos e diretivas, *Jornal Oficial da União Europeia*, L, 13 de junho de 2024 (Regulamento Inteligência Artificial).

⁹ Acórdão *A. K. contra Krajowa Rada Sądownictwa e CP e DO contra Sąd Najwyższy*, 19 de novembro de 2019, C-585/18, C-624/18 e C-625/18, EU:C:2019:982, 118; Acórdão *Associação Sindical dos Juizes Portugueses contra Tribunal de Contas*, 27 de fevereiro de 2018, C-64/16, EU:C:2018:117, 41-44. Cf. Alessandra Silveira, Pedro Froufe, Sophie Perez, Joana Abreu, “União de direito para além do direito da União – as garantias de independência judicial no acórdão Associação Sindical dos Juizes Portugueses”, *Julgar* (2018): 7-8. Disponível em <https://julgar.pt/uniao-de-direito-para-alem-do-direito-da-uniao-as-garantias-de-independencia-judicial-no-acordao-associacao-sindical-dos-juizes-portugueses/>.

os juízes não podem delegar noutrem o julgamento dos casos que têm em mãos – e têm de assegurar sempre o controlo funcional e a comunicação entre eles e os seus assistentes, independentemente de a assistência ser prestada por um ser humano ou por um sistema de IA.¹⁰ O uso de centros de dados para digitalizar decisões judiciais, o processo de seleção de dados de treino para sistemas de IA, e o próprio desenho do algoritmo podem suscitar dúvidas sobre a independência dos tribunais.¹¹

Assim, é importante perscrutar de que modo as reformas judiciais que envolvem IA devem ser implementadas, a fim de evitar a criação de regimes de responsabilidade que possam influenciar negativamente a independência dos juízes. Sobretudo no que toca à sentença que põe termo ao processo, apesar das alegadas vantagens da introdução de ferramentas algorítmicas, questiona-se se seria uma decisão suscetível de ser influenciada por “*machine learning*.” O fenómeno “*garbage in, garbage out*” – ou seja, a introdução de conceitos discriminatórios e problemáticos resultantes da informação histórica utilizada para programar estes algoritmos¹² – conduz a resultados que são inaceitáveis num ordenamento jurídico baseado no Estado de direito.¹³

Adicionalmente, a complexidade técnica da IA acarreta a necessidade de conhecimento especializado nos tribunais para supervisionar o funcionamento destes sistemas e identificar problemas potenciais. Identificam-se aqui três cenários ou soluções possíveis: *i*) especialização dos juízes: o que impõe determinar quais conhecimentos e competências são necessários para lidar com questões de IA; *ii*) suporte técnico especializado: o que torna crucial a garantia de independência para técnicos que operem no campo judicial; ou *iii*) regime de responsabilidade conjunta: o que parece apropriado, dado o papel compartilhado entre juiz e técnico, mas sempre salvaguardando a independência da função judicial.¹⁴

A crescente integração da IA nos sistemas judiciais desafia não apenas os modelos tradicionais de tomada de decisão, mas também as competências exigidas dos magistrados. A utilização de sistemas avançados de IA como ferramentas de apoio à decisão – ou como elementos integrados ao processo judicial – exige que os juízes desenvolvam novos conhecimentos técnicos, especialmente para lidar com os desafios éticos, jurídicos e práticos impostos pela tecnologia. Deverá passar a ser exigida a formação técnica dos juízes? Em caso afirmativo, que conhecimentos deverão ser adquiridos e que competências, em termos de *know-how*, são consideradas suficientes para lidar com os “*pecados capitais*” da IA sem dependerem exclusivamente de peritos?¹⁵

Adicionalmente, tendo em conta as assimetrias internas e externas dentro do espaço da UE, sobretudo entre as capacidades tecnológicas e financeiras dos judiciários dos Estados-Membros, como pode garantir-se a igualdade dos cidadãos

¹⁰ Thomas Julius Buocz, “Artificial intelligence in court – legitimacy problems of AI assistance in the judiciary”, *Retskraft – Copenhagen Journal of Legal Studies* 2, no. 1 (2018): 47.

¹¹ Giulia Gentile, *AI in the courtroom and judicial independence: an EU perspective* (CIVICA Research, 2022), 2. Disponível em <https://ssrn.com/abstract=4198145>.

¹² Neste sentido, refira-se o emprego do *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS) nos Estados Unidos da América, uma ferramenta usada para prever a probabilidade de reincidência em casos criminais. Ao utilizar dados do passado, o COMPAS sobrestima sistematicamente a reincidência entre arguidos afro-americanos em comparação com americanos caucasianos. Cf. D. Reiling, “Courts and artificial intelligence”, 2-5.

¹³ Jasper Ryberg, “Criminal justice and artificial intelligence: how should we assess the performance of sentencing algorithms?”, *Philosophy & Technology*, 37, no. 9 (2024): 2-3.

¹⁴ Gentile, “AI in the courtroom”, 2-3.

¹⁵ Gentile, “AI in the courtroom”, 2.

no acesso à justiça e, consequentemente, de garantia dos seus direitos fundamentais? (especialmente numa perspetiva de solidariedade e de coesão necessárias ao funcionamento do projeto europeu, e tendo em conta o princípio de base da transição digital, qual seja, “*leave no one behind*”).

Tendo em conta a natureza específica da UE – que se baseia num diálogo entre todos os ordenamentos jurídicos dos Estados-Membros, havendo uma exigência de que que norma europeia, nomeadamente no que toca à proteção de direitos fundamentais, seja aplicada da mesma forma em todo o espaço europeu¹⁶ –, importa questionar se a existência de vários produtos de IA a funcionar em ordenamentos jurídicos que se pretendem harmonizados seria uma boa opção.

A UE afirma querer prosseguir uma transição digital sustentável e centrada no ser humano, onde ninguém é deixado para trás, todos gozam de liberdade, proteção e equidade.¹⁷ Para isso foi assinada pelos presidentes da Comissão, do Parlamento Europeu e do Conselho a “*Declaração Europeia sobre os Direitos e Princípios Digitais*”, cujos princípios se articulam em torno de seis eixos: *i)* colocar as pessoas e os seus direitos no centro da transformação digital; *ii)* apoiar a solidariedade e a inclusão; *iii)* garantir a liberdade de escolha em linha; *iv)* promover a participação no espaço público digital; *v)* aumentar a segurança, a proteção e a capacitação das pessoas (especialmente dos jovens); *vi)* promover a sustentabilidade do futuro digital.¹⁸

Reconhece-se que a introdução da IA nos tribunais é inevitável, mas as reformas devem respeitar o princípio da independência judicial e, de forma mais alargada, o princípio do Estado de direito – pedra de toque dos ordenamentos jurídicos da UE e dos seus Estados-Membros. A cooperação leal entre as instituições da UE e seus Estados-Membros neste domínio é essencial para preservar os valores constitucionais europeus, incluindo um judiciário independente.

O referido Regulamento IA adota uma abordagem baseada no risco e estabelece regras harmonizadas, proporcionando aos criadores e implementadores de IA requisitos e obrigações quanto as utilizações específicas da IA.¹⁹ Neste âmbito, pode perspetivar-se o surgimento de questões ao nível da sua interpretação e efetiva aplicação – que, eventualmente, o TJUE terá que resolver.

Das respostas orais às inquietações colocadas aos intervenientes no painel III – cujos textos são publicados de seguida –, depreende-se que partilham de algumas das preocupações de que demos conta *supra*. Por exemplo, da resposta do Juiz Conselheiro Luís Mendes no que toca à implementação e controle da utilização da IA, fica a ideia de que deve ser regulamentada, em termos confiáveis sem intromissão do executivo – pois tendo em conta a disponibilização muito alargada de fundos do Plano de Recuperação e Resiliência (PRR) para a transição digital, poderá haver um excessivo entusiasmo que conduzirá à implementação de ferramentas erradas. É importante que esta implementação seja supervisionada pelos profissionais da área – nomeadamente por juizes – que sabem realmente como melhor proteger os direitos fundamentais dos cidadãos perante as necessidades de eficiência do sistema. Adicionalmente, é necessária uma vigilância contínua dessas ferramentas,

¹⁶ Miguel Poiars Maduro, *A Constituição plural* (São João do Estoril: Princípia, 1.ª ed., 2006), 9–10.

¹⁷ Comissão Europeia, “*Década digital da Europa*.” Disponível em <https://digital-strategy.ec.europa.eu/pt/policies/europes-digital-decade>.

¹⁸ Comissão Europeia, “*Direitos e princípios digitais europeus*.” Disponível em <https://digital-strategy.ec.europa.eu/pt/policies/digital-principles>.

¹⁹ Comissão Europeia, “*Regulamento Inteligência Artificial*.” Disponível em <https://digital-strategy.ec.europa.eu/pt/policies/regulatory-framework-ai>.

nomeadamente através de procedimentos de certificação e fiscalização.

Na mesma senda, Joana Covelo Abreu defende que a coordenação entre os sistemas judiciais, à luz dos novos desenvolvimentos de implementação da justiça eletrónica no âmbito da cooperação judiciária, tem beneficiado de grandes investimentos europeus – de fundos profundamente vocacionados àquilo que é a digitalização –, a fim de transpor as assimetrias territoriais e tornar os sistemas comunicáveis. No fundo, agora é que vai começar a ser visível aquilo que foi a aposta da UE na digitalização do sistema, pois há uma motivação também económica, de apoio significativo aos diversos Estados-Membros, e auxiliada por uma dimensão tecnológica da interoperabilidade. Assim promove-se uma interoperabilidade semântica, organizacional e legal. A oradora explicou ainda que, nos termos do n.º 8 do artigo 74.º do Regulamento IA, as responsabilidades de supervisão podem caber à Comissão Nacional de Proteção de Dados (CNPD) ou a entidades administrativas semelhantes. Sublinhou que as decisões dessas autoridades continuam a estar sujeitas a controlo judicial, garantindo a independência institucional.

Tiago Sérgio Cabral manifestou a sua preocupação com a confiança europeia na autoavaliação da conformidade, alertando para a falta de independência genuína. Criticou as sugestões que têm vindo a ser propaladas quanto à possível atribuição de funções de supervisão à ANACOM em Portugal, questionando a sua capacidade de supervisionar a IA em ambientes judiciais complexos. Apelou, em contrapartida, à aprovação de quadros nacionais de supervisão específicos – logo, adaptados ao ecossistema jurídico-tecnológico.

Nuno Coelho reforçou as preocupações expostas, sublinhando a necessidade de distinguir entre a utilização da IA em tarefas administrativas e a sua potencial influência nas decisões judiciais, sendo que esta última coloca riscos significativos para a autonomia. Abordando o desenvolvimento endógeno de ferramentas como o *Magistratus* e *MP Codex* em Portugal, cotejou o “estado da arte” nacional com modelos controversos como o COMPAS nos EUA e os quadros disciplinares chineses – que considerou antitéticos à luz dos padrões democráticos.

Finalmente, Paulo Novais abordou a questão da transparência da IA na tomada de decisões judiciais e na atribuição de processos, fazendo uso de uma metáfora em que comparou as ferramentas de IA a telescópios ou raios X – extensões ou ferramentas que melhoram a perceção, mas não substituem o julgamento humano. Alertou para o facto de não se dever sobrevalorizar excessivamente a *explicabilidade* como única salvaguarda – e insistiu que os juízes devem manter a responsabilidade final.

Embora reconhecendo o seu potencial para aumentar a eficiência judicial, os oradores convergiram na necessidade de serem aprovadas e implementadas salvaguardas sólidas para defender o Estado de direito, a transparência e, especialmente, a independência judicial na transição digital na UE. Nos textos que se seguem, os oradores vão explorar, numa abordagem crítica e interdisciplinar, os desafios emergentes da transição digital nos sistemas de justiça. Através das suas intervenções, irão abordar questões fundamentais sobre regulamentação, supervisão, transparência e igualdade no acesso à justiça na UE, num momento em que a IA se afirma como vetor de transformação profunda do exercício jurisdicional.

Funcionamento do sistema de justiça e independência judicial – desafios ao Estado de direito e aos tribunais diante da transição digital

*Luís Azevedo Mendes**

Saúdo este Congresso e os seus organizadores pela atenção dada ao importante tema, tão malcuidado, do *Estado de direito e transição digital*. Tão malcuidado em especial na dimensão que toca o desempenho do poder judicial e, também, o desempenho dos sistemas de justiça conexos que o alimentam (como é o caso do Ministério Público, das polícias e dos órgãos estatais de fiscalização ou supervisão).

1. A transição digital como uma questão de governação e separação de poderes

No nosso país, Portugal, no discurso que faz caminho desde há vinte anos, com expressividade maior nas leis de organização judiciária de 2008 e 2013, os tribunais e os seus sistemas de governação privativos são projetados como organizações autónomas e competentes para a rigorosa utilização dos recursos afetos à sua missão, nos limites da separação e da independência do poder judicial. E nesse contexto, ninguém negará que a operação tecnológica digital se transforma cada vez mais num recurso imprescindível para a jurisdição, uma vez estabelecida no judiciário a utilização intensiva e extensiva das modernas ferramentas tecnológicas e a desmaterialização dos processos, alojados e comunicáveis em rede.

Transição digital nos tribunais é, por conseguinte, matéria de organização judiciária, matéria respeitante à sua governação.

Organização judiciária é, por sua vez, matéria adjectiva com incidência constitucional, justamente porque é necessária para o funcionamento do Estado de direito em cuja arquitetura o poder judicial é, tem de ser, independente nos princípios e separado por instrumento.

E se assim é, no respeito devido à separação de poderes, é imperativa a autonomia do poder judicial quanto à governação, desenvolvimento e também segurança das suas redes informáticas e plataformas tecnológicas.

Há muito que o Conselho Superior da Magistratura (CSM) português luta por ela e a defende nas soluções que preconiza no dia-a-dia prático para as pequenas e grandes crises de funcionamento do sistema. Há muito, contudo, que infelizmente o legislador nacional e o governo da República a tendem ignorar, por via da distração ou pela via da incapacidade de mudar.

Há muito, também, que na Europa em que nos integramos essa é a abordagem para as boas práticas-padrão quanto ao respeito do Estado de direito. E quando

* Juiz Conselheiro, Vice-presidente do Conselho Superior da Magistratura (Portugal).

essa abordagem é desrespeitada têm ocorrido “*crises relacionais*” de consequências sistêmicas desqualificadoras.

2. Lições da crise na Roménia: riscos para a independência do poder judicial

Não há melhor para ilustrar o que digo do que a observação sobre a recentíssima crise na Roménia que opõe o Conselho Superior da Magistratura romeno ao governo do seu país e que suscitou uma assertiva declaração de princípios por parte do Conselho Executivo da Rede Europeia dos Conselhos de Justiça,¹ de 15 de novembro de 2024, sobre o envolvimento dos conselhos do judiciário na governação das tecnologias de informação no judiciário.

O estado de crise iniciou-se em agosto de 2024 quando o ministério da justiça romeno iniciou um processo de instalação dos equipamentos informáticos dos tribunais – então alojados e geridos ao nível de cada tribunal – num sistema centralizado alojado e gerido pelo ministério, sem que tenha havido debate e consentimento informado por parte do Conselho romeno. Segundo este, a medida conduzia à apropriação de todos os computadores dos juízes e funcionários, bem como de toda a base de dados do judiciário e de todos os dados relativos aos processos dos tribunais, num servidor do ministério, gerido e à disposição de entidade do poder executivo, levantando sérias preocupações quanto à independência do poder judicial pelo risco de acesso não autorizado a dados de arquivos e informações confidenciais tratadas pelos tribunais.

Por tudo isso, o Conselho Superior da Magistratura romeno considerou que a centralização comprometia o princípio da separação de poderes e o princípio da independência judicial e, para a proteger, decidiu suspender o processo de centralização e emitiu recomendações para a reconfiguração do sistema de modo que o controle fosse mantido no judiciário.

Essencialmente, o Conselho acentuou que estava em causa a segurança dos dados, uma vez que com a qualidade de gestor e administrador do sistema, ao menos teoricamente, os dados processuais poderiam ser facilmente alterados pelo ministério da justiça sem possibilidade de oposição ou conhecimento dessas mudanças e até as auditorias de controlo seriam feitas pelo ministério, não deixando ao Conselho, em caso de suspeita de acesso não autorizado, meios para auditar diretamente a suspeita. Por outro lado, sendo o Conselho a autoridade responsável pelos dados pessoais tratados, ser-lhe-ia praticamente impossível cumprir as atribuições correspondentes, uma vez que deixaria de ser o titular físico dos dados e não teria acesso direto aos mesmos, mas apenas um acesso intermediado.

À data deste Congresso em que participo o impasse romeno ainda não foi superado, mas o Conselho Executivo da Rede Europeia dos Conselhos de Justiça, como já disse, emitiu uma forte declaração na qual reafirmou posição já antes expressa e sublinhou que os Conselhos do Judiciário, sujeitos ao seu mandato, devem ter poder de decisão tanto em termos da gestão dos dados do judiciário (também tendo presentes as suas funções relativas à proteção de dados pessoais), como sobre as

¹ Rede (ENCJ) que integra o nosso país, a Bélgica, Bulgária, Croácia, Dinamarca, Eslováquia, Eslovénia, Espanha, Grécia, Hungria, Irlanda, Itália, Letónia, Lituânia, Malta, Holanda, Polónia, Reino Unido e Roménia; e tem como observadores: Albânia, Alemanha, Áustria, Chipre, República Checa, Estónia, Finlândia, Luxemburgo, Macedónia, Montenegro, Noruega, Sérvia, Suécia, Turquia e, também, o Tribunal de Justiça da União Europeia.

aplicações que são usadas no judiciário. Por conseguinte, afirmou que os processos de reforma quanto às tecnologias de informação no judiciário devem apenas ser realizados com o consentimento dos conselhos judiciários, em linha com seu papel de garantes da independência do poder judicial.

E a este respeito, lembrou as seguintes referências relevantes:

- de acordo com o § 24 do Parecer n.º 24/2021 do Conselho Consultivo dos Juízes Europeus,² o CCJE observou a crescente importância das tecnologias de informação para o futuro do judiciário e recomendou que, onde existam, os conselhos do judiciário devem ter um papel nesse campo para proteger adequadamente a independência judicial e garantir a qualidade do trabalho dos juízes;
- de acordo com o § 57 do Parecer n.º 26/2023 do CCJE,³ as medidas eficazes de segurança e proteção de dados exigem uma supervisão eficaz e independente da tecnologia usada pelo judiciário. Tal supervisão pode representar um risco significativo para a independência do poder judicial se for feita pelo executivo ou por um órgão regulador, como um Supervisor Nacional de Proteção de Dados, em vez de por órgão dentro do judiciário;
- de acordo com o § 9 da Declaração de Roma de 14 de junho de 2024 da Rede Europeia de Conselhos de Justiça,⁴ os conselhos judiciários devem desempenhar um papel ativo e de liderança na avaliação de soluções de inteligência artificial (IA) propostas para uso do judiciário e devem também definir os padrões para o uso de tecnologias digitais, incluindo aquelas tecnologias de IA.

3. A realidade portuguesa: desafios tecnológicos e constrangimentos

Feita esta breve ilustração de atualidade europeia, não exagerarei se disser que a realidade portuguesa no que toca às plataformas tecnológicas dos tribunais não é melhor do que a da Roménia.

Na realidade, no nosso país o poder executivo detém desde sempre a propriedade e o domínio total dos sistemas. Sem que haja qualquer consulta ou discussão sobre essa titularidade com os órgãos e governo do poder judicial, designadamente com o CSM.

O resultado vai de um desconforto ruidoso até a uma tensa conversa de surdos. O IGFEJ (Instituto de Gestão Financeira e das Estruturas da Justiça), o organismo do ministério da justiça responsável por esse domínio inapropriado, representa hoje uma “*bated brand*” para todo o judiciário [e falo dos sentimentos que vou colhendo no CSM, no CSTAF (Conselho Superior dos Tribunais Administrativos e Fiscais) e na PGR (Procuradoria-Geral da República), designadamente], acabando por traduzir-se num peso morto, sem dinâmica de progresso. Porquê? Em razão da sua ilegitimidade no plano dos princípios, como a primeira das respostas, e depois em razão da sua falta de empatia funcional, porque não se assume como mero prestador institucional de serviços como, quando muito, seria esperado que fosse. Por consequência, como

² Conselho Consultivo dos Juízes Europeus, Parecer n.º 24/2021, de 5 de novembro de 2021, <https://rm.coe.int/opinion-no-24-2021-of-the-ccje/1680a47604>.

³ Conselho Consultivo dos Juízes Europeus, Parecer n.º 26/2023, de 1 de dezembro de 2023, <https://rm.coe.int/ccje-opinion-no-26-2023-final/1680adade7>.

⁴ Rede Europeia de Conselhos de Justiça, Declaração de Roma “Acesso à Justiça”, de 14 de junho de 2024, https://pgwrk-websitemedia.s3.eu-west-1.amazonaws.com/production/pwk-web-encj2017-p/Adopted_Final%20TEXT%20.pdf.

terceira das respostas, em razão da incapacidade de perceber as necessidades dos tribunais, já que estes porque não são ouvidos como clientes, não lhe reconhecem autoridade de pertença e não aceitam uma cadeia hierárquica externa que é a da administração pública à qual não pertencem e da qual são constitucionalmente separados.

Este é um, portanto, um constrangimento de delito na transição digital do estado de direito que é necessário identificar, enfrentar e superar.

Demasiadas vezes se sucedem efetivas ou possíveis intrusões e fugas de dados informativos nos processos judiciais, algumas conhecidas, outras desconhecidas, sem qualquer possibilidade de controlo por sistema de auditoria a cargo do judiciário, como tal previsto na lei.

Mais do que a segurança relativa aos dados, o judiciário não tem qualquer conhecimento, controlo ou clara competência para a auditar, incluindo a auditoria sobre a infraestrutura crítica que suporta os servidores que operam a plataforma informática de tramitação processual. Em 2023, essa plataforma parou durante quase três dias porque uma retroescavadora em obra danificou cabos de fibra ótica em zona pública. Foi revelada a inexistência ou insuficiência de redundâncias que recuperassem a pronta normalidade. A governação do poder judicial, o CSM, mostrou séria inquietação, solicitou informação que durante meses não lhe foi fornecida e quando o foi tal aconteceu a contragosto.

Quando se fala em intrusões ou fugas, pensa-se quase só na questão do segredo de justiça processual penal. Mas uma outra dimensão do segredo é especialmente tutelada pelo moderno sistema de proteção de dados pessoais.

E é também por ele que se torna mais urgente eliminar as zonas de penumbra, concorrência e sobreposição na responsabilidade sobre a gestão das plataformas tecnológicas no judiciário. Não é apenas uma questão de bandeira – a da separação de poderes –, é também a questão da adulteração maliciosa dos procedimentos.

E é também a questão de acautelar a transição digital de que falamos, garantindo a correta definição dos padrões para o uso de tecnologias digitais, incluindo as novas tecnologias de inteligência artificial de rápida evolução e com rápida possibilidade de adesão por parte de um enorme conjunto de operadores judiciais.

4. Dados do sistema judicial, revisão legislativa e a proposta do CSM

Há 15 anos, a Lei n.º 34/2009 estabeleceu o chamado “*regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial*.” Instituiu uma *Comissão para a Coordenação da Gestão dos Dados Referentes ao Sistema Judicial*, integrada pelo CSM, CSTAF e PGR, entre outras entidades alheias ao judiciário. O CSM apareceu como responsável de gestão de dados nos processos dos tribunais judiciais, mas com competências quase irrelevantes. Tal comissão podia promover auditorias de segurança e definir algumas orientações. Porém, todo o sistema de recolha e tratamento automatizado de dados ficava no ministério da justiça: a conceção, o desenvolvimento e a manutenção das aplicações para a tramitação dos processos e gestão do sistema, incluindo a análise, implementação, suporte e segurança.

Essa lei, ainda em vigor, mas tão desajeitada, foi ignorada por todos, conselhos, ministério da justiça e Assembleia da República. A Comissão de Coordenação instituída chegou a ser nomeada, tomou posse em 2010, reuniu por uma vez no

dia da posse, não mais reunindo, e ao fim do período de quatro anos do mandato previsto não foi renovada. Não houve empenhamento político sério para isso...

Entretanto, o Regulamento Geral sobre a Proteção de Dados Pessoais (RGPD), aplicável desde 2018, introduziu uma nova realidade normativa e uma nova pressão. Sendo de aplicação direta, toda a sua matéria regulatória prevalece sobre a Lei n.º 67/98 e, também, sobre a Lei n.º 34/2009. Na nova norma, as competências da autoridade de controlo nacional, no nosso caso a Comissão Nacional de Proteção de Dados, não abrangem o tratamento de dados pessoais na função jurisdicional, mas é afirmado que este deve ser confiável e de acordo com os padrões do Regulamento.

O que veio abrir a necessidade de rever a lei de tratamento de dados referentes ao sistema judicial. Em 2019, nesse processo de revisão, a Assembleia da República aprovou a Proposta de Lei n.º 126/XIII/3.^a, origem do Decreto n.º 333/XIII que veio a ser objeto de veto por parte do Presidente da República, depois duma tomada de posição conjunta do CSM e da PGR que alertaram para a existência de desconformidade com os imperativos da separação de poderes e do Estado de direito, existindo um manifesto risco de desconformidade e de desrespeito pelo primado do direito da União. O diploma previa designadamente a criação de uma *Comissão para Gestão da Informação do Sistema Judiciário* presidido pelo ministro da justiça, envolvendo sérios riscos de uma indevida ingerência de entidade administrativa e/ou governamental no tratamento dos dados judiciais, perigando a defesa da independência judicial, no sentido amplo da interpretação fixada pela jurisprudência do Tribunal de Justiça da União Europeia. No diploma não era criado o organismo independente no âmbito do sistema judicial para fiscalização e controlo do tratamento dos dados pelos tribunais, como imposto pelo RGPD.

Falta rever a lei, após o veto presidencial. No tardar da iniciativa legislativa, pelo governo ou pelo parlamento, o CSM construiu uma proposta finalizada em 2024 que conjuga todos os órgãos jurisdicionais visados, não só o CSM, mas também os tribunais administrativos e fiscais, o Tribunal Constitucional, o Ministério Público e o Tribunal de Contas. Esta proposta colheu os seus contributos e já foi apresentada ao parlamento, ao governo e ao Presidente da República. A proposta prevê uma alta *Autoridade da Proteção de Dados Judiciais* como organismo específico de supervisão das operações de tratamento efetuadas pelos tribunais no exercício da função jurisdicional e pelo Ministério Público no âmbito das suas competências, integrado por juízes designados pelo CSM, pelo CSTAF, pelo Tribunal Constitucional e pelo Tribunal de Contas, para além de um procurador designado pela PGR.

Esta proposta contém já, assim, um enquadramento para uma nova autonomia do judiciário na conceção, desenvolvimento e manutenção das aplicações para a tramitação dos processos e gestão do sistema, incluindo na implementação e segurança e abre caminho para uma transição judicial na justiça do Estado de direito de acordo com os modelos europeus de elevada fiabilidade.

5. Caminho para a autonomia tecnológica nos tribunais portugueses

Em Portugal, no futuro da administração e gestão das plataformas tecnológicas do poder judicial, o IGFEJ e o ministério da justiça não podem deter mais do que o domínio sobre os servidores de rede, os quais de resto servem também as aplicações e os dados dos organismos do ministério da justiça e não apenas os dos tribunais.

O domínio e as demais competências e atributos necessários para a governação tecnológica do suporte automatizado da atividade jurisdicional, devem separadamente pertencer a cada um dos conselhos judiciais do poder judicial. O que significa que têm de ter o domínio proprietário das respetivas plataformas, ou seja, dos servidores de aplicações e dos servidores de bases de dados, devendo caber a eles a análise e desenvolvimento dos seus conteúdos operativos, porque só eles saberão construir ou adotar o que melhor serve o seu trabalho.

A autonomia sustentada nessas novas atribuições induzirá maior conhecimento e mais competências técnicas em todas as áreas, sobretudo nas novas áreas que a evolução tecnológica abre cada vez mais rapidamente. E é toda uma nova capacidade proprietária e autónoma que servirá para identificar as novas soluções para as velhas e novas dificuldades. No caso do CSM, este está já a desenvolver essa capacitação autónoma de forma muito esclarecida.

Por exemplo, visualizando a atual agenda, foi a coragem em desenvolver uma nova capacitação tecnológica própria que permite agora a gestão digital rápida da informação nos chamados megaprocessos, um dos novos desafios que teve resposta utilíssima, perante a forte perceção de que a respetiva morosidade afeta intensamente a confiança social nos tribunais e, consequentemente, no Estado de direito.

Para responder a novíssimos desafios, importa absorver a transição para o que se pode chamar de “*justiça digital*” que prepara a perspetiva futura de uma “*justiça inteligente*.” A implementação de novas tecnologias, especialmente sistemas de IA, desponta como solução para otimizar o processamento e a análise de dados judiciais. A chamada “*justiça inteligente*” propõe o uso de IA não apenas para automatizar tarefas, mas também para auxiliar juízes a identificar e avaliar rapidamente as informações mais relevantes, contribuindo para julgamentos mais rápidos e mais bem informados.

O uso de IA na justiça levanta, porém, preocupações que vão além da eficiência. Sem uma regulamentação adequada, a IA pode comprometer direitos fundamentais, como a privacidade. O conceito de “*open justice*”, por exemplo, promove a transparência, mas sem os devidos cuidados na proteção de dados pessoais, pode violar a privacidade das partes e terceiros envolvidos. Outro risco é a criação de perfis de juízes com base nas suas sentenças, o que pode limitar a independência ou, pelo menos, comprometer a imparcialidade. Além disso, há o risco de consolidação de padrões conservadores a partir de decisões passadas, limitando a adaptabilidade da justiça.

A IA deve permitir que os juízes percebam e avaliem os processos por ela geridos, assegurando o direito ao contraditório em todas as fases judiciais. Para tanto, as ferramentas de IA têm de permitir a sua “*leitura*”, deixando de ser caixas indecifráveis ao utilizador. Os juízes precisam de formação contínua para que possam compreender tais ferramentas e possam utilizá-las de maneira eficaz, preservando a sua função de garante dos direitos fundamentais.

Com esse objetivo, o CSM em Portugal adotou uma posição firme quanto ao desenvolvimento da IA na justiça, defendendo que o envolvimento de juízes no processo é fundamental. O CSM acredita que os juízes devem participar da conceção e implementação de sistemas de IA, para que eles traduzam valores alinhados às expectativas sociais e à democracia. A aposta no caminho da inovação e da gestão tornou-se a mais forte aposta.

6. O ALTEC-CSM como exemplo de solução prática na transição digital ao serviço do Estado de direito

Para tanto, o CSM, com competências na gestão dos tribunais e no seu bom funcionamento, criou em 2023 a estrutura ALTEC (Apoio Logístico para a Tramitação de Elevada Complexidade) que se constitui como uma equipa multidisciplinar formada por juízes e cerca de 24 pessoas com conhecimentos muito distintos (juristas, psicólogos, oficiais de justiça, economistas e programadores com conhecimentos em inteligência artificial).

A atuação desta equipa, centra-se nos três seguintes planos distintos, mas complementares:

- o plano “*apoio logístico aos processos de elevada complexidade*”, no qual o ALTEC funciona como uma equipa de suporte que vai trabalhar o processo na perspetiva apenas de tratamento de informação. Num primeiro momento, há uma reunião com o juiz titular do processo, para empreender as dificuldades e necessidades do processo. É o juiz do processo que determina as concretas ações da intervenção do ALTEC, as quais podem passar pelo tratamento da prova (agregação da prova, criação de “*mindmaps*”, sumarização da informação mais importante para o juiz, etc.), apresentação da prova em julgamento através do SEGIP (*Sistema Eletrónico de Gestão da Informação Processual*, uma ferramenta desenvolvida internamente), tradução de documentos, formatação de texto, adequação dos equipamentos informáticos, etc. Em todas estas situações o ALTEC aplica as melhores tecnologias ao seu dispor, permitindo que o juiz não se preocupe com esses problemas (focando-se apenas em decidir o caso), tornando o processo mais célere. Para o efeito, é sempre criado um plano personalizado de atuação, que respeita sempre as necessidades do juiz do caso e que visa apenas potenciar o seu trabalho, para que o mesmo se foque na decisão e não em todos os demais aspetos secundários que consomem muito do tempo e energia do juiz nos processos judiciais mais complexos. O ALTEC funciona como uma interface entre os problemas existentes nos casos volumosos e complexos e o juiz que tem de decidir estes casos. Tenta-se digerir os problemas e apresentar ao juiz as melhores soluções. É o “*backoffice*” do juiz/tribunal para os casos mais complexos;
- o plano “*desenvolvimento de aplicação informáticas e sua introdução nos tribunais*”, quando os avanços tecnológicos se sucedem a um ritmo vertiginoso e não é possível aplicar todo esse avanço nos tribunais sem que haja uma triagem dos mesmos. Triagem que assenta essencialmente no critério da tecnologia ser útil para a prática diária dos tribunais e como pode ser implementada de forma que os utilizadores tirem dela o maior proveito. Para tanto, os juízes que integram o ALTEC participam em vários grupos de desenvolvimento de aplicações informáticas para os tribunais da responsabilidade do ministério da justiça, o que permite que tais aplicações sejam desenvolvidas, desde o seu início, com uma preocupação prática, assegurando o respeito pelos princípios constitucionais que conformam a atuação dos tribunais. Por outro lado, esse grupo está em permanente contacto com universidades portuguesas e respetivos departamentos informáticos, tentando antecipar as aplicações que nos próximos anos serão úteis nos tribunais, com especial enfoque no uso de ferramentas de inteligência artificial. Por fim, mesmo internamente o grupo tem a capacidade de criar micro aplicações que permitem resolver concretos problemas dos

juízes no seu dia a dia nos tribunais. Isto permite gerar um fluxo constante de inovação nos tribunais, antecipando-se sempre o valor da aplicação para o trabalho concreto dos juízes. Deste modo, é construído um interface humano que torna mais gerível a introdução de novas tecnologias nos tribunais e a sua real adoção pelos juízes;

- o plano “*formação contínua dos juízes*”, quando a formação dos juízes nas novas tecnologias existentes é atualmente um dos fatores mais estruturais e impactantes na adoção das novas tecnologias nos tribunais e um dos mais desprezados nos modelos de introdução de novas tecnologias nos tribunais. Neste plano, o ALTEC cria planos de formação dos utilizadores nas novas tecnologias antes da sua colocação nos tribunais. Nenhuma tecnologia é introduzida por esta equipa nos tribunais, sem que haja previamente a formação dos seus utilizadores e depois o devido acompanhamento da sua utilização. Este é um facto absolutamente decisivo para alcançar o objetivo pretendido de uso eficiente das novas tecnologias nos tribunais. Por outro lado, esta formação tem contornos distintos das típicas formações uma vez que é sempre dada por juízes a juízes, um fator decisivo na adesão às novas tecnologias, já que assegura uma compreensão mútua dos problemas e limitações existentes e um muito importante respeito interpessoal. E também uma vez que as formações são práticas e personalizadas ao utilizador, com características e tempos de aprendizagem distintos – seja quanto ao tempo da formação, o modo de transmitir a informação ou o volume de informação a transmitir, tudo é adaptado para melhor satisfazer as necessidades do utilizador e otimizar os resultados da formação.

É nesta abordagem vertical dos problemas que reside a mais-valia deste grupo do CSM enquanto dinamizador da introdução das novas tecnologias nos tribunais em Portugal. Só assim é possível resolver ou mitigar os problemas presentes e criar as bases para que a adoção de novas tecnologias cada vez mais complexas no futuro se possa fazer de uma forma operacional.

7. Conclusão

O ALTEC/CSM tornou-se uma solução humana para problemas e desafios tecnológicos colocados à justiça nos tribunais e o exemplo do que a governação autónoma do poder judicial pode alcançar de substancialmente novo e útil e que de outra forma não seria conseguido.

Nesta casuística operacional se pode ilustrar, assim e em ação, o melhor das respostas disponíveis aos desafios dos tribunais diante da transição digital, desafios que são angulares no progresso e futuro do Estado de direito.

O digital e o Estado de direito na governação da justiça, na administração dos tribunais e na decisão jurisdicional

Nuno Coelho *

1. Contexto e pressupostos epistemológicos. Estádios de desenvolvimento: sistemas de informação, digitalização e automação (inteligência artificial)

Imaginem-se a entrar numa catedral gótica. Adicionem a essa imagem um envelope sonoro de um órgão de tubos nos seus matizes mais sensíveis e envolventes. O organista pode ser Juan de la Rubia a interpretar uma transcrição do ato 1, cena 4, da ópera Ouro do Reno de Wagner, a célebre entrada dos deuses em Valhala.

Não nos critiquem, desde já, pelo aparente lirismo desta imagem. A imagem em causa (órgão de tubos e organista) e aquilo que representa enquanto simbolismo ou metáfora são, no seu conjunto, o resultado de uma reflexão mais lata que procura desbravar os pressupostos sistémicos da realização do direito pelo juiz (jurisdição), nas suas plúrimas dimensões, abordagens, escalas e disciplinas, tudo isto com vista a obter uma definição mais nítida do espaço de interpretação, de aplicação ou de criação do direito pelo juiz (ou pelos juízes, quando o tribunal funciona em coletivo), que pode e deve ser encarado, também, enquanto espaço de liberdade operacional e funcional.

A verdade é que depois de ouvirmos Juan de la Rubia na catedral de Santo Estevão, em Viena, a metáfora do órgão de tubos – o órgão de uma catedral feita de pilares e de simbolismo, na interpretação criativa, mas sempre canonizada, adaptada aos timbres e às dinâmicas do local e do tempo¹ – não tem deixado de nos acompanhar.

Segundo esta analogia, a estrutura em que assenta a pronúncia do direito, pelo juiz, é a própria organização dos tribunais, com toda a sua amplitude descritiva, incluindo a tecnológica (a máquina); a sua pior ou melhor definição, construção e integração no edifício que é, também, catedral, faz toda a diferença e constitui a noção de espaço e de tempo na qual o humano pode ganhar o sentido da sua plenitude na relação com a realidade que o rodeia.

Neste texto pretende-se refletir, na linha de abordagem sobre os desafios colocados pela transição digital ao Estado de direito (funcionamento da justiça e independência

* Juiz Conselheiro, Tribunal de Contas (Portugal).

¹ O organista, para além da normal interpretação da peça musical inscrita em partitura, ainda assim com todas as suas opções de dinâmica interpretativa, terá de escolher e ajustar os seus registos, timbres, volumes, intensidades, opções de utilização, técnicas de dedilhado, além de outros pormenores relativos ao desempenho do próprio mecanismo (ou sistema) sonoro ali em presença (*organum*), de acordo com os aspetos oferecidos pela própria estrutura do órgão em presença (mais ou menos imponente, sofisticado ou apetrechado, de acordo com a sua maior ou menor modernidade e tecnologia correspondente), que é sempre diferenciada pela sua adaptação e integração ao local em presença, também este composto dos seus próprios condicionamentos acústicos.

judicial), sobre o tema da Justiça Digital no pressuposto de uma sistemática alargada, tal como explica o nosso livro *Organização do Sistema Judicial e Jurisdição*.²

A partir da assunção do contexto atual e dos pressupostos considerados pertinentes, enquanto dados prévios, iremos, depois, abordar o mesmo tema nas escalas da governação (macro), da administração dos tribunais (meso) e da própria decisão jurisdicional (micro), naqueles que se podem chamar como níveis ou espaços diversos de realização jurisdicional.

Numa prévia abordagem contextual sabemos que as últimas duas décadas nos oferecem uma sucessão inesgotável de alterações a vários níveis, a par de acontecimentos e de fenómenos de diversa ordem, uns mais esperados do que outros, os quais, necessariamente, terão de ser analisados e refletidos mais aprofundadamente.

Na área da justiça, as mudanças económicas, climáticas, políticas, organizativas e tecnológicas, projetam-se, de forma difusa, nos diversos eixos da estrutura da jurisdição, entre os quais se conta, precisamente, o da digitalização da justiça.

A atualidade está muito marcada pela dimensão tecnológica, potenciada que ela foi pelo mais vasto contexto crítico económico, pandémico, climático e bélico (*polycrisis*)³ que caracteriza os últimos tempos da nossa vida comum. Nessa medida, nenhuma instituição pública é imune e pode ser indiferente às alterações significativas a que estamos a assistir, a diversos níveis, e que reivindicam um novo olhar sobre o seu modo de atuação e a sua adaptação ao novo ambiente criado, necessariamente mais complexo, acrescidamente mutável e mais exigente com a qualidade e a sustentabilidade das correspondentes respostas políticas, económicas e culturais, mas também legislativas, administrativas e jurisdicionais.

O mundo atual, a sua forma de organização, a sua economia e política, o desenvolvimento, o ambiente e a indústria, o Estado e a administração pública, todos se condicionam à disrupção tecnológica, nas suas várias dimensões de mudança. Nos seus agentes ou atores, nos seus diversos dispositivos, na inovação tecnológica, na internet das coisas, nas mutações dos modelos de negócios e dos fluxos financeiros, na exploração da informação e dos dados, na inteligência artificial (IA) e na robótica, em todos estes domínios, vamos encontrar os quatro ingredientes principais dessa transformação (digital): dispositivos, conectividade, desmaterialização e disponibilidade emocional.⁴

A revolução digital⁵ abrange todos os sectores da vida, a uma escala global, exigindo um esforço de adaptação de todas as organizações, na sua gestão e nos seus procedimentos, ao ambiente digital e ao funcionamento dos dispositivos que

² Nuno Coelho, *Organização do sistema judicial e jurisdição. Para uma sistemática alargada da realização do direito pelo juiz* (Coimbra: Almedina, 2024). Salienta-se que muito do que aqui tratamos desta forma mais sintetizada se encontra desenvolvida nesta obra, numa articulação e estrutura mais densa e justificada, que aqui acompanhamos de perto.

³ Uma crise múltipla global (pluricrise) enquanto fator de instabilidade multi-sistémica que, não obstante se evidenciar como um “*emaranhado*” causal, não deixa de poder ser enquadrada teoricamente nas suas sincronias próprias. Michael Lawrence *et al.*, “Global polycrisis: the causal mechanisms of crisis entanglement”, *Global Sustainability*, v. 7, no. 6 (2024):1-16, doi: [10.1017/sus.2024.1](https://doi.org/10.1017/sus.2024.1).

⁴ Rogério Carapuça, *Revolução digital: quando quase tudo é possível* (Lisboa: Glaciar/Fundação Luso-Americana para o Desenvolvimento, 2018), 91-107.

⁵ Para muitos qualificável, na linha evolutiva dos sistemas de informação, da digitalização e da inteligência artificial, como a 4.^a revolução industrial e assim assinalada, sintomaticamente, por exemplo, pela plataforma do Fórum Económico Mundial em <https://www.weforum.org/centre-for-the-fourth-industrial-revolution/>. Numa alusão aos vários elementos definitórios desta 4.^a revolução e de como ela conforma a realidade humana. Luciano Floridi, *The 4th Revolution. How the infosphere is reshaping human reality* (Oxford: Oxford University Press, 2014).

o proporcionam. O funcionamento em rede da sociedade e a utilização das plataformas eletrónicas é uma evidência a que nenhuma sociedade escapa e às quais as instituições judiciais nacionais e internacionais se têm de adaptar ou mesmo reconfigurar nos seus diversos níveis de amplitude (do macro ao micro).⁶

Ao abordar este tema, necessariamente amplo na sua própria latitude de abordagem, pretende-se, em primeiro lugar, desenhar o horizonte da relação entre o sistema tecnológico conexo com aquilo que vulgarmente se denomina como ciberespaço constituído pelos estádios sucessivos de evolução tecnológica – *i*) sistemas de informação *ii*) digitalização e *iii*) automação e IA⁷ –, com as instituições públicas segundo uma perspetiva político-jurídica.⁸

Os estádios e as preocupações, assim delineados e distinguidos, escondem, no entanto, um campo de complexidades, de dispersão e de fragmentação, todas caracterizadoras daquilo que tem sido designada como a regulação digital global ou integrada. Tanto dos diversos pontos de vista de amplitude de aplicação (local, internacional, regional, transnacional, global, multinível), como da natureza, abrangência ou intensidade normativa do direito (*soft law/hard law*), dos seus sujeitos (entidades públicas, privadas, mistas ou híbridas) e dos espaços organizativos e tecnológicos onde o próprio direito é produzido, realizado e aplicado.⁹

Daí que só possa fazer sentido partir dos próprios pressupostos do conhecimento da realidade do direito e dos seus espaços de concretização, onde o tecnológico interage com os seus condicionalismos específicos.

Teremos de dar relevo, aqui, aos contributos da teoria sistémica, numa ponderação da realização com o direito, entre o fechamento, a abertura e a moldura (jurisprudencial do direito). Onde necessariamente será importante proceder ao cruzamento dinâmico de perspetivas que não podem deixar de

⁶ Em vez de se falar de revolução fará mais sentido, numa melhor ponderação, compreender a transformação muito acelerada com que nos vimos a deparar no seio de um processo social de mudança que pode e deve ser analisado no longo prazo. Trata-se, na verdade, de um processo complexo e heterogéneo e que não pode ser reduzido a uma uniformidade explicativa ou consequencial (v.g. *disrupção* v. *continuidade*) e que deve ser integrado em análises temporais, organizativas, culturais e multidimensionais (micro, meso e macro). Stefanie Büchner, Jannis Hergesell, Jannis Kallinikos, “Digital transformation(s): on the entanglement of long-term processes and digital social change. An Introduction”, *Historical Social Research*, v. 47, no. 3, (2022): 7-39, doi: <https://doi.org/10.12759/hsr.47.2022.25>.

⁷ Ao falar de estádios de desenvolvimento não pretendemos fazer uma cronologia estanque destas várias etapas nem sequer fazer entender que as tecnologias não tiveram percursos paralelos de génese, de evolução e até de interpenetração. Apenas estamos a aludir a etapas da sua profusão e utilização mais corrente e que dessa forma passaram a influenciar de forma determinante as organizações e, desse modo, a vida social e institucional.

⁸ É conhecida a razão justificativa desta evolução e será difícil encontrar uma melhor síntese do que esta para caracterizar a atual situação tecnológica dos diversificados (em termos evolutivos) sistemas judiciais em ação – assim, para uma caracterização mais detalhada, remete-se para a nossa referência: Coelho, *Organização do sistema*, 339-370.

⁹ Num plurinormativismo em que se denota uma indefinição na própria génese e tipologia das normas, muitas vezes impulsionadas pelo direito reflexivo ou autorregulatório das organizações tecnológicas (v.g. plataformas tecnológicas). Um direito que apresenta, ele próprio, vários níveis de intensidade (do *soft* ao *hard law*) e a presença necessariamente híbrida da norma técnica ou do algoritmo. Segundo refere Raquel Brízida de Castro, as relações entre os sistemas tecnológico e digital e o sistema jurídico configuram autênticos paradoxos no contexto de uma (des)regulação global digital e tecnológica de cariz híbrido e plural, fator de erosão jurídico-constitucional. Raquel Brízida de Castro, *Direito Constitucional: ciberespaço e tecnologia. Declínio do constitucionalismo na UE?* (Coimbra: Almedina, 2023), 168-186 e 212-217.

ser históricas (nas abordagens estruturais e de longo prazo),¹⁰ epistemológicas,¹¹ biográficas, ecológico-sociais (Urie Bronfenbrenner),¹² multi-dimensionais (no cruzamento entre ambiente e sistema nas suas diversas escalas e magnitudes (micro, meso e macro) – e adequadas a um tempo de “modernidade líquida” (Zygmunt Bauman),¹³ da “bio-política” (Roberto Esposito),¹⁴ da “sociedade em rede” (Manuel Castells),¹⁵ da “sociedade do risco e da emergência” ou da “sociedade em metamorfose” Ulrich Beck.¹⁶

Pensamos que as considerações de cariz epistemológico possibilitam uma referência mais detalhada.

Assim, considera-se que o sistema cognitivo está imerso no mundo social e tecnológico,¹⁷ com ele interage e com ele se potencia, sendo que as alterações paradigmáticas na organização social causadas pelas mutações nas redes de comunicação e interações inerentes à revolução tecnológica em curso não deixam

¹⁰ Não é à toa que historiadores como Yuval Noah Harari têm vindo a ganhar um crescente espaço de divulgação para as suas especulações, tanto quanto ao que se passa no presente como ao que se vai passar no futuro, do *Sapiens* ao *Nexus*.

¹¹ Considerações em torno da epistemologia histórica e social, desde logo nas ponderações cognitivas mais aptas a explicar a virtualidade dos contextos sociais, organizativos e tecnológicos para uma definição mais sustentada da atividade jurisdicional. Assim, segundo a epistemologia histórica e social o conhecimento será altamente dependente de habilidades práticas e aptidões pessoais. Sobre o conhecimento tácito ou implícito, consulte-se: Michael Polanyi, “Planning and spontaneous order”, in *The Manchester School*, Volume 16, Issue 3 (1948): 237-301. Michael Polanyi, *The tacit dimension* (Chicago/London: The University of Chicago Press, 2009), 3-25. O próprio direito, nesta abordagem, sem esquecer a sua articulação essencialmente sistémica (ou sistemática), assenta numa contextualização de práticas instituídas e, por essa via, é objeto de transformações sucessivas e disruptivas causadas pelo funcionamento em rede que é próprio da atual sociedade informativa e tecnológica. Karl-Heinz Ladeur, “The role of contracts and networks in public governance: the importance of the ‘social epistemology’ of decision making”, *Indiana Journal of Global Legal Studies*, v. 14, no. 2 (2007): 329-351. Thomas Vesting, “Modern law and the crisis of common knowledge”, *Revista de Informação Legislativa*, Brasília, v. 54, no. 214 (2017): 11-29. Thomas Vesting, *Legal theory and the media of Law* (Cheltenham/Northampton: Edward Elgar Publishing, 2018), 5-28.

¹² Urie Bronfenbrenner, 1979, *The ecology of human development: experiments by nature and design*, (Cambridge/London: Harvard University Press, 1979). Urie Bronfenbrenner, Pamela A. Morris, “The Bioecological Model of Human Development”, in *Handbook of Child Psychology, Volume I, Theoretical Models of Human Development*, Wiley Online Library (2007): 793-828, doi: 10.1002/9780470147658.chpsy0114.

¹³ Se, no contexto da modernidade sólida, era ao Estado que cabia a regulação do medo de origem social a que Freud se referia em *Civilization and its discontents*, agora, no quadro da modernidade líquida, “a dissolução da solidariedade assinalou o final da luta contra o medo adoptada pela modernidade sólida.” Zygmunt Bauman, *Confiança e medo na cidade* (Lisboa: Relógio D’Água Editores, 2006). Consulte-se, também, do mesmo autor, na senda da modernidade líquida: Zygmunt Bauman, *Liquid modernity* (Malden: Polity Press, 2000).

¹⁴ Roberto Esposito, *Bíos: Biopolítica e filosofia* (Torino: Giulio Einaudi editore, 2004), 101-138.

¹⁵ A propósito do conceito de tempo e da mutação operada pelo paradigma das tecnologias da informação, pelas práticas sociais que lhe estão inerentes e pelo surgimento do espaço de fluxos. “O tempo como repetição da rotina diária (...)” que se encontrava “no âmago do capitalismo industrial e do estadismo (...)” esse “tempo linear, irreversível, mensurável e previsível está a ser fragmentado na sociedade em rede, num movimento de extraordinária importância histórica.” Manuel Castells, *A sociedade em rede - a era da informação*, Volume I (Lisboa: Fundação Calouste Gulbenkian, 2002), 561.

¹⁶ Ulrich Beck, *Sociedade de risco mundial: em busca da segurança perdida* (Lisboa: Edições 70, 2016). Ulrich Beck, *A metamorfose do mundo: como as alterações climáticas estão a transformar a sociedade* (Lisboa: Edições 70, 2017).

¹⁷ Andy Clark, David Chalmers, “The extended mind”, *Analysis*, v. 58, no. 1 (January 1998): 7-19. Paul Smart, “Extended cognition and the Internet. A review of current issues and controversies”, *Philosophy & Technology*, v. 30 (2017): 357-390, <https://link.springer.com/article/10.1007/s13347-016-0250-2>. Giulio Ongaro, Doug Hardman, Ivan Deschenaux, “Why the extended mind is nothing special but is central”, in *Phenomenology and the Cognitive Sciences* (2022), doi: 10.1007/s11097-022-09827-5.

de afetar o próprio direito,¹⁸ o qual, para além da sua articulação sistémica, não deixa de assentar numa contextualização de práticas instituídas.¹⁹

No sentido de que a tecnologia não pode ser considerada apenas enquanto ferramenta, na sua dimensão instrumental, pois a mesma se integra com o direito no conjunto das interações humanas no triplo ponto de vista organizativo, procedimental e institucional,²⁰ como podemos salientar a propósito, por exemplo, de definições concetuais como as de organização, de sistema e de decisão e da sua relevância dentro do mais vasto universo jurisdicional.²¹ As sobreposições institucionais²² que resultam das mutações acima identificadas podem ser caracterizadas com recurso às noções de ator, de rede e de agência, pois nelas ocorrem processos de transferência das regulações normativas (e dos respetivos comandos) para os códigos informáticos. Por via deste fenómeno de agência (ou delegação), os componentes processuais definidos pela lei são inscritos na tecnologia. A delegação ou agência para as máquinas é dupla, pois as máquinas realizam ações anteriormente desempenhadas por humanos (automação), ao mesmo tempo que orientam os humanos na execução das suas tarefas.²³

¹⁸ Sendo que a operacionalidade do direito é questionada pela proliferação dos padrões em rede e pela intervenção dos inerentes quasi-atores (mais ou menos complexos e multi-nível) e das plataformas - onde as figuras das conexões e das parcerias contratuais assumem a maior relevância, na fronteira entre a regulação privada e pública, ao lado dos indivíduos e das organizações, que ultrapassam as inerentes fronteiras organizativas, cognitivas e semânticas. Ladeur, “The role”, 329-351. Karl-Heinz Ladeur, “The transformation of legal semantics in postmodern society. From the ‘subsumption’ of cases to ‘balancing’ and a semantics of networks”, *Revista de Informação Legislativa*, Brasília, v. 54, no. 215 (2017): 13-26. Gunther Teubner, Gunther, “The anonymous matrix: human rights violations by ‘private’ transnational actors”, in *Modern Law Review*, v. 69, no. 3 (2006): 338-342. Gunther Teubner, Hugh Collins, *Networks as connected contracts*, (Oxford/Portland: Hart Publishing, 2011), 113-178. Thomas Vesting, “The autonomy of Law and the formation of network standards”, *German Law Journal*, v. 05, no. 06 (2004): 639-668. François Ost, Michel van de Kerchove, *De la pyramide au réseau? Pour une théorie dialectique du droit*, (Bruxelles: Publications des Facultés universitaires Saint-Louis, 2002), 23-32.

¹⁹ Nas referências já anteriormente citadas de Karl-Heinz Ladeur (2007), e Thomas Vesting (2017) e (2018), páginas 5-28, com alusão à epistemologia histórica e social e ao contexto prático-institucional, onde o conhecimento dos fenómenos coletivos e da rede redundaram num novo paradigma da cultura jurídica e científica.

²⁰ Dinâmica organizacional que se desdobra nas componentes institucional, estrutural e tecnológica, para que aponta Bruno Maggi. – assim, Bruno Maggi, “Teoria dell’organizzazione e sociologia del diritto”, in *Società, norme e valori. Studi in onore di Renato Treves*, eds. Uberto Scarpelli e Vincenzo Tomeo (Milano: Giuffrè, 1984), 289-294, ou num ajustamento (acoplamento) estrutural entre as realizações técnicas e o sistema social com recurso à redução da complexidade por via da simplificação funcional e do fechamento operacional inerentes à programação e codificação tecnológicas, tal como defendido por Luhmann – assim, Niklas Luhmann, *Risk: a sociological theory*, tradução do original alemão *Soziologie des Risikos* do mesmo ano, (Berlin/New York: Walter de Gruyter, 1993), 76-100. Neste mesmo sentido, consulte-se: Jannis Kallinikos, “The order of technology: complexity and control in a connected world”, *LSE Research Online*, available november 2005, <https://eprints.lse.ac.uk/457/>, e Jannis Kallinikos, *Governing through technology. Information artefacts and social practice* (Hampshire/New York: Palgrave Macmillan, 2011), 12-33.

²¹ Num estudo a que poderíamos apelidar de fenomenologia da jurisdição inerente a uma sistemática alargada da realização do direito pelo juiz que corresponde à nossa proposta de base na *Organização do sistema judicial e jurisdição*. Coelho, *Organização do sistema*, 865-870.

²² A expressão utilizada por Giovan Lanzara é de “assemblages”, no sentido que lhe é dado nas artes enquanto montagem ou colagem, numa estética de sobreposições e acumulação de materiais – assim, Giovan Francesco Lanzara, “Building digital institutions: ICT and the rise of assemblages in government”, in *ICT and Innovation in the Public Sector. European Studies in the Making of E-Government*, eds. Francesco Contini e Giovan Francesco Lanzara (New York: Palgrave MacMillan, 2009), 9-48.

²³ Sendo que quanto mais a justiça eletrónica é difundida mais a autoridade da lei (entenda-se processual) é delegada para os códigos de *software* – cfr. Lanzara, “Building digital institutions”, 9-13, e Giovan Francesco Lanzara, “The circulation of agency in judicial proceedings: designing for interoperability and complexity”, in *The circulation of agency in E-Justice. Interoperability and infrastructures for European transborder judicial proceedings*, eds. Francesco Contini e Giovan Francesco Lanzara (Dordrecht/Heidelberg/New York/London: Springer, 2014). 4-6; e Francesco Contini, “Artificial Intelligence and the transformation of humans, law and technology interactions in judicial proceedings”, in *Law, Technology and Humans*, v. 2, no. 1, (2020): 4-7.

À medida que a digitalização remodela cada vez mais as organizações empresariais e as entidades públicas, incluindo aqui o sistema judicial, passaram-se a destacar duas perspetivas nesta interseção entre a tecnologia e o direito, coincidentes com a dualidade “*Code as Law*” vs. “*Law as Code*”, conceitos que terão como base a definição inicial de Lawrence Lessig²⁴ mas que passaram a refletir a diferenciação de abordagem no que respeita à incorporação de sistemas baseados em códigos no domínio jurídico, cada uma com implicações distintas para as estruturas regulamentares, a tomada de decisões e a supervisão humana.²⁵

É este pano de fundo que melhor pode servir as ambições teóricas e metodológicas que melhor explicam a melhor forma com que os juristas podem vir a assimilar as componentes desta revolução tecnológica e perceber da real dimensão do seu impacto na estrutura da jurisdição. Podemos vir a falar de uma *artificial judicial decision making*? Será que o fator humano virá a estar em risco no momento de julgar, podendo o juízo decisório do juiz, com a sua face humana, ser substituído por uma máquina inteligente? Qual a capacidade de diálogo e de parceria metodológica do campo jurídico e judicial com o saber científico e tecnológico associado a essa revolução tecnológica? Que papel para a verdade na sociedade, no direito e na justiça digital? Quais são os limites da justiça preditiva na teoria e na prática jurídica?

Todas estas interrogações congregam diferentes preocupações sobre o descrito ambiente político, social e económico, as quais podem, depois, ser devidamente trabalhadas ou analisadas, em metodologia necessariamente pluridisciplinar, nos diversos níveis de abordagem,²⁶ e que é sempre fundamentada numa reflexão teórica e filosófica.

Essas mesmas abordagens, passam pelo nível político-constitucional, pelas respostas normativas e legais, pelas soluções governativas e gestionárias, pela análise

²⁴ *Code as Law* é um conceito introduzido por Lawrence Lessig mediante o qual se entende que no ciberespaço o código (*software* e *hardware*) atua como uma forma de regulação, semelhante às leis no mundo físico. O código define as regras e limitações do que é possível fazer *online*, influenciando a privacidade, a liberdade de expressão e o acesso à informação. Assim, em Lawrence Lessig, *Code and other laws of cyberspace* (New York: Basic Books, 1999).

²⁵ Stefan Eder, «“Code as Law” vs. “Law as Code”: shaping public administration, judiciary, and corporate compliance in the digital age», *Legal Informatics Newsletter*, 10 de novembro de 2024, *Linkedin*.

²⁶ O que passa, como se viu, não só pela assunção dos tribunais enquanto espaços organizacionais e estruturas organizativas, nos seus diversos componentes (institucionais, procedimentais, metodológicos, tecnológicos e estruturais) mas, também, pela abordagem que se possa fazer sobre o impacto no direito (e no direito realizado nos tribunais) das incisivas mutações sociais, económicas e culturais trazidas pela revolução tecnológica e pela sociedade digital, assentes nas tecnologias de informação e na globalização. Este fenómeno veio trazer uma nova articulação, de alguma forma inesperada, entre reflexões sobre o jurídico que à partida se encontravam algo distanciadas entre si: semióticas, discursivas, sistémicas, organizativas, tecnológicas, comunicativas, económicas e institucionalistas, entre outras, como se pode concluir das leituras, para além dos autores já citados no texto, de Alfred Büllesbach, “Saber jurídico e ciências sociais”, in *Introdução à filosofia do direito e à teoria do direito contemporâneas*, A. Kaufmann e W. Hassemer (Lisboa: Fundação Calouste Gulbenkian, 2002), 491; Óliver Williamson, “Why Law, economics, and organization?”, *Annual Review of Law and Social Science*, (December 2005): 369-396, doi: 10.1146/annurev.lawsocsci.1.031805.111122; Walter W. Powell, “Fields of practice: connections between Law and organizations”, *Law and Social Inquiry*, v. 21, no. 4 (1996): 954-966; Pierre Guibentif, *Teorias sociológicas comparadas e aplicadas. Bourdieu, Foucault, Habermas e Luhmann face ao Direito*, Lição síntese apresentada no âmbito das provas de agregação (Janeiro 2006), Lisboa: ISCTE (mimeo), também em *Cidades – comunidades e territórios*, no. 14, (Lisboa: CET – Centro de Estudos Territoriais, 2007), 89-104; Niklas Luhmann, *Law as a social system*, eds. Fatima Kastner, Richard Nobles, David Schiff e Rosamund Ziegert, tradução do título original *Das Recht der Gesellschaft* de 1993 (New York: Oxford University Press, 2004), 298-301; Gunther Teubner, “Altera pars audiatur: le droit dans la collision des discours”, in *Droit et Société*, v. 35 (1997): 99-123; e Ricardo Campos, *Metamorfoses do Direito global. Sobre a interação entre Direito, tempo e tecnologia* (São Paulo: Contracorrente, 2022), 264-340.

económica do digital e da IA (aplicados à justiça), pela vertente tecnológica em si (*design* e inovação), e, sem descurar a sua importância central, pelo tratamento processual e procedimental ligado com a gestão tecnológica e com aquilo que se pode designar pelo processo tecnológico, culminando pela própria decisão judicial (nas suas várias expressões e formas).

Neste texto pretendemos dar conta, desta forma mais sintética, dessas diferentes visões sobre aqueles mesmos problemas essenciais, dando conta de algo aparentemente evidente, mas que não é assumido como pressuposto central. O direito realizado pelos tribunais acontece e não deixa também de ser efetivamente moldado nos espaços organizativos, tecnológicos e de governação que são inerentes à instituição judicial.

2. Ambiente tecnológico, Estado de direito e governação do sistema judicial

A análise de contexto antecedente visou criar a sustentação para uma análise mais consistente e coerente sobre a relação que pode ser estabelecida entre o Estado de direito e o digital numa perspectiva jurisdicional.

Na verdade, a jurisdição obedece a uma estruturação constitucionalmente determinada e que, partindo na sua contextualização política, social e económica, passa para a sua definição institucional e procedimental, passando por temas mais específicos como, por exemplo, a independência judicial e as suas garantias, a governação da justiça e a sua autonomia, a reforma judiciária e as políticas públicas da justiça, os estatutos das profissões forenses, a ética e a deontologia, e, até, a gestão dos tribunais e a gestão processual.

A noção de Estado de direito reflete o essencial do enquadramento valorativo e principiológico a que deve obedecer essa estrutura jurisdicional. É nossa afirmação corrente que *“a ideia de Estado de direito constitui, para além de todas as controvérsias, uma pedra de toque de todas as ordens jurídicas em democracia e um referencial para apurar do grau da consistência e da integridade dos regimes políticos nacionais e das instituições que os suportam.”*²⁷

Esta afirmação, contudo, precisa de ser justificada com algum desenvolvimento, partindo-se da sua noção e dos seus quadros referenciais, pois esse conceito político fundamental tem evoluído e beneficiado a ideia primacial da determinação e limitação pelo direito dos poderes estatais e da separação de poderes, com sucessivos sedimentos fundados nas ideias da democracia, da defesa dos direitos humanos, do desenvolvimento e da paz, da justiça social e da igualdade e da proteção ambiental.

Estes critérios também se estabelecem em torno de determinados mecanismos de avaliação. Por exemplo, em 2016 o Comité dos Ministros do Conselho da Europa recomendou a utilização por todos os Estados europeus da lista de critérios elaborada pela Comissão de Veneza,²⁸ difundindo-a em larga escala. Mais

²⁷ Assim, em Coelho, *Organização do sistema*, 239.

²⁸ Consultável em *Rule of Law Checklist*, adoptada pela Comissão de Veneza na 106.ª Sessão Plenária (11-12 Março de 2016), Veneza: Comissão de Veneza/Conselho da Europa, 2016, [http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD\(2016\)007-e](http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)007-e). Comissão de Veneza essa que, em 2011, tinha adotado um outro relatório justamente sobre este tema e em que procura reconciliar os conceitos diversos e similares dos países de influência do Conselho da Europa em torno de elementos comuns, como um processo legislativo transparente, responsável e democrático, a certeza e a segurança jurídicas, a proibição da arbitrariedade, o acesso à justiça administrada por tribunais independentes e imparciais, o respeito pelos direitos humanos e a igualdade e a não discriminação na aplicação do direitos.

recentemente, desde 2020, a Comissão Europeia tem produzido relatórios anuais a apresentar às demais instituições europeias, sobre a situação nos seus Estados membros reportada a determinadas matérias de referência, como os sistemas judiciais, a estrutura anticorrupção, a liberdade e o pluralismo da imprensa e o desempenho dos respetivos esquemas constitucionais de *checks and balances*, com vista a acompanhar as diversas situações críticas e com vista a reforçar a cooperação interinstitucional em torno do Estado de direito.²⁹

Essa listagem passa em revista os tópicos mais recorrentes do Estado de direito, como a legalidade, a segurança jurídica, a prevenção do abuso de poder, a igualdade perante a lei e a não-discriminação, o acesso à justiça, para além de salientar dois dos maiores desafios colocados ao Estado de direito: de um lado, a corrupção e o conflito de interesses, e, do outro, a fiscalização da recolha e utilização de dados pessoais.

Uma realidade que decorre, do mesmo modo, do processo de reforço do Estado de direito que, em primeira linha se centrou em programas de desenvolvimento, e, agora, após o início desta fase de regressão e de erosão em que nos encontramos, em programas de resiliência e garantia do mesmo princípio, tal como se pode encontrar no avivamento da jurisprudência mais recente do Tribunal Europeu dos Direitos Humanos e do Tribunal de Justiça da União Europeia sobre este tema (tanto por via dos reenvios prejudiciais como das chamadas ações de incumprimento).³⁰

O contexto do digital, com toda a densidade de conteúdo afirmada anteriormente, não deixa de influenciar determinantemente a dinâmica institucional e de concretização dos princípios do Estado de direito, entre os quais se inclui a independência judicial. Este princípio tem vindo a ser reconceptualizado não só à luz da sua relação com o outro princípio da *accountability* (transparência e responsabilidade)³¹ mas também com as novas exigências sistémicas derivadas das descritas transformações no ambiente tecnológico (onde se inclui a automação e a IA).

Neste contexto já não se trata de complementar a realidade física dos processos com ferramentas de agilização e mobilização das tarefas e dos procedimentos. A transição digital tem por incumbência a migração para um ambiente integralmente

²⁹ Assim, neste ano de 2024, consulte-se Relatório sobre o Estado de direito, em https://commission.europa.eu/publications/2024-rule-law-report-communication-and-country-chapters_pt?prefLang=pt&ettrans=pt, que se conjugam numa iniciativa da Comissão Europeia de abril de 2019 para o fortalecimento do Estado de direito na Europa, com a assunção de ações concretas para reforçar a capacidade da União Europeia neste domínio através da promoção de uma cultura do Estado de direito, a prevenção dos seus problemas e uma efetiva resposta a estes últimos, tal como relatado num comunicado da Comissão Europeia ao Parlamento Europeu, ao Conselho Europeu e ao Conselho de 3/4/2019. Estabelece-se, aqui, um quadro de resposta às ameaças contra o Estado de direito, com vista a prevenir as ameaças emergentes ao Estado de direito que possam vir a desencadear os mecanismos previstos no artigo 7.º do Tratado da União Europeia – cf. União Europeia, *Prosseguir o reforço do Estado de direito na União: ponto da situação e eventuais medidas futuras*, COM (2019) 163, Comunicação da Comissão ao Parlamento Europeu e ao Conselho, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52019DC0163&from=EM>.

³⁰ Veja-se, sobre este tema, a análise recente do Ceeli Institute, 2024, *Navigating the jurisdiction and landmark rulings of the European Court of Human Rights and the Court of Justice of the EU. A guide to protecting the rule of law in european courts amid democratic backsliding* (Prague: Ceeli Institute, 2024), https://ceeliinstitute.org/assets/resources/ceeli_guide_protecting_rule_of_law_interactive.pdf, e, também, a análise jurisprudencial a propósito do tema da independência judicial em Coelho, *Organização do Sistema*, 391-410.

³¹ Confronte-se esta visão pluridimensional em torno da relação da independência e da *accountability*, também em Coelho, *Organização do sistema*, 412-425.

digital, assumido como regra,³² passando as plataformas digitais a assumir o suporte tecnológico de todas as atividades inerentes aos tribunais e à justiça.

Para além das questões de direito probatório que suscitam a realidade digital e a utilização mais ou menos massiva dos dados, na seleção e valoração do material probatório relevante, nas tarefas processuais de recolha da informação jurídica ou da própria argumentação suscitada nos casos, discute-se a utilização das ferramentas digitais e de automação, bem como a IA, nas próprias tarefas decisórias, tanto do ponto de vista auxiliar ou instrumental, como para a geração automática de decisões judiciais (diferenciando aí os níveis de intervenção do juiz humano).³³

A digitalização da justiça tem uma dimensão inequívoca de impacto no funcionamento do sistema judicial, em diversos níveis de abordagem e de tópicos, como a independência e a *accountability* judiciais, a sua transparência e acessibilidade, pois o tratamento em linha dos casos e das disputas judiciais tem como pressuposto a implementação de um sistema de justiça digital verdadeiramente holístico – um sistema integrado de serviços de aconselhamento *online*, serviços *online* de resolução extrajudicial de litígios públicos e privados (portais de mediação e arbitragem, serviços de provedoria) e tribunais *online* – poderá tornar este futuro uma realidade.³⁴

Assim, não é indiferente a forma como se encontra estruturado e organizado o sistema judicial, assim como não se pode prescindir de uma análise institucional de grande latitude (profunda e rigorosa) sobre o Estado e o Estado de direito, de uma atenção ponderada sobre a relação destes pressupostos com o seu contexto social,

³² Daí se entenda a estratégia europeia de articulação dos princípios da justiça eletrónica e da administração em linha, em que se assume o princípio do “*digital por definição*” na Estratégia de justiça eletrónica para 2019-2023 – assim, União Europeia, *Estratégia de justiça eletrónica para 2019-2023* (2019/C 96/04), elaborada pelo Conselho Europeu, 2019, [https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52019XG0313\(01\)&from=EM](https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52019XG0313(01)&from=EM). Sobre a estratégia da União Europeia para 2024-2028, recentemente aprovada pelo Conselho Europeu, numa preocupação do desenvolvimento de vários princípios operacionais para além do digital por defeito, para além da garantia dos direitos fundamentais, do acesso à justiça, da centralidade nas pessoas, da equidade digital, do reforço da posição dos utilizadores e na sustentabilidade, veja-se <https://data.consilium.europa.eu/doc/document/ST-15509-2023-INIT/en/pdf>. Esta transição para o digital e para a *Ciberjustiça* assenta, também, por exemplo, em diversa documentação suportada ao nível do Conselho da Europa pela Comissão Europeia para a Eficiência da Justiça, em várias ferramentas técnicas, de boas práticas e de políticas públicas – assim, no grupo de trabalho *Cyberjustice and artificial intelligence used in the field of justice*, <https://www.coe.int/en/web/cepej/cepej-working-group-cyber-just>, e Marco Fabri, “From court automation to e-justice and beyond in Europe”, *International Journal for Court Administration*, no. 7 (2024), doi: [10.36745/ijca.640](https://doi.org/10.36745/ijca.640). Assinale-se, do mesmo modo, a recente assinatura em 5/9/2024 da Convenção Quadro do Conselho da Europa sobre Inteligência Artificial e os direitos humanos, a democracia e o Estado de direito, aprovada na 133.ª Sessão do Comité de Ministros da Justiça - <https://rm.coe.int/1680afae3d>.

³³ Assim, em Jordi Nieva Fennol, *Inteligencia artificial y proceso judicial* (Madrid: Marcial Pons, 2018), 23-41 e 79-125; José Ignacio Solar Cayón, “Inteligencia artificial y justicia digital”, in *Inteligencia artificial y filosofía del derecho*, dir. Fernando H. Llano Alonso (Murcia: Laborum Ediciones, 2022), 386-415; David Freeman Engstrom, “The new judicial governance: courts, data, and the future of civil justice”, *DePaul Law Review*, v. 72, no. 2 (Spring 2023): 171-238; Elisa Alfaia Sampaio e Paulo Jorge Gomes, “A Inteligência artificial como auxiliar das decisões judiciais”, in *Direito e inteligência artificial*, coords. Maria Raquel Guimarães e Rute Teixeira Pedro (Coimbra: Almedina, 2023), 203-227; e Erik Longo, *Giustizia digitale e Costituzione. Riflessioni sulla trasformazione tecnica della funzione giurisdizionale* (Milão: FrancoAngeli, 2023), 255-323. Na proposta que ficou conhecida em Portugal como “*Agenda da reforma da justiça*” são apresentadas determinadas propostas, devidamente fundamentadas, ao nível da justiça digital e inteligência artificial, mas também no que respeita à transição digital da atividade processual e de gestão dos tribunais, não esquecendo a formação nesta área tecnológica e digital – assim, em Nuno Coelho et al., *Agenda da reforma da justiça. Uma reflexão aberta e alargada do judiciário* (Coimbra: Almedina, 2023), 569-589.

³⁴ Assim, na realidade britânica, consulte-se Andrii Koshman, “Judicial accountability in the digital justice system of tomorrow”, *U.K. Const. L. Blog*, 3 outubro 2024, <https://ukconstitutionallaw.org/>.

económico e tecnológico, e, do mesmo modo, com as garantias procedimentais e da independência judicial, de uma visão sobre a reforma do sistema judicial e das políticas públicas da sua governação e de adequada abordagem sobre o processo (nas suas plúrimas incidências), o modelo profissional dos juízes e a gestão dos tribunais.

Sabendo que, neste âmbito, o próprio direito se pode demarcar (ou especializar) em várias perspetivas, preocupações ou sensibilidades (de funcionalidade ou de objetivos regulação), que se podem tomar como os eixos da *i)* cibersegurança, da *ii)* ciberdemocracia e da *iii)* cibergovernação.

Sendo que na *i)* cibersegurança se atende à defesa, garantia ou robustez do sistema tecnológico face a intervenções agressivas ou malévolas providas do exterior ou de pontos externos da rede a que se encontra ligados estes sistemas tecnológicos.

Que na *ii)* ciberdemocracia se pode compreender a defesa ou garantia dos direitos fundamentais dos utilizadores ou de terceiros abrangidos ou implicados pela atividade do sistema (*v.g.* na proteção dos dados pessoais), do Estado de direito ou da autonomia de governação dos vários poderes separados (*v.g.* órgãos de soberania) relativamente ao mesmo sistema tecnológico, segundo os parâmetros comparados do constitucionalismo digital.

E, por último, que na *iii)* cibergovernação teremos a regulação do próprio sistema tecnológico que se pretende organizado, regulado, seguro, inteligente e integrado com a ciberdemocracia (e com o direito constitucional) e procedimentalizado, de forma a garantir a integridade política e jurídica das instituições públicas em causa (legislativo, executivo, tribunais, administração pública em geral).

A questão da governação entronca, desta forma, com a questão latente da democracia preocupada com o espaço digital ou tecnológico do sistema judicial.

Neste ponto a atualidade foi capturada pela discussão em torno dos aspetos éticos e sociais da IA e é dada cada vez maior atenção às políticas da mesma IA e à ciência de dados. Por exemplo, tem sido dada atenção às violações da privacidade e dos direitos fundamentais em geral, aos perigos da desinformação e da desinformação, ao preconceito e à discriminação, à manipulação de eleições, às assimetrias significativas do poder, ao enfraquecimento da confiança social, aos custos ambientais e à criação de bolhas epistémicas e, por último, à polarização social e política.³⁵

Mas a questão é também um problema económico intrínseco à evolução tecnológica e presumivelmente da reinvenção da economia através dos dados (ambiente de dados abertos *v.* ambiente circunscrito de dados).³⁶

Depois, no que respeita ao domínio da segurança, há que referir que os ciberataques se encontram potenciados por via da infeção, contaminação ou intrusão nos sistemas de IA que não deixam de conter vulnerabilidades específicas (*v.g.*

³⁵ Sobre este ponto, para um apuramento do contexto político, social e económico com que se tem confrontado o princípio do Estado de direito, consulte-se Coelho, *Organização do sistema*, 291-337. Salienta-se, ainda, a metodologia de avaliação do risco do impacto dos sistemas de inteligência artificial no domínio dos direitos humanos, da democracia e do Estado de direito (Huderia) recentemente proposta pelo Comité sobre Inteligência Artificial do Conselho da Europa – assim, em <https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f>.

³⁶ Assim, por todos, Cristina Alaimo e Jannis Kallinikos, *Data rules. Reinventing the market economy* (Cambridge/London: The MIT Press, 2024). Este também é um assunto inerente aos sistemas judiciais, numa governação dos dados naqueles trabalhados e nos quais se pode e deve ponderar, por exemplo, a utilização de sistemas de inteligência artificial – assim, Natalie Byrom, Mariane Piccinin-Barbieri e Peter Wells, “Towards effective governance of justice data”, *OECD Working Papers on Public Governance*, no. 74 (2024): https://www.oecd.org/en/publications/towards-effective-governance-of-justice-data_d2950e02-en.html.

adversarial machine learning, data poisoning, backdoors embedded)³⁷ e uma potenciação preocupante dos danos que lhes estará inerente.

Tal como acontece com o sistema governativo em geral também a transformação informacional e digital, bem como a automação e a IA, terão de implicar notáveis alterações na governação do sistema judicial e no desenho das políticas públicas correspondentes.

A tecnologia introduziu mecanismos transformativos da realidade organizacional e procedimental da justiça e a sua abordagem não se pode limitar, por isso, à mera preocupação de introduzir eficiência ou agilidade (qualidade/excelência) no sistema respetivo.

Assim, o funcionamento em rede e o recurso ao modelo informativo e de comunicação da plataforma, ponto de encontro do sistema informativo e externo, para além da introdução de ferramentas de trabalho eletrónicas em rede e em linha, e do registo em memória digital em nuvem, reforça a necessidade de adaptação e reconfiguração das organizações que são os tribunais e também as estruturas que os pretendem organizar e gerir, como são os Conselhos Judiciais, para além das próprias estruturas de governo do executivo para a área da justiça.

O funcionamento em rede também irá permitir uma nova configuração do papel e do lugar do sistema de justiça pública em face do mais global sistema de resolução de litígios (incluindo ADR e ODR's³⁸ ao lado ou em conexão com a justiça pública e a arbitragem), em disponibilidade multiportas, que ficará assim mais integrado e com possibilidade de um maior entrosamento e sincronização.

Num plano gradativo, a automação e a introdução de ferramentas de IA exigem das estruturas de governação da justiça um acréscimo no esforço de regulação, de organização e de gestão, de forma a instituir robustos mecanismos de avaliação que acompanhem não só a adoção dessas soluções tecnológicas de grande impacto e de assinalável risco, com uma preocupação essencial da sua certificação, mas também na sua implementação e operacionalidade. Assinale-se, como se referiu atrás, que a adoção destas ferramentas implica agência ou processos de transferência das regulações normativas (e dos respetivos comandos) para as próprias máquinas e para os códigos informáticos. A certificação dos sistemas exige um sistema de coordenação de todos os subsistemas da justiça, num plano de regulação que deverá atender aos níveis de coordenação considerados necessários para a instituição dos mecanismos de avaliação (prévios, concomitantes e posteriores) dos sistemas tecnológicos a utilizar com vista a sua ponderar da sua compatibilidade com os critérios mais ou menos exigentes a delinear para o sistema judicial.

Tudo este contexto salienta a necessidade de um maior nível de programação e coordenação – também ao nível político-constitucional – dos vários níveis de governação e gestão do sistema judicial.

Os sistemas de automação e de IA aplicados à atividade dos tribunais terão de ser condicionados a um princípio geral de avaliação, desde logo pelos condicionamentos, impactos e riscos envolvidos, atrás descritos de forma desenvolvida. Este enquadramento normativo e ético, para a utilização destas tecnologias no domínio da justiça, traça bem os desafios que se levantam, tanto do ponto de vista substantivo como de governação.

³⁷ Verificar em Micah Goldblum *et al.*, “Dataset security for machine learning: data poisoning, backdoor attacks, and defenses”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v. 45, no. 2 (2023): 1563-1580, <https://ieeexplore.ieee.org/abstract/document/9743317>.

³⁸ Como se sabe, acrónimos para Alternative Dispute Resolution (ADR) e Online Dispute Resolution (ODR).

Recorde-se que a consideração destes sistemas como de alto risco [cf. artigos 6.º a 27.º do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13/6/2024 sobre IA no seio da União Europeia] exige o preenchimento de requisitos apertados, para além da precisão, robustez e segurança e do princípio de supervisão humana (restrição dos sistemas em que o humano se possa encontrar totalmente fora do circuito).³⁹

Esta avaliação, no campo da justiça, deve ser apurada em ambiente necessariamente multidisciplinar e interinstitucional, pois terá de reportar valências de cariz diverso e ser capaz de fazer uma análise de prevenção, de acompanhamento e de inventariação dos efeitos e das consequências da adoção dos sistemas tecnológicos em causa (avaliação *ex ante* e *ex post*).

Do ponto de vista nacional, exige-se uma coordenação dos níveis de governação das várias ordens judiciais ou de tribunais (Tribunais Judiciais, Tribunais Administrativos e Fiscais, Tribunal Constitucional, Tribunal de Contas) para tal tarefa regulativa, avaliativa e até certificativa.

Tal mecanismo avaliativo terá de ponderar entre, por um lado, eficiência, eficácia e celeridade, e, pelo outro, qualidade, equidade e justiça, para além de ser capaz de realizar uma análise de impacto destes sistemas de IA para os direitos fundamentais (*v.g.* acesso à justiça e dados pessoais), para os princípios fundamentais do processo jurisdicional, para as garantias essenciais do Estado de direito (como a independência e a imparcialidade do juiz), para outras garantias inerentes à atividade jurisdicional (*v.g.* a fundamentação das decisões) e, ainda, outras considerações respeitantes à dimensão simbólica e cultural inerente ao processo judicial e à atividade dos tribunais.

Os padrões normativos suscitados apelam sempre à consideração do direito ao tribunal e a um julgamento justo e equitativo e também à consistência do sistema em causa com o direito à privacidade e à proteção dos dados pessoais (cf. artigos 6.º e 8.º, ambos da Convenção Europeia dos Direitos Humanos, e 8.º e 47.º da Carta dos Direitos Fundamentais da União Europeia).

Este assunto merece, também, uma ponderação ao nível da indispensável autonomia tecnológica do sistema judicial.

Para a justiça, esses mecanismos devem envolver tanto a legislação processual como de organização judiciária, e, do mesmo modo, a legislação atinente à segurança e robustez dos sistemas tecnológicos instalados.

Primeiro, no domínio processual, entrando agora na situação portuguesa, pensamos que a previsão genérica de tramitação eletrónica, enquanto modelo de habilitação normativa, com remissão para instrumento legal de menor força legal, e com um acentuado cariz regulamentador e administrativo como a Portaria, não assegura de forma satisfatória, em profundidade, latitude e legitimidade política, a resolução dos problemas que são agora colocados pela tecnologia (aplicada à justiça) ao processo jurisdicional, em todos os focos de irradiação devidamente acentuados no texto.

³⁹ Podemos dar conta, por exemplo, do relatório produzido pelo Centro de Pesquisa de Ciência e Conhecimento da Comissão Europeia, que aponta para um conjunto de requisitos de cibersegurança a que devem obedecer os sistemas de inteligência artificial de alto risco, nos padrões deste Regulamento sobre Inteligência Artificial – H. Junklewitz et al., *Cybersecurity of artificial intelligence in the AI Act. Guiding principles to address the cybersecurity requirement for high-risk AI systems* (Luxembourg: Publications Office of the European Union, 2023), <https://publications.jrc.ec.europa.eu/repository/handle/JRC134461>.

Depois, no que respeita à organização judiciária, denota-se a ausência de previsão e tratamento legal específico e integrado, nas próprias lei orgânicas dos Tribunais ou nos estatutos legais que tratam dos Conselhos Judiciais, das matérias atinentes ao domínio, à competência e à gestão dos sistemas de informação e tecnologias, para além do sector específico da proteção dos dados referentes ao sistema judicial, através da Lei n.º 34/2009 de 14 de julho. A gestão das infraestruturas e recursos tecnológicos, assim como a conceção, execução e avaliação dos planos e projetos de informatização, encontram-se entregues ao Instituto de Gestão Financeira e Equipamentos da Justiça, um instituto público inserido na orgânica do Ministério da Justiça, partilhando com a Direção-geral da Política da Justiça e com Direção-geral da Administração da Justiça a definição da planificação e desenvolvimento das políticas públicas definidas pelo Governo e o Ministério da Justiça [cf. artigos 10.º, n.º 2, alínea f), 11.º, n.º 2, alínea g), e 14.º, todos do Decreto-lei n.º 123/2011 de 29/12].

Do mesmo modo e na decorrência do que se acabou de descrever, a questão da cibersegurança dos tribunais será um assunto indefinido entanto estas diferenças legais e institucionais, acima assinaladas, até do ponto de vista da almejada autonomia tecnológica de todo o sistema judicial, não forem esclarecidas em face daquele que deve ser o lugar do sistema de informação e tecnologia do sistema judicial, até em face da administração pública e das estruturas governamentais, no esquema mais vasto e integrado de segurança do Ciberespaço na República Portuguesa. Sabendo que o desejável incremento da utilização das tecnologias aludidas (sistemas de informação, plataformas e redes digitais, automação e IA) tem como contrapartida uma maior exposição e potenciação do grau de intrusão e dos danos que podem ser provocados pelo cibercrime ou mesmo ao nível dos padrões da guerra tecnológica.⁴⁰

3. Administração dos tribunais e processo tecnológico

A dimensão tecnológica passou a influenciar, como vimos, as várias dimensões do sistema de justiça, incluindo na sua vertente de organização e procedimentalização. O processo tecnológico⁴¹ tem uma relevância crescente na administração dos tribunais e na gestão dos processos ali tramitados e apreciados.

A administração dos tribunais, naquele que será o segmento meso ou mediano de funcionamento do sistema judicial, impõe-se pela dimensão da sua importância reticular, nos pontos de interceção entre a governação do sistema no seu todo (assim, por exemplo, Parlamento, Governo/Ministério da Justiça e Conselhos Judiciais) com as dimensões de gestão dos tribunais, da sua gestão, presidência, relação com os Conselhos Judiciais, gestão de recursos humanos, tecnologia, e, também, gestão processual.

Na análise desta dimensão processual que se torna, no fundo, na própria elucidação do percurso, tramitação, fluxo e regulação dos atos inerentes à atividade dos tribunais, sabe-se que se não pode descurar a preservação de um justo equilíbrio entre os diversos compromissos aqui em presença. Designadamente, percebendo se as soluções encontradas, mais ou menos gestionárias, mais ou menos racionais em termos económicos ou eficientes, aptas a resolver as disfunções do sistema, podem e devem

⁴⁰ Sobre este ponto, especificamente, Coelho *et al.*, *Agenda da reforma da justiça*, 310-318.

⁴¹ Compreendendo o processo tecnológico como uma evolução natural das preocupações gestionárias na dimensão processual (processo gestionário) e da vontade de introduzir a dimensão digital e de automação no tratamento e resolução dos processos, o que pode ser explicado pelas etapas sucessivas atrás mencionadas dos sistemas de informação, da digitalização e da automação e inteligência artificial. Sobre esta evolução na dimensão processual, consulte-se Coelho, *Organização do sistema*, 664-690.

ser conciliadas com o respeito das garantias procedimentais e, fundamentalmente, do direito a um processo justo e equitativo.⁴²

A questão da gestão processual conectou-se com a utilização dos meios informáticos e das demais tecnologias de informação no tratamento dos processos – o que inclui a digitalização dos processos e a desmaterialização dos atos processuais –, na circulação da informação e dos dados referentes à realidade processual e dos tribunais, sem se descurar a elaboração de peças processuais ou ofícios tipificados, em linha com os circuitos telemáticos de informação.

Nesse sentido, o sistema judicial pode e deve ser analisado enquanto sistema complexo de processamento da informação, que se consubstancia nos vários atos praticados em tribunal, tenham eles um conteúdo dispositivo, enunciativo ou constitutivo, mas sempre de cariz comunicacional e relacional. Num processamento informativo e comunicacional que se dinamiza e articula para culminar no proferimento de uma última decisão jurisdicional, a qual terá de sair reforçada na sua fundamentação e credibilidade pela gestão de informação potenciada pela utilização das ferramentas tecnológicas e pelo conhecimento alargado e apurado que lhe é apanágio.⁴³

Nos tempos que correm e em pleno processo de transição digital das organizações públicas e na introdução de mecanismos de automação e IA, passam-se a encarar alternativas como o tratamento em linha (*online*) de todos os processos, a gestão eletrónica dos processos pelos vários tipos de utilizadores registados na rede, tanto internos como externos, a criação de um ambiente de trabalho digital e eletrónico em que o princípio do digital será tomado como defeito, a realização de diligências e audiências através de vídeo conferência e/ou de plataformas eletrónicas de reunião e trabalho remoto, o processamento eletrónico em rede, a comunicação eletrónica do/e com o tribunal, a desmaterialização acentuada ou mesmo total dos serviços prestados por um tribunal com a disponibilização de plataformas *online* de resolução de litígios (ODR's), onde os tribunais *online*, como dissemos atrás, se podem articular com outros meios de resolução de litígios (em sistema de multiportas).⁴⁴

⁴² Um processo digital que terá de ser marcado pelas componentes de garantia jurisdicional inerentes ao Estado de direito adaptadas às suas novas características (desmaterialização, virtualização e inteligência artificial) – assim, Erik Longo, *Giustizia digitale*, 325-355; Giovanni De Gregorio e Simona Demková, “The constitutional right to an effective remedy in the digital age: a perspective from Europe”, in *European Yearbook of Constitutional Law 2023*, eds. C. van Oirsouw *et al.* (Berlim: Springer, 2024), 223-254; e Marcin Górski, “Why a human court? on the right to a human judge in the context of the fair trial principle”, *eu crim*, v. 1 (2023): 83-87.

⁴³ Na consideração dos tribunais enquanto organizações de conhecimento e aprendizagem, neste domínio tecnológico e informativo caracterizado por uma grande especificidade. Uma diferenciação organizativa que se manifesta tanto no domínio estrutural como ambiental, gerando os fluxos processuais de acordo com as características tecnológicas e informativas adequadas, mormente na gestão dos processos e da dinâmica dos seus fluxos, na utilização da internet, no controlo da informação, na governação eletrónica, mas também na utilização de ferramentas (plataforma eletrónica de acesso e comunicação, gestão processual e de ficheiros e suporte digital e tecnológico) e na supervisão do acesso aos sistemas (segurança, autenticação, confidencialidade, sigilo, regras processuais, diretivas e legislação) – assim, Dougal McKechnie, *The use of the internet by courts and the judiciary: findings from a study trip and supplementary research* (Wellington, New Zealand: Department for Courts/The Law Foundation, 2002), 10-31.

⁴⁴ Coligir em A. Dory Reiling, “Courts and artificial intelligence”, *International Journal for Court Administration*, v. e11, no. 2 (2020), doi: 10.36745/ijca.343; Cayón, “Inteligencia artificial”, 381-427; Albert H. Yoon, “Technological challenges facing the judiciary”, in *Legal tech and the future of civil justice*, ed. David Freeman Engstrom (Cambridge: Cambridge University Press, 2023), 349-367; e David Freeman Engstrom e R. J. Vogt, “The new judicial governance: courts, data, and the future of civil justice”, *DePaul Law Review*, v. 72, no. 2 (Spring 2023): 171-238.

O que suscita algumas dificuldades acrescidas, como vimos, em face da natureza procedimental, ritual e simbólica que foi sempre atribuída à justiça enquanto sistema histórico sedimentado e público (portanto, com publicidade) de dirimção de conflitos e de reintegração da ordem jurídica violada.

Trata-se, afinal, de um debate que se veio a tornar mais vivo ou pertinente, nestes últimos anos, em torno da cibernetização da justiça, em torno das dimensões do numérico, do digital, da justiça *online* e do humano na realização da justiça.⁴⁵ Suscitam-se, assim, determinadas objeções a este fenómeno e que não deixam de ter óbvia pertinência, às quais os mais otimistas pretendem responder através de argumentos mais ou menos convincentes: – desaparecimento do espaço do tribunal e da cena judiciária, que passam a estar integralmente virtualizados e desenquadrados do seu simbolismo, com a absolutização da dimensão de serviço do tribunal; – uma justiça, assim, desumanizada, sistémica e sem alma, com empobrecimento da experiência do processo; – perda da natureza sincrónica do processo com tudo o que isso implica de deterioração da natureza e da garantia do direito processual; – os tribunais *online* e a justiça digital dependem do acesso à tecnologia e um nível de literacia computacional que muitos cidadãos ainda não possuem; – a independência judicial e a separação de poderes não é compatível com um tribunal *online* que possa guiar as partes e os intervenientes do ponto de vista do direito e do processo; e – perda progressiva (do parcial ao total) da intervenção humana e do juízo que lhe corresponde no ato de julgar e nos seus procedimentos.

Sendo certo que as ferramentas digitais e de automação, mesmo de inteligência (artificial), podem assumir diversa índole e alcance, desde aspetos que terão a ver com a gestão dos tribunais e dos procedimentos de gestão (de cariz considerado instrumental ou complementar em face da função jurisdicional, como vimos), atinentes à assim designada administração judiciária, até à verdadeira tramitação processual e proferimento de decisões.

No caso da IA as suas possíveis aplicações podem também passar pela classificação automática de informação, pela análise previsional de grandes quantidades de dados e correlação de diferentes naturezas e fontes de informação (*data mining*), pela deteção de padrões e correlação de eventos e pela produção de conhecimento, por exemplo, para analisar cada processo judicial (na sua argumentação jurídica intrínseca – *argument mining*) e identificar outros que possam estar relacionados, incluindo jurisprudência nacional ou internacional, propondo aos juizes um sumário do processo ou sugerindo sentidos de decisões.⁴⁶

⁴⁵ Um debate que se adensa nas perspetivas mais ou menos pessimistas ou otimistas sobre o futuro da justiça tecnológica, e que perpassam, com aqueles questionamentos, nas leituras das referências Antoine Garapon Jean Lassègue, *Justice digitale. Révolution graphique et rupture anthropologique* (Paris: Presses Universitaires de France, 2018); e Richard Susskind, 2019, *Online courts and the future of justice* (Oxford: Oxford University Press, 2019); e também no debate ocorrido, por exemplo, nos diversos painéis da conferência de alto nível realizada pelo Ministério da Justiça português aquando da presidência da União Europeia – assim, em Ministério da Justiça, *Conferência de Alto Nível. Para uma justiça eletrónica centrada nas pessoas. E-Justice* (Lisboa: Ministério da Justiça, 2021): <https://justica.gov.pt/Portals/0/Ficheiros/Organismos/JUSTICA/eBook%20Conferencia%20eJustice%202021-PT.pdf?ver=nzVG9Qa2B83cfM9ej5w9mA%3d%3d>. Certo que se terá de atender, sempre, que o direito (produzido pelas fontes formais) corre o risco de perder influência sobre os cidadãos ao não reconhecer o quanto o ambiente digital precisa de novos modelos de realização da justiça – Ethan Katsh e Orna Rabinovich-Einy, *Digital justice: technology and the internet as disputes* (New York: Oxford University Press, 2017), 174.

⁴⁶ Nesta diversidade de aplicações tecnológicas merece ponderação uma distinção introduzida pela cientista Cassie Kozyrkov nas suas palestras, ao diferenciar na atividade cognitiva em geral os processos automáticos e subconscientes em que nos envolvemos constantemente (repetitivos), assim

À medida que se vai avançando para mais perto da decisão jurisdicional, passando do mero plano do assistente judicial para a substituição efetiva do juiz humano,⁴⁷ como vimos noutros pontos, as escolhas ficam mais sensíveis (nas opções de ponderação políticas, governativas e constitucionais), pois a salvaguarda da integridade do juízo humano na justiça, entendida como radicalidade (desde logo na sua dimensão ética), pode ficar em causa.

Importa aqui atender à importância de refletir este tema à luz da diferenciação processual, à luz dos valores e da matéria em questão (*v.g.* criminal ou civil), bem como da natureza do processo e da sua complexidade.

De assinalar aqui que após a pandemia e a disseminação generalizada dos sistemas de IA de inegável potencial já referidos de início muitos dos judiciários sentiram necessidade de acompanhar esta evolução tecnológica de grande repercussão social, económica e política, com informação e formação também disponibilizada aos juízes e a quem trabalha nos tribunais. Pensamos que essa será uma inevitabilidade e uma ação necessária a par da urgente certificação destas ferramentas para uso nas funções judiciais e jurisdicionais, de forma consistente, regulada e de acordo com as boas práticas entretanto desenvolvidas, também na maior parte dos fóruns de discussão destes temas a nível internacional.

4. Decisão judicial. O espaço, também tecnológico, de realização jurisdicional

As considerações teóricas e epistemológicas iniciais e também o desenvolvimento antecedente das diferenças escalas em que se pode dimensionar o sistema judicial fazem apurar estas considerações a propósito do espaço mais íntimo de realização jurisdicional.

Qual o impacto na estrutura e no sentido da jurisdição que nos trouxeram as fortes mutações operadas no ambiente social, político e tecnológico que acima ficaram descritas?

Como vimos, a tecnologia não pode ser considerada apenas como uma ferramenta pois a mesma integra-se com o direito no conjunto das interações humanas no triplo ponto de vista organizativo, procedimental e institucional. Uma aceção que faz todo o sentido repetir, dada a sua repercussão sistémica.

Atendendo ao nexos relevante que pode ser estabelecido entre decisão e organização, teremos de decifrar na dinâmica da tomada de decisão judicial, o lugar que a tecnologia

designados na gíria da computação como “*thunking*”, dos demais processos cognitivos ativos e de maior envolvimento (e satisfação intelectual), que implicam criatividade, inspiração e assunção crítica e ética, e que se devem estar associados ao verdadeiro pensamento – “*thinking*.” Para este nível, as respetivas competências, capacidades ou virtudes devem estar de alguma forma associadas à presença do fator humano no circuito de processamento (*v.g.* decisão, *design*, criatividade, comunicação, resolução de problemas, engenharia, relações interpessoais, colaboração, confiança e adaptabilidade). Sobre este ponto, consulte-se Cassie Kozyrkov, “Thinking vs thinking: whose job does AI automate? Which tasks are on AI’s chopping block?”, *Medium*, 2023, disponível em <https://kozyrkov.medium.com/thinking-vs-thinking-whose-job-does-ai-automate-959e3585877b>.

⁴⁷ Ainda aqui podemos encontrar os clássicos níveis de intervenção humana no circuito de inteligência artificial: *human in-the-loop* (o sistema autónomo foi projetado para trabalhar cooperativamente com o humano para concluir as suas tarefas, podendo em regra ser estabelecido que a tomada de decisão fica dependente da intervenção humana nos casos de ponderação moral ou ética), *human on-the-loop* (o sistema autónomo foi projetado para a supervisão humana, em que o humano pode intervir facilmente se as decisões da inteligência artificial estiverem erradas, representarem um perigo significativo ou comprometerem a ética), e *human out-of-the-loop* (o sistema é integralmente autónomo pois foi projetado para operar sem supervisão ou envolvimento humano).

assume nos demais fatores organizativos e as condições organizativas na jurisdição, com especial relevância para a independência jurisdicional, a governação da justiça, a gestão dos tribunais, a gestão processual e o ato jurisdicional enquanto tal.

A este nível decisional sabemos que o princípio da independência jurisdicional deve ter uma maior amplitude de aplicação e de garantias, pois estamos no nível máximo de aproximação com o núcleo do decisor jurisdicional (juiz ou juízes, conforme o pendor singular ou coletivo do tribunal).

A orientação mais alargada de que se partiu sobre a própria jurisdição não descarta nem pretende minorar o momento essencialmente jurídico da aplicação ou realização do direito, mas que não pode deixar de estar incluído – sob pena de isolamento sistémico – num horizonte ou estrutura mais vasta, inerente às suas condições estruturais de concretização.

As considerações teóricas e epistemológicas iniciais e também o desenvolvimento antecedente das diferenças escalas em que se pode dimensionar o sistema judicial fazem apurar estas considerações a propósito do espaço mais íntimo de realização jurisdicional.

À medida que se vai avançando para mais perto da decisão jurisdicional, passando do mero plano do assistente judicial para a substituição efetiva do juiz humano, como veremos noutros pontos, as escolhas ficam mais sensíveis (nas opções de ponderação políticas, governativas e constitucionais), pois a salvaguarda da integridade do juízo humano na justiça, entendida como radicalidade (desde logo na sua dimensão ética e filosófica), pode ficar em causa.

As linhas demarcadoras desta reserva do humano no ciclo de tomada de decisão judicial podem e devem admitir alguma ponderação concreta, admitindo-se, nesta reflexão, uma diferenciação que tenha como pressuposto, por exemplo, a distinção de qual a matéria jurisdicional em que nos encontramos (*v.g.* jurisdição civil e administrativa ou jurisdição criminal ou constitucional), a natureza probatória ou jurídica da informação trabalhada, ou, do mesmo modo, a complexidade ou o valor dos interesses colocados pela ação judicial em curso.⁴⁸

Mas, sendo certo que o grau de introdução destes automatismos poder ter lugar numa lógica de diferenciação, a verdade é que o tratamento das decisões judiciais, que podem assumir diferentes matrizes e ajustamentos em função do estilo ou das especificidades de cada uma dessas jurisdições, não pode omitir uma dimensão unitária na metodologia de abordagem gestionária da decisão. Com a otimização do trabalho judicial no seu núcleo mais essencial que é a decisão, quer do ponto de vista das decisões interlocutórias, quer sobretudo do ponto de vista da sentença, impõe a adoção de estratégias ou mecanismos de racionalização normativa ou jurídica (com a convocação da gramática própria dos juristas)⁴⁹ que são comuns a qualquer que seja o sistema ou a jurisdição onde se proferem decisões, nomeadamente no modo como se decide, na forma como a decisão é elaborada ou nos mecanismos tecnológicos e de comunicação que a envolvem.⁵⁰

⁴⁸ Numa diferenciação que é marcada pela intensidade social das situações em presença e pelos valores normativos ou bens jurídicos em questão.

⁴⁹ O que é diferenciador na ação do direito e da realização da justiça passa pela imparcialidade assente na legitimação conferida pela norma jurídica enquanto compromisso social e ético que supera a controvérsia ali em presença, com todos os seus inerentes interesses – assim, Ralf Poscher, “The common error in theories of adjudication: An inferentialist argument for a doctrinal conception”, in *The pragmatic turn in Law. Inference and interpretation in legal discourse*, eds. Janet Giltrow e Dieter Stein (Boston/Berlin: De Gruyter Mouton, 2019), 328-329.

⁵⁰ Sendo certo que a introdução de ferramentas ou automatismos inteligentes como auxiliares à decisão, de grande alcance de conteúdo e assertividade estatística, trará alterações nítidas na operação

Os exemplos extraídos das experiências em torno da justiça preditiva nos Estados Unidos da América e na Inglaterra (sistemas *Compas* e *Hart*) e da esmagadora reforma tecnológica da justiça na China (“*tribunal inteligente*” e “*juízos semelhantes para casos semelhantes*”)⁵¹ podem traçar os limites da adoção de mecanismos de automação e de IA na gestão dos procedimentos judiciais e no próprio processo de tomada da decisão judicial.

Estas mutações – e nomeadamente aquelas provocadas pela tecnologia na atividade judicial – fazem agudizar a necessidade de alterações no paradigma decisório ainda prevalecente e um reforço da ética judicial na atividade judicial, de forma mais marcante no domínio decisório.⁵²

Trata-se de um trabalho de extrema sensibilidade, como o do ourives ou do joalheiro, em que as referências sistémicas, o sentido de apuramento da diferenciação processual e a importância que terá o humano no apuramento das melhores soluções metodológicas e procedimentais, terão de ser equacionadas numa ponderação finalística – na obtenção de um sentido mais enriquecido de jurisdição – mas com componentes também tecnológicas e pluridisciplinares.

Essa definição de jurisdição deve, pois, ser aprofundada e densificada nos seus diversos níveis de apreciação, também no que respeita à capacidade do sistema de realização do direito, a cargo dos juizes, de se abrir ou fechar aos componentes externos à disciplina normativa do direito, de se legitimar e fortalecer no seu próprio contexto de realização (enquanto espaço organizativo, institucional ou tecnológico), mas, também, na virtualidade de reponderação dessa mesma atividade judicativa (apta a justificar a decisão jurisdicional) de acordo com a moldura⁵³ que é delineada pelas exigências metodológicas, principiológicas e, do mesmo modo, institucionais, que marcam a identidade do direito.⁵⁴

de composição e elaboração dos próprios textos decisórios, suscitando um maior apuramento nas capacidades de edição e de confirmação dos enunciados propostos pelos automatismos (de vigilância) com a veracidade factual, normativa, jurisprudencial e normativa, sem perdas do carácter de inovação nas soluções jurídicas encontradas em face do risco de padronização e de sobrevalorização das possíveis analogias – para alguns destes aspetos, Damien Charlotin, “Les Large Language Models et le future du droit” in *L'intelligence artificielle face à l'État de droit*, dir. Charly Derave, Benoit Frydman e Nathan Genicot (Bruxelas: Bruylant, 2024), 121-136. Será, aqui, que se demonstra mais necessário recompor o ciclo renovado do paradigma decisório e de reforço da ética judicial, tudo acompanhado da necessária capacitação dos juizes neste domínio de intercessão entre a atividade judicial e a tecnologia.

⁵¹ Sobre estes exemplos de aplicação de sistemas de inteligência artificial no domínio decisório, consulte-se descritiva e criticamente em Coelho, *Organização do sistema*, 360-363.

⁵² E, tal como se afirmou anteriormente, também ao nível da capacitação dos juizes nestes domínios, o que tem sido salientado pela experiência internacional que nos tem oferecido várias referências de manuais neste domínio – assim, Consultative Council of European Judges, 2023, *Opinion No. 26 (2023): Moving forward: the use of assistive technology in the judiciary*; Courts and Tribunals Judiciary, 2023, *Artificial Intelligence (AI). Guidance for judicial office holders*, 12 December 2023, London: Judicial Office, <https://www.judiciary.uk/wp-content/uploads/2023/12/AI-Judicial-Guidance.pdf>; Federal Judicial Center, 2023, *An Introduction to Artificial Intelligence for federal judges*, Washington: Federal Judicial Center; e UNESCO – United Nations Educational, Scientific and Cultural Organization, *Global toolkit on AI and the rule of law for the judiciary* (Paris: UNESCO, 2023).

⁵³ A representação da moldura aplicada ao contexto jurídico e judicial, pode assumir uma diversidade de sentidos, desde a amplitude da tarefa interpretativa ou aplicativa do direito (realização do direito), até ao papel do direito na organização social, passando pela ideia de equilíbrio e justiça na ponderação de valores e interesses contrapostos. Neste último sentido, aviva-se o pensamento de Ronald Dworkin, ao estabelecer a moldura como modelo da relação entre os princípios jurídicos e a decisões judiciais, em que aqueles desempenham um papel delimitador da ação do intérprete, imprimindo coerência e significado a estas últimas, e, por último, concedendo ao sistema a pretendida integridade – cfr. Ronald Dworkin, *Taking rights seriously* (Cambridge: Harvard University Press, 1978), 28-80.

⁵⁴ O direito, e, assim, a jurisdição, manifestam-se segundo a metáfora da moldura, entre a abertura e

A liberdade e autonomia (até criativa) de interpretação e de realização do direito tem como pressuposto uma autonomia e independência nas condições estruturais, organizativas e tecnológicas. As garantias constitucionais e procedimentais do direito terão de zelar por esse espaço autónomo da prática jurisdicional.

Daí se compreende o cuidado tomado pelo direito público e constitucional sobre essa dimensão organizativa, como se depreende dos esforços em torno da defesa e garantia do Estado de direito, tanto na compreensão material ou substantiva do direito organizatório⁵⁵ e da teoria da direção do assim designado Novo Direito Administrativo⁵⁶ como no desenvolvimento jurisprudencial e recomendatório a nível internacional e nacional como ficou assinalado.

Também comprova esta alusão, a definição dos estados sucessivos de apreciação e controlo da jurisdição advogados por Benoît Frydman,⁵⁷ que desde a apreciação da legalidade (nomofilaquia), desembocam numa sindicância sobre a qualidade ou a excelência da administração da justiça, ou a superação para um modelo recursivo que incrementa o desenvolvimento criativo do direito, tal como salientado por Michele Taruffo.⁵⁸

A linha de base jurisprudencial pode ser revigorada caso as suas condições de exercício e de estruturação sejam bem pensadas, otimizadas e adequadas às novas

o fechamento, na latente oposição entre os discursos juristicistas e os discursos de área aberta, numa dialética entre problema e sistema. A aludida metáfora da moldura entre a pluralidade de sentidos possíveis, admitida por Kelsen quanto à tarefa do intérprete e o seu ato interpretativo – Hans Kelsen, *Pure Theory of Law* (Clark: The Lawbook Exchange, 2005), 350-352, é aqui assumida como uma característica própria do sistema. Por seu turno, a opção jurisprudencialista assenta nessa conceção do sistema jurídico e em diversas contraposições que marcam a validade comunitária e os contextos de realização do direito – assim, em José M. Aroso Linhares “Jurisdição, diferendo e área aberta: a caminho de uma teoria do Direito como moldura?”, in *Ars Iudicandi – Estudos em homenagem ao Prof. Doutor Jorge de Figueiredo Dias*, Volume IV, Boletim da Faculdade de Direito da Universidade de Coimbra, (Coimbra: Coimbra Editora, 2010), 443-477, e José M. Aroso Linhares, “Validade comunitária e contextos de realização: anotações em espelho sobre a concepção jurisprudencialista do sistema”, *Revista da Faculdade de Direito da Universidade Lusófona do Porto*, v. 1, no. 1 (2012): 1-42, e José M. Aroso Linhares, “The rehabilitation of practical reasoning and the persistence of deductivism: an impossible challenge”, *International Journal for the Semiotics of Law*, v. 33, no. 1 (2020): 155-174, com alusão a esta imagem da moldura e aos contrapontos pluralidade/unidade, dogmática/reflexão crítica, sociedade/comunidade e legalidade/moralidade. Trata-se de uma abordagem que parte do pensamento fundamental de Castanheira Neves e que também pode ser revisitada em Coelho, *Organização do sistema*, 190-193 e 831-842.

⁵⁵ Assim, Gomes Canotilho, *Direito Constitucional e teoria da constituição*, 7.ª edição (Coimbra: Almedina, 2003) 542.

⁵⁶ Um novo direito administrativo salientado, entre outros, por José Carlos Vieira de Andrade, *Lições de Direito Administrativo* (Coimbra: Imprensa da Universidade de Coimbra, 2010), 25-26, resultado das transformações do direito administrativo clássico operadas pela sua socialização, pelo novo contexto institucional de poder e pelas transformações do jurídico (*soft law*, policentralidade, economicização do direito, conectividade multi-nível, desmaterialização e digitalização). Com maior evidência na linha de reforma do direito administrativo encetada, entre outros, por Eberhard Schmidt-Aßman e pelo já identificado Andreas Voßkuhle – cf. Andreas Voßkuhle, “Sobre el método del Derecho Administrativo”, in *Innovación y Reforma en el Derecho Administrativo*, ed. Javier Barnes, 2.ª edição (Sevilha: Global Law Press – Editorial Derecho Global, 2012), 185-188; Eberhard Schmidt-Aßman, *La Teoría general del Derecho Administrativo como sistema. Objeto y fundamentos de la construcción sistemática* (Madrid: Marcial Pons, 2003), 3-26, e Ricardo Alexandre Sousa da Cunha, *Constituição e legalidade administrativa cosmopolita: O Direito Administrativo global entre a constitucionalização e a fragmentação* (Coimbra: Almedina, 2016), 434-445.

⁵⁷ Fazendo realçar a evolução dos critérios e os meios de controlo da qualidade das decisões judiciais – assim, Benoît Frydman, “L’évolution des critères et des modes de contrôle de la qualité des décisions de justice”, in *La qualité des décisions de justice*, CEPEJ Studies no. 4, Actes du colloque de Poitiers, 8-9 março 2007, 18-29.

⁵⁸ Assim, em Michele Taruffo, “Las Funciones de las Cortes Supremas”, in *La misión de los tribunales supremos*, coords. Michele Taruffo, Luiz Guilherme Marinoni e Daniel Mitidiero (Madrid/Barcelona/Buenos Aires/São Paulo: Marcial Pons, 2016), 231-251.

e radicais exigências sociais, económicas, tecnológicas e ambientais, e devidamente integradas, num comprometimento com a incondicionalidade da concretização do Estado de direito e com a democracia. A afirmação do direito enquanto síntese tridimensional: social, institucional e ética.

As dimensões do Estado de direito são convocadas de forma a perceber como a sua estrutura, a sua fortaleza ou a sua debilidade podem colocar em causa o papel do juiz e da justiça, como se pode salientar bem a propósito da reflexão do judiciário alemão do período nazi (por exemplo nas conclusões aludidas na investigação liderada por Hans Petter Graver, *Judges Under Stress*),⁵⁹ ou da experiência mais recente das alterações introduzidas na governação e na organização da justiça nos regimes populistas ou autocráticos europeus.

Só a consciência desse sistema, dos seus condicionalismos pode fazer libertar e reforçar a ação do direito realizado pelos juízes de forma a ele se apresentar da forma mais eficiente, efetiva, qualificada, mas também comunicativa, atrativa, transparente, treinada, ágil, tecnicamente rigoroso, de molde a reintegrar o dano, o prejuízo, os valores em crise, a ilicitude, a violação dos direitos fundamentais ou mesmo a transgressão de princípios prudenciais conexos com a natureza animal ou ambiental.

Também aqui, tal como no desempenho do organista, para além do domínio da técnica e da condicionante mais ou menos rica da tecnologia (literalmente), existe um limite sempre insuperável: há que interpretar o direito até aos limites quase transcendentais da realidade espessa e desafiante do contexto interpretativo (da vida), mas sem o prostituir. Sendo inevitável, tal como para Juan de la Rubia,⁶⁰ o retorno a Wagner, isto é, no caso da jurisdição, o retorno à moldura jurisprudencial do direito.

Terminamos como começamos. O que é que Wagner e um órgão de tubos de uma catedral tem a ver com o tema do direito e tecnologia e como a dedicação a um horizonte mais alargado sobre a função do juiz e da justiça enquanto organização pode desembocar no retorno ao que mais íntimo e mais expansivo pode ter a ideia de justo e a realização da justiça?

Na verdade, neste espaço íntimo da decisão jurisdicional, individual ou coletiva, acontece a concretização vivencial do direito, qualquer que seja a sua via, integrada de mais ou menos algoritmos, mas necessariamente treinada, qualificada, tecnicamente e esteticamente apurada, pacificadora, humana. A ligação com a tecnologia é feita por este apuramento da nossa relação com o mundo exterior, mais ou menos potenciada pela máquina. Porém há sempre que retornar ao essencial, a essa moldura onde reencontramos o outro e a possibilidade de resolvermos os seus dilemas. A moldura jurisprudencial do direito. Mas o caminho é integrativo e aberto ao conhecimento da nossa própria condição e dos nossos condicionamentos, também tecnológicos.

⁵⁹ Mais genericamente sobre a adesão dos juízes ao direito autoritário e injusto, resultado das experiências nazis, fascistas, do apartheid ou das ditaduras dos países latinos, em Hans Petter Graver, *Judges against justice: on judges when the rule of law is under attack* (Heidelberg/New York/Dordrecht/London: Springer 2014).

⁶⁰ Seguir os passos de uma entrevista notável que é também o retrato de um organista primoroso, <https://www.youtube.com/watch?v=cVrzrSwIGtE&t=9s>.

Sustentabilidade tecnológica e justiça eletrónica europeia numa União de direito: a interoperabilidade judiciária e o papel da inteligência artificial no domínio da justiça

*Joana Covelo de Abreu**

1. Introdução

A União tem um objetivo específico de proporcionar “aos seus cidadãos um espaço de liberdade, segurança e justiça sem fronteiras internas”, proclamado no artigo 3.º, n.º 2 do Tratado da União Europeia (doravante, TUE), e devidamente concretizado à luz do disposto nos artigos 67.º e seguintes do Tratado sobre o Funcionamento da União Europeia (TFUE). Assim, empenhou-se na criação de um espaço onde os direitos fundamentais fossem protegidos e respeitados, tendo em conta os “*diferentes sistemas e tradições jurídicos dos Estados-Membros*” (artigo 67.º, n.º 1 do TFUE). Caraterizado como um espaço de justiça, “*o acesso à justiça é um direito fundamental basilar da União Europeia*”,¹ na medida em que, no seu contexto, a União tem a missão de “*facilita[r] o acesso à justiça, nomeadamente através do princípio do reconhecimento mútuo das decisões judiciais e extrajudiciais em matéria civil*” – artigo 67.º, n.º 4 do TFUE.

Ora, “[a] utilização de meios e instrumentos tecnológicos aumentou nas nossas sociedades nos últimos anos, tendo sido particularmente acelerada pela pandemia da COVID-19, dando origem a expectativas crescentes no que diz respeito aos serviços digitais.”² Neste contexto, e na senda de anteriores soluções confluentes, em janeiro de 2025, o Conselho da União Europeia adotou a estratégia e o plano de ação para a justiça eletrónica relativos ao período de 2024 a 2028, visando equacionar soluções que, continuando a afirmar a União como um espaço de liberdade, segurança e justiça, pudessem contemporaneizar os desafios que a digitalização levanta à justiça europeia e incorporar as suas vantagens na promoção da tutela jurisdicional efetiva.

Na realidade, qualquer profissão jurídica está a ser submetida a uma transformação desafiante, sobretudo causada por alguns fatores que, por si só, já eram suficientemente impactantes mas que, cada vez mais, devem ser perspetivados de forma confluyente: a par da globalização, a liberalização dos serviços jurídicos (seguindo a tendência verificada no âmbito da prestação de outros serviços) veio acompanhada pelo uso de novas e inteligentes tecnologias que passaram a desempenhar funções que, até muito recentemente, eram confiadas aos operadores judiciais

* Professora na Escola de Direito da Universidade do Minho. Membro do Centro de Excelência Jean Monnet CitDig (Cidadania Digital e Sustentabilidade Tecnológica) da Escola de Direito da Universidade do Minho (Portugal).

¹ Cfr. Conselho da União Europeia, Estratégia europeia para a justiça eletrónica 2024-2028, C/2025/437, de 16.01.2025, parágrafo 2

² Cfr. Conselho da União Europeia, Estratégia europeia para a justiça eletrónica 2024-2028, C/2025/437, de 16.01.2025, parágrafo 3.

como advogados, funcionários judiciais e juízes. Tal teve um impacto significativo na própria perceção do que é a justiça eletrónica europeia nos dias de hoje, cabendo compreender o sedimento jurídico-constitucional que lhe pode dar consubstanciação para, num segundo momento, analisarmos o caminho que a presente estratégia visa percorrer. Num terceiro momento, a atenção incidirá sobre duas das suas principais apostas: a sedimentação das soluções de interoperabilidade judiciária e a exploração da inteligência artificial ao serviço da justiça.

2. Sustentabilidade como fundamento jurídico-constitucional para a União Europeia

Atendendo aos novos desafios que a sociedade enfrenta, o princípio da sustentabilidade tem sido discutido como um “*elemento estrutural típico*”³ de um ordenamento jurídico que tem uma base jurídico-constitucional: a partir da perceção de que o conceito de sustentabilidade pode emergir como um interesse público primário a ser prosseguido e concretizado, já que “*a sustentabilidade configura-se como uma dimensão autocompreensiva de uma constituição que lev[a] a sério a salvaguarda da comunidade política em que se insere*”, ele tem a suscetibilidade de atuar como um novo paradigma secular.⁴

No entanto, para que possa operar enquanto tal, o princípio da sustentabilidade tem de ser suficientemente integrativo e “*aberto*”:⁵ para além de contemplar as dimensões (ou pilares) que tradicionalmente lhe estão associadas – aquelas relativas à sustentabilidade económica, social e ambiental⁶ – cabe-lhe ainda assumir uma nova dimensão tecnológica que, à luz da revolução agora vivenciada, pode ser capaz de atuar como o elemento de articulação entre as três dimensões tradicionais.⁷

Através da Decisão 2022/2481,⁸ a União Europeia proclamou esta década como digital⁹ e chamou a atenção para a instrumentalidade das ferramentas tecnológicas e digitais ao princípio da sustentabilidade, transformando – sem impor limitações – a natureza do crescimento económico, o sentido da inclusão social e o desafio da proteção ambiental. Nesta Decisão, sublinhou-se que “[a] via da União para a transformação digital da economia e da sociedade [abrange] a soberania digital de forma aberta”, respeitando os diversos princípios e valores identitários europeus, onde se destaca também a sustentabilidade.¹⁰ É também reconhecido que “[a] União precisa de um setor digital que coloque a sustentabilidade no seu centro.”¹¹ Nos termos do artigo

³ Cfr. Peter Häberle, “Nachhaltigkeit und Gemeineuropäisches Verfassungsrecht”, in *Nachhaltigkeit als Verbundbegriff*, org. Wolfgang Kahl (Tübingen, 2008), 8 (tradução livre).

⁴ Cfr. José Joaquim Gomes Canotilho, “O princípio da sustentabilidade como princípio estruturante do Direito Constitucional”, *Revista de Estudos Politécnicos*, Vol. VIII, no. 13 (2010): 7-18, 8.

⁵ Cfr. José Joaquim Gomes Canotilho, “O princípio da sustentabilidade”, 8.

⁶ Cfr., para maiores desenvolvimentos, Wolfgang Kahl, “Einleitung: Nachhaltigkeit als Verbundbegriff”, in *Nachhaltigkeit als Verbundbegriff*, org. Wolfgang Kahl (Tübingen, 2008), 12 e seguintes.

⁷ Aderimos à posição professada por Alessandra Silveira. Cfr., para maiores desenvolvimentos, Alessandra Silveira, “Apresentação”, in *Sustentabilidade tecnológica: o papel das tecnologias digitais na promoção do desenvolvimento sustentável*, coord. científica Alessandra Silveira *et al.* (Universidade do Minho, Escola de Direito, 2020), 4-5.

⁸ Cfr. Decisão (UE) 2022/2481 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, que estabelece o programa Década Digital para 2023.

⁹ Cfr. Comissão Europeia, *Comunicação ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões “Orientações para a Digitalização até 2030: a via europeia para a Década Digital”*, Bruxelas, 9.3.2021, COM(2021) 118 final.

¹⁰ Cfr. Decisão (UE) 2022/2481, considerando 1.

¹¹ Cfr. Decisão (UE) 2022/2481, considerando 6.

3.º, n.º 1, e) da Decisão, é objetivo geral da Década digital “[d]esenvolver um ecossistema abrangente e sustentável de infraestruturas digitais interoperáveis”, em que [...] a inteligência artificial, entre outras soluções tecnológicas inovadoras “funcionem em convergência, para promover a sua aceitação pelas empresas da União e para criar oportunidades de crescimento e emprego através da investigação, do desenvolvimento e da inovação.”

No mesmo sentido, a Declaração Europeia sobre os direitos e princípios digitais para a década digital¹² assume a sustentabilidade como um arquétipo que funciona como fundamento e teleologia para uma compreensão jurídico-constitucional de que a comunidade politicamente organizada da União Europeia está empenhada na dimensão digital e tecnológica: considerando que “[a] transformação digital afeta todos os aspetos da vida das pessoas”, a promoção da sustentabilidade surge como objetivo a ser prosseguido quer pela União, quer através das orientações que são dadas aos decisores políticos tendentes à sua reflexão sobre a transformação digital.¹³ Assim, sob o seu capítulo VI, dedicado à “Sustentabilidade”, a Declaração em causa avança, a partir da perspetiva tecnológica e digital (= da sustentabilidade tecnológica), soluções que se comprometem com a promoção da sustentabilidade ambiental, económica e social: por um lado, sublinhando que “os produtos e serviços digitais devem ser concebidos, produzidos, utilizados, reparados, reciclados e eliminados de forma a atenuar o seu impacto negativo no ambiente e na sociedade e a evitar a obsolescência prematura”;¹⁴ por outro, asseverando que “[t]odas as pessoas devem ter acesso a informações exatas e de fácil compreensão sobre o impacto ambiental e o consumo de energia dos produtos e serviços digitais, bem como sobre a sua reparabilidade e durabilidade, permitindo-lhes fazer escolhas responsáveis.”¹⁵

Posto isto, os objetivos delineados para esta década digital (aqueles que reputam essencial que a União se afirme soberana digitalmente, conseguindo garantir os seus valores essenciais, onde se inclui a sustentabilidade, designadamente através da implementação e sedimentação de soluções interoperáveis e da criação de um ambiente favorável à criação e ao recurso a tecnologias disruptivas, como a IA) têm observado seguimento institucional, equacionando o “Estado da Década Digital”: através da Comunicação “Estado da Década Digital 2024”,¹⁶ a Comissão Europeia faz um segundo balanço sobre a década digital que atravessamos, na sequência do relatório anteriormente apresentado, em setembro de 2023.¹⁷

Assim, se, por um lado, o quadro jurídico criado é único no mundo, continuando a permitir uma influência internacional, verifica-se a “necessidade crítica de ação e investimento a nível nacional e da UE” em vários domínios como, por exemplo, as competências digitais, os especialistas de TIC, a conectividade de elevada qualidade e a disseminação da Inteligência Artificial e da análise de dados,

¹² Cfr. Parlamento Europeu, Conselho e Comissão Europeia, *Declaração Europeia sobre os direitos e princípios digitais para a década digital*, Bruxelas, 23.1.2023, 2023/C 23/01.

¹³ Cfr. Parlamento Europeu, Conselho e Comissão Europeia, *Declaração Europeia sobre os direitos e princípios digitais para a década digital*, Bruxelas, 23.1.2023, 2023/C 23/01, considerando 2 e 7.

¹⁴ Cfr. Parlamento Europeu, Conselho e Comissão Europeia, *Declaração Europeia sobre os direitos e princípios digitais para a década digital*, Bruxelas, 23.1.2023, 2023/C 23/01, declaração n.º 23.

¹⁵ Cfr. Parlamento Europeu, Conselho e Comissão Europeia, *Declaração Europeia sobre os direitos e princípios digitais para a década digital*, Bruxelas, 23.1.2023, 2023/C 23/01, declaração n.º 24.

¹⁶ Cfr. Comissão Europeia, *Comunicação ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões “Estado da Década Digital 2024”*, Bruxelas, 2.7.2024, COM(2024) 260 final.

¹⁷ O primeiro relatório foi apresentado em setembro de 2023, substituindo o anteriormente conhecido Índice de Digitalidade da Economia e da Sociedade – IDES. Cfr. Comissão Europeia, *Comunicação ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões “Relatório sobre o estado da Década Digital 2023”*, Bruxelas, 27.9.2023, COM(2023) 570 final.

entre outros.¹⁸ Cabe, assim, à União e aos seus Estados-Membros uma ação mais coordenada e coesa de forma a dar cumprimento ao quadro regulatório entretanto adotado. Do mesmo modo, a redução dos encargos administrativos é essencial, *“tanto na aplicação como na execução dos atos legislativos em vigor”*, designadamente criando *“sinergias”*, evitando *“duplicações”* e adotando *“uma abordagem coordenada para a gestão das estruturas de governação existentes, com coerência entre a política digital e a política de cibersegurança.”* Esta abordagem releva especificamente em matéria de interoperabilidade, já que visa permitir *“uma partilha harmoniosa de dados e informações entre os [...] sistemas”* já existentes nos Estados-Membros, no âmbito das suas respetivas entidades competentes, enquanto impõe que a União esteja preparada *“para assegurar a disponibilidade de redes de conectividade e informáticas colaborativas fiáveis, rápidas e seguras [...], promovendo a digitalização das empresas e dos serviços públicos em prol dos utilizadores nacionais e transfronteiriços.”*¹⁹ Simultaneamente, a contínua aposta na criação de um ambiente convidativo à criação e ao desenvolvimento de tecnologias disruptivas no contexto europeu, onde a inteligência artificial pode ter um papel relevante, é um ponto estratégico para, por um lado, aumentar a competitividade da União²⁰ enquanto se promove uma *“transição ecológica inteligente.”*²¹

Posto isto, o conceito de sustentabilidade – quer na sua dimensão analítica (descritiva) mas, sobretudo, na sua dimensão normativa (prescritiva) – é chamado a compreender a forma como os contínuos desenvolvimentos tecnológicos impactam e interagem na economia (mundial), na sociedade (global) e no ambiente (sem fronteiras) do planeta, conduzindo a um crescimento económico socialmente inclusivo, ambientalmente sadio e tecnologicamente equitativo.

Assim, enquanto complexo sinérgico das dinâmicas económicas, sociais, ambientais e tecnológicas que interagem e revolucionam o processo de desenvolvimento, a sustentabilidade tem a potencialidade de atuar como um conceito essencial à era digital que agora vivemos, definindo as condições e os pressupostos para a regulação jurídica e a tomada de decisões políticas e administrativas, num contexto em constante evolução.²²

3. A interoperabilidade judiciária e a inteligência artificial à luz da estratégia da justiça eletrônica europeia de 2024 a 2028

A nova estratégia da justiça eletrônica europeia parte da premissa de que o sistema judiciário *“adere à digitalização e aos desafios que lhe estão associados”*, movimento

¹⁸ Cfr. Comissão Europeia, *Comunicação ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões “Estado da Década Digital 2024”*, Bruxelas, 2.7.2024, COM(2024) 260 final, 18.

¹⁹ Cfr. Comissão Europeia, *Comunicação ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões “Estado da Década Digital 2024”*, Bruxelas, 2.7.2024, COM(2024) 260 final, 18 e 19.

²⁰ Cfr. Comissão Europeia, *Comunicação ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões “Estado da Década Digital 2024”*, Bruxelas, 2.7.2024, COM(2024) 260 final, 18.

²¹ Cfr. Comissão Europeia, *Comunicação ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões “Estado da Década Digital 2024”*, Bruxelas, 2.7.2024, COM(2024) 260 final, 19.

²² Cfr., para maiores concretizações, Alessandra Silveira, Joana Abreu *et al.*, “Sustentabilidade tecnológica e discriminação algorítmica: o problema da regulamentação de algoritmos de aprendizagem”, in *IV Seminário Internacional Hispano-Luso-Brasileiro sobre direitos fundamentais e políticas públicas*, ed. Rogério Gesta Leal *et al.* (Bubok Publishing, 2018), 143-154, 154.

este que *“visa facilitar e melhorar o acesso à justiça, aumentar a eficácia e eficiência do sistema judiciário, [...] oferecendo assim melhores serviços de justiça a todos.”*²³

A estratégia perceciona que o período antecedente (de 2019 a 2023) foi marcado por uma extensa produção legislativa empenhada em *“acelerar o processo de digitalização e promover a utilização dos serviços digitais na justiça eletrónica”*: desde a adoção do Regulamento e-CODEX²⁴ e a sua articulação com os renovados Regulamentos sobre citação ou notificação de atos²⁵ e de obtenção de prova,²⁶ à viabilização do Pacote Digitalização – que inclui o Regulamento²⁷ e a Diretiva²⁸ relativos à digitalização da cooperação judiciária transfronteiriça e do acesso à justiça – cabendo verificar, à sua luz, de que forma estas soluções são objeto de operacionalização.

Posto isto, *“a justiça eletrónica nos próximos anos”* será marcada pela aplicação do Pacote Digitalização, sobretudo no que diz respeito ao sistema informático descentralizado *“que terá de ser estabelecido através de pontos de acesso nacionais, ligando o conteúdo da aplicação informática de referência e/ou das soluções nacionais”* enquanto *“os princípios da comunicação eletrónica e o ponto de acesso eletrónico europeu estabelecidos [...] deverão ser considerados uma base para qualquer nova iniciativa legislativa no domínio da justiça eletrónica europeia.”*²⁹ Afinal, as soluções de interoperabilidade que o Pacote de Digitalização implementa e a consolidação do uso e do desenvolvimento do sistema e-CODEX demandam uma articulação reflexiva entre a União Europeia e os Estados-Membros: *“[i]gualmente importante será o papel dos Estados-Membros, uma vez que a ligação ao e-CODEX continua a ser uma prerrogativa nacional.”*³⁰

A estratégia também destaca uma mudança de atitude face à digitalização da justiça: se inicialmente o impulso dado à justiça eletrónica resultava de uma *“abordagem baseada na participação voluntária em iniciativas de digitalização”*, agora verifica-se *“uma abordagem obrigatória baseada em atos legislativos que proporcionem maior segurança jurídica.”*³¹

²³ Cfr. Conselho da União Europeia, *Estratégia europeia para a justiça eletrónica 2024-2028*, C/2025/437, de 16.01.2025, parágrafo 4.

²⁴ Cfr. Regulamento (UE) 2022/850, do Parlamento Europeu e do Conselho, 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) e que altera o Regulamento (UE) 2018/1726.

²⁵ Cfr. Regulamento (UE) 2020/1784, do Parlamento Europeu e do Conselho, de 25 de novembro de 2020, relativo à citação ou notificação de atos judiciais e extrajudiciais em matérias civil e comercial nos Estados-Membros (citação ou notificação de atos).

²⁶ Cfr. Regulamento (UE) 2020/1783, do Parlamento Europeu e do Conselho, de 25 de novembro de 2020, relativo à cooperação entre os tribunais dos Estados-Membros no domínio da obtenção de prova em matéria civil ou comercial (obtenção de prova).

²⁷ Cfr. Regulamento (UE) 2023/2844, do Parlamento Europeu e do Conselho, 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.

²⁸ Cfr. Diretiva (UE) 2023/2843, do Parlamento Europeu e do Conselho, de 13 de dezembro de 2023, que altera as Diretivas 2011/99/EU e 2014/41/EU 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, 2008/947/JAI, 2009/829/JAI e 2009/948/JAI do Conselho no que diz respeito à digitalização da cooperação judiciária.

²⁹ Cfr. Conselho da União Europeia, *Estratégia europeia para a justiça eletrónica 2024-2028*, C/2025/437, de 16.01.2025, parágrafo 11.

³⁰ Cfr. Conselho da União Europeia, *Estratégia europeia para a justiça eletrónica 2024-2028*, C/2025/437, de 16.01.2025, parágrafo 14.

³¹ Cfr. Conselho da União Europeia, *Estratégia europeia para a justiça eletrónica 2024-2028*, C/2025/437, de 16.01.2025, parágrafo 15.

Do mesmo modo, a estratégia convida à ponderação de “*novas ações em resposta aos desafios e oportunidades criadas por tecnologias emergentes, como a inteligência artificial (IA)*.”³² A partir da proclamação de alguns “*princípios de funcionamento*”, a estratégia desenha os princípios de uma “*justiça dinâmica*” e de uma “*justiça baseada em dados*”; no seu âmbito explora-se a ideia do uso responsável, de confiança e centrado nas pessoas da inteligência artificial no domínio da justiça: como a justiça tem de ser capaz de acompanhar as mudanças e responder “*às necessidades da sociedade*”, os operadores judiciais encontram-se numa situação única no contexto do poder judiciário atual pois “*as suas capacidades e competências*” estão a ser desafiadas por “*circunstâncias únicas*” ditadas pelo novo contexto digital.³³ Posto isto, uma justiça dinâmica é essencial já que “*a análise de dados e a IA*” têm de ser soluções tecnológicas integradas nos serviços da justiça. Para o efeito, “*a recolha e a análise de dados [...] são fundamentais para orientar adequadamente a ação*” enquanto se continuam a abordar “*eventuais riscos associados, como os enviesamentos tecnológicos ou dos dados*.”³⁴

A estratégia vai desenhando algumas dimensões em que a inteligência artificial pode acarretar um contributo positivo. Desde logo, “*a interpretação digital em tempo real com recurso à IA*” é um exemplo concreto que pode auxiliar as autoridades judiciais nas audiências, evitando custos, atrasos e dificuldades associadas à designação de intérpretes.³⁵ No entanto, em termos de boa administração da justiça – com ganhos efetivos em termos de celeridade processual – há outros exemplos que vão sendo alinhados: “*a anonimização das decisões judiciais*” com recurso a ferramentas digitais, “*a distribuição automática de processos, os instrumentos de transcrição para o registo de processos e das provas recolhidas pelo tribunal, [e] a automatização robotizada de processos*.”³⁶ Aqui, o Regulamento da Inteligência Artificial³⁷ – e as suas normas relativas à administração da justiça – e as Conclusões do Conselho sobre a utilização de inteligência artificial no setor da justiça³⁸ assumem particular relevância, já que combinam as soluções jurídicas existentes em matéria de utilização de inteligência artificial no domínio da justiça e a tomada de decisão política europeia quanto à sua utilização especificamente ponderada à luz do exercício do poder judicial.

A partir do princípio substantivo da tutela jurisdicional efetiva – especialmente, sob o prisma da sua dimensão concretizadora do acesso à justiça – a estratégia reconhece que “[a] maior digitalização dos sistemas judiciais dos Estados-Membros, bem como a utilização da IA nos sistemas judiciais, tem um enorme potencial para continuar a facilitar e a melhorar o acesso à justiça para todos em toda a União Europeia”, destacando

³² Cfr. Conselho da União Europeia, *Estratégia europeia para a justiça eletrônica 2024-2028*, C/2025/437, de 16.01.2025, parágrafo 21.

³³ Cfr. Conselho da União Europeia, *Estratégia europeia para a justiça eletrônica 2024-2028*, C/2025/437, de 16.01.2025, parágrafo 36.

³⁴ Cfr. Conselho da União Europeia, *Estratégia europeia para a justiça eletrônica 2024-2028*, C/2025/437, de 16.01.2025, parágrafo 38.

³⁵ Cfr. Conselho da União Europeia, *Estratégia europeia para a justiça eletrônica 2024-2028*, C/2025/437, de 16.01.2025, parágrafo 60.

³⁶ Cfr. Conselho da União Europeia, *Estratégia europeia para a justiça eletrônica 2024-2028*, C/2025/437, de 16.01.2025, parágrafo 63.

³⁷ Cfr. Regulamento (UE) 2024/1689, do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial).

³⁸ Cfr. Conselho da União Europeia, *Conclusões do Conselho sobre a utilização de inteligência artificial no setor da justiça*, Bruxelas, 16.12.2024, 16933/24.

existirem casos “*em que a IA pode ser utilizada para finalidades de baixo risco e ser muito útil para os cidadãos como para as autoridades judiciárias.*”³⁹

Cabe agora tentar compreender como as soluções de interoperabilidade judiciária – intrinsecamente associada às dinâmicas de digitalização da justiça europeia – e a perspetiva de uso da IA em prol da tutela jurisdicional efetiva têm sido desenvolvidas na União Europeia.

3.1. A interoperabilidade judiciária a partir do Pacote “Digitalização” e a experiência do e-CODEX

A União Europeia, na senda da anterior estratégia e plano de ação para a justiça eletrónica europeia, continua a prosseguir alguns objetivos que, para além de estratégicos, mantêm a sua atualidade; na realidade, a União visa promover “*as comunicações eletrónicas entre as autoridades judiciárias, os cidadãos e os profissionais da justiça e a interoperabilidade entre as aplicações e os domínios judiciários.*”⁴⁰ Neste contexto, estes dois objetivos passam a estar interligados na medida em que os sistemas interoperáveis visam também permitir que os tribunais, os cidadãos e os profissionais da justiça possam comunicar, melhorando a tutela jurisdicional efetiva (desde o acesso à justiça e ao exercício dos direitos de defesa, com o caso a ser conhecido em prazo razoável, por uma instituição independente e imparcial).

Neste cerne, houve dois momentos decisivos para que estes esforços se tornassem palpáveis e pudessem, à luz da atual estratégia, ser devidamente adensados e prosseguidos: por um lado, a adoção do Regulamento 2022/850, relativo ao sistema e-CODEX;⁴¹ por outro, a concretização do ímpeto da digitalização da justiça – e, especificamente, da cooperação judiciária – através do Pacote Digitalização, *i.e.*, Regulamento 2023/2844⁴² e Diretiva 2023/2843,⁴³ relativos à digitalização da cooperação judiciária e do acesso à justiça em matéria civil, comercial e penal com incidência transfronteiriça.

O Regulamento e-CODEX visa, à luz do seu considerando 1, “[g]arantir o acesso eficaz dos cidadãos e das empresas à justiça e facilitar a cooperação judiciária em matéria civil, inclusive comercial, e penal entre os Estados-Membros.” O sistema e-CODEX (sistema *e-Justice Communication via Online Data Exchange*) define-se, tecnologicamente, como um “*sistema descentralizado e interoperável de comunicação transfronteiriça destinado a facilitar o intercâmbio eletrónico de dados, que inclui qualquer conteúdo transmissível em formato eletrónico, de forma rápida, segura e fiável no domínio da cooperação judiciária em*

³⁹ Cfr. Conselho da União Europeia, *Estratégia europeia para a justiça eletrónica 2024-2028*, C/2025/437, de 16.01.2025, parágrafo 26.

⁴⁰ Cfr. Conselho da União Europeia, *Estratégia europeia para a justiça eletrónica 2024-2028*, C/2025/437, de 16.01.2025, parágrafo 5.

⁴¹ Cfr. Regulamento (UE) 2022/850, do Parlamento Europeu e do Conselho, 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) e que altera o Regulamento (UE) 2018/1726.

⁴² Cfr. Regulamento (UE) 2023/2844, do Parlamento Europeu e do Conselho, 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.

⁴³ Cfr. Diretiva (UE) 2023/2843, do Parlamento Europeu e do Conselho, 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.

matéria civil e penal” – artigo 3.º, n.º 1. De forma simplificada, permite a conectividade entre os sistemas judiciários nacionais dos diversos Estados-Membros.

Assim, os seus utilizadores – as autoridades judiciárias competentes, os profissionais da justiça e os particulares – podem enviar e receber eletronicamente documentos, formulários, provas ou outras informações, o que passa a ocorrer de forma mais rápida, simples e expectavelmente cumprindo elevados padrões de segurança: “[o] sistema e-CODEX proporciona uma solução interoperável que permite ao sector da justiça conectar os sistemas informáticos das autoridades nacionais competentes, tais como as autoridades judiciárias, ou outras organizações”, devendo ser encarado “como a solução privilegiada para uma rede de comunicação interoperável, segura e descentralizada entre sistemas informáticos nacionais no domínio da cooperação judiciária em matéria civil e penal” – considerando 8.

Deste modo, o sistema e-CODEX é composto por dois elementos de *software*: uma porta de ligação para o intercâmbio de mensagens com outras portas de ligação; e um conector que apresenta diversas funcionalidades relacionadas com o intercâmbio de mensagens entre os sistemas informáticos nacionais – considerando 11. Nos termos do artigo 5.º, n.º 1 do Regulamento, o sistema e-CODEX assenta, então, na existência de *i*) um ponto de acesso e-CODEX, *ii*) normas processuais digitais (*i.e.*, as especificações técnicas para os modelos dos processos operacionais e esquemas de dados que determinam a estrutura eletrónica dos dados trocados através do sistema e-CODEX com base no vocabulário de base da justiça eletrónica da União, nos termos do artigo 3.º, n.º 9) e *iii*) produtos de *software*, a documentação e outros recursos de apoio. Os referidos “pontos de acesso e-CODEX” são compostos por uma porta de ligação que permite o intercâmbio seguro de informações numa rede de telecomunicações com outras portas de ligação que utilizam o mesmo conjunto comum de protocolos e um conector, que torna possível estabelecer a ligação dos sistemas conectados à porta de ligação, assente num conjunto comum de protocolos abertos (artigo 5.º, n.º 2 do Regulamento).

A eu-LISA (Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça) gere e controla atualmente o sistema e-CODEX, nos termos do artigo 7.º do Regulamento, cujo Conselho de Administração é aconselhado pelo Conselho de Gestão do Programa do e-CODEX – nos termos do artigo 13.º – e acompanhado pelo Grupo Consultivo e-CODEX – nos termos do artigo 12.º.

Nos termos do artigo 14.º do Regulamento, todas as entidades envolvidas estão obrigadas a respeitar o princípio da independência do poder judicial, atendendo à separação de poderes, designadamente cabendo à eu-LISA assegurar a participação de representantes da justiça na gestão do sistema e-CODEX, designadamente integrando o Grupo Consultivo e o Conselho de Gestão do Programa e-CODEX.

Apesar de a operacionalização do e-CODEX já estar em marcha há vários anos – pelo menos, desde a atribuição de um financiamento a um projeto-piloto para esta finalidade –, a realidade é que a adoção de um ato jurídico era necessária. Independentemente das suas disposições eminentemente técnicas e organizativas, o regulamento reconhece o e-CODEX como “um pacote de *software* que liga sistemas nacionais, permitindo que os utilizadores, como as autoridades judiciais, os operadores legais e os membros do público, enviem e recebam documentos, formulários legais, provas e outras informações de uma forma ágil e segura”, não substituindo “as aplicações [...] usadas

*nacionalmente: este apenas harmoniza os pontos centrais de entrada, de forma a permitir comunicações transfronteiriças.*⁴⁴

Mais recentemente, o Pacote Digitalização – adotado em dezembro de 2023 e aplicável a partir de 1 de maio de 2025 – veio recuperar o sistema e-CODEX como um instrumento tendente a uma mais estreita integração judiciária transfronteiriça no contexto do Espaço de Liberdade, Segurança e Justiça. Na realidade, o Regulamento sobre a digitalização da cooperação judiciária *“procura melhorar a eficiência e a eficácia dos processos judiciais e facilitar o acesso à justiça mediante a digitalização dos canais de comunicação existentes, o que deverá conduzir a economias de custos e de tempo, à redução de encargos administrativos e a uma maior resiliência em circunstâncias de força maior para todas as autoridades que participam na cooperação judiciária transfronteiriça.”* A utilização de soluções digitais nas articulações entre as autoridades judiciais dos Estados-Membros pode reduzir atrasos no tratamento de processos, reforçar a confiança nos sistemas judiciais, e promover o papel da União no combate contra a criminalidade – considerando 4. Posto isto, a abordagem que lhe subjaz é fundamentalmente baseada na eficiência.⁴⁵

Posto isto, o Regulamento, para além de estender o uso do e-CODEX, adensando o recurso a canais digitais de comunicação entre autoridades judiciais que aplicam diversos instrumentos no âmbito da cooperação judiciária civil, comercial e penal, também determina a criação de um sistema de comunicação eletrónica entre as pessoas singulares e coletivas e as autoridades competentes em processos judiciais em matéria civil e comercial. No entanto, o regime jurídico criado ainda estabelece um conjunto de regras em matéria de videoconferência e à aplicação de assinaturas e selos eletrónicos, fixa os efeitos jurídicos dos documentos eletrónicos e regula o pagamento eletrónico de custas (artigo 1.º do Regulamento).

Visa, deste modo, dar cumprimento ao princípio geral do digital por definição no cerne da atividade processual em matéria de cooperação judiciária em matéria civil, comercial e penal. Tal fito tem limites materiais: desde logo, o Regulamento não visa a digitalização de todas as soluções processuais dos Estados-Membros, pois não compromete o princípio da autonomia processual dos Estados-Membros (artigo 19.º do TUE); por outro lado, não visa *“digitalizar os processos de cooperação judiciária em matéria civil, comercial e penal como um todo.”* Na realidade, *“o único objetivo do legislador europeu é o de alargar o princípio do digital por definição à atividade de comunicação em sentido estrito entre entidades judiciais e o resto das autoridades e agências potencialmente envolvidas nos vários instrumentos regulatórios através dos quais a cooperação judiciária na União Europeia é desenvolvida.”*⁴⁶

Esta opção de digitalização teve em consideração quais os aspetos da cooperação judiciária e da litigância transfronteiriça que com ela mais beneficiariam: os canais de comunicação digitais, se seguros e interoperáveis, poupam tempo que pode ser crucial para efetivar a salvaguarda jurisdicional de direitos, a prossecução criminal e a defesa jurídica.⁴⁷

⁴⁴ Cfr., Fernando Gascón Inchausti, “The new regulation on the digitalisation of judicial cooperation in the European Union: something old, something new, something borrowed and something blue”, *ERA Forum*, 24 (2023): 535-552, <https://doi.org/10.1007/s12027-024-00782-z>.

⁴⁵ Cfr., para maiores considerações, Fernando Gascón Inchausti, “The new regulation on the digitalisation of judicial cooperation...”.

⁴⁶ Cfr., Fernando Gascón Inchausti, Fernando Gascón Inchausti, “The new regulation on the digitalisation of judicial cooperation...”.

⁴⁷ Cfr., Fernando Gascón Inchausti, “The new regulation on the digitalisation of judicial cooperation...”.

Afinal, no que diz respeito às comunicações entre autoridades dos Estados-Membros, o e-CODEX passa a ser a ferramenta essencial para as comunicações transfronteiriças – considerando 20. Apesar de não ser formalmente mencionado no artigo 3.º, este já se reputa como um “*sistema informático descentralizado, seguro, eficaz e fiável*” e, partir de um argumento sistemático, no que diz respeito aos custos do sistema informático descentralizado, o artigo 13.º expressamente menciona este sistema interoperável.

No entanto, o grande contributo do Regulamento é a criação de um ponto de acesso eletrónico europeu. Nos termos do artigo 2.º, n.º 4, define-se como “*um portal acessível a pessoas singulares e coletivas ou aos seus representantes, em toda a União, que está ligado a um ponto de acesso interoperável no contexto do sistema informático descentralizado*” e, atendendo ao disposto no artigo 4.º, n.º 2, estará acessível a partir do Portal Europeu de Justiça. Trata-se, assim, de uma forma de ligação de qualquer pessoa singular ou coletiva, ao e-CODEX, disponível a partir do Portal Europeu da Justiça – plataforma de informação jurídica, ao lado do eur-lex, relevante no seio das várias estratégias de justiça eletrônica europeia –, visando permitir-lhe a interação jurisdicional de forma mais simples, fácil e acessível. À luz do artigo 4.º, n.º 4 do Regulamento, ainda que o seu escopo principal inicial sejam o de fornecer, às pessoas singulares e coletivas, informações sobre o seu direito a apoio judiciário, inclusivamente em processos transfronteiriços, também é equacionada para permitir, aos mandatários, agir em nome dos representados como, ainda, intentar ações, apresentar pedidos, transmitir ou receber informações pertinentes do ponto de vista processual, comunicar com as autoridades competentes ou ser citadas ou notificadas de atos judiciais e extrajudiciais, podendo este ponto de acesso ser usado com base no consentimento prestados para o efeito, nos termos do artigo 4.º, n.º 6. Por força do disposto no artigo 4.º, n.º 2, o ponto de acesso eletrónico europeu será, pelo menos inicialmente, apenas usado para instrumentos jurídicos adotados no seio da cooperação judiciária em matéria civil e comercial.

Por último, o Regulamento tem ainda um escopo que extravasa as ferramentas de comunicação: este também integra normas relativas a videoconferências, a serviços de confiança, aos efeitos jurídicos dos documentos eletrónicos e ao pagamento eletrónico de custas.

Em matéria de videoconferência, o artigo 5.º estabelece o regime no âmbito da cooperação em matéria civil e comercial, visando que se generalize a sua utilização pelas partes e pelos seus representantes. Se a videoconferência tiver o objetivo de recolher prova, o regime aplicável é o que resulta do disposto no Regulamento relativo à obtenção transfronteiriça de provas.⁴⁸ O Regulamento privilegia o uso de videoconferência para a participação das partes e representantes na audiência mas não como elemento de promoção de audiências de julgamento síncronas. Já no que diz respeito à cooperação judiciária em matéria penal, o artigo 6.º estabelece um regime mais restritivo: desde logo, o suspeito, arguido ou condenado tem de consentir o recurso à videoconferência, podendo ser devidamente aconselhado por advogado a propósito desse consentimento, tendo este de ser dado de forma voluntária e inequívoca. Para além disso, o regime jurídico da videoconferência não deverá aplicar-se às audições ou audiências tendentes a obter provas ou a realizar um

⁴⁸ Cfr. Regulamento (UE) 2020/1783, do Parlamento Europeu e do Conselho, relativo à cooperação entre os tribunais dos Estados-Membros no domínio da obtenção de prova em matéria civil e comercial (obtenção de prova).

juízo que possa resultar numa decisão sobre a culpa ou a inocência de um suspeito ou de um arguido. Um regime protetivo é incluído no que diz respeito à audição de crianças (artigo 6.º, n.º 6).

Seguidamente, o Regulamento articula o regime jurídico proclamado com o que resulta do Regulamento 910/2014 (Regulamento eIDAS),⁴⁹ no que diz respeito às assinaturas eletrónicas e aos selos eletrónicos: à luz do artigo 7.º, os documentos transmitidos através dos canais de comunicação digitais (incluindo o ponto de acesso eletrónico europeu) deverão conter um selo eletrónico qualificado ou uma assinatura eletrónica qualificada.

Por seu lado, o artigo 8.º inclui uma obrigação de reconhecer os efeitos jurídicos e de admitir os documentos transmitidos numa comunicação eletrónica. A sua recusa não é admissível pelo simples facto de se encontrarem em formato eletrónico. Neste contexto, o legislador europeu adota uma postura que já devia ser consensual em todos os seus Estados-Membros, mesmo perante litígios puramente internos.⁵⁰

Por fim, o artigo 9.º estabelece uma concretização do princípio da acessibilidade – e uma demanda de vários anos diretamente relacionada com os litígios transfronteiriços, designadamente as ações de pequeno montante:⁵¹ a possibilidade de proceder ao pagamento das custas através de meios eletrónicos.

Por tudo o que se sublinhou, há um desígnio que se pode adivinhar: o Regulamento em causa *“convida os Estados-Membros, internamente e em contexto transfronteiriço, a fazer o que ele prevê: usar canais digitais de comunicação, padronizar o uso de videoconferência e de serviços eletrónicos de confiança, reconhecer eficácia legal plena aos documentos eletrónicos e permitir o pagamento eletrónico de custas processuais.”*⁵² Verifica-se, assim, uma clara afirmação do padrão europeu.

3.2. A inteligência artificial no domínio da justiça: o Regulamento da inteligência artificial e as Conclusões do Conselho de dezembro de 2024

O Regulamento da Inteligência Artificial surgiu, no contexto mundial e globalizado, como o primeiro instrumento legislativo abrangente a nível mundial para regular a inteligência artificial, *“optando por uma abordagem centrada no risco, adaptando as obrigações dele resultantes de acordo com o risco que diferentes sistemas/modelos de IA representam para os direitos fundamentais.”*⁵³

Posto isto, a abordagem centrada no risco tem particulares repercussões no domínio da justiça e na utilização de sistemas de inteligência artificial neste contexto. A partir da leitura combinada do disposto no artigo 6.º, n.º 2 do Regulamento e o parágrafo 8, a) do seu Anexo III, *“os sistemas de IA a que se refere o anexo III são também considerados de risco elevado.”* Assim, são considerados de risco elevado os *“sistemas de IA concebidos para serem utilizados por uma autoridade judiciária, ou em seu nome, para auxiliar uma autoridade judiciária na investigação ou 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.”*

⁴⁹ Cfr. Regulamento (UE) 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.

⁵⁰ Cfr. Fernando Gascón Inchausti, “The new regulation on the digitalisation of judicial cooperation...”.

⁵¹ Cfr. Joana Covelo de Abreu, *Tribunais nacionais e tutela jurisdicional efetiva. Da cooperação à integração judiciária no Contencioso da União Europeia* (Almedina, 2019), 316-329.

⁵² Cfr. Fernando Gascón Inchausti, “The new regulation on the digitalisation of judicial cooperation...”.

⁵³ Cfr. Tiago Sérgio Cabral, “Rethinking the list-based approach to high-risk systems under the AI Act”, *Nordic Journal of European Law*, 8(1) (2025): 32-48, 32.

O regime agora adotado, no entanto, incorpora uma exceção, sob a forma de norma derogatória, à regra de classificação como risco elevado dos sistemas de inteligência artificial vocacionados a ser usados no domínio da administração da justiça: para o efeito, se o sistema de inteligência artificial 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 decisão*”, o sistema não será qualificado como sendo de risco elevado – artigo 6.º, n.º 3, 1.º parágrafo.

Para concretizar este regime derogatório, o legislador europeu adiantou algumas situações que, verificadas, permitem concluir que o sistema de inteligência artificial não acarreta risco elevado: *i)* se o sistema se destinar “*a desempenhar uma tarefa processual restrita*” [artigo 6.º, n.º 3, 2.º parágrafo, *a*)]; *ii)* se o sistema se destinar “*a melhorar o resultado de uma atividade humana previamente concluída*” [artigo 6.º, n.º 3, 2.º parágrafo, *b*)]; *iii)* se o sistema se destinar “*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*” [artigo 6.º, n.º 3, 2.º parágrafo, *c*)]; e *iv)* se o sistema se destina “*a executar uma tarefa preparatória no contexto de uma avaliação pertinente para efeitos dos casos de utilização enumerados no anexo III*” [artigo 6.º, n.º 3, 2.º parágrafo, *d*)].

Quando o prestador do serviço considere que o sistema de inteligência artificial em causa cabe na derrogação à regra geral de classificação do sistema como sendo de risco elevado, deve observar as exigências decorrentes do artigo 6.º, n.º 4, *i.e.*, incumbe ao prestador o dever de “*documentar a sua avaliação antes de esse sistema ser colocado no mercado ou colocado em serviço*” para além de cumprir a obrigação de registo, à luz do artigo 49.º, n.º 2 do Regulamento, na base de dados da União Europeia relativa a sistemas de inteligência artificial de risco elevado (artigo 71.º, n.º 1 do Regulamento).

No entanto, o 3.º parágrafo do artigo 6.º, n.º 3 contempla um afastamento da possibilidade de derrogação da classificação como risco elevado: quando os sistemas de inteligência artificial em causa executarem a definição de perfis de pessoas singulares, sempre terão de ser considerados de risco elevado.

A abordagem baseada no risco, justificada por alguns como assegurando maior certeza jurídica – sobretudo numa perspetiva económica de tornar a União atrativa ao desenvolvimento de *know-how* específico e ao desenvolvimento de sistemas de inteligência artificial no seu seio, estimulando a inovação –, conduziu à adoção de listas tendentes a esta classificação, designadamente recorrendo aos anexos I e III. No entanto, há vozes que recordam que esta solução pode impedir a maior maleabilidade e adaptabilidade do texto jurídico à (rápida) evolução tecnológica, podendo representar “*um risco acrescido para os direitos fundamentais dos indivíduos (particularmente num campo inovativo como é o da LA)*.”⁵⁴

No entanto, o artigo 7.º, n.º 1 prevê a possibilidade de a Comissão, através de atos delegados, estar habilitada a promover a alteração do anexo III, “*aditando ou modificando casos de utilização de sistemas de LA de risco elevado*” nos casos em que, cumulativamente, as seguintes condições sejam observadas: *i)* os sistemas se destinam a ser utilizados em qualquer um dos domínios enumerados no referido anexo [artigo 7.º, n.º 1, *a*)]; e *ii)* representam um risco de danos para a saúde e a segurança ou de repercussões negativas nos direitos fundamentais, e esse risco é equivalente ou

⁵⁴ Cfr. Tiago Sérgio Cabral, “Rethinking the list-based approach to high-risk systems under the AI Act.”

superior ao risco de danos ou repercussões negativas representado pelos sistemas de IA de risco elevado já referidos no anexo III [artigo 7.º, n.º 1, *b*)]. Daqui resulta, portanto, que, quanto à segunda condição cumulativa, se exija, como fundamento à alteração do anexo III por ato delegado da Comissão, que:

- para além de se preencher o requisito do artigo 7.º, n.º 1, *a*), o sistema representar um risco de dano para a saúde e a segurança e esse risco é equivalente ou superior ao risco de danos ou repercussões negativas representado pelos sistemas de IA de risco elevado já contemplados no anexo III;
- o sistema representar um risco de repercussões negativas nos direitos fundamentais e esse risco é equivalente ou superior ao risco de danos ou repercussões negativas representado pelos sistemas de IA de risco elevado já contemplados no anexo III.

Na realidade, o segundo requisito cumulativo encerra, na sua literalidade, uma alternatividade de situações – ou um dano para a saúde e a segurança ou um risco de repercussões negativas nos direitos fundamentais – não se exigindo a sua observância concomitante. A concretização de qualquer uma destas eventualidades do artigo 7.º, n.º 1, *b*) opera-se à luz dos critérios taxativos do artigo 7.º, n.º 2, atendendo, entre outros, à finalidade prevista do sistema; ao grau de utilização ou à probabilidade de utilização; à natureza e à quantidade de dados tratados e utilizados pelo sistema, especificamente, ao facto de serem tratadas categorias especiais de dados pessoais; se atua (e em que medida) de forma autónoma e se um humano tem a suscetibilidade de anular decisões ou recomendações que possam causar danos; à medida em que já se verificaram danos ou repercussões negativas ou há uma forte convicção que tal possa vir a ocorrer, designadamente pela existência de relatórios ou alegações documentadas; ou à potencial dimensão desses danos ou repercussões negativas (por ter a intensidade e a capacidade de afetar várias pessoas ou de afetar desproporcionadamente um determinado grupo).

Do mesmo modo, a Comissão pode adotar atos delegados para suprimir sistemas de inteligência artificial de risco elevado se preencher as seguintes condições cumulativas: *i*) o sistema deixa de representar risco significativo para os direitos fundamentais, a saúde ou a segurança (o que é avaliado a partir dos critérios do disposto no artigo 7.º, n.º 2) e se a supressão não diminui o nível geral de proteção da saúde, da segurança e dos direitos fundamentais ao abrigo da União – artigo 7.º, n.º 3 do Regulamento.

Deste modo, o Regulamento da Inteligência Artificial representa ainda um ato legislativo com alguma capacidade de se adaptar à evolução tecnológica e, no domínio da justiça, permitindo distinguir, através de diferentes classificações de risco, sistemas de inteligência artificial *i*) de organização da informação, *ii*) de mobilização de jurisprudência útil pré-existente e *iii*) de previsão de tendências decisórias. Afinal, como já anteriormente defendemos, se os dois primeiros se configuram sistemas instrumentais de inteligência artificial ao serviço da justiça – sobretudo vocacionados a diminuir a exigência burocrática associada ao exercício da função jurisdicional, enquanto podem evitar trabalho repetitivo ainda confiado a juízes – e a sua classificação de sistemas como sendo de risco elevado pode não se justificar, a realidade é que os terceiros são sistemas que, por definição, configuram um risco elevado e podem, se assentes na criação de perfis, subsumir-se à impossibilidade de recurso ao regime derogatório, por força do artigo 6.º,

n.º 3.⁵⁵ Assim, os sistemas de organização da informação judicial e de mobilização de jurisprudência são sistemas usados no âmbito da administração da justiça e, portanto, em regra classificáveis como sendo de risco elevado mas podem congrega, em concreto, as condições para se enquadrarem no regime derogatório do artigo 6.º, n.º 2 do Regulamento. Neste caso, a obrigação de documentação e de registo na base de dados da União podem assegurar a salvaguarda da tutela jurisdicional efetiva mas sem ataviar o desenvolvimento tecnológico e a sua rápida repercussão no domínio da justiça. Já, por sua vez, os sistemas com características de previsão de tendências decisórias – pela sua natureza mais intrusiva na esfera decisória do juiz, pela experiência antecedente e pela possibilidade de, mais facilmente, determinarem a construção de qualquer técnica de perfilagem – continuam a ser classificados como sendo de risco elevado, à luz da regra geral e, em casos de criação de perfis, esta consolida-se, inviabilizando-se a possibilidade de os prestadores recorrerem à sua derrogação.

Do mesmo modo, a 16 de dezembro de 2024, o Conselho da União Europeia adotou umas Conclusões sobre a utilização de inteligência artificial no setor da justiça, atendendo ao facto de a inteligência artificial ter evoluído consideravelmente e a sua utilização se ter generalizado enquanto se caminha para uma integração mais aprofundada no “*acesso à justiça em matéria civil, comercial e penal transfronteiras*.” Afinal, a integração bem-sucedida de sistemas de inteligência artificial no sistema judiciário europeu “*é particularmente importante a fim de garantir o acesso equitativo à justiça em toda a UE*.”⁵⁶

Assim, as Conclusões apresentadas seguem-se a um longo caminho previamente percorrido no âmbito institucional da União Europeia: desde a já analisada Estratégia Europeia para a justiça eletrónica de 2024 a 2028, do Conselho, aos Relatórios da Agência dos Direitos Fundamentais da União Europeia subordinados aos temas “*Preparar o futuro – Inteligência artificial e direitos fundamentais*”, de 2021,⁵⁷ e “*Bias in algorithms – Artificial intelligence and discrimination*”, de 2022.⁵⁸

Afinal, reconhecendo o potencial da inteligência artificial em “*facilitar o acesso à justiça e melhorar a pontualidade, a eficiência e a eficácia dos processos judiciais*”, sublinha exemplos concretos para a sua utilização com menores riscos associados, desde “*programar audiências*”, “*reservar salas de audiências*”, “*impedir a reidentificação das pessoas em causa através da anonimização e pseudonimização das decisões judiciais*”, sempre observando o padrão da proteção de dados pessoais.⁵⁹ No entanto, e apesar de reconhecer o envolvimento de mais riscos, o conselho sublinha o papel relevante da utilização de inteligência artificial em algumas atividades de apoio à função judicial, “*nomeadamente, no resumo dos conteúdos judiciais, na análise de jurisprudência, na proposta*

⁵⁵ Cfr., para maior reflexão, Joana Covelo de Abreu, «The “Artificial Intelligence Act” proposal on European e-Justice domains through the lens of user-focused, user-friendly and effective judicial protection principles», *Multidisciplinary perspectives on artificial intelligence and the law*, ed. H. Sousa Antunes *et al.*, Law, Governance and Technology Series, vol. 58 (Cham: Springer, 2024), 397-414.

⁵⁶ Cfr. Conselho da União Europeia, Conclusões do Conselho sobre a utilização de inteligência artificial no setor da justiça, 16933/24, Bruxelas, 16.12.2024, 2.

⁵⁷ Cfr. Agência Europeia dos Direitos Fundamentais, “Preparar o futuro – Inteligência artificial e direitos fundamentais”, Relatório, 29.01.2021, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_pt.pdf [acesso: 23.5.2025].

⁵⁸ Cfr. Agência Europeia dos Direitos Fundamentais, “Bias in algorithms – artificial intelligence and discrimination”, Report, 8.12.2022, in https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf [acesso: 23.5.2025].

⁵⁹ Cfr. Conselho da União Europeia, Conclusões do Conselho sobre a utilização de inteligência artificial no setor da justiça, 16933/24, Bruxelas, 16.12.2024, parágrafo 9, 6.

de textos, na interpretação em tempo real, no tratamento de litígios em massa ou no apoio à tomada de decisões.”⁶⁰

No entanto, para que tais soluções possam ser equacionadas, é necessário desenvolver sistemas de inteligência artificial especialmente vocacionados ao sistema de justiça, ajustados à sua realidade e particulares especificidades, onde “[a] colaboração entre o meio académico, a indústria, as autoridades judiciais ou outras autoridades públicas e os profissionais da justiça é fundamental para impulsionar a inovação e promover o progresso neste domínio”, enquanto os operadores judiciais (juizes, advogados, funcionários judiciais) são dotados das competências técnicas e digitais adequadas.⁶¹

Assim, alinhando-se com o padrão normativo mobilizável – designadamente, o Regulamento da Inteligência Artificial e os instrumentos legais existentes em matéria de proteção de dados pessoais – sublinha a necessidade de “orientações e normas práticas e de fácil utilização para o desenvolvimento e a utilização da IA na justiça de forma ética e responsável”, partindo da estreita cooperação entre a Comissão Europeia, os Estados-Membros e as partes interessadas, sempre afirmando o princípio da centralidade humana.⁶² A existência de “decisões judiciais anonimizadas ou pseudonimizadas” é fundamental para o desenvolvimento de sistemas de inteligência artificial no âmbito da justiça, sobretudo para assegurar um treino assente em dados atuais e fiáveis dos algoritmos.⁶³

4. Conclusões

O valor do Estado de direito – expressamente acautelado no catálogo de valores da União Europeia, consagrado no artigo 2.º do TUE – significa que o exercício do poder público na sua ordem jurídica se submete ao direito, da mesma maneira que, nos respetivos Estados-Membros, enquanto tradição constitucional comum, o poder público também encontra o seu fundamento, limite e finalidade no direito.

Como ordem jurídica autónoma, a União Europeia tem, no seu direito originário (Tratados e, por força do artigo 6.º, n.º 1, in fine do TUE, a Carta dos Direitos Fundamentais da União Europeia – CDFUE), uma base eminentemente jurídico-constitucional, onde as várias dimensões concretizadoras de uma ordem jurídico-política submetida ao direito encontram a sua concretização: aí encontramos a indicação dos valores e objetivos para essa comunidade politicamente organizada; encontramos um arranjo institucional próprio, que se explica através de princípios específicos, entre os quais se destaca o princípio do equilíbrio institucional;⁶⁴ tem um sistema de normas jurídicas próprias, estabelecendo os procedimentos tendentes à sua adoção assim como os mecanismos adequados para promover a sua interpretação e a sua aplicação; e, por fim, aí encontramos um arranjo judicial

⁶⁰ Cfr. Conselho da União Europeia, *Conclusões do Conselho sobre a utilização de inteligência artificial no setor da justiça*, 16933/24, Bruxelas, 16.12.2024, parágrafo 10, 6.

⁶¹ Cfr. Conselho da União Europeia, *Conclusões do Conselho sobre a utilização de inteligência artificial no setor da justiça*, 16933/24, Bruxelas, 16.12.2024, parágrafos 11 e 12, 6.

⁶² Cfr. Conselho da União Europeia, *Conclusões do Conselho sobre a utilização de inteligência artificial no setor da justiça*, 16933/24, Bruxelas, 16.12.2024, parágrafos 15 e 16, 8.

⁶³ Cfr. Conselho da União Europeia, *Conclusões do Conselho sobre a utilização de inteligência artificial no setor da justiça*, 16933/24, Bruxelas, 16.12.2024, parágrafo 18, 8.

⁶⁴ Cfr. Joana Covelo de Abreu e Liliana Reis, “Introdução – Instituições, órgãos e organismos da União Europeia: um quadro institucional único?”, in *Instituições, órgãos e organismos da União Europeia*, coords. Joana Covelo de Abreu e Liliana Reis (Almedina, 2020), 7-25.

típico, que visa assegurar a tutela jurisdicional efetiva dos direitos conferidos por esta ordem jurídica autónoma.⁶⁵

Neste contexto, verificam-se alguns desafios ao valor do Estado de direito – quer enquanto valor essencial aos Estados-Membros, quer afetando a perceção da União como uma União de direito – cabendo assegurar a sua sustentabilidade. Afinal, sustentabilidade significa “*modelo de sistema que tem condições para se manter ou conservar*”⁶⁶ ou, em termos mais científicos, procura “*satisfazer as necessidades das gerações existentes sem comprometer as necessidades das gerações futuras.*”⁶⁷

De forma a dar resposta a esta crise do valor do estado de direito, a Comissão Europeia adotou algumas medidas estruturais, algumas vocacionadas ao domínio da justiça e, especificamente, pensadas para assegurar que as dimensões da tutela jurisdicional efetiva não saem perturbadas. Como afirmou a Comissão Europeia, “*o estado de direito é um dos valores fundamentais sobre o qual a União Europeia é construída*”, significando que “*todos, incluindo os membros do parlamento e do executivo estão igualmente submetidos à lei e sob o controlo de tribunais independentes e imparciais*”, reforçando o papel que a justiça tem na afirmação do valor do estado de direito e da construção contínua da União como uma União de direito.⁶⁸

Ora, a sustentabilidade do estado de direito determina que a justiça europeia seja adaptada às exigências atuais: não só reformas tendentes à maior eficiência dos sistemas de justiça, mas também algumas de carácter mais estrutural vocacionadas a fortalecer a independência judiciária, a reduzir a duração dos processos e a melhorar a qualidade da justiça.

Neste sentido, a justiça eletrónica europeia serve como uma ferramenta, equacionando o uso de tecnologias de informação e de comunicação para melhorar o sistema judiciário dos Estados-Membros e da União mas, simultaneamente, para afirmar o poder judiciário e as suas prerrogativas de independência e de imparcialidade. Afinal, atendendo ao caminho trilhado em matéria de interoperabilidade judiciária e da equação do uso de inteligência artificial no domínio da justiça, verifica-se que as soluções pensadas visam melhorar o acesso à justiça, imprimir uma perceção de proximidade da justiça (tornando-a “*tão aberta quanto possível e ao nível mais próximo possível dos cidadãos*” – artigo 1.º do TUE) até no âmbito dos litígios com configuração transfronteiras e continuando a afirmar a centralidade do homem – e do juiz – no processo decisório, o que, no contexto jurisdicional, determina que o recurso às tecnologias de informação e de comunicação não podem beliscar a independência do poder judiciário nem as garantias conferidas às partes envolvidas no processo.

Afinal, se a justiça cumprir o seu papel com a suficiente plasticidade que os tempos exigem, designadamente acompanhando a evolução tecnológica e digital – através do paradigma da justiça eletrónica europeia, agora desenvolvido a partir do fundamento da sustentabilidade tecnológica –, é capaz de conduzir a

⁶⁵ Cfr., para maiores desenvolvimentos a propósito da perceção da União Europeia como uma União de direito, Alessandra Silveira, *Princípios de direito da União Europeia. Doutrina e jurisprudência*, 2.ª edição (Quid Juris, 2011).

⁶⁶ Cfr. Priberam – Dicionário online, “Sustentabilidade”, <https://dicionario.priberam.org/sustentabilidade> [acesso: 26.5.2025].

⁶⁷ Cfr. Infopédia – Dicionários Porto Editora online, “Sustentabilidade”, <https://www.infopedia.pt/dicionarios/lingua-portuguesa/sustentabilidade> [acesso: 26.5.2025].

⁶⁸ Cfr. Comissão Europeia, “The EU’s rule of law toolbox”, 2023, in https://commission.europa.eu/document/download/3aea3989-972b-4ec0-8d7a-8b88495d497b_en?filename=125_1_58129_rol_toolbox_factsheet_en.pdf&prefLang=pt [acesso: 26.5.2025].

uma sustentabilidade do conceito de Estado de direito, proactivamente alimentando a sua consubstanciação hodierna, não comprometendo as gerações futuras, antes contribuindo para uma perceção dinâmica do direito e de como uma comunidade politicamente organizada a ele se submete e exige que o exercício de poder público no seu seio busque no direito a sua conformação.

O conforto do velho e a arrogância do novo: os desafios de um mundo com pressa!

*Paulo Novais**

A história da humanidade está marcada por uma cíclica tensão entre o “*mundo velho*” e o “*mundo novo*.” Desde, pelo menos, o momento da invenção da roda até à revolução industrial, em cada avanço tecnológico tivemos promessas de um progresso transformador, mas também receios e resistências. A Inteligência Artificial (IA) é o mais recente capítulo de uma história sem fim, mas com uma diferença fundamental, a velocidade desta mudança.

Neste nosso tempo, estamos a viver com uma peculiar e estranha sensação de que o tempo está a andar depressa (cada vez mais célere). Um tempo em que queremos (nos é exigido) fazer cada vez mais em menos tempo. A tecnologia apresenta-se simultaneamente como a causa e a solução para esta pressão. Um pouco à imagem do que Paul Virilio¹ expressou que a modernização se caracteriza pela compressão do tempo e do espaço com o advento das novas formas de telecomunicações e dos meios de transporte (rápidos), criando uma sensação de aceleração constante na vida contemporânea (Dromologia).

O nosso mundo acelerou (e muito!), e a IA está a redefinir a forma como vivemos, trabalhamos e nos relacionamos. Esta aceleração está a amplificar o confronto entre o mundo “*velho*” e o “*novo*”, criando um paradoxo complexo, em que por um lado, queremos a inovação e as promessas do novo, mas por outro, receámos perder o conforto e fundamentalmente o controlo² que o velho nos proporciona.

Afinal, este novo mundo com IA estará a desenvolver um futuro melhor ou apenas mais célere?

Reinhart Koselleck, em *Futuro passado*,³ analisava os efeitos da modernidade como uma perceção de um tempo que acelera e que se separa do velho (o espaço da experiência) de um novo (o horizonte de expectativa).

Neste contexto, coloca-se uma questão “*Como podemos garantir que o mundo novo seja não apenas inevitável, mas também desejável?*”

Se por um lado, a transformação operada pela IA é feita numa velocidade sem precedente, distinguindo-se tanto pelo potencial que carrega como pelos desafios que transporta, por outro lado, não se trata (somente) de uma tecnologia voltada para o futuro, mas de uma realidade concreta. A título de exemplo, tivemos recentemente

* Professor na Escola de Engenharia da Universidade do Minho, ALGORITMI Research Centre/ LASI, Braga. Membro do Centro de Excelência Jean Monnet CitDig (Cidadania Digital e Sustentabilidade Tecnológica) da Escola de Direito da Universidade do Minho (Portugal).

¹ Paul Virilio, *Vitesse et Politique* (Galilee, 1977).

² Stuart Russell, *Human compatible: artificial intelligence and the problem of control* (Viking, 2019).

³ Reinhart Koselleck, *Futuro passado: contribuição à semântica dos tempos históricos*, trad. Wilma Mas e Carlos Pereira (Rio de Janeiro: Contraponto, 1979).

um sistema de geração de texto a atingir os 100 milhões de utilizadores em apenas dois meses.

Esta apropriação tecnológica, sem paralelo na história, manifesta-se em múltiplas e diversificadas áreas de atuação. Em atividades do quotidiano com os robôs aspiradores, na saúde com os sistemas de análise de imagens que detetam atualmente alguns tipos de cancro com uma precisão equiparável à de radiologistas especialistas, e na indústria com sistemas de previsão de falhas em máquinas, que reduzem significativamente os custos de manutenção.

Provoca, de algum modo, um efeito de extensão da cognição humana, ao permitir automatizar tarefas que abrangem desde a criação de apresentações e a geração de conteúdos visuais até à produção de vídeos.⁴ Estas ferramentas de criação assistida estão a tornar estas atividades mais acessíveis, permitindo que pessoas sem competências técnicas possam materializar as suas ideias. Além disto, estão a alterar significativamente a forma como podemos procurar e organizar informação, com recurso a assistentes digitais e sistemas de procura inteligente que tornam a pesquisa de conhecimento mais rápida, intuitiva e eficiente.

Contudo, não há bela sem senão (como nunca há!), a IA traz também consigo desafios significativos. A automação de empregos manuais ou cognitivos está a suscitar preocupações sobre o futuro do trabalho e o aumento das desigualdades económicas. Questões como a dependência excessiva da tecnologia, os preconceitos eventualmente existentes nos dados e nos algoritmos, precisam de ser analisadas para assegurar que a sua utilização seja de facto feita de uma forma justa, responsável e ética.

Uma nota prévia, que considero ser necessário esclarecer é que a IA não é inteligente, consciente ou criativa no sentido humano, porque, entre outras razões, não compreende nem vê o mundo como nós o fazemos. Trata-se de uma tecnologia muito poderosa, mas que, pelo menos por enquanto, não substitui a complexidade e a profundidade da inteligência humana.

A IA está, de facto, a reforçar a criatividade humana, com o aumento da produtividade e com a democratização do acesso a áreas que outrora eram da exclusividade de especialistas. Um caso ilustrativo desta realidade são os sistemas de geração de conteúdo, que estão a permitir que artistas possam ampliar a sua capacidade de trabalho e a automatizar tarefas repetitivas, o que lhes liberta tempo para a realização de atividades mais complexas e imaginativas, dando a possibilidade de explorar novos caminhos criativos. No entanto, esta democratização também está a perturbar os modelos tradicionais, colocando em causa o valor do trabalho humano e criando (novas) dinâmicas de mercado.

Estes sistemas trazem consigo desafios éticos e regulatórios significativos, em particular no que diz respeito à privacidade dos dados e aos direitos de autor, mas também sobre o rigor da informação gerada. Ademais, levanta questões sobre a equidade e o acesso, uma vez que nem todos dispõem das mesmas oportunidades para beneficiar destas tecnologias. Em particular, uma excessiva dependência tem o efeito de poder diminuir a quantidade e qualidade das interações humanas, bem como a exposição a perspetivas diversas, criando a ilusão de um saber fictício e alimentando bolhas de opinião inibidoras de um pensamento crítico.

Assumindo como adquirido que a IA está a assumir um papel central nas nossas vidas, é imprescindível desenvolver uma compreensão sólida sobre os seus

⁴ Ethan Mollick, *Co-Intelligence: living and working with AI* (Penguin USA, 2024).

fundamentos, do seu funcionamento, das suas capacidades e, naturalmente, das suas limitações.

Neste enquadramento, o pensamento crítico e a criatividade são competências fundamentais, pese embora “ela” seja capaz de realizar inúmeras tarefas. A capacidade de identificar problemas, formular hipóteses e de conceber soluções inovadoras continuam e continuarão a ser exclusivas do Homem.

Num mundo em constante aceleração, apreender ao longo da vida é uma aptidão crucial. Ter a capacidade de se manter atualizado sobre os mais recentes avanços é uma condição essencial para se adaptar a um mercado de trabalho em permanente evolução. Eu diria, ainda, que temos de ser capazes de desenvolver um pensamento ético, que permita dar respostas a questões complexas relacionadas com questões como a privacidade, os preconceitos e a responsabilidade. Uma outra competência, preciosa num mundo onde a tecnologia é onnipresente, é ter uma consciência ética. Esta, para além de nos ajudar a discernir entre o certo e o errado, deve ter em conta os valores morais e o impacto das ações sobre os outros e o meio ambiente, bem como a capacidade de tomar decisões informadas e conscientes.

Perante este cenário em que a tecnologia tem um papel preponderante, ter uma abordagem multidisciplinar é uma capacidade crítica para a sobrevivência. De algum modo, ser capaz de ver o mundo por diferentes janelas, integrando o conhecimento de várias áreas na resolução de problemas de uma forma eficaz. Não podemos esquecer que a adaptabilidade e a flexibilidade são, neste contexto, importantes. De igual forma, a capacidade de colaborar e a empatia são também elas essenciais, uma vez que a capacidade de trabalhar em equipa e de compreender as necessidades dos outros não podem ser, por enquanto, replicadas.

O futuro tem em si uma característica imutável, ninguém o para. Assim, inevitavelmente, a tecnologia (seja a IA ou outra) continuará a avançar e a modelar a nossa sociedade⁵ (e a nossa vida), de formas que ainda não conseguimos sequer integralmente imaginar. Podemos tentar parar o vento com as mãos, resistindo à mudança, mas será, no entanto, mais inteligente “abraçá-la” com consciência e responsabilidade.⁶ Para mim, é muito claro que temos de seguir um caminho de convergência, em que a tecnologia está ao serviço das pessoas, e não o seu contrário.

Um processo gradual, mas assertivo, de transformação digital e de uso da IA têm o poder de transformar o sistema judicial, com benefícios consideráveis como uma maior eficiência, acessibilidade e transparência. Através deste processo de digitalização, os processos judiciais passam para um formato eletrónico, permitindo o seu acesso remoto, a utilização de assinaturas digitais e a realização de julgamentos online.^{7/8}

A IA desempenha, aqui, um papel fundamental ao automatizar tarefas repetitivas, como a organização de documentos, a gestão de prazos processuais, a possibilidade de análise de grandes volumes de dados para a previsão (recomendação) de sentenças e a identificação de eventuais padrões em jurisprudência. Novas ferramentas avançadas estão a ser introduzidas (com recurso a processamento de linguagem natural), fornecendo a possibilidade de pesquisas jurídicas complexas e a

⁵ Stuart Russell, *Human Compatible*.

⁶ Gary Marcus and Ernest Davis, *Rebooting AI: building artificial intelligence we can trust* (Pantheon Books, 2019).

⁷ Richard Susskind, *Online courts and the future of justice* (Oxford: Oxford University Press, 2019).

⁸ Ethan Katsh and Orna Rabinovich-Einy, *Digital justice: technology and the internet of disputes* (Oxford: Oxford University Press, 2017).

extração de informações relevantes de documentos judiciais (e.g., contratos), enquanto assistentes virtuais assistem os cidadãos, respondendo a dúvidas e orientando-os nos procedimentos legais.

Este processo de transformação tem como alicerce um conjunto de requisitos, tais como a existência de dados fiáveis, precisos e atualizados, a garantia de interoperabilidade entre sistemas e um rigoroso controlo na proteção de dados e privacidade. Em concreto, o Regulamento Geral sobre a Proteção de Dados - UE 2016/679 (RGPD) que determina o uso de recomendações/regras estritas para a recolha e uso de dados pessoais, incentivando tecnologias seguras como o recurso a encriptação, entre outras.

Ao nível regulatório, o Regulamento sobre Inteligência Artificial [UE 2024/1689 (AI Act)] procura, ainda, harmonizar o uso da IA, proibindo práticas arriscadas, definindo requisitos para sistemas de alto risco e promovendo transparência, com o objetivo de garantir uma IA (mais) confiável.

A interação entre humanos e IA no contexto judicial vai muito além da simples automação. A IA pode atuar como uma extensão das nossas capacidades cognitivas, estendendo o raciocínio humano, e como uma parceira em processos colaborativos de resolução de problemas. Este novo tempo da justiça abre caminhos para uma justiça mais ágil e acessível, mas exige um compromisso contínuo com a qualidade dos dados, a segurança e uma colaboração “*harmoniosa*” entre tecnologia e intervenção humana.

A IA pode ser uma aliada poderosa, mas o sucesso da sua aplicação dependerá da forma como seremos capazes de a integrar de uma forma ética e crítica (e porque não criativa!) no nosso quotidiano.

Para concluir, o futuro está (ainda) nas nossas mãos, mas a arrogância do “*mundo novo*” necessita de ser temperada com a sabedoria existente no “*mundo velho*.”

Lewis Carroll, em *Alice no País das Maravilhas*, escrevia que “*Se não sabes para onde vais, qualquer caminho serve.*” Neste tempo de disrupção tecnológica, é crucial definir um rumo claro, incorporando a IA com responsabilidade,⁹ para garantir que o caminho que trilharmos nos leve a um futuro que seja sedutor e desejável para todos, e não apenas acelerado.

⁹ Virginia Dignum, *Responsible Artificial Intelligence - how to develop and use AI in a responsible way* (Springer Nature, 2019).

PAINEL IV

**CONTROLOS E EQUILÍBRIOS INSTITUCIONAIS
(CHECKS AND BALANCES) – DESAFIOS AO ESTADO
DE DIREITO DIANTE DA TRANSIÇÃO DIGITAL**

PAINEL IV

Controlos e equilíbrios institucionais (checks and balances) – desafios ao Estado de direito diante da transição digital

Gonçalo Martins de Matos*

Larissa Araújo Coelho**

O tema deste II Congresso Ibero-Americano sobre “*Direito e tecnologias digitais*”, qual seja, “*Estado de direito e transição digital*”, convoca uma gama muito ampla de reflexões sobre os temas propostos. Com base no Relatório de 2024 sobre o Estado de direito da Comissão Europeia,¹ as reflexões repartem-se por quatro eixos principais, correspondentes aos quatro pilares de análise do mesmo Relatório. As questões que nos concernem prendem-se com o quarto pilar, relativo ao capítulo dos controlos e equilíbrios institucionais (*checks and balances*). A presente reflexão serve de introdução e enquadramento para as observações dos ilustres oradores que compuseram o painel sobre os controlos e equilíbrios institucionais.

Neste contexto, para uma compreensão introdutória e sistemática, os controlos e equilíbrios institucionais integram a matéria do Estado de direito, que por sua vez pode ser apreciada sob dois planos.² Em primeiro lugar, no *plano das ideias*, prepondera uma perceção sob a ótica da Filosofia Política e História das Ideias Políticas, que fez escola desde os tempos aristotélicos, através de diversos questionamentos que podem ser resumidos na seguinte interrogação: *a gestão dos interesses e bens comuns deveria ser realizada pelo governo das leis ou pelo governo dos homens?* Numa exposição mais ampla do pensamento, questiona-se o quê ou quem são os gestores do poder. A resposta defendida em termos doutrinários foi no sentido de que a lei deveria governar os homens e para tal estar isenta de interesses privados,³ embora a realidade política em diversas latitudes nem sempre tenha caminhado de acordo com essa interpretação.

No segundo patamar, encontramos o plano orgânico-funcional, também designado de plano da institucionalização ou ainda de princípio da governança.⁴

* Estudante de doutoramento em Ciências Jurídicas Públicas na Escola de Direito da Universidade do Minho. Mestre em Direito Judiciário.

** Bolseira da Fundação para a Ciência e Tecnologia (FCT), com referência SFRH/BD/140897/2018, e estudante de doutoramento em Ciências Jurídicas Públicas na Escola de Direito da Universidade do Minho.

¹ Comissão Europeia, Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, *Relatório de 2024 sobre o Estado de direito – situação na União Europeia*, COM(2024) 800 Bruxelas, 24.7.2024.

² Nuno Piçarra, *A separação de poderes como doutrina e princípio constitucional: um contributo para o estudo das suas origens e evolução* (Coimbra: Coimbra Editora, 1989), 11-15.

³ Aleardo Zanghellini, “The foundations of the rule of law”, *Yale Journal of Law and the Humanities*, v. 28, no. 2 (2017): 213-240, <https://centaur.reading.ac.uk/54870/>. Norberto Bobbio, *O futuro da democracia: uma defesa das regras do jogo* (Rio de Janeiro: Paz e Terra, 1986). Marc Hertog, “Your rule of law is not mine: rethink empirical approaches to EU rule of law promotion”, *Asia Europe Journal*, v. 14 (2016): 43-59, <https://link.springer.com/article/10.1007/s10308-015-0434-x> e Gopal Prasad Dahal, “The rule of law as political philosophy”, *NUTA Journal*, v. 5, no. 1-2 (2018): 95, <https://doi.org/10.3126/nutaj.v5i1-2.23465>.

⁴ Nuno Piçarra, *A separação de poderes como doutrina e princípio constitucional*, 11-15.

Esta vertente também buscou na Antiguidade Clássica o seu fundamento, baseado na premissa de que entre os homens e o poder político deveria existir a *instituição*, ou seja, entidade(s) independente(s) da identidade dos indivíduos, regida pelo princípio da moderação e racionalização, cuja atuação decorreria da lei,⁵ uma vez que “*é a lei que promove o bem comum.*”⁶

É essencialmente neste segundo pilar que o conceito de Estado de direito e seus corolários se desenvolvem nas ciências jurídicas, fruto do modelo de organização do poder político estadual de matriz liberal, cultura que se inicia em Inglaterra no século XVII, mas cujo expoente decorre no século seguinte nos Estados Unidos da América. É este modelo que reflete a explicação conceitual a seguir – e que se encontra no citado Relatório da Comissão Europeia.

O conceito de Estado de direito reconduz-se a uma ideia essencial: a noção de que o exercício do poder público deve estar sempre sujeito ao Direito, que atua como limite desse exercício de poder, em ordem à proteção, garantia e realização efetiva dos direitos fundamentais dos indivíduos. Apesar de o Estado de direito se materializar numa panóplia de princípios que o concretizam, dada a circunscrição da temática que nos serve de mote, vamos focar-nos no princípio da separação de poderes e no princípio da legalidade.

Corolário fundamental do princípio do Estado de direito, o princípio da separação de poderes divide o poder público por entidades a quem compete o seu exercício, de modo a evitar que o poder se concentre nas mãos de um único indivíduo. Para além desta dimensão negativa, o princípio da separação de poderes apresenta uma dimensão positiva, de interdependência de poderes, estabelecendo-se meios de controlo recíproco entre eles numa lógica de esquema relacional de competências, funções e responsabilidades pelo exercício desses poderes. Estas dimensões apenas são possíveis graças aos controlos e aos equilíbrios que as materializam – portanto, os *checks and balances*.

Outro corolário fundamental do Estado de direito é o princípio da legalidade, talvez o controlo mais relevante no que toca ao exercício do poder público, uma vez que desempenha um papel fundamental na limitação da arbitrariedade desse exercício. Porque parte da ideia seminal do *rule of law*, pressupõe necessariamente que as estruturas do poder público e a organização da sociedade sejam conformadas segundo a medida do direito, estabelecendo para isso regras e medidas, prescrevendo formas e procedimentos e criando instituições, numa lógica de hierarquia e de mútua responsabilização.

Dois principais corolários que resultam dos dois princípios fundamentais do Estado de direito acabados de analisar são o princípio da segurança jurídica e o princípio da transparência. O princípio da segurança jurídica implica que a atuação dos poderes públicos há de ser (desejavelmente) mensurável, traduzindo-se na garantia de um mínimo de previsibilidade em relação aos atos do poder público. O princípio da transparência implica que todos os procedimentos relacionados com o exercício do poder público devem ser tendencialmente públicos e acessíveis pelos cidadãos.

Embora seja difícil resumir em fórmulas simples a complexidade conceitual de princípios estruturantes⁷ (como é o princípio do Estado de direito), não se trata

⁵ Nuno Piçarra, *A separação de poderes como doutrina e princípio constitucional*, 26-32

⁶ Jeremy Waldron, “The concept and the rule of law”, *Georgia Law Review*, v. 43 (2008-2009): 33.

⁷ Jorge Reis Novais, *Princípios estruturantes de Estado de direito* (Coimbra: Almedina, 2019), 11.

de uma realidade *in abstracto*. A sua conformidade por parte de todos – entidades públicas, mas também privadas – serve a garantir a integridade de valores, como seja o respeito pela dignidade humana, e a permitir aos cidadãos a maior liberdade de todas, qual seja, a de planearem as suas próprias vidas.⁸ Por isso, é o mecanismo que, democraticamente e por via pacífica, permite o tratamento das desigualdades e problemas resultantes da convivência em sociedade, das debilidades e instrumentalização das instituições, da corrupção, da violência, da discriminação e vulnerabilidades dos direitos fundamentais.⁹

A partir de uma leitura atenta e transversal aos quatro Relatórios sobre o Estado de direito publicados entre os anos de 2020 e 2024 pela Comissão Europeia,¹⁰ podemos identificar que no pilar “*questões institucionais relacionadas com o equilíbrio de poderes*” foram destacados os seguintes assuntos: *i)* inclusividade, qualidade e transparência do processo legislativo; *ii)* reforma constitucional e fiscalização da constitucionalidade; *iii)* criação de instituições nacionais de defesa dos direitos humanos; e *iv)* participação das organizações da sociedade civil.

Em termos sucintos, no primeiro ponto – inclusividade, qualidade e transparência do processo legislativo –, podemos notar um posicionamento crítico da Comissão Europeia quanto à morosidade nos procedimentos legislativos dos Estados-Membros, bem como a instigação para que exista uma maior participação da sociedade civil nos processos decisórios. No âmbito das reformas constitucionais e da fiscalização da constitucionalidade, diversos Estados-Membros ponderam a criação de Tribunais Constitucionais e de instituições para defesa dos direitos humanos, com destaque ao papel do Provedor de Justiça. Por fim, em relação à participação das organizações da sociedade civil, os Relatórios revelam preocupação com restrições ao funcionamento e financiamento de organizações (especialmente organizações não governamentais) que são críticas às políticas de governo em alguns Estados-Membros.

Embora os Relatórios abordem questões institucionais relevantes sobre o equilíbrio de poderes nos Estados-Membros da União Europeia, nota-se uma lacuna significativa quanto ao impacto das tecnologias digitais nesse equilíbrio. O tema da transição digital – que é alvo deste Congresso – é apenas tangenciado com menções esparsas à adoção de plataformas eletrónicas para consulta pública no domínio do processo legislativo e à utilização de *software* de vigilância intrusivo (comumente conhecido por *software* espião) mas de forma ainda muito tímida.

O poder sistémico – designação introduzida pela literatura das ciências sociais e económicas para identificar um novo tipo de poder com capacidade e meios para se imiscuir no equilíbrio de poderes públicos – não foi ainda alvo de reflexão nos citados Relatórios. Esse poder é atribuível aos ditos “*gigantes da tecnologia*” – que têm sido considerados “*uma ameaça existencial para as democracias*”, por exercerem uma influência passível de “*substituir ou opor-se aos Estados*.”¹¹

Com a digitalização da sociedade e o surgimento de plataformas digitais – que são, na prática, espaços públicos digitais –, as empresas tecnológicas granjearam

⁸ Joseph Raz, “The rule of law and its virtue”, *Law Quarterly Review*, v. 93 (1977): 219-222.

⁹ United Nations, Secretary General, *New vision of Secretary-General for the rule of law* (New York: OHCHR, 2023), 2-4, <https://www.ohchr.org/sites/default/files/2023-08/230511-new-vision-for-rule-of-law.pdf>.

¹⁰ Comissão Europeia, Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, *Relatório de 2020 sobre o Estado de direito – situação na União Europeia*, COM(2020) 580 final de 30.9.2020; COM(2022) 500 final de 13.7.2022; COM(2023) 800 final, de 5.7.2023 e COM (2024) 800 final de 24.7.2024.

¹¹ Cristine Kerdellant, *Mais poderosos do que os Estados* (Coimbra: Edições 70, 2025).

um imenso poder – que se caracteriza cada vez mais como “quase” público. E se as plataformas digitais exercem poderes materialmente públicos, talvez seja de equacionar a qualificação da inteligência artificial como uma manifestação de um poder público, algo aflorado em algumas das reflexões que se seguem.

Porque as dimensões do Estado de direito acima referidas se integram nas estruturas fundamentais do constitucionalismo, tem-se usado o termo “*constitucionalização do digital*” ou “*constitucionalismo digital*” para definir a regulamentação das plataformas digitais no que toca à esfera pública digital – porque procura criar, efetivamente, controlos ao poder público digital e equilíbrios ao exercício desse mesmo poder. Também se tem recorrido à expressão “*constitucionalização da autorregulação*”, que acaba por expressar a mesma ideia ou intenção, mas com pormenores diferenciadores. Isto conflui para a ideia de que o poder público das plataformas digitais carece de se reger por padrões constitucionais – que se concretizam necessariamente nos controlos e equilíbrios que os princípios densificadores do Estado de direito implicam. Legalidade, transparência, (ciber)segurança são aspetos relevantes a ter em conta quando refletimos sobre o Estado de direito e a transição digital.

Serve este breve enquadramento para apoiar a leitura dos interessantes estudos que se seguem – e para fornecer algumas bases de interpretação. Mas também serve para colocar algumas reflexões prévias, que serviram precisamente para promover o debate das questões suscitadas *in loco*, no âmbito da iniciativa #Juniors2Seniors.

A primeira, reportando-se precisamente ao enquadramento acabado de fazer, materializou-se da seguinte forma: quanto às atuações materialmente públicas das plataformas digitais, bastará a exigência de transparência, enquanto controlo do exercício do poder público, ou será mais apropriado sujeitar as plataformas digitais às exigências que advêm da efetiva separação de poderes, carreando a legalidade e, principalmente, a interdependência dos poderes que materialmente exerce?

A segunda questão parte de uma perspectiva holística e foi pensada a partir dos seguintes termos: vivemos numa era classificada por muitos pensadores como distópica, pós-moderna, “*metamoderna*”, etc., mas quanto ao exercício do poder, acabamos por retornar à questão aristotélica: quem tem o poder de gerir o espaço público? Com a tónica cada vez maior entre a interação dos espaços físico e digital, o poder de decisão passa a ser pensado de forma “*rivalizada*” entre o humano e o algoritmo. Esse ser humano encontra-se sujeito a manipulações e refém do crescimento de uma hiperindividualização, de um sentimento de desconfiança, descrédito e desinteresse pelas instituições públicas clássicas – o que é aproveitado por movimentos autocráticos e populistas com discursos simplistas, que buscam o controlo enquanto “*representam o papel de democratas*.”¹² Neste cenário, como pode o princípio do Estado de direito prevalecer (ou sobreviver)?

Para finalizar – e retornando aos Relatórios da Comissão Europeia que conclamam uma “*cultura do Estado de direito*” no quadro institucional – como podem as entidades dedicadas ao ensino desempenharem um papel mais efetivo no sentido de “*educar para o Estado de direito*”? É através da educação que se pode fornecer aos indivíduos conhecimento e valores adequados para exigir transparência e responsabilidade das instituições públicas, ou seja, prover o cidadão de meios para decidir de forma ética e responsável e contribuir de forma contínua na

¹² Serguei Guriev e Daniel Treisman, *A ditadura adaptada ao século XXI: como os novos tiranos se reinventaram* (Estoril: Desassossego, 2024), 27.

sociedade, bem como fomentar uma cultura de legalidade.¹³ E, nesta medida, o Estado de direito – e o equilíbrio institucional que implica – são indispensáveis ao funcionamento do ecossistema digital.

¹³ Marlova Jovchelovitch Noletto e Maria Rebeca Otero Gomes (coords.), *Fortalecimento do Estado de direito por meio da educação: um guia para formuladores de políticas* (Brasília: Escritório de Ligação e Parcerias do UNODC Brasil; Representação da UNESCO Brasil, 2019), 16-23.

Checks and balances no exercício da função legislativa e da função jurisdicional da União Europeia

Nuno Piçarra*

Esta intervenção centra-se na análise dos *checks and balances* (expressão habitualmente traduzida por freios e contrapesos) que, por imposição do princípio fundamental do Estado de Direito, plasmado, antes de mais, no artigo 2.º do Tratado da União Europeia (TUE), enquadram a titularidade e o exercício da função legislativa e da função jurisdicional na União Europeia (“UE” ou “União”), enquanto quadro institucional e decisório autónomo em relação aos Estados-Membros, com vista a identificar desafios específicos com que a “*transição digital*” a confronta. Mas antes parece-me oportuna uma breve nota sobre o próprio conceito de *checks and balances*.

I

1. Como o nome indica, este conceito é de origem anglo-saxónica e foi objeto de desenvolvimentos importantes na discussão política muito viva travada no século XVII em Inglaterra, onde nasceu também o conceito de *rule of law* ou Estado de Direito. Os dois conceitos ficaram indissociavelmente ligados desde então, tendo como pano de fundo uma conceção essencialmente liberal e não absolutista do poder político, que atende à necessidade de limitar sempre o seu exercício, independentemente da sua titularidade. Isto porque “*o poder corrompe e o poder absoluto corrompe absolutamente.*”

Enquanto meio ao serviço da limitação e da racionalização do poder político, o conceito de *checks and balances* constitui uma das aceções do conceito polissémico de separação de poderes.¹

2. Nesta aceção, tal conceito encontrou a sua primeira e mais conhecida expressão jurídica, enquanto princípio fundamental de organização do poder político-estadual, na constituição federal norte-americana de 17 de setembro de 1787, com todo o aprofundado debate político que a antecedeu, refletido nos *Federalist Papers* (sobretudo cartas n.º 47 a n.º 51), e a influência decisiva de James Madison.

Madison, por sua vez, inspirou-se antes de mais em Montesquieu e na sua ideia, essencialmente liberal, de que o poder, independentemente da legitimidade

* Juiz no Tribunal de Justiça da União Europeia. As opiniões expressas neste texto são estritamente pessoais. Agradeço a leitura atenta da Doutora Sophie Perez Fernandes, referendária no meu gabinete, que não me exime da responsabilidade exclusiva por qualquer deficiência.

¹ Sobre o tema ver o estudo fundamental de William B. Gwyn, *The meaning of the separation of powers: an analysis of the doctrine from its origin to the adoption of the United States Constitution* (Haia: Martinus Nijhoff, 1965), especialmente 28-82. Em língua portuguesa, ver recentemente Paulo Rangel, *As raízes do parlamentarismo e a revolução conservadora*, 2021, ISBN 978-989-331391, especialmente 61-81.

em que se funda, deve ser limitado, através da sua distribuição por vários pólos, de maneira a que, na formulação famosa, “*le pouvoir arrête le pouvoir*.” Para este efeito, numa estrutura institucional caracterizada pelos *checks and balances*, isto é, pela separação de poderes, nesta sua aceção, devem existir duas categorias essenciais de poder: o de decisão (*pouvoir de statuer*) e o de controlo (*pouvoir d’empêcher*), isto é, “*de tornar nula uma decisão tomada por qualquer outro*.” Estas duas categorias podem e devem coexistir inclusive dentro do mesmo pólo de poder.

Neste contexto, consolidou-se também a dualidade fundamental entre *gubernatio* e *jurisdictio*, ou seja, de um lado, o poder de direção e decisão políticas enquadrado por um *higher law* plasmado na constituição e, de outro lado, um poder jurisdicional encarregado nomeadamente de controlar os poderes legislativo e executivo pelo parâmetro de validade material, e não meramente formal e procedimental, constituído por esse *higher law*.²

Na perspetiva de James Madison, os *checks and balances* tinham também um objetivo muito preciso: uma vez que a constituição de 1787 excluía a monarquia e a legitimidade monárquica, para se basear unicamente na legitimidade democrático-representativa – assente, de resto, em colégios eleitorais restritos –, importava, antes de mais, impedir a formação de “*maiorias tiránicas*” que, a partir de um dos pólos de poder político criados pela constituição, designadamente o poder legislativo, pudesse assenhorear-se de todo o poder e exercê-lo sem freios nem contrapesos em detrimento das minorias.³

3. O que Madison não podia prever é que “*maiorias tiránicas*”, claramente iliberais, se formariam no século XXI e na era da “*transição digital*” da maneira como se formam em regimes democráticos. Na realidade, tal “*transição*” também faculta a políticos e governantes assim como aos seus potenciais eleitores meios antes desconhecidos para combaterem eficazmente os valores que se encontram plasmados no artigo 2.º do TUE, também enquanto valores comuns aos Estados-Membros. Como que por ironia, o exemplo da pátria de Madison é o mais recente e inquietante.

Estudos recentes têm chegado à conclusão de que “*os meios de comunicação social digital baixam a confiança nas instituições democráticas e nos meios de comunicação social clássicos, fomentando o populismo e a polarização [...] pelo menos em democracias consolidadas*.”⁴

Trata-se de um tema capital que já foi objeto de amplos e estimulantes desenvolvimentos ao longo deste congresso bracarense, para os quais me limito a remeter, salientando que uma das questões mais prementes que se coloca à UE é a de determinar em que medida esta e as suas instituições dispõem de meios para evitar derrapagens a nível dos Estados-Membros na garantia dos valores comuns em causa, sem prejuízo da questão autónoma de saber em que medida a própria União se pode considerar, por reflexo, imune a tais derrapagens.

² Ver Alain Laquièze, “Séparation des pouvoirs et balance des pouvoirs au XVIIIe siècle: Montesquieu et la Constitution des États-Unis”, *L’Europe des Lumières et la Constitution américaine*, dir. Jean-Pierre Machelon e Charles-Philippe de Vergennes (Éditions mare & martin, 2017), 31-55, salientando que a separação/balança dos poderes à americana só pode compreender-se no quadro federal, o qual pretende reforçá-la (52-53).

³ Ver Gwyn, *The meaning of the separation of powers...*, 100-130; Nuno Piçarra, *A separação dos poderes como doutrina e princípio constitucional. Um contributo para as suas origens e evolução* (Coimbra Editora, 1989), especialmente 89-124.

⁴ Ver, por exemplo, Thomas Thiel, “Die Demokratisierung der Netze. Soziale Netzwerke gefährden laut einer Metastudie die Demokratie: Welche Massnahmen sind zu ergreifen?”, *Frankfurter Allgemeine Zeitung*, 9 de abril de 2025 (tradução livre), com referência a um estudo citado.

II

4. A UE, entidade política indubitavelmente muito diferente de um Estado federal, mas com certos traços federais,⁵ é tributária, estrutural e funcionalmente, do tandem *checks and balances/rule of law*, como o testemunha o já referido artigo 2.º do TUE, nos termos do qual “[a] União funda-se nos valores do respeito pela dignidade humana, da liberdade, da democracia, da igualdade, do Estado de Direito e do respeito pelos direitos fundamentais, incluindo os direitos das pessoas pertencentes a minorias. Estes valores são comuns aos Estados-Membros, numa sociedade caracterizada pelo pluralismo, a não discriminação, a tolerância, a justiça, a solidariedade e a igualdade entre homens e mulheres.”⁶

Resulta deste artigo que o princípio do Estado de Direito engloba os *checks and balances*, uma das diversas aceções do princípio da separação de poderes, enquanto elemento estruturante do quadro institucional da UE – onde assume a denominação de princípio do equilíbrio institucional.⁷ O artigo 13.º do TUE, depois de enumerar taxativamente, no n.º 1, segundo parágrafo, as instituições da União – o Parlamento Europeu, o Conselho Europeu, o Conselho, a Comissão Europeia, o Tribunal de Justiça da União Europeia, o Banco Central Europeu e o Tribunal de Contas – determina, no n.º 2, que cada uma delas “*atua dentro dos limites das atribuições que lhe são conferidas pelos Tratados, de acordo com os procedimentos, condições e finalidades que estes estabelecem*”, todas devendo “*manter[er] entre si uma cooperação leal*.”

5. Pela grande atualidade de que se reveste, parece-me importante salientar, em breve excursão, que a alegada violação do artigo 2.º do TUE constitui o fundamento de uma ação por incumprimento pendente no Tribunal de Justiça (TJ)⁸ e intentada nos termos do artigo 258.º do Tratado sobre o Funcionamento da União Europeia (TFUE) pela Comissão Europeia contra a Hungria (processo C-769/22), por causa de uma lei de 2021, que alterou, entre outras, a lei sobre proteção das crianças.

Esta última lei, na versão que lhe foi dada pela primeira, proíbe que sejam colocados à disposição das pessoas de menos de dezoito anos conteúdos que, entre outros, “*promovam a divergência em relação à identidade pessoal correspondente ao sexo à nascença, a mudança de sexo e a homossexualidade*.” A mesma proibição foi também incluída na lei sobre a publicidade comercial. Por seu lado, a lei sobre os meios de comunicação social passou a proibir a qualificação como “*anúncio de interesse público ou mensagem de sensibilização*” de qualquer conteúdo que tenha tal “*promoção*” ou “*apresentação*” como “*elemento determinante*.” Além disso, a lei sobre a educação pública, na versão que lhe foi dada pela lei de 2021, proíbe a “*organização de atividades sobre cultura sexual, vida sexual, orientação sexual e desenvolvimento sexual destinadas a alunos*”, que “*visem promover a divergência em relação à identidade pessoal correspondente ao sexo à nascença, a mudança de sexo e a homossexualidade*.”

Na audiência pública deste processo, realizada em novembro de 2024, alegou-se contra a justiciabilidade do artigo 2.º do TUE o facto de incluir conceitos polissémicos como, por exemplo, o de “*liberdade*” e o de “*democracia*.” A isto pode

⁵ Sobre o tema, ver recentemente Francisco Pereira Coutinho, *Ensinar Direito Constitucional da União Europeia* (Lisboa: Petrony, 2023), 19-123.

⁶ Para um conspecto, ver Alessandra Silveira, *Fundamentos jurídico-políticos da integração europeia* (Lisboa: Quid Juris, 2024), 119-123.

⁷ Como observa Koen Lenaerts, “On checks and balances: the rule of law within the EU”, *Columbia Law Review (Special Issue)* (2024): 7: “*the Court of Justice has interpreted the rule of law within the EU in keeping with the checks and balances laid down in the Treaties*.”

⁸ Para a distinção entre Tribunal de Justiça da União Europeia e Tribunal de Justiça, ver infra n.º 9.

responder-se que o elemento sistemático ou contextual de interpretação deste artigo reduz substancialmente a polissemia do conceito de “*liberdade*.” Na realidade, este coexiste, entre outros, com o de “*igualdade*” e de “*solidariedade*.” Fica assim excluído, parece-me, um conceito de liberdade suscetível de o reduzir à liberdade económica e ao direito do mais forte a enriquecer em detrimento do mais fraco. No que respeita ao conceito de “*democracia*”, o facto de ele coexistir, designadamente, com o conceito de Estado de Direito, que engloba o de *checks and balances*/separação de poderes, exclui manifestamente que possa englobar democracias iliberais, assentes no poder de uma maioria determinada em reduzir ou aniquilar “*os direitos das pessoas pertencentes a minorias*”, a começar pelas minorias políticas e as minorias sexuais.⁹

III

6. Passando à análise da função legislativa da UE à luz do conceito de *checks and balances* plasmado também no artigo 13.º, n.º 2, do TUE, parece-me de salientar liminarmente que a própria UE se centra na titularidade e no exercício desta função, a qual, à luz da dicotomia recordada no n.º 2 deste texto, releva do *gubernatio*. Para utilizar a sugestiva expressão anglo-saxónica, a UE é “*legislation centered*”, dada a opção estruturante dos Tratados constitutivos por um sistema descentralizado de execução desta legislação pelas administrações dos Estados-Membros e, portanto, da limitada competência executiva própria de que a União foi dotada, como o confirma o artigo 291.º do TFUE.

Este artigo, incumbindo os Estados-Membros de tomarem “*todas as medidas de direito interno necessárias à execução dos atos juridicamente vinculativos da União*” (n.º 1), precisa que, quando forem “*necessárias condições uniformes de execução*” destes atos, os mesmos conferirão “*competências de execução*” à Comissão ou, “*em casos específicos devidamente justificados*”, ao Conselho (n.º 2). As regras e princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução da Comissão são previamente definidas por ato legislativo da UE (n.º 3), atualmente o Regulamento n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011.

Como ser verá adiante (n.º 11), o sistema de execução descentralizado da legislação da União encontra o seu lugar paralelo no sistema descentralizado de aplicação jurisdicional da mesma legislação.

7. Dos artigos 13.º a 18.º do TUE resulta que, se a titularidade e o exercício da função legislativa da UE revelam traços federais, esta constatação não põe de todo em causa que, mesmo neste domínio, o contraste da UE com um Estado federal é nítido.

Na realidade, enquanto que num Estado federal, para efeitos da respetiva função legislativa, os Estados federados estão representados numa das câmaras do Parlamento, representando a outra câmara os cidadãos, no quadro institucional da UE, os Estados-Membros estão representados no Conselho através de membros dos respetivos governos no ativo, em função das suas competências ministeriais.

Sobre o Conselho Europeu, a outra instituição de representação dos Estados-Membros no quadro institucional da União, através dos Chefes de Estado e de

⁹ Ver Conclusões da Advogada-Geral Tamara Čapeta apresentadas em 5 de junho de 2025, processo C-769/22, ECLI:EU:C:2025:408 (edição provisória). Sobre o tema ver Lucia Serena Rossi, «“Concretised”, “Flanked” or “Standalone”? Some reflections on the application of Article 2 TEU», *European Papers* 1 (2025): 1-24.

Governo em exercício – testemunhando o peso dos Estados-Membros no quadro institucional da UE, sem paralelo em Estados federais –, o artigo 15.º, n.º 1, segunda frase, do TUE dispõe expressamente que tal instituição “*não exerce a função legislativa.*” A esta delimitação negativa de competência não terá sido estranha uma lógica de *checks and balances*, que se oporia à acumulação desta função numa instituição dotada da competência para “*d[ar] à União os impulsos necessários ao seu desenvolvimento e defin[ir] as orientações e prioridades políticas gerais da União.*”

Por seu lado, os cidadãos da União, definidos pelo artigo 20.º, n.º 1, do TFUE como “*qualquer pessoa que tenha a nacionalidade de um Estado-Membro*”, estão diretamente representados no Parlamento Europeu unicameral.

Finalmente, a própria União está representada pela Comissão Europeia, que tem por atribuição primeira a de promover o interesse geral da União e de tomar as iniciativas adequadas para esse efeito, tal como determina o artigo 17.º, n.º 1, do TUE.¹⁰

A função legislativa (e também a função orçamental) da UE são assim exercidas, nos termos do artigo 14.º, n.º 1, e 16.º, n.º 1, do TUE, pelo Parlamento Europeu e pelo Conselho. O artigo 17.º, n.º 2, deste tratado, sem coatribuir à Comissão o exercício da função legislativa, prevê expressamente que “*os atos legislativos da União só podem ser adotados sob proposta da Comissão, salvo disposição em contrário dos Tratados.*”

Esta última disposição deve ser lida em conjugação com o artigo 293.º, n.º 1, do TFUE, nos termos do qual “*[s]empre que, por força dos Tratados, delibere sob proposta da Comissão, o Conselho só pode alterar a proposta deliberando por unanimidade.*” Daqui resulta a vontade dos autores do Tratados de garantir o peso da Comissão no exercício da função legislativa, impedindo, de acordo com uma lógica de *checks and balances*, que o Conselho, deliberando de acordo com a regra da maioria qualificada, tal como definida no artigo 16.º, n.º 4, do TUE, descaracterize as propostas legislativas da Comissão em detrimento do interesse geral da União que cabe a esta instituição promover.

Das exceções que o artigo 293.º, n.º 1, do TFUE abre em relação à deliberação por unanimidade no Conselho, para efeitos da alteração de propostas da Comissão, só uma diz respeito a propostas legislativas apresentadas no quadro do chamado processo legislativo ordinário, contemplado pelo artigo 294.º do TFUE e em larga medida inspirado pelo processo legislativo federal alemão. A deliberação por unanimidade no Conselho, para efeitos da alteração das propostas legislativas da Comissão, só é assim dispensada, nos termos dos n.ºs 10 e 13 deste artigo, na chamada fase do Comité de Conciliação, o qual reúne os membros do Conselho ou os seus representantes e igual número de membros representando o Parlamento Europeu, com a missão de chegar a acordo sobre um projeto comum, por maioria qualificada dos membros do Conselho ou dos seus representantes e por maioria dos membros que representam o Parlamento Europeu, no prazo de seis semanas a contar da sua convocação.

De tudo isto resulta claro que a função legislativa, função central da UE, é exercida de acordo com uma lógica positiva de *checks and balances*, que também comporta correlações e comparticipações entre o Parlamento Europeu, o Conselho e a Comissão.

¹⁰ Para maiores desenvolvimentos, ver, por exemplo, S. Roland, *Le triangle décisionnel communautaire à l'aune de la théorie de la séparation des pouvoirs. Recherches sur la distribution des pouvoirs législatif et exécutif dans la Communauté* (Bruxelas: Bruylant, 2008).

8. A interpretação e aplicação do artigo 293.º, n.º 1, do TFUE, já originou litígios interinstitucionais dirimidos pelo TJ, no típico exercício da função de tribunal constitucional, tomando como pano de fundo o princípio do equilíbrio institucional consagrado pelo artigo 13.º, n.º 2, do TUE – definido como “*característico da estrutura institucional da União, que implica que cada uma das instituições exerça as suas competências com respeito pelas das outras*” – e à luz do qual a primeira disposição deve ser lida.

No recurso de anulação na origem do acórdão de 22 de novembro de 2022, *Comissão contra Conselho (Adesão ao Ato de Genebra)* (C-24/20, EU:C:2022:911), a Comissão alegou a violação do artigo 293.º, n.º 1, do TFUE na medida em que, ao abrigo desta disposição – deliberando, portanto, por unanimidade –, o Conselho tinha introduzido na proposta legislativa uma disposição que obstaría à realização do objetivo por ela prosseguido, a saber permitir à União exercer corretamente a sua competência exclusiva nos domínios abrangidos pelo ato em processo de aprovação.

O TJ começou por recordar que o artigo 293.º, n.º 1, do TUE assegura o respeito do princípio do equilíbrio institucional, ponderando, nomeadamente, as competências da Comissão, ao abrigo do artigo 17.º, n.º 2, do TUE, e as do Conselho, previstas no artigo 16.º, n.º 1, do TUE, e que o poder de alteração assim conferido ao Conselho “*não pode estender-se a ponto de lhe permitir desvirtuar a proposta da Comissão num sentido que obsta à realização dos objetivos prosseguidos por esta e que, assim, a priva da sua razão de ser*”, sob pena de violação do equilíbrio institucional cujo respeito a primeira disposição visa assegurar (n.ºs 92, 93 e 112).

No caso em apreço, o TJ constatou que a alteração introduzida pelo Conselho, por unanimidade, na proposta da Comissão desvirtuava a finalidade da proposta, na medida em que habilitava os Estados-Membros a exercer uma competência exclusiva da UE e julgou, portanto, a decisão impugnada contrária ao artigo 293.º, n.º 1, do TFUE, em conjugação como o artigo 13.º, n.º 2, do TUE (n.ºs 105 e 113).

Em acórdão de 14 de abril de 2015, *Conselho contra Comissão* (C-409/13, EU:C:2015:217, n.ºs 70 e 74), o TJ tinha declarado que, não se resumindo o poder de iniciativa da Comissão contemplado pelo artigo 17.º, n.º 1, do TUE à apresentação de propostas, esta instituição está habilitada a retirar a sua proposta em casos como o que deu origem ao acórdão de 22 de novembro de 2022, embora nenhuma disposição dos Tratados o preveja expressamente.

IV

9. Tratando-se da função jurisdicional, parece-me de realçar liminarmente que a UE, não obstante as suas origens inequivocamente jus-internacionais, é estruturalmente marcada pela dualidade *gubernatio/jurisdictio*, enquanto refração da dualidade *pouvoir de statuer/pouvoir d'empêcher*. Isto resulta não só implicitamente do próprio artigo 2.º do TUE, mas expressamente do artigo 19.º, n.º 1, primeiro parágrafo, segunda frase, deste tratado, nos termos do qual, em formulação feliz, o “*Tribunal de Justiça da União Europeia garante o respeito do direito na interpretação e aplicação dos Tratados*” que, juntamente com a Carta dos Direitos Fundamentais da União Europeia (Carta), conformam a constituição material da UE.

Em acórdão de 20 de abril de 2021, *Repubblica* (C-896/19, EU:C:2021:311, n.º 63), o TJ teve ocasião de precisar que o valor “*Estado de Direito*”, enunciado no artigo 2.º do TUE, é concretizado nomeadamente por este artigo 19.º.

Como o indica a primeira frase do artigo 19.º, n.º 1, do TUE, a designação “*Tribunal de Justiça da União Europeia*” engloba atualmente dois órgãos jurisdicionais

organicamente pertencentes à UE: o TJ e o Tribunal Geral (TG). O primeiro é simultaneamente o tribunal constitucional e o tribunal supremo da UE, cabendo-lhe a última palavra sobre a interpretação de todo direito desta e sobre a validade do direito derivado ou infraconstitucional da mesma, a começar pelos atos legislativos, tal como os define o artigo 289.º, n.º 3, do TFUE. É o que resulta, no essencial, das disposições conjugadas do artigo 256.º deste último tratado e do artigo 51.º do Estatuto do Tribunal de Justiça da União Europeia (Estatuto), constante do Protocolo n.º 3, anexo ao TUE e ao TFUE.

O TG é no essencial um tribunal administrativo, destinado a dirimir, também em segunda instância, o contencioso gerado pelos atos da administração própria da União. As decisões deste tribunal “*podem ser objeto de recurso para o [TJ] limitado às questões de direito, nas condições e limites previstos no Estatuto.*”

10. As exigências quanto ao perfil dos juízes dos dois órgãos jurisdicionais não são exatamente as mesmas, embora todos eles devam, nos termos do artigo 19.º, n.º 2, terceiro parágrafo, do TUE e dos artigos 253.º e 254.º do TFUE, ser “*nomeados de comum acordo, por seis anos, pelos governos dos Estados-Membros, após consulta ao comité previsto no artigo 255.º*”, e “*escolhidos de entre personalidades que ofereçam todas as garantias de independência.*”

Os juízes do TJ devem, nos termos do artigo 253.º, primeiro parágrafo, do TFUE, reunir “*as condições exigidas, nos respetivos países, para o exercício das mais altas funções jurisdicionais*”, ou ser “*jurisconsultos de reconhecida competência*”, enquanto que, nos termos do artigo 254.º, segundo parágrafo, do TFUE, os juízes do TG “*serão escolhidos de entre pessoas que [...] possuam a capacidade requerida para o exercício de altas funções jurisdicionais.*”

As diferenças quanto à competência destes dois tribunais e ao perfil dos respetivos juízes, assim resultantes do TFUE, têm duas consequências de peso. Por um lado, o TJ não deve ser visto como um mero tribunal (administrativo) de última instância em relação ao TG, que devesse ser composto progressivamente por juízes que já exerceram o seu mandato no TG. De resto, os acórdãos ou despachos do TJ proferidos em recurso de decisões do TG não representam normalmente mais do que um quarto do total da atividade jurisdicional anual do primeiro órgão jurisdicional.

Por outro lado, a natureza de tribunal constitucional do TJ implica que pelo menos uma parte dos seus juízes e advogados-gerais deva ser escolhida em função da familiaridade, seja a que título for (juiz, jurisconsulto, académico, advogado), com a “*administração específica da justiça em matérias de natureza jurídico-constitucional*”, para empregar a expressão constante do artigo 221.º da Constituição da República Portuguesa de 1976.

Como esclareceu, em termos sempre atuais, o antigo presidente do Tribunal Constitucional português, Conselheiro Luís Nunes de Almeida, a qualificação de um órgão jurisdicional como tribunal constitucional depende decisivamente da existência no seu interior de um equilíbrio entre blocos político-culturais, isto é, “*conceções de vida, pré-compreensões, opções sobre a organização da sociedade.*” Para citar as palavras eloquentes do autor, é fundamental que exista no colégio de juízes formado por esse órgão jurisdicional – a título de “*separação de poderes dentro dos poderes*”¹¹ ou de “*checks and balances* intraorgânicos ou intrainstitucionais” – “*um equilíbrio entre*

¹¹ Sobre este conceito, ver, por exemplo, Walter Leisner, “Gewaltenteilung innerhalb der Gewalten”, *Festgabe für Theodor Maunz* (Berlim, 1971).

os que defendem, sobretudo, a liberdade e os que propendem mais para a autoridade; entre os que acentuam mais a necessidade de garantir os direitos do cidadão e os que atribuem maior importância à salvaguarda das instituições; entre os que pendem para as prerrogativas do Parlamento e os que simpatizam mais com o reforço dos poderes do Executivo; entre os que veem a realização da justiça social através do reconhecimento de direitos e aqueles que a veem sobretudo realizada através de formas assistenciais; entre os que se preocupam com a redistribuição da riqueza e os que dão maior ênfase à produção; entre os que têm uma formação laica e os que têm uma formação confessional.”¹²

11. De acordo com a opção estruturante dos Tratados por um sistema descentralizado de aplicação jurisdicional do direito da UE pelos tribunais dos Estados-Membros, que faz destes os tribunais de direito comum da União, o TJ e o TG são órgãos jurisdicionais especializados. A articulação dos tribunais dos Estados-Membros com o TJ, de modo a viabilizar o exercício da competência deste último, enquanto tribunal supremo e tribunal constitucional da UE, responsável final pela interpretação e aplicação uniformes do direito da UE, faz-se através do reenvio prejudicial tal como o configuram o artigo 19.º, n.º 3, alínea *b*), do TUE e sobretudo o artigo 267.º do TFUE – e não, em absoluto, através de um sistema de recursos jurisdicionais para o TJ das decisões dos tribunais dos Estados-Membros que aplicam o direito da UE.¹³ Esta característica constitui, de resto, uma notória singularidade da UE em relação a uma federação de natureza estadual.

O facto de, desde 1 de outubro de 2024, o TG também dispor de competência prejudicial designadamente no âmbito de determinados direitos administrativos especiais da União, como o direito tributário e o direito aduaneiro, não retirou ao TJ o essencial daquela competência de última instância, como o atesta desde logo o artigo 256.º, n.º 3, terceiro parágrafo, do TFUE. Com efeito, segundo esta disposição, “[a]s decisões proferidas pelo [TG] sobre questões prejudiciais podem ser reapreciadas a título excecional pelo [TJ], nas condições e limites previstos no Estatuto, caso exista risco grave de lesão da unidade e da coerência do direito da União.”¹⁴

V

12. Para terminar, gostaria de fazer uma brevíssima referência à interação entre o legislador da União e o TJ, enquanto tribunal constitucional, no âmbito da legislação em matéria de proteção de dados, tão essencial na “era da transição digital”, como é sabido.

O *leading case* na matéria, continua a ser o acórdão de 8 de abril de 2014, *Digital Rights Ireland e o.* (C-293/12 e C-594/12, EU:C:2014:238), em que o TJ anulou a diretiva 2006/24, de 15 de março de 2004 – 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 – essencialmente com o fundamento de que, à luz dos direitos fundamentais à proteção de dados pessoais e ao respeito pela vida privada garantidos pelos artigos 7.º e 8.º da Carta,

¹² Ver Luís Nunes de Almeida, “Da politização à independência (algumas reflexões sobre o Tribunal Constitucional)”, in *Legitimidade e legitimação da justiça constitucional. Colóquio no 10.º Aniversário do Tribunal Constitucional* (Coimbra, 1995), 252-253.

¹³ Para uma exposição recente, ver Koen Lenaerts, “On checks and balances: the rule of law within the EU”, 8 e seguintes.

¹⁴ Para maiores desenvolvimentos, ver José Martín y Pérez de Nanclares, “La reforma del Tribunal de Justicia de la Unión Europea: La ruptura de un tabú”, *Revista Española de Derecho Europeo*, 90 (2024): 21-63.

a margem de apreciação do legislador é reduzida e o controlo jurisdicional dessa margem de apreciação deve ser estrito, só sendo admissíveis limitações a estes direitos na medida em que se comprovem como estritamente necessárias.

Esta jurisprudência foi retomada no âmbito da chamada *mass surveillance*. Significa isto que a retenção generalizada de dados pessoais e o acesso a esses dados constituem ingerências distintas nos direitos fundamentais consagrados pelos artigos 7.º e 8.º da Carta e, portanto, que cada uma dessas ingerências exige uma justificação autónoma, em conformidade com o artigo 52.º, n.º 1, desta. Mesmo quando se trata apenas da retenção indiscriminada de endereços IP, o TJ não abandonou a exigência de que a importância do objetivo prosseguido pela medida deve ser proporcional à gravidade da ingerência que implica nos direitos fundamentais em causa. Atesta-o, por último, o acórdão de 30 de abril de 2024, *La Quadrature du Net e o. (Dados pessoais e combate à contrafação)* (C-470/21, EU:C:2024:370).

Pode dizer-se que esta jurisprudência do TJ, de resto, em larga sintonia com a do Tribunal Europeu dos Direitos Humanos, garante aos direitos fundamentais em causa um nível de proteção elevado perante os poderes crescentes que os Estados-Membros assumem em matéria de *mass surveillance* na “*era da digitalização*.” Tal jurisprudência constitui certamente um desincentivo para o legislador da União e os legisladores dos Estados-Membros fazerem novas tentativas de introdução de regimes gerais de retenção preventiva de dados de comunicação.

Isto mesmo foi dito recentemente pelo vice-presidente do TJ.¹⁵ Subscribo plenamente as suas afirmações. Mas pergunto: e se se chegar a uma situação em que o TJ – com renovada composição, suscetível de pôr em causa o equilíbrio referido no n.º 10 do presente texto, e perante a insistência restritiva de legisladores dispostos a fazer prevalecer nesta matéria a segurança sobre a liberdade, valores em permanente tensão, no contexto dos riscos e perigos para a democracia e o Estado de Direito supra-assinalados (n.º 3) – opte por revogar esta jurisprudência?

Podemos excluir semelhante hipótese na “*era da digitalização*”?

¹⁵ Ver Thomas von Danwitz, *Mass surveillance and personal data protection – common methodical principles and distinctive characteristics*, conferência proferida em 18 de novembro de 2024 no âmbito da visita oficial de uma delegação do TJ ao Tribunal Europeu dos Direitos Humanos.

Inteligencia Artificial y Constitución: un análisis desde la perspectiva de los controles y equilibrios institucionales

Ana Carmona Contreras*

1. Aproximación preliminar a la cuestión

Con la finalidad de situar la cuestión propuesta en su preciso ámbito de referencia resulta necesario aludir a una serie de cuestiones básicas que, no por su obviedad, resulta imprescindible tomar en consideración. Contextualizar y enmarcar el debate de los retos que la Inteligencia Artificial proyecta sobre la comprensión de la normatividad constitucional, así como su impacto sobre esenciales componentes del Estado de Derecho se muestran, pues, como referentes insoslayables.

A este respecto, en primer lugar, se presenta como un lugar común afirmar la trascendente magnitud de la revolución tecnológica, la cual ha traído consigo la denominada Inteligencia Artificial predictiva o generativa. El vertiginoso avance experimentado en este campo nos enfrenta a lo que no cabe calificar sino como un auténtico “*tsunami digital*.” En efecto, la expansión irrefrenable de la referida modalidad de Inteligencia Artificial, también denominada “*machine learning*”, abre campos ingentes de actuación, tanto en términos cuantitativos como cualitativos, a esos sistemas en los que los correspondientes algoritmos desarrollan estrategias de “*aprendizaje*” progresivo de cara a la adopción de decisiones y a la resolución de conflictos.

Por otra parte, no cabe desconocer el punto de inflexión, el indudable salto cualitativo que trae aparejado el avance de este tipo de Inteligencia Artificial, superponiéndose y sobrepasando ampliamente los efectos anudados a la existencia de Internet y de las redes sociales. Desde esta perspectiva, la dimensión planetaria, esto es, el ámbito universal en el que se desarrollan estas herramientas tecnológicas produce un impacto frontal tanto sobre el Estado de Derecho como en relación con los derechos fundamentales.

Comenzando por el **Estado de Derecho**, ha de recordarse que el mismo se rige por un principio esencial, a saber, el ejercicio del poder aparece sometido al imperio de la ley y a las prescripciones normativas establecidas. Inmediata manifestación expresa de la inescindible vinculación entre Poder y Derecho es la disposición contenida en el artículo 9.1 de la Constitución española, en donde se establece lo siguiente: “*Los ciudadanos y los poderes públicos están sometidos a la Constitución y al resto del ordenamiento jurídico.*” Tan esencial axioma, auténtico eje articulador de la comprensión del ejercicio del poder en el seno estatal, experimenta una quiebra mayúscula en relación con los prestadores de los servicios de Inteligencia Artificial. En efecto, al tratarse de grandes plataformas privadas que operan a escala planetaria,

* Profesora de Derecho Constitucional en la Facultad de Derecho de la Universidad de Sevilla.

éstas tienden a eludir el sometimiento a las regulaciones jurídicas vigentes en aquellos Estados en donde desarrollan su actividad. Actuando de este modo, no cabe duda alguna de que la capacidad para mantener incólume el Estado de Derecho sufre una sustancial erosión.

Así se constata atendiendo a la considerable desvirtuación que experimentan buena parte de sus principios fundadores:

i) Es el caso del **principio de legalidad**, puesto que las dinámicas decisionales que determinan el *modus operandi* de las referidas plataformas digitales se rige por normas y decisiones establecidas por dichos sujetos, prescindiendo de los procedimientos de creación jurídica previstos por las Constituciones de los Estados donde actúan y, asimismo, ignorando el sistema de fuentes operativos en los mismos. De este modo, surge un circuito rector propio que no se cohesiona con el determinado a escala constitucional y que discurre al margen del mismo. Las fricciones entre ambos, lejos de ser la excepción, se afirman como una tendencia arraigada en la práctica.

ii) En una situación igualmente desfavorable queda el respeto del **principio de publicidad normativa**, que se prevé para las normas aprobadas en sede estatal, pero no así para las que son fruto de la decisión de las empresas prestadoras de servicios de Inteligencia Artificial. En relación con estas, el principio dominante es justamente el contrario, puesto que lo que caracteriza al conjunto de regulaciones adoptadas por estos sujetos privados es su opacidad.

iii) A una conclusión similar se llega en relación con otro de los principios basilares del Estado de Derecho, el de **seguridad jurídica**. En virtud del mismo, como es sabido, se garantiza el conocimiento de las normas que operan en el ordenamiento jurídico (vertiente objetiva). Pero no solo, puesto que adicionalmente, la seguridad jurídica trae consigo, como otro de sus rasgos consustanciales, la predictibilidad, esto es, la posibilidad de que la ciudadanía conozca las consecuencias que se derivan de la inobservancia de las referidas previsiones y pueda ajustar su conducta a las mismas (vertiente subjetiva). Algo que no concurre en el caso de las decisiones adoptadas por los proveedores de servicios digitales.

iv) Directamente conectado con el desconocimiento del principio anterior se muestra el de **interdicción de la arbitrariedad**, que limita la capacidad decisoria de los poderes públicos dentro de unos márgenes trazados por la ley. Esta, desde una perspectiva sustantiva, debe esquivar la introducción en su texto de previsiones desprovistas de razonabilidad y justificación, tanto objetiva como subjetiva. Lo contrario, esto es, su desconocimiento conduce al terreno de lo arbitrario, algo que choca frontalmente con el Estado de Derecho. En la lógica privada rectora de las dinámicas operativas de las grandes compañías, por su parte, el espacio vetado a la arbitrariedad tiende a reducirse sustancialmente, cediendo ante la lógica del intercambio económico y comercial entre partes (proveedores y ciudadanía) que se relacionan en términos dominados por la idea de verticalidad y jerarquía.

v) Atendiendo a lo expuesto hasta ahora no resulta extraño que la idea de control, esa dinámica institucional propia de los sistemas políticos democráticos que incorporan mecanismos de frenos, contrapesos y rendición de cuentas, tienda a diluirse hasta desaparecer cuando fijamos nuestra atención en el circuito decisional y operativo de las plataformas digitales.

Por su parte, la situación en la que se encuentran los **derechos fundamentales** ante los avances de la Inteligencia Artificial generativa no resulta menos preocupante. A este respecto resulta pertinente recordar que en sus orígenes el Estado constitucional surge precisamente para garantizarlos. Concebidos como derechos vinculados a la dignidad humana y, por tanto, preexistentes al Estado, éste justifica su existencia como instancia llamada a prestarles la imprescindible tutela que permita su efectividad en la práctica (en la teoría contractualista así sucede en el tránsito del estado naturaleza al estado social). Así pues, los derechos y sus mecanismos de garantía permean de forma inmediata e insoslayable la actividad de los poderes públicos. Por su parte, los sujetos privados no quedan exentos de mantener, cumpliendo determinados requisitos, una actitud de respeto y no agresión frente a los mismos (*Drittwirkung*).

Es en este contexto general de referencia en el que se insertan las grandes plataformas prestadoras de servicios de Inteligencia Artificial a escala supraestatal, suponiendo una amenaza seria y cierta para el mantenimiento de determinados derechos fundamentales en el seno de los Estados en los que actúan. La perspectiva relacional en clave vertical que dichas plataformas imponen a las dinámicas iusfundamentales resultan determinantes es este sentido, poniendo en evidencia la preeminencia de una lógica contractual de derecho privado en la que aquellas ocupan una posición dominante frente a sus destinatarios (ciudadanía), constreñidos al desarrollo de un rol eminentemente pasivo.

En función de las ideas esbozadas una atenta mirada a la incidencia de la Inteligencia Artificial sobre los derechos fundamentales arroja el siguiente diagnóstico:

- i) El primero de los afectados en sentido negativo es, sin lugar a dudas, el que afirma **la igualdad** de los individuos, así como su lógica contrapartida, la prohibición de la discriminación. La existencia de sesgos discriminatorios desarrollados por los algoritmos es un hecho contrastado y, por lo demás, extraordinariamente extendido en la práctica. De hecho, se han dictado importantes sentencias judiciales en distintos países (es el caso de Holanda, pero también de los Estados Unidos, por citar dos ejemplos dotados de indudable relevancia) en las que constatados tales sesgos, el uso de las correspondientes herramientas digitales ha quedado proscrito.
- ii) A un resultado igualmente insatisfactorio se llega en relación con el **derecho a la intimidad o privacidad**, emergiendo la necesidad inequívoca de implementar mecanismos que garanticen efectivamente la necesaria anonimización de las personas afectadas por la inteligencia predictiva.
- iii) En los supuestos en que se han producido conflictos que han llegado al ámbito jurisdiccional y cuya causa se encuentra en el uso de estas herramientas, un idóneo ejercicio del **derecho fundamental de defensa** exige situar en primer término la necesidad de explicabilidad, esto es, de que los prestadores del servicio controvertido proporcionen una completa información sobre los procesos algorítmicos. Solo de esta forma será posible configurar un juicio adecuado de cara a la resolución de la controversia generada.

2. Los retos constitucionales de la regulación en materia de Inteligencia Artificial generativa: algunas propuestas

A la luz de lo hasta aquí expuesto resulta evidente que el contexto concurrente no se muestra precisamente halagüeño ni por lo que a la vigencia del Estado de Derecho se refiere ni tampoco en términos de preservación de la efectividad integral

de los derechos aludidos. No obstante, es preciso añadir, a modo de contrapunto, que, a día de hoy, no puede afirmarse la existencia de un contexto presidido por la anomia o la desregulación. De hecho, se constatan significativas regulaciones a escala supranacional, entre las que brilla con luz propia el Reglamento de Inteligencia Artificial aprobado recientemente en el ámbito de la Unión Europea. La finalidad que alumbra tales normas no es otra que la de erigir diques de contención a la actividad desarrollada por las referidas plataformas, estableciendo disposiciones orientadas a garantizar el respeto de los derechos fundamentales afectados por aquella. Asimismo, antes de explorar posibles vías de superación – o al menos, de amortiguación – de los déficits señalados, es preciso poner en valor la extraordinaria oportunidad que trae aparejada la implantación y consiguiente expansión de la Inteligencia Artificial generativa de cara a promover la renovación de las dinámicas operativas de los poderes públicos, adaptándolas a las exigencias de lo que podríamos denominar un Estado democrático y digital de derecho.

2.1 Empezando por el principio: diseño y planificación de las herramientas

A la hora de eliminar flancos jurídicamente problemáticos en el uso de esta modalidad de Inteligencia Artificial es imprescindible que, ya desde su planteamiento inicial y en primer lugar, esta se refiera y venga a establecer objetivos legítimos. En este sentido, debe exigirse la activación de un proceso deliberativo de carácter público, presidido por la debida atención a las exigencias genéricas que se derivan de la Constitución y que, en clave específica, lleve a cabo una evaluación del impacto que la herramienta en cuestión proyecta sobre los derechos fundamentales afectados.

Establecidas las bases previas que circunscriben los objetivos de la acción promovida, inmediatamente a continuación, se pasa a una segunda fase en la que lo que corresponde es recabar los correspondientes datos. A este respecto, ha de requerirse activamente que dichos datos sean de calidad y, asimismo, se muestren suficientemente representativos. De la conjunción de ambas exigencias (que, no se olvide, pivotan sobre la definición de unos objetivos legítimos previamente establecidos) se derivará la existencia de un contexto de trabajo idóneo que hará posible neutralizar los sesgos discriminatorios derivados de la activación de la herramienta algorítmica.

Es claro que para lograr efectivamente unos datos con las características apuntadas resulta insoslayable desarrollar una atenta tarea no solo de cribado sino también de análisis de los mismos. De modo más preciso, esa imprescindible labor de índole analítica debe valorar si el proceso de captación de los datos en cuestión ha estado presidido por la aplicación de un juicio de proporcionalidad. En la constatación de tal requerimiento será preciso verificar que se han cumplido las tres exigencias que son propias del mismo, a saber, respeto de los principios de *(a)* idoneidad, puesto que los datos son adecuados y se corresponden con la finalidad individualizada por la operación desplegada; *(b)* necesidad, determinándose que los datos son precisos e indispensables para el desarrollo de la herramienta; y *(c)* proporcionalidad en sentido estricto, esto es, siendo idóneos y necesarios, los datos recabados guardan una relación de equilibrio armónico con los objetivos legítimos establecidos. Únicamente si se superan todas las exigencias marcadas por el test referido, se habrá superado con éxito – entendido en términos jurídico-constitucionales – esta primera y decisiva fase.

2.2 Fase intermedia: el desarrollo efectivo de la herramienta

A continuación, una vez establecidos los cimientos de la operación, lo que corresponde es proceder a su activación. No obstante, con carácter previo, es preciso llamar la atención sobre la necesidad de realizar pruebas preliminares, esto es, poner en marcha previamente la herramienta con la finalidad de constatar en la práctica sus funcionalidades. De lo que se trata es de activar un período de prueba que da lugar a un proceso, el cual consta de las etapas que a continuación se enumeran: en primer lugar, llevar a cabo el procesamiento de los datos previamente obtenidos, dejando expedita la vía para una necesaria y fundamental fase de entrenamiento/aprendizaje del algoritmo. Una vez concluida esta, a continuación, lo que corresponde es dar paso a una labor no menos esencial, puesto que es preciso determinar si se ha verificado o no la hipótesis de partida establecida. En caso de no ser así, esto es, cuando se constate la existencia de desviaciones, no cabe sino abrir un proceso de redefinición y puesta a punto.

En todo caso, es imprescindible llamar la atención sobre la inequívoca necesidad de que el sector público cuente con recursos humanos preparados para afrontar el reto que plantean las tareas aludidas. Que estas se desarrollen de forma adecuada y cumplan la finalidad que las inspira depende necesariamente de que el personal al servicio de las instancias públicas cuenten no solo con una sólida cultura algorítmica sino también con el asesoramiento técnico correspondiente. Asesoramiento que, debido es subrayarlo, no se limita a la recepción de orientación desde un punto de vista jurídico, incluyendo, asimismo, imprescindibles pautas orientadoras de naturaleza ética. La articulación de estructuras públicas en las que tales exigencias lejos de configurarse como un mero desiderátum se afirmen como una realidad efectiva, se muestra como una asignatura fundamental para que el Estado de Derecho incorpore a su arsenal de principios basilares esa dimensión algorítmica requerida por los avances de la Inteligencia Artificial generativa.

2.3 El momento de la verdad: la implementación y el desarrollo de la herramienta predictiva

Superados con éxito los estadios precedentes, ahora ya sí, se da paso a la efectiva puesta en marcha de la herramienta diseñada y previamente verificada según las exigencias del Estado de Derecho. Como es lógico, dichos requerimientos también harán acto de presencia en esta última etapa, asumiendo, como no puede ser de otra forma, un rol determinante.

Sentada tal premisa, el primero de los requisitos que deben cumplir las plataformas prestadoras de servicios de Inteligencia Artificial es el de la **transparencia técnica**. En efecto, los proveedores quedan constreñidos por el deber de proporcionar toda la serie de elementos fundamentales que han confluído en la configuración de la herramienta, a saber, el código fuente, los datos recabados, el proceso de obtención, así como el concreto modelo elegido. La magnitud de las exigencias previstas es incuestionable, pero la necesidad de respetar los márgenes del Estado de Derecho y los derechos fundamentales así lo imponen. Precisamente, desde este punto de vista, las plataformas deberían estar obligadas a realizar evaluaciones internas cuyo objeto no sería otro que determinar cuál es el efectivo rendimiento de la herramienta. En tal sentido, considero muy pertinente la existencia de mecanismos de autocontrol, así como el establecimiento de protocolos éticos que sean producto de la voluntad de los proveedores. Ese carácter autoimpuesto, sin lugar a dudas, es un signo de saludable de

la existencia de una voluntad de control endógeno. No obstante, siendo condición necesaria tales códigos de conducta pueden resultar insuficientes si no cumplen con las pautas de transparencia aludidas. Así pues, sin minusvalorar la importancia de la implicación activa de las plataformas, los poderes públicos no pueden renunciar a su función de garantes últimos del cumplimiento de dichas exigencias.

Por otra parte, las plataformas también están vinculadas por el requisito de la **explicabilidad**, esto es, por la obligación no solo de poner de manifiesto los elementos clave que han servido como pautas de referencia al algoritmo en el proceso que ha conducido a la adopción de sus decisiones sino también de manifestar la motivación que ha regido tal proceso. He aquí que nos topamos con una exigencia que se identifica con una obligación de naturaleza compleja o bifronte que adquiere una importancia capital no solo para los proveedores sino también para los usuarios. Es gracias al cumplimiento del deber de motivación que es posible y se hace realidad la exigencia de responsabilidad y la efectiva rendición de cuentas.

A este respecto, nuevamente es preciso apelar a las dinámicas endógenas articuladas por las plataformas y más concretamente a su disposición a llevar a cabo auditorías internas, cuyos resultados estén disponibles para los receptores de los servicios prestados. Ahora bien, la exigencia de responsabilidad no puede en modo alguno limitarse a dicho ámbito interno, reduciendo sus efectos exclusivamente al mismo. En tal sentido, resulta incuestionable el recurso, llegado el caso, a la vía jurisdiccional, puesto que de constatare un conflicto no resuelto en vía extrajudicial, aquella debe quedar expedita. Y concurriendo tal hipótesis, contar con un completo conocimiento de los elementos configuradores de la herramienta algorítmica y del proceso de implementación y desarrollo llevado a cabo, se erige como factor clave a la hora de que el juez esté en condiciones de determinar si se ha producido el quebrantamiento de las obligaciones que vinculan a los proveedores y en tal caso, exigir las correspondientes responsabilidades e imponer las sanciones pertinentes.

3. Algunas reflexiones finales en clave conclusiva

Una vez expuestos los razonamientos genéricos que podrían conducir a una situación de mejor acople entre las exigencias inherentes al Estado de Derecho y la tutela de los derechos fundamentales con la realidad indiscutible de los avances de la Inteligencia Artificial predictiva, considero imprescindible formular algunas reflexiones de índole conclusiva. Movida por tal intención, es preciso insistir en la idea de que abandonar el terreno del mero desiderátum teórico para alcanzar la efectividad práctica de las propuestas realizadas requiere indudablemente impulsar mecanismos que contribuyan a la generación y desarrollo de una cultura algorítmica en sintonía con los principios que fundamentan el Estado de Derecho en su comprensión constitucional.

La tarea propuesta no es fácil ni tampoco arrojará resultados inmediatos, pero tal constatación en modo alguno puede ser un obstáculo para reivindicar la necesidad insoslayable de que desde las instancias públicas, nacionales y supranacionales, se activen y desarrollen sinergias cooperativas entre los actores concernidos. Estas contarán con los actores públicos y los operadores tecnológicos como sujetos protagonistas, ya que no es posible crear dinámicas respetuosas de las exigencias jurídicas de espaldas a la colaboración e implicación activa de los expertos en Inteligencia Artificial. Considero indudable que el auxilio de los técnicos se perfila como referente imprescindible para los operadores jurídicos, los cuales

están llamados a tomarlos en consideración en la esencial tarea de definir el marco jurídico rector de las prestaciones realizadas por las herramientas algorítmicas. Desde tal perspectiva, los procedimientos normativos han de contar con el apoyo de especialistas en la materia que pongan de manifiesto los riesgos inherentes a los algoritmos cuya regulación se pretende. La creación de grupos de expertos, que bien podrían asumir la condición formal de agencias independientes, se torna de esta manera un imperativo de cumplimiento obligado. Todo ello sin perder de vista la necesidad de implicar activamente a representantes de las empresas tecnológicas en estas dinámicas institucionales, teniendo un conocimiento inmediato de sus percepciones, inquietudes y observaciones. Resulta, de este modo, que los procesos decisionales se gestan en el ámbito público, pero han de mostrar un perfil abierto y participativo, implicando en su desarrollo no solo a los representantes populares (quienes discutirán y aprobarán las correspondientes leyes) y a los responsables administrativos (habilitados para la trascendental misión de ejecutar y desarrollar las previsiones legales) sino también a sujetos procedentes del ámbito científico (los expertos en Inteligencia Artificial) y a las plataformas digitales prestadoras de los servicios en cuestión. Es en este complejo caleidoscopio cooperativo que la idea de equilibrios y controles que tiene lugar en la esfera institucional experimenta un indudable salto cualitativo, una profunda transformación como consecuencia de la incorporación al proceso creativo de actores y sujetos no institucionales.

Planteada la cuestión en los términos expuestos resulta que, en la fase de la definición de las normas rectoras, debería concurrir una dinámica de naturaleza multilateral, en la que han de converger las perspectivas de los diversos sujetos concernidos por la aplicación de la Inteligencia Artificial. Una índole igualmente compleja se afirma, asimismo, como elemento imprescindible en relación con la resolución de los conflictos que puedan generarse en la práctica. En efecto, si la decisión final sobre el litigio planteado corresponde a la autoridad competente (sic un juez o a un árbitro) basándose en la regulación aplicable al caso, lo cierto es que para poder emitir una resolución idónea, dicha autoridad deberá contar necesariamente en el curso del procedimiento con el asesoramiento y el auxilio de peritos informáticos, esto es, de personas con formación en el campo de la Inteligencia Artificial.

Para terminar se impone un ejercicio de realidad que conduce a admitir que queda todavía un largo camino por recorrer. Aun así, es deber de quienes defendemos la Constitución, el Estado de Derecho que la misma establece y los derechos fundamentales que esta garantiza contribuir a la creación de un estado de opinión, de una conciencia activa mediante la que se pongan de manifiesto no solo los problemas (muchos) generados por la Inteligencia Artificial predictiva sino también, y sobre todo, la necesidad de abrir espacios que permitan que esta encuentre un cauce de desarrollo acorde con el Derecho, esto es, la afirmación de un Estado democrático y algorítmico de Derecho.

A Lei dos Metadados: crónica de um fim (há muito) anunciado

Francisco Pereira Coutinho *

1. Introdução

Em meados de abril de 2022, as habitualmente plácidas águas da ordem jurídica portuguesa foram abaladas por decisão do Tribunal Constitucional que desencadeou um maremoto na investigação da criminalidade grave.¹ Normas da chamada “Lei dos Metadados”,² adotada com o propósito de transpor a “Diretiva Conservação de Dados”,

* Professor da NOVA School of Law (Faculdade de Direito da Universidade NOVA de Lisboa). Membro do Centro de Excelência Jean Monnet CitDig (Cidadania Digital e Sustentabilidade Tecnológica) da Escola de Direito da Universidade do Minho (Portugal).

Este artigo baseia-se em textos do autor sobre o tema (Francisco Pereira Coutinho, “Better late than never: blanket data retention struck down at last by the Portuguese Constitutional court”, *Diritti Comparati* (2022) e Francisco Pereira Coutinho, “The Charter of Fundamental Rights of the European Union at the Portuguese Constitutional court: the data retention cases”, in *On the relation between the EU Charter of Fundamental Rights and national fundamental rights*, ed. Moritz Malkmus e Alexander Heger (Springer, 2024), 155. São devidos agradecimentos à Bárbara Sacramento pela sua leitura crítica, que muito o valorizou. Eventuais incorreções que nele se encontrem são da minha responsabilidade exclusiva.

¹ Carla Caixinha, “Preso por pornografia de menores libertado ao abrigo dos metadados”, *Rádio Renascença*, 10 de junho de 2022, <https://rr.sapo.pt/noticia/pais/2022/06/10/preso-por-pornografia-de-menores-%20libertado-ao-abrigo-dos-metadados/287941/>.

² Lei n.º 32/2008, de 17 de julho. Metadados são “dados sobre dados.” São dados gerados por pessoas singulares (“titulares de dados”) através da utilização de telefones fixos, fax, telemóveis e internet. Podem tomar a forma de dados de tráfego – “dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma” – e dados de localização – “dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas publicamente disponível” [artigo 2.º, alínea b) e c), 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 sector das comunicações eletrónicas (“Diretiva ePrivacy”)]. Incluem, designadamente, números de telefone de origem, chamadas telefónicas, endereços web (URL), endereços de protocolo IP e emails. Os metadados são dados pessoais sempre que possam ser utilizados para rastrear e identificar pessoas envolvidas nas comunicações eletrónicas. Sempre que tal suceda, podem apenas ser recolhidos para finalidades determinadas, explícitas e legítimas (princípio da finalidade) [artigo 5.º, n.º 1, alínea b), do Regulamento Geral sobre a Proteção de Dados (“RGPD”)] [(Regulamento (UE) 2016/679], e ser conservados de modo a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados (princípio da limitação da conservação) [artigo 5.º, n.º 1, alínea e), RGPD]. Exceto quando tecnicamente necessário para a transmissão de comunicação ou quando consentido pelo titular dos dados, é proibido o seu armazenamento e acesso por operadores de serviços de comunicações eletrónicas acessíveis ao público ou de redes públicas de comunicações (“operadores de serviços”) (princípio da confidencialidade das comunicações) (artigo 5.º da Diretiva ePrivacy). A conservação de dados de tráfego é permitida exclusivamente para efeitos de faturação dos assinantes (em benefício do titular de dados/consumidor) ou de marketing (com consentimento do titular dos dados) (artigo 6.º da Diretiva ePrivacy). Já os dados de localização “só podem ser tratados se forem tornados anónimos ou com o consentimento dos utilizadores ou assinantes (de sistemas de comunicação eletrónicas), na medida do necessário e pelo tempo necessário para a prestação de um serviço de valor acrescentado” (artigo 9.º da Diretiva ePrivacy). Por outras palavras, salvo se o consentimento for prestado pelo titular dos dados,

foram declaradas inconstitucionais pelo Tribunal Constitucional, por violarem o direito à privacidade, à proteção de dados e a uma tutela jurisdicional efetiva.³

A decisão judicial teve repercussões políticas imediatas, desencadeando uma (putativa) crise constitucional,⁴ que levou o Presidente da República⁵ e o Primeiro-Ministro⁶ a sugerir a necessidade de uma (inútil) revisão constitucional num domínio objeto de preempção pelo direito da União Europeia. A crise adquiriria dimensão tragicómica quando a Procuradora-Geral da República requereu a nulidade do acórdão constitucional,⁷ uma iniciativa inédita, prontamente rejeitada pelo Tribunal Constitucional.⁸

Volvida perto de uma década sobre a decisão do Tribunal de Justiça que anulou a Diretiva Conservação de Dados no processo *Digital Rights Ireland*,⁹ proponho-me analisar os motivos que explicam a eliminação tardia do regime jurídico emergente do que foi descrito como o “*instrumento mais atentatório para a privacidade alguma vez adotado pela União Europeia, em termos de escala e número de pessoas afetadas.*”¹⁰ Para o efeito, abordarei o processo de implementação da Diretiva Conservação de Dados na ordem jurídica portuguesa, focando-me no comportamento dos principais atores do plano legislativo, administrativo e judicial.

os metadados devem ser apagados ou tornados anónimos pelos operadores de serviços após deixarem de ser necessários para fins de interconexão ou de faturação (*Télé2 Sverige*, acórdão de 21 dezembro de 2016, C-203/15 e C-698/15, ECLI:EU:C:2016:970, §86). De forma a auxiliar a investigação, deteção e repressão de crimes graves, especialmente quando a descoberta da verdade ou a obtenção de prova seja, de outra forma, impossível ou muito difícil, os artigos 4.º e 6.º da Lei dos Metadados (Lei 32/2008, de 17 de junho) transpuseram a 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 ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (“Diretiva Conservação de dados”), adotada na sequência dos atentados terroristas de Madrid (2004) e de Londres (2005) [Conselho Europeu, Declaration on Combating Terrorism (Bruxelas, 25 de março de 2004)], obrigando os operadores de serviços de comunicações a recolher e a conservar, por um período de um ano, dados necessários ao rastreamento e identificação da origem e destino da comunicação, à identificação da data, hora, duração e tipo de comunicação, à identificação do equipamento de comunicação dos titulares dos dados e à determinação da localização do equipamento de comunicação móvel.

³ Acórdão do Tribunal Constitucional n.º 268/2022, 19 de abril, processo n.º 828/19.

⁴ Miguel Mota Delgado, “The EU law of a Portuguese institutional crisis: the data retention ruling of the Portuguese Constitutional court”, *EU Law Live*, 23 de maio de 2022, <https://eulawlive.com/the-eu-law-of-a-portuguese-institutional-crisis-the-data-retention-ruling-of-the-portuguese-constitutional-court-by-miguel-mota-delgado/> e Teresa Violante, “How the data retention legislation led to a national constitutional crisis in Portugal”, *Verfassungsblog*, 9 de junho de 2022, <https://verfassungsblog.de/how-the-data-retention-legislation-led-to-a-national-constitutional-crisis-in-portugal/>.

⁵ Cátia Carmo, “Marcelo admite alterações à Constituição por causa da lei dos metadados: «O problema é que não há revisões pontuais»”, *TSF*, 11 de maio de 2022, <https://www.tsf.pt/portugal/politica/o-problema-e-que-nao-ha-revisoes-pontuais-%20marcelo-admite-alterar-constituicao-por-causa-da-lei-dos-metadados-14847184.html/>.

⁶ Cátia Carmo, “Costa admite revisão constitucional, mas que pode ser «cirúrgica» por causa dos metadados”, *TSF*, 11 de maio de 2022, <https://www.tsf.pt/portugal/politica/costa-admite-revisao-constitucional-mas-que-%20pode-ser-cirurgica-por-causa-dos-metadados-14847812.html/>.

⁷ Rui Gustavo, “Procuradoria pede anulação do acórdão do Constitucional sobre os metadados. E apresentou dois motivos para o fazer”, *Expresso*, 9 de maio de 2022, <https://expresso.pt/sociedade/2022-05-09-Procuradoria-pede-anulacao-do-acordao-do-Constitucional-sobre-os-metadados.-E-apresentou-dois-motivos-para-o-fazer-f37c2671>.

⁸ Acórdão do Tribunal Constitucional n.º 382/2022, de 13 de maio, processo n.º 828/19.

⁹ Acórdão do TJUE *Digital Rights Ireland*, 8 de abril de 2014, C-293/12 e C-594/12.

¹⁰ Autoridade Europeia para a Proteção de Dados, *The “moment of truth” for the Data Retention Directive: EDPS demands clear evidence of necessity*, Bruxelas, 3 de dezembro de 2010.

2. Crónica de um fim anunciado

Os Tratados que regem a União Europeia “*instituíram uma ordem jurídica própria que está integrada no sistema jurídico dos Estados-Membros (...) e que se impõe aos seus órgãos jurisdicionais nacionais.*”¹¹ Esta fórmula judicial é a mais importante na história da integração jurídica europeia. Determina que, ao contrário do que sucede com o direito internacional público, o direito da União Europeia tem aplicabilidade direta.

A “*justiciabilidade*” decorrente do efeito direto das normas de direito da União abre a possibilidade de conflitos normativos com o direito nacional. Mas como devem os órgãos jurisdicionais e administrativos nacionais resolver conflitos numa estrutura federativa como a União Europeia? Segundo o princípio do primado do direito europeu, as normas da União prevalecem sobre as normas nacionais:

“*[O]rgãos encarregados de aplicar, no âmbito das respetivas competências, o direito da União têm a obrigação de tomar todas as medidas necessárias para garantir a plena eficácia desse direito, não aplicando, se necessário, qualquer disposição ou jurisprudência nacionais contrárias ao referido direito. Isso implica que esses órgãos, para garantir a plena eficácia do direito da União, não devem pedir nem aguardar pela eliminação prévia dessa disposição ou jurisprudência por via legislativa ou por qualquer outro procedimento constitucional.*”¹²

O estatuto jurídico da Lei dos Metadados não suscitava dúvida após as decisões do Tribunal de Justiça nos processos *Digital Rights Ireland* e *Tele2 Sverige*. Na sequência da anulação da Diretiva Conservação de Dados, a legislação nacional de transposição caiu automaticamente no âmbito de aplicação do artigo 15.º, n.º 1, da Diretiva *ePrivacy*, que autoriza os Estados-Membros a “*adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado.*”¹³ Daqui decorre a conclusão de que a Lei dos Metadados consubstanciava medida de implementação do direito da União, sujeita à aplicação da Carta dos Direitos Fundamentais da União Europeia (CDFUE).¹⁴ O regime de conservação geral e indiferenciada de dados nele previsto era, portanto, inaplicável, por violar os artigos 7.º e 8.º da CDFUE.¹⁵

O princípio da cooperação leal, previsto no artigo 4.º, n.º 3, segundo parágrafo, do Tratado da União Europeia (TUE), exigia intervenção corretiva adequada do Estado português. A persistência da aplicação da Lei dos Metadados, na ordem jurídica portuguesa, até meados de 2022, é o reflexo de um legislador relapso, de uma autoridade de controlo ausente e de um Tribunal Constitucional errático.

¹¹ Acórdão do TJUE *Costa v. ENEL*, 15 de julho de 1964, processo 6/64.

¹² Acórdão do TJUE *Minister for Justice and Equality*, 4 de dezembro de 2018, C-378/17, considerando 50.

¹³ Acórdão do TJUE *Tele2 Sverige*, 21 de dezembro de 2016, C-203/15 e C-698/15, considerandos 65-81.

¹⁴ Acórdão do TJUE *Fransson*, 26 de fevereiro de 2013, C-617/10, considerandos 20-21.

¹⁵ Clara Guerra e Filipa Galvão, “Anotação ao Acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014”, *Fórum de proteção de dados*, n.º 1 (2015), 79-80, David Silva Ramalho e José Duarte Coimbra, “A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves”, *O Direito*, n.º 147, vol. IV (2015), 1038-1039, Alessandra Silveira e Pedro Miguel Freitas, “The recent jurisprudence of the CJEU on personal data retention: implications for criminal investigation in Portugal”, *UNIO – EU Law Journal*, n.º 3, vol. 2 (2017), 52-53, Francisco Pereira Coutinho e Nuno Piçarra, “Portugal: the impact of european integration and the economic crisis on the identity of the constitution”, in *National constitutions in European and global governance: democracy, rights, the rule of law*, ed. Anneli Albi e Samo Bardutzki (Haia: Asser Press, 2019), 616.

3. Um legislador relapso

O Estado português adotou, inicialmente, posição ambivalente a respeito da adoção de regime de conservação preventiva de dados para fins de investigação criminal. Se no plano europeu se manifestava favorável,¹⁶ internamente postergou a implementação de obrigações internacionais relativas à preservação expedita de dados (“*quick-freeze*”),¹⁷ um instrumento jurídico menos problemático no domínio jusfundamental.

O Governo votou favoravelmente a Diretiva Conservação de Dados¹⁸ e aprovou proposta de lei relativa à sua implementação, ainda que a menos de duas semanas do final do prazo de transposição.¹⁹ Mas as dúvidas sobre a proporcionalidade da medida nunca desapareceriam por completo. Nas observações escritas apresentadas no processo *Digital Rights Ireland*, foi questionada a respetiva adequação ao objetivo professo de combate à criminalidade grave, na medida em que não se permitia a conservação de dados de comunicações anónimas e não estavam abrangidos dados gerados por outras modalidades de comunicações eletrónicas.²⁰

A proposta de lei seria aprovada, por larga maioria, pela Assembleia da República. Apenas o Partido Comunista Português e o Bloco de Esquerda suscitaram objeções, caracterizando enfaticamente a iniciativa como um ataque sem precedentes às liberdades civis decorrente de uma deriva securitária descontrolada.²¹ O Governo retorquiu, garantindo que o regime jurídico continha “*especiais cautelas para salvaguardar integralmente os direitos fundamentais dos cidadãos, em especial o direito à privacidade.*”²²

A alegada robustez das cautelas levou, inclusivamente, alguns autores a descrever a lei portuguesa como um “*caso particular*” e um “*exemplo*” a seguir nas demais ordens jurídicas europeias.²³ Lamentavelmente, o Governo acreditou nesta mistificação jurídica. Depois de ter notificado o Conselho do entendimento de que a decisão do Tribunal de Justiça no acórdão *Télé2 Sverige* não exigia qualquer alteração legislativa,²⁴ ignorou ostensivamente pareceres em sentido contrário da Comissão Nacional de

¹⁶ Conselho da União Europeia, “Answer to questionnaire on traffic data retention”, 14107/02 (Bruxelas, 20 de novembro 2002.), *Statewatch*, vol. 12, no. 6 (2002), 20-22.

¹⁷ Nos termos do artigo 12.º, n.º 1, da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), que transpõe o artigo 16.º da Convenção sobre o Cibercrime do Conselho da Europa, ETS 105 (assinada a 23 de novembro de 2001; entrada em vigor a 1 de julho de 2004), “*se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa.*”

¹⁸ Conselho da União Europeia, 2709.ª reunião do Conselho da União Europeia, 6598/06 ADD 1, Bruxelas, 27 de fevereiro de 2006, 4.

¹⁹ Projeto de Lei 161/X/3, aprovado pelo Conselho de Ministros, a 6 de setembro de 2007.

²⁰ Acórdão *Digital Rights Ireland*, considerando 50.

²¹ Deputado António Filipe (PCP), *Diário da Assembleia da República*, Série I, no. 31 (2008), 22: “*Esta proposta de lei e a diretiva comunitária que ela se propõe transpor são mais dois exemplos da paranoia securitária que anda à solta por essa Europa fora.*”

²² João Tiago Silveira (Secretário de Estado da Justiça), *Diário da Assembleia da República*, Série I, no. 31 (2008), p. 19.

²³ Irene Maria Portela e Maria Manuela Cruz-Cunha, “What about the balance between law enforcement and data protection?”, in *Information Communication Technology Law, protection and access rights: global approaches and issues*, ed. Irene Maria Portela e Maria Manuela Cruz-Cunha (Nova York: IGI Global, New York, 2010), p. 3 e 10.

²⁴ Conselho da União Europeia, *Retention of electronic communication data*, 6726/1/17 REV 1, Bruxelas, 7 de março de 2017.

Proteção de Dados²⁵ e da Provedora de Justiça,²⁶ promovendo o alargamento do acesso a dados conservados, ao abrigo da Lei dos Metadados, aos crimes de contrafação de cartões ou outros dispositivos de pagamento e de uso e aquisição de cartões ou outros dispositivos de pagamento contrafeitos.²⁷

A ilusão governamental carecia, em absoluto, de fundamento. O acórdão *Tele2 Sverige* não deixa margem para dúvidas quanto à inconstitucionalidade da obrigação imposta aos fornecedores de serviços de conservar *todos* os dados (de tráfego e localização) de todos os utilizadores e assinantes registados relativamente a *todos* os meios de comunicação eletrónica, para fins de investigação, deteção e repressão de crimes graves.²⁸ Legislação, como a portuguesa, que postulava a conservação generalizada e indiferenciada de dados, ultrapassava, por defeito, os limites do estritamente necessário.²⁹ A proporcionalidade estava, designadamente, comprometida, ao fixar-se um período único de conservação de um ano, sem se operar qualquer distinção entre as categorias de dados conservados, seja em função da sua eventual utilidade para a investigação da criminalidade grave, seja em função das pessoas em causa.³⁰

A natureza das salvaguardas incluídas na regulamentação nacional no domínio da segurança e da transmissão dos dados conservados seria sempre irrelevante para justificar uma ingerência tão intensa nos direitos fundamentais dos titulares dos dados.³¹ Acresce que as “*cautelais especiais*” introduzidas pelo legislador português, como a necessidade de autorização judicial para a transmissão de dados às autoridades de investigação criminal,³² estavam muito aquém do necessário para proteger os titulares dos dados contra riscos de abuso e de utilização ilícita dos seus dados pessoais. Em primeiro lugar, os fornecedores de serviços não estavam obrigados a conservar dados no território da União Europeia, pelo que não estava garantida a fiscalização, pelas autoridades nacionais de proteção de dados, do respeito pelas exigências de proteção e segurança de dados pessoais.³³ Em segundo lugar, a ausência de obrigatoriedade de notificação dos titulares dos dados do acesso a dados conservados, a partir do momento em que essa comunicação não fosse suscetível de comprometer as investigações levadas a cabo pelas autoridades de investigação criminal, prejudicava o exercício do respetivo direito de recurso.³⁴ Em terceiro lugar, os operadores de

²⁵ Comissão Nacional de Proteção de Dados, Deliberação 641/2017, de 9 de maio de 2017.

²⁶ Provedora de Justiça, Recomendação 1/B/2019, de 22 de janeiro de 2019.

²⁷ Através da Proposta de Lei n.º 98/XIV/2, que deu origem à aprovação do artigo 4.º da Lei n.º 79/2021, de 24 de novembro, que altera o artigo 2.º, alínea g), da Lei 32/2008, de 17 de julho.

²⁸ Acórdão *Tele2 Sverige*, considerando 112.

²⁹ *Idem*, considerando 107.

³⁰ Acórdão *Digital Rights Ireland*, considerando 63.

³¹ O Tribunal de Justiça pronunciou-se sobre esta questão no processo *Commissioner of An Garda Síochána*, acórdão de 5 de abril de 2020, C-140/20, considerando 47: “[U]ma legislação nacional que assegura o pleno respeito das condições que resultam da jurisprudência que interpretou a Diretiva 2002/58 em matéria de acesso aos dados conservados não pode, por natureza, ser suscetível de restringir nem sequer de corrigir a ingerência grave, que resultaria da conservação generalizada desses dados prevista por esta legislação nacional, nos direitos garantidos nos artigos 6.o e 5.o desta diretiva e pelos direitos fundamentais de que esses artigos constituem a concretização.”

³² Artigos 3.º, n.º 2, e 9.º da Lei 32/2008, de 17 de julho.

³³ Acórdão *Digital Rights Ireland*, considerando 68 e Acórdão *Tele2 Sverige*, considerandos 122-123. Esta não é uma questão “*menor*” (Ramalho e Coimbra, “A declaração de invalidade da Diretiva 2006/24/CE”, 1038), na medida em que abria, designadamente, a possibilidade de dados serem transferidos para Estado terceiro (os Estados Unidos da América), cuja legislação concedia, às respetivas autoridades públicas, acesso generalizado a dados pessoais, não prevendo nenhuma possibilidade de o titular dos dados recorrer a vias de direito para exercer os seus direitos (Acórdão do TJUE *Schrems I*, 6 de outubro de 2015, C-362/14, considerandos 93-95).

³⁴ Acórdão *Tele2 Sverige*, considerando 121.

serviços de telecomunicações não estavam obrigados a adotar medidas de ordem técnica que garantissem a *destruição definitiva* dos dados no termo do respetivo período de conservação.³⁵ Em quarto lugar, não foram estabelecidos critérios objetivos que permitam limitar o número de pessoas autorizadas a aceder e a utilizar os dados conservados.³⁶ Em quinto lugar, a proteção dos dados contra riscos de abuso na transmissão às autoridades de investigação criminal dos dados conservados estava prejudicada pela natureza não vinculativa da aplicação informática criada para esse fim pela Portaria n.º 469/2009, de 6 de maio.³⁷

O princípio da cooperação leal impunha a adoção das medidas legislativas necessárias para assegurar o cumprimento das obrigações decorrentes dos Tratados (artigo 4.º, n.º 3, do TUE). Tal implicava harmonizar o regime jurídico da conservação preventiva de dados com a CDFUE, como interpretada pelo Tribunal de Justiça. Ao alargar o acesso das autoridades de investigação criminal a dados conservados, o legislador apenas agravou o incumprimento das obrigações do Estado português à luz do direito constitucional da União Europeia.

4. Uma autoridade de controlo ausente

A *Comissão Nacional de Proteção de Dados* é a entidade administrativa independente fiscalizadora do cumprimento do direito da União, em matéria de proteção de dados, na ordem jurídica portuguesa.³⁸ Trata-se de uma missão explicitamente exigida pelo artigo 8.º, n.º 3, da CDFUE, que constitui um elemento essencial do direito fundamental à proteção de dados.³⁹

As autoridades nacionais de controlo da proteção de dados diferem dos demais órgãos administrativos, em virtude de a sua instituição resultar diretamente do direito primário da União e de as respetivas atribuições e competências estarem previstas no direito secundário da União.⁴⁰ Fazem parte da “*administração europeia compósita*”, integrando o Comité Europeu para a Proteção de Dados e participando em procedimentos administrativos complexos, como os de cooperação e de consistência.⁴¹ Possuem, portanto, uma natureza híbrida: se, por um lado, são entidades criadas ao abrigo do direito interno; por outro lado, desempenham funções características de uma agência europeia.⁴² Por esta razão, devem agir com “*total independência*”, não podendo estar sujeitas, direta ou indiretamente, a influências externas, nem solicitar ou receber instruções de outrem.⁴³

Chamada a pronunciar-se sobre o projeto de proposta de lei que daria origem à Lei dos Metadados, a CNPD sugeriu a redução do período de conservação de dois anos para um, de modo a seguir-se o padrão maioritário vigente nos Estados-

³⁵ Acórdão *Digital Rights Ireland*, considerando 67, e Acórdão *Tele2 Sverige*, considerando 122.

³⁶ Acórdão *Digital Rights Ireland*, considerando 62.

³⁷ Acórdão do TJUE *Privacy International*, 6 de outubro de 2020, C-623/17, considerando 68. Em 2017, a aplicação informação permanecia em desuso (Comissão Nacional de Proteção de Dados Deliberação 641/2017, 9).

³⁸ Artigos 3.º e 4.º da Lei n.º 58/2019, de 8 de agosto.

³⁹ Acórdão *Tele2 Sverige*, considerando 123.

⁴⁰ Artigo 8.º, n.º 3, da CDFUE e artigos 55.º a 59.º RGPD.

⁴¹ Artigos 60.º a 62.º, 63.º a 67.º, e 68.º, n.º 3, RGPD.

⁴² Hielke Hijmans, “The European Union as a constitutional guardian of internet privacy and data protection” (diss. Doutoramento, Universidade de Amsterdão, 2016), 309-311; Francisco Pereira Coutinho, “A independência da Comissão Nacional de Proteção de Dados”, *Anuário da Proteção de Dados* (2020), 16-17.

⁴³ Artigo 52.º, n.º 1 e 2, RGPD.

Membros, alguns dos quais tinham sofrido ataques terroristas.⁴⁴ A harmonização não constituía, no entanto, critério objetivo para a definição de período de conservação preventiva de dados limitado ao estritamente necessário.⁴⁵ Portugal nunca foi alvo de ameaças securitárias graves, pelo que a conservação deveria ter-se cingido ao período “*mais curto possível*”,⁴⁶ que seria, no caso da transposição da diretiva, de seis meses.

Outro contributo relevante foi a advertência para a necessidade de definição da finalidade da conservação de dados. A CNPD enfatizou a importância “*crucial*” do princípio da finalidade, “*dada a natureza dos dados a conservar e o facto da sua conservação implicar restrições a direitos fundamentais dos titulares dos dados.*”⁴⁷

Resta então saber por que razão nunca recorreu aos poderes corretivos, previstos no artigo 58.º, n.º 2, do RGPD, para fiscalizar e sancionar o acesso ilícito, por parte das autoridades de investigação criminal, a dados conservados pelos operadores de serviços para fins de faturação, ao abrigo do artigo 6.º da Lei n.º 41/2004, de 18 de agosto. Esta constituía prática adotada com o propósito deliberado de contornar a limitação de acesso a dados conservados a investigações relacionadas com a lista de crimes graves elencados no artigo 2.º, n.º 1, alínea g), da Lei dos Metadados. Este catálogo foi considerado excessivamente restritivo, ao não incluir alguns dos crimes previstos no artigo 187.º, n.º 1, do Código de Processo Penal e no artigo 11.º da Lei do Cibercrime, nomeadamente crimes de calúnia, contrabando ou cibercrimes.⁴⁸ Uma vez que os metadados eram tidos como “*prova essencial*” para a investigação criminal,⁴⁹ foi então aberta uma via dual para a transmissão às autoridades de dados conservados pelos operadores de serviços para fins de faturação: *i*) dados de tráfego e de localização, mediante autorização judicial, nos termos do artigo 189.º, n.º 2, do Código de Processo Penal, em investigações relacionadas com os crimes previstos no artigo 187.º, n.º 1, do Código de Processo Penal; *ii*) endereços de protocolo IP e dados de identificação civil, *sem* necessidade de autorização judicial, em investigações relacionadas com *qualquer* crime previsto nos artigos 11.º e 14.º da Lei do Cibercrime.⁵⁰

A prática descrita constitui uma violação flagrante do princípio da finalidade, na medida em que o artigo 6.º, n.º 7, da Lei n.º 41/2004, de 12 de julho, limita o acesso das autoridades a dados pessoais armazenados a questões relacionadas com litígios relativos a interligações e à faturação de serviços de comunicações eletrónicas. Outras exceções ao princípio da confidencialidade poderiam apenas ser admitidas, ao abrigo do artigo 15.º, n.º 1, da Diretiva *ePrivacy*, quando previstas em normas claras e precisas, que devem também proteger eficazmente os dados pessoais contra os riscos de abuso.⁵¹

⁴⁴ Comissão Nacional de Proteção de Dados, Parecer 47/07, de 29 de agosto de 2007, 3; João Tiago Silveira (Secretário de Estado da Justiça), *Diário da Assembleia da República*, 20-21.

⁴⁵ Acórdão *Digital Rights Ireland*, considerando 64.

⁴⁶ Grupo de Trabalho do Artigo 29.º, Parecer 4/2005, de 21 de setembro de 2005, 6.

⁴⁷ Comissão Nacional de Proteção de Dados, Parecer 38/07, de 16 de julho de 2007, 3-4.

⁴⁸ Carlos Pinho, “Lei de retenção de dados de comunicações eletrónicas: aposentar ou reformar?”, *Revista do Ministério Público*, no. 154 (2018), 169-170.

⁴⁹ *Idem*, 169.

⁵⁰ Gabinete de Cibercrime (Ministério Público), Nota Prática n.º 8, de 18 de fevereiro de 2016, 7. No processo *Prokuratuur*, acórdão de 2 de março de 2021, C-746/18, considerando 57, o Tribunal de Justiça considerou que o Ministério Público estónio não podia ser reconhecido como “*autoridade independente*” responsável pela fiscalização prévia da licitude do acesso de uma autoridade nacional a dados conservados preventivamente para fins de investigação criminal.

⁵¹ Acórdão do TJUE *Quadrature du Net*, 6 de outubro de 2020, C-511/18, C-512/18 e C-520/18, considerando 132. A este propósito, Carlos Pinho notou que a circunstância de o armazenamento de dados para efeito de faturação, ao abrigo da Lei n.º 41/2004, de 12 de julho, não ser realizado para

De acordo com a jurisprudência constante do Tribunal de Justiça,⁵² a conservação generalizada e indiferenciada de metadados é admissível em circunstâncias muito específicas (ameaças graves à segurança nacional) ou para determinadas categorias de dados (endereços de protocolo IP e dados de identidade civil dos titulares de dados), e apenas para fins de investigação criminal e/ou de salvaguarda da segurança nacional. Mas nada disto impediu o Ministério Público de referir, em maio de 2022, que iria persistir na violação do direito constitucional da União, solicitando a transmissão de endereços de protocolo IP aos operadores de serviços, ao abrigo do artigo 14.º, n.º 1 e 4, da Lei do Cibercrime.⁵³ Uma intervenção pública absurda, na medida em que, não sendo os endereços de protocolo IP dados de tráfego necessários para fins de faturação, não podem ser conservados pelos operadores de serviços, ao abrigo do artigo 6.º da Lei n.º 41/2004, de 12 de julho.⁵⁴

A “*saga dos metadados*” revelou uma CNPD inoperante. Após a decisão do Tribunal de Justiça no acórdão *Digital Rights*, de 8 de abril de 2014, manteve um silêncio sepulcral durante catorze meses, interrompido apenas para declarar, elípticamente, que a “*legitimidade*” da conservação preventiva de dados na ordem jurídica portuguesa, ao abrigo da Lei n.º 32/2008, de 17 de julho, necessitava de clarificação.⁵⁵ Posteriormente, na sequência do acórdão *Tele2 Sverige*, a CNPD veio afirmar que a falta de proporcionalidade na conservação generalizada e indiferenciada de dados “*faz(ia) perigar*” a “*validade*” da lei que transpôs a Diretiva e, portanto, a sua conformidade à Constituição, antecipando mesmo a inevitabilidade de decisão do Tribunal Constitucional sobre esta matéria.⁵⁶ Volvidas algumas semanas, solicitou ao parlamento a alteração da Lei dos Metadados.⁵⁷

A passividade do legislador levou a que a CNPD invocasse o princípio do primado para declarar que iria deixar de exercer poderes sancionatórios ao abrigo da Lei dos Metadados.⁵⁸ O efeito prático deste entendimento foi, todavia, a diluição dos incentivos dos operadores de serviços de telecomunicações para cumprir as exigências de garantia de “*um nível particularmente elevado de proteção e segurança*” dos dados conservados.⁵⁹ O problema ficaria apenas resolvido a 7 de junho de 2022, depois de a CNPD decidir, finalmente, utilizar o poder previsto no artigo 58.º, n.º 2, alínea d), do RGPD, para obrigar os operadores de serviços de comunicações a apagar, no prazo de 72 horas, todos os dados conservados ao abrigo da Lei dos Metadados.⁶⁰ Na

fins de deteção, investigação e repressão criminal, determina que não esteja “*abrangido pelas especiais garantias que devem ser aplicáveis para esta finalidade específica*” (Pinho, “Lei de retenção de dados de comunicações eletrónicas”, 171).

⁵² Acórdão *Quadrature du Net*.

⁵³ Gabinete de Cibercrime (Ministério Público), Nota Informativa: *Retenção de Dados de Tráfego – Acórdão do Tribunal Constitucional*, de 17 de maio de 2022, 2-3.

⁵⁴ Pinho, “Lei de retenção de dados de comunicações eletrónicas”, 171 e Acórdão *Quadrature du Net*, considerando 134-168.

⁵⁵ Comissão Nacional de Proteção de Dados, Parecer 51/2015, de 16 de junho de 2015, 10.

⁵⁶ Comissão Nacional de Proteção de Dados, Parecer 24/2017, de 18 de abril de 2017, 20-21.

⁵⁷ Comissão Nacional de Proteção de Dados, Deliberação 641/2017.

⁵⁸ Comissão Nacional de Proteção de Dados, Deliberação 1008/2017, de 18 de julho de 2017.

⁵⁹ Provedora de Justiça, Recomendação 1/B/2019, 18.

⁶⁰ Comissão Nacional de Proteção de Dados, “CNPD ordena eliminação dos dados das comunicações conservados ao abrigo de norma declarada inconstitucional”, *Notícias*, 9 de junho de 2022, <https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-ordena-eliminacao-dos-dados-das-comunicacoes-conservados-ao-abrigo-de-norma-declarada-inconstitucional/#:~:text=CNPD%20ORDENA%20ELIMINA%C3%87%C3%83O%20DOS%20DADOS,a%20inconstitucionalidade%20de%20algumas%20normas>.

semana seguinte, e com um chocante atraso de 2933 dias,⁶¹ os operadores de serviços anunciaram publicamente a destruição dos dados.⁶²

A injunção administrativa escudou-se na implementação do Acórdão n.º 268/2022, de 19 de abril, do Tribunal Constitucional, que, tendo declarado, com força obrigatória geral, a inconstitucionalidade de diversas normas da Lei dos Metadados, determinou a impossibilidade da respetiva aplicação na ordem jurídica portuguesa após a publicação do aresto no Diário da República, ocorrida a 3 de junho de 2022.⁶³ Acontece, porém, que a inaplicabilidade normativa já resultava, como reconhecido *expressamente* pela CNPD, em julho de 2017,⁶⁴ da incompatibilidade com a CDFUE, tal como interpretada pelo Tribunal de Justiça nos acórdãos *Digital Rights Ireland* e *Tele2 Sverige*. Se assim era, então por que não foi ordenado o apagamento imediato dos dados conservados pelas operadoras de serviços de comunicações? O fim da conservação preventiva, generalizada e indiferenciada, de dados resolveria automaticamente o problema da sua transmissão ilícita às autoridades de investigação criminal. Sem conservação não pode haver acesso.

A CNPD falhou redondamente, permanecendo inerte e observando passivamente, durante mais de oito anos, violações massivas dos direitos fundamentais que tem como missão primordial proteger.

5. Um Tribunal Constitucional errático

Os tribunais nacionais devem aplicar, integralmente, o direito da União e proteger os direitos que este confere aos particulares, afastando, se necessário, disposições conflitantes de direito interno.⁶⁵ Após os Acórdãos *Digital Rights Ireland* e *Tele2 Sverige*, da obrigação de os tribunais portugueses respeitarem a CDFUE decorria, de forma evidente, o dever de recusa de utilização, como meio probatório, de dados pessoais conservados preventivamente ao abrigo do regime jurídico dos metadados previsto na Lei n.º 32/2008, de 17 de julho.

O “*mandato Simmenthal*” foi, todavia, incorretamente cumprido, a 16 de outubro de 2016, por magistrado do tribunal de instrução criminal de Lisboa, que invocou a constituição portuguesa (e não o direito constitucional da União) para recusar pedido de acesso do Ministério Público a dados que permitissem a identificação de

⁶¹ Os operadores de serviços de comunicações já se encontravam obrigados, desde os acórdãos *Digital Rights* e *Tele2 Sverige*, a destruir a base de dados criada ao abrigo da Lei dos Metadados, na medida em que o tratamento destes dados não era necessário para o cumprimento de obrigação jurídica aplicável a que estivessem sujeitos enquanto responsáveis pelo tratamento [artigo 6.º, n.º 1, alínea c), do RGPD]. Na ausência de qualquer outro fundamento jurídico para o tratamento de dados, a conservação de dados em violação do princípio da licitude seria passível de ser sancionada. Contra, Silva Ramalho e Duarte Coimbra (Ramalho e Coimbra, “A declaração de invalidade da Diretiva 2006/24/CE”, 1040), rejeitaram tal possibilidade, alegando que os operadores de serviços “*não têm obrigação*” de desaplicar lei nacional que violasse o direito da União Europeia, podendo, deste modo, continuar a cumprir norma que os próprios autores consideraram estar num estado de “*verdadeira latência*” (Ramalho e Coimbra, “A declaração de invalidade da Diretiva 2006/24/CE”, 1042).

⁶² Filipa Ambrósio de Sousa, “Nos, Vodafone e Altice garantem cumprimento da lei de metadados”, *Eco*, 12 de junho de 2022, <https://eco.sapo.pt/2022/06/12/vodafone-e-altice-garantem-cumprimento-da-lei-de-metadados/>.

⁶³ Comissão Nacional de Proteção de Dados, “CNPD ordena eliminação dos dados.”

⁶⁴ Comissão Nacional de Proteção de Dados, Deliberação 1008/2017.

⁶⁵ Monica Claes, *The national courts’ mandate in the European Constitution* (Oxford: Hart, 2006), 108; Robert Schütze, *European Constitutional Law*, 2.ª ed. (Cambridge: Cambridge University Press, 2012), 125-126; Acórdão do TJUE *Simmenthal*, 9 de março de 1978, 106/77, considerando 21; Acórdão do TJUE *Elchinov*, 5 de outubro de 2010, C-173/09, considerando 31.

utilizador registado de sistema de comunicação eletrónica associado a endereço de protocolo IP relacionado com a prática do crime de pornografia de menores.

No lugar de rejeitar o recurso de constitucionalidade apresentado pelo Ministério Público, considerando que a questão *sub judice* se enquadrava no âmbito de aplicação do direito da União e que, portanto, deveria ser apreciada exclusivamente pelos tribunais ordinários com o (eventual) auxílio do Tribunal de Justiça,⁶⁶ o Tribunal Constitucional caucionou o acesso a dados pessoais conservados preventivamente ao abrigo da Lei dos Metadados.⁶⁷

Negligenciando o facto de que qualquer legislação nacional que obrigasse à conservação preventiva de metadados por fornecedores de serviços de comunicações eletrónicas se encontrar necessariamente abrangida pelo artigo 15.º, n.º 1, da Diretiva *ePrivacy* e, portanto, sujeita à aplicação da CDFUE, o Tribunal Constitucional considerou não estar *in casu* sujeito à jurisprudência do Tribunal de Justiça. Optou, em consequência, por um caminho hermenêutico autónomo, fundado na qualificação dos dados de identificação civil associados a endereços de protocolo IP como “*dados de base*” e, portanto, não abrangidos pelo escopo do acórdão *Digital Rights*.⁶⁸ Acontece que estes metadados são, de acordo com a jurisprudência constante do Tribunal de Justiça, dados de tráfego.⁶⁹ No que configura uma violação flagrante da obrigação de submeter uma questão prejudicial ao abrigo do artigo 267.º, n.º 3, do Tratado sobre o Funcionamento da União Europeia (TFUE), o Tribunal Constitucional admitiu a sua conservação preventiva, relevando a “*natureza relativamente pouco invasiva*” para a privacidade e o exíguo tempo de preservação de um ano,⁷⁰ questões que apenas viriam a ser discutidas pelo Tribunal de Justiça, em termos radicalmente distintos, nos acórdãos *La Quadrature du Net* e *Space Net*.⁷¹

⁶⁶ O Tribunal Constitucional recusou sempre qualificar a compatibilidade entre a legislação portuguesa e o direito da União como uma questão constitucional sujeita à apreciação dos juizes do Palácio Ratton (cfr., entre outros, o Acórdão n.º 466/2003, de 14 de outubro, processo n.º 125/02, o Acórdão n.º 46/04, de 19 de janeiro, processo n.º 885/03, o Acórdão n.º 598/04, de 12 de outubro, processo n.º 685/03 ou o Acórdão n.º 569/2016, de 19 de outubro, processo n.º 238/16). Como explicou José Manuel Cardoso da Costa (José Manuel Cardoso da Costa, “O Tribunal Constitucional português e o Tribunal de Justiça das Comunidades Europeias”, in *Ab uno ad omnes*, AA.VV. (Coimbra: Coimbra Editora, 1998), 1371), não deve “*reconduzir-se a contrariedade de uma norma interna com outra de direito (da União) a uma categoria ou a um conceito dogmático cuja utilização ou aplicação na hipótese (embora possível num certo entendimento dele) implicaria retirar aos tribunais internos comuns a decisão definitiva daquela questão, na correspondente esfera.*” O Acórdão n.º 198/2023, de 18 de abril, veio também, recentemente, esclarecer que o direito da União Europeia não configura uma convenção internacional para efeitos da aplicação da alínea i) do n.º 1 do artigo 70.º, da Lei do Tribunal Constitucional, pelo que o Tribunal Constitucional não pode ser chamado a intervir, enquanto órgão de recurso, relativamente a decisão judicial que se tenha pronunciado sobre a contrariedade entre norma interna e norma de direito primário da União.

⁶⁷ Acórdão do Tribunal Constitucional n.º 420/17, de 13 de julho, processo n.º 452/17.

⁶⁸ Acórdão n.º 420/17, considerando 10.

⁶⁹ Acórdão do TJUE *Ministerio Fiscal*, 2 de outubro de 2018, C-207/16, considerando 42: “[R]esulta do considerando 15 da Diretiva 2002/58 (*ePrivacy*) que os dados de tráfego podem, nomeadamente, incluir o nome e o endereço do remetente de uma comunicação (...). Os dados relativos à identidade (...) podem, além disso, ser necessários para a faturação dos serviços de comunicações eletrónicas fornecidos e fazem, por conseguinte, parte dos dados de tráfego, conforme definidos no artigo 2.º, segundo parágrafo, alínea b), desta diretiva. Consequentemente, esses dados estão abrangidos pelo âmbito de aplicação da Diretiva 2002/58”, e Acórdão *Quadrature du Net*, considerando 152.

⁷⁰ Acórdão n.º 420/17, considerando 13.

⁷¹ Acórdão *Quadrature du Net*, considerandos 153-155, e Acórdão do TJUE *Space Net*, 20 de setembro de 2022, C-793/19 e C-794/19, considerandos 85-90.

O acórdão *Tele2 Sverige*, ainda que citado, foi ostensivamente ignorado. O Tribunal Constitucional baseou-se, em contrapartida, em doutrina⁷² e em diretrizes não vinculativas do Gabinete de Cibercrime do Ministério Público,⁷³ em que se assevera a robustez das salvaguardas legislativas contra os riscos de abuso e de acesso ilícito a dados conservados preventivamente. Concluiu que tanto a conservação como o acesso aos metadados solicitados pelo Ministério Público consubstanciavam restrições proporcionais ao direito à privacidade.⁷⁴

A decisão do Tribunal Constitucional funcionou como luz verde para a aplicação judicial de regime jurídico flagrantemente violador do direito constitucional da União. Por exemplo, a 28 de novembro de 2018, o Tribunal da Relação de Lisboa alcandorou-se no acórdão constitucional de 13 de julho de 2017, para revogar decisão de tribunal de primeira instância que, aplicando a jurisprudência *Digital Rights*, tinha recusado dar acesso a metadados, conservados para fins de faturação, ao abrigo dos artigos 14.º, n.º 1 e n.º 4, da Lei do Cibercrime.⁷⁵

Inconformada com a perpetuação de regime jurídico gravemente atentatório dos direitos de milhões de titulares de dados, uma associação de defesa dos direitos digitais recorreu, em dezembro de 2017, à Provedora de Justiça.⁷⁶ A defensora dos cidadãos resolveu – ainda que, lamentavelmente, apenas mais de um ano e meio depois, a 26 de agosto de 2019 – solicitar ao Tribunal Constitucional a fiscalização abstrata da constitucionalidade de várias disposições da Lei dos Metadados.⁷⁷

A provedora colocou o Tribunal Constitucional perante um dilema cuja resolução implicava seguir um de dois caminhos. O mais fácil seria não se pronunciar sobre a substância do pedido de fiscalização, declarando não ter competência para apreciar a constitucionalidade de disposições que, por serem contrárias à CDFUE, eram manifestamente inaplicáveis na ordem jurídica portuguesa. A fiscalização constitucional poderia ser considerada, neste contexto, hipotética, semelhante à levada a cabo perante disposições normativas revogadas antes de entrarem em vigor.

Os juízes do Palácio Ratton optaram, acertadamente, por seguir caminho distinto, ainda que mais complexo, o que, todavia, não justifica terem demorado 966 (!) dias para se pronunciar sobre a constitucionalidade de normas responsáveis por restrições muito amplas de direitos fundamentais da quase totalidade da população residente em Portugal.

As disposições da Lei dos Metadados contrárias à CDFUE, apesar de inaplicáveis, derivavam de fonte de direito nacional. A sua vigência formal não foi, por isso, afetada pelas decisões do tribunal do Luxemburgo nos processos *Digital Rights* ou *Tele2 Sverige*. Recorrendo à Declaração n.º 1/2004 do Tribunal Constitucional Espanhol sobre o Tratado que estabelece uma Constituição para a Europa, de 13

⁷² Ramalho e Coimbra, “A declaração de invalidade da Diretiva 2006/24/CE”.

⁷³ Gabinete de Cibercrime (Ministério Público), Nota Prática n.º 7, de 30 de dezembro de 2015.

⁷⁴ Acórdão n.º 420/17, considerandos 12-14. V. também Teresa Violante, “Data retention in Portugal”, in *European constitutional courts towards data retention law*, ed. Marek Zubik, Jan Podkowik e Robert Rybski (Berlim: Springer, 2021), 183-184.

⁷⁵ Acórdão do Tribunal da Relação de Lisboa, de 28 novembro de 2018, processo n.º 8617/17.8T9LSB-A. L1-3, considerandos 3.3 e 3.4.

⁷⁶ D3, “D3 pede à Provedora de Justiça que leve metadados ao Constitucional”, Nota de Imprensa de 27 de dezembro de 2017, <https://direitosdigitais.pt/comunicacao/comunicados/38-d3-pede-a-provedora-de-020justica-que-leve-metadados-ao-constitucional>.

⁷⁷ Provedora de Justiça, “Provedora de Justiça requer ao Tribunal Constitucional a fiscalização abstrata da constitucionalidade do diploma que estabelece uma obrigação geral de conservação de dados relativos às telecomunicações”, 26 de agosto de 2019, https://www.provedor-jus.pt/documentos/2019_08_26_Q_7746_2017_Tribunal_Constitucional.pdf.

de dezembro de 2004, o Tribunal Constitucional esclareceu que o direito da União tem primazia, mas não supremacia sobre o direito nacional – *i.e.*, prevalece, mas não derroga direito interno.⁷⁸ Ora, tal implicava que as disposições contestadas da Lei dos Metadados, relativas à conservação e acesso a dados pessoais, apenas poderiam ser formalmente afastadas da ordem jurídica através de revogação expressa pelo legislador competente em razão da matéria, a Assembleia da República, ou por via de declaração de inconstitucionalidade do Tribunal Constitucional, no âmbito de processo de fiscalização abstrata da constitucionalidade.

Uma vez que o regime jurídico dos metadados continuava a ser profusamente aplicado na ordem jurídica portuguesa, inclusivamente pelo próprio Tribunal Constitucional, a questão relativa à sua fiscalização constitucional não podia ser tida como meramente hipotética. Em causa estava, para além do mais, a violação de disposições da CDFU que encontram igualmente respaldo na Constituição portuguesa. De acordo com princípio da cooperação leal previsto no artigo 4.º, n.º 3, do TUE, o Tribunal Constitucional estava, portanto, obrigado a adotar todas as medidas ao seu alcance para assegurar a aplicação uniforme do direito da União na ordem jurídica portuguesa.⁷⁹ Por outras palavras, tinha o dever de intervir.

O Tribunal Constitucional cumpriu exemplarmente o dever de cooperação leal, declarando a inconstitucionalidade, com força obrigatória geral, de várias normas da Lei dos Metadados, por violação de disposições constitucionais relativas a direitos fundamentais, que interpretou à luz do padrão de proteção definido pelo Tribunal de Justiça relativamente a disposições análogas da CDFUE.

Mas não deveria o Tribunal Constitucional, enquanto “*órgão jurisdicional de direito comum do direito da União*”,⁸⁰ ter aplicado diretamente a CDFUE? Foi esta a posição, exarada em declaração de voto, por seis juízes conselheiros.⁸¹ A crítica, contudo, não procede.

O Tribunal Constitucional foi chamado, no âmbito de processo de fiscalização abstrata, a apreciar a compatibilidade de normas nacionais com a constituição portuguesa. Uma vez que nos encontrávamos num domínio normativo objeto de preempção pelo direito da União, sujeito ao âmbito de aplicação da Carta dos Direitos Fundamentais da União Europeia, os juízes do Palácio Ratton incorporaram o padrão jusfundamental europeu, tal como definido pelo Tribunal de Justiça, na interpretação das normas constitucionais aplicáveis, de modo a chegar ao resultado que lhes era exigido à luz do princípio da cooperação leal.⁸² Este percurso hermenêutico replica o adotado por outros tribunais constitucionais,⁸³ e encontra-se perfeitamente

⁷⁸ Acórdão n.º 268/2022. Cfr., também, Acórdão do TJUE *IN. CO. GE.*, 22 de outubro de 1998, C-10/97 a C-22/97, considerando 21, e Acórdão do TJUE *Filipiak*, 19 de novembro de 2009, C-314/08, considerando 83.

⁷⁹ Davide Paris [Davide Paris, “Constitutional courts as European Union courts: the current and potential use of EU law as a yardstick for constitutional review”, *Maastricht Journal of European and Comparative Law*, vol. 24, no. 6 (2018), 24-25] argumenta, a este respeito, que, em cumprimento do “*mandato Simmenthal*”, os tribunais constitucionais devem contribuir para reduzir a incerteza jurídica, utilizando o processo de fiscalização abstrata da constitucionalidade para eliminar da ordem jurídica normas que sejam suscetíveis de comprometer a efetividade do direito da União.

⁸⁰ Francisco Pereira Coutinho, *Os tribunais nacionais na ordem jurídica da União Europeia: o caso português* (Coimbra: Coimbra Editora, 2013), 14.

⁸¹ Acórdão n.º 268/2022 (declaração de voto apresentada conjuntamente pelos Conselheiros José António Teles Pereira, Maria Benedita Urbano, Pedro Machete, Joana Fernandes Costa, Gonçalo de Almeida Ribeiro e João Pedro Caupers).

⁸² Acórdão n.º 268/2022, considerando 8.2.

⁸³ Foi o caso do Tribunal Constitucional belga (Patritia Popelier e Catherine Van de Heyning,

alinhado com a obrigação de aplicar o direito europeu nos termos previstos na ordem jurídica da União,⁸⁴ a qual se baseia na premissa constitucional pluralista (federal) da existência de uma harmonia sistémica entre a proteção de direitos fundamentais nas ordens constitucionais portuguesa e europeia.⁸⁵ Este caminho inviabilizava, por outro lado, a adoção de decisão que modelasse os efeitos temporais da declaração de inconstitucionalidade, nos termos do artigo 282.º da Constituição, nomeadamente os relativos à salvaguarda de casos julgados, o que foi explicitamente reconhecido, pelo Tribunal Constitucional, ao invocar, na resposta ao pedido de nulidade remetido pela Procuradora-Geral da República,⁸⁶ a decisão do Tribunal de Justiça no processo *Commissioner of An Garda Síochána*.⁸⁷ Em suma, o Tribunal Constitucional limitou-se a certificar o obituário de normas nacionais de fonte europeia que, há muito, se encontravam desvitalizadas por ação do Tribunal de Justiça.

O Acórdão n.º 268/2022, de 19 de abril, será, porventura, o mais relevante da história do Tribunal Constitucional no que concerne à relação entre o direito constitucional da União e o direito constitucional português. Adotado com apenas um voto desfavorável, resolveu definitivamente um problema decorrente da resiliência de regime jurídico de fonte europeia manifestamente inconstitucional.

O Tribunal Constitucional veio reconhecer que a Lei dos Metadados tinha, afinal, problemas estruturais, que foram completamente ignorados pelo Acórdão n.º 420/17, de 13 de julho. Em primeiro lugar, ao não exigir que os dados fossem armazenados no território da União Europeia, comprometia a efetividade dos direitos dos titulares de dados, permitindo a conservação de dados em Estados terceiros não sujeitos aos poderes de fiscalização das autoridades administrativas nacionais de proteção de dados.⁸⁸ Em segundo lugar, ao não exigir a notificação dos visados sempre que os seus dados pessoais fossem acedidos pelas autoridades de investigação criminal, limitava o controlo jurisdicional contra arbitrariedades ou abusos.⁸⁹

Embora estas inconstitucionalidades fossem suficientes para invalidar o regime jurídico dos metadados *in totum*, o Tribunal Constitucional entendeu aplicar o teste da proporcionalidade à conservação preventiva de determinadas categorias de dados, admitindo expressamente, em linha com a jurisprudência do tribunal do Luxemburgo, a constitucionalidade da conservação generalizada e indiferenciada de dados de identificação civil de utilizadores de serviços de comunicações eletrónicas e, em casos de criminalidade grave como a pornografia de menores, dos endereços de protocolo IP que identificam a fonte de comunicações.⁹⁰

“The Belgian constitution: the efficacy approach to European and global governance”, in *National constitutions in European and global governance*, ed. Albi e Bardutzki, 1249), do Tribunal Constitucional eslovaco (Zuzana Vikarská e Michal Bobek, “Slovakia: Between Euro-Optimism and Euro-Concerns”, in *National Constitutions in European and Global Governance*, ed. Albi e Bardutzki, 868), e do Tribunal Constitucional esloveno (Samo Bardutzki, “the future mandate of the constitution of Slovenia: a potent tradition under strain”, in *National constitutions in European and global governance*, ed. Albi e Bardutzki, 714).

⁸⁴ Artigo 8.º, n.º 4, da Constituição da República Portuguesa.

⁸⁵ Como salientado por Teresa Violante (Teresa Violante, “How the data retention legislation”, 5), o princípio da interpretação conforme permitiu ao Tribunal Constitucional “vincular o padrão nacional de proteção aos parâmetros europeus, permitindo o estabelecimento de um quadro de proteção de direitos fundamentais plenamente harmonizado e congruente através da aplicação de disposições constitucionais nacionais.”

⁸⁶ Acórdão n.º 382/2022, considerando 4.

⁸⁷ Acórdão *Commissioner of An Garda Síochána*, considerando 128.

⁸⁸ Acórdão n.º 268/2022, considerando 16.

⁸⁹ *Idem*, considerando 19.

⁹⁰ *Idem*, considerandos 17.1-17.4.

O Tribunal Constitucional procurou evitar o “*elefante na sala*” – a constitucionalidade da conservação generalizada e indiferenciada de metadados de quase toda a população residente em Portugal –, preferindo centrar inicialmente a fiscalização nas salvaguardas legislativas relativas ao acesso, proteção e segurança dos dados, argumentando que, *em abstrato*, a sua robustez possibilitaria restrições mais amplas a direitos fundamentais no plano do regime da conservação de dados.⁹¹ Esta ideia, que está na base do Acórdão n.º 420/17, de 13 de julho, não encontra, todavia, respaldo na jurisprudência europeia, da qual resulta evidente a conclusão de que um regime de conservação preventiva de metadados, como aquele que estava previsto na lei portuguesa, representava, *por si só*, uma ingerência “*muito ampla*” e “*particularmente grave*” nos direitos dos titulares dos dados.⁹² A transmissão e acesso aos dados conservados constitui ingerência distinta nos direitos fundamentais dos titulares dos dados cuja admissibilidade requer justificação autónoma.⁹³ Em todo o caso, ainda que existissem salvaguardas que garantissem a proteção efetiva contra o risco de abuso e acesso ilícito a dados pessoais, o regime jurídico previsto na Lei n.º 32/2008, de 17 de julho, seria sempre inconstitucional, em razão de prever uma conservação preventiva, generalizada e indiferenciada, de dados de localização e de tráfego.

O Tribunal Constitucional fez um esforço titânico para tentar harmonizar a decisão com a sua jurisprudência constante. Só assim se explica a conclusão de que a conservação preventiva de endereços de protocolo IP dinâmicos que identificam a fonte de comunicações – os quais agora parece admitir que se podem, afinal, inserir conceptualmente na categoria dos dados de tráfego – por um período de um ano, não seria inconstitucional, caso o legislador tivesse exigido o respetivo armazenamento na União Europeia.⁹⁴ A ponderação de proporcionalidade levada a cabo no Acórdão n.º 420/17, de 13 de julho, assegura o Tribunal Constitucional, alinha-se perfeitamente com a do Tribunal de Justiça.⁹⁵ Aliás, esta é uma posição incompatível com o facto de o período de conservação ter excedido o estritamente necessário à luz do objetivo pretendido,⁹⁶ não tendo, para além do mais, sido estabelecidos requisitos e garantias legislativas estritas quanto ao tratamento desta categoria de dados, nomeadamente no que diz respeito ao rastreio das comunicações e atividades efetuadas em linha pelos titulares dos dados.⁹⁷

Não fiquei também convencido pelo juízo de constitucionalidade levado a cabo pelo Tribunal Constitucional relativamente à conservação generalizada e indiferenciada de dados de tráfego e de localização prevista na Lei dos Metadados. Falhando no teste de proporcionalidade, esta medida foi declarada inconstitucional por violar os direitos à privacidade e à proteção de dados.⁹⁸

⁹¹ *Idem*, considerando 14.

⁹² Acórdão *Télé2 Sverige*, considerando 100, Acórdão *Quadrature du Net*, considerando 118.

⁹³ Acórdão *Quadrature du Net*, considerando 115-119, Acórdão *Commissioner of An Garda Síochána*, considerando 47.

⁹⁴ Acórdão 268/2022, considerando 17.4.

⁹⁵ *Idem*, considerando 17.3.

⁹⁶ Em termos comparativos, o artigo 113b.º, da Lei Alemã relativa às Telecomunicações, objeto de discussão no processo *Space Net*, considerando 39, estabelecia um período máximo de conservação de 10 semanas.

⁹⁷ Acórdão *Quadrature du Net*, considerando 156. De acordo com o Tribunal de Justiça, os endereços de protocolo IP “*podem ser utilizados para efetuar, nomeadamente, o rastreio exaustivo da navegação de um internauta e, por conseguinte, da sua atividade em linha*”, pelo que permitem estabelecer o perfil pormenorizado do titular dos dados (*idem*, considerando 153).

⁹⁸ Acórdão n.º 268/2022, considerando 18.

É verdade que tanto o direito à privacidade como o direito à proteção de dados não consubstanciam prerrogativas absolutas. Devem, por conseguinte, ser lidos de acordo com a sua função na sociedade.⁹⁹ No entanto, a natureza sensível das informações fornecidas pelos dados de tráfego e, especialmente, pelos dados de localização, determina que a sua confidencialidade seja essencial para garantir o direito ao respeito pela vida privada.¹⁰⁰ Não seria, então, lógico inferir que a conservação generalizada e indiferenciada de dados de tráfego e de localização compromete o núcleo essencial do direito à privacidade?

No processo *Tele2 Sverige*, o Tribunal de Justiça entendeu que não. Embora tenha qualificado a ingerência, nos direitos fundamentais, de legislação nacional similar à Lei dos Metadados, como “*muito ampla*” e “*particularmente grave*”, afastou a violação do núcleo essencial do direito à privacidade, na ausência de obrigação de conservação do conteúdo das comunicações.¹⁰¹ Paradoxalmente, veio, contudo, reconhecer que os dados conservados podiam fornecer meios para determinar o perfil das pessoas em causa, consubstanciando, portanto, “*informação tão sensível, à luz do direito ao respeito da privacidade, como o conteúdo das próprias comunicações*.”¹⁰²

A ideia de que a conservação generalizada e indiferenciada de dados de tráfego e de localização é necessariamente menos invasiva do que a resultante da conservação do conteúdo das comunicações foi também rejeitada, pelo Tribunal Europeu dos Direitos Humanos, no acórdão *Big Brother Watch*.¹⁰³ Como afirmou Stewart Baker, antigo dirigente da *National Security Agency* dos Estados Unidos da América, “*os metadados fornecem todas as informações sobre a vida de uma pessoa*”, o que significa que, se as autoridades de segurança e de investigação criminal tiverem acesso a metadados em número suficiente, “*não necessitam, de facto, do conteúdo (das comunicações)*.”¹⁰⁴

Não parecem, por isso, subsistir razões de monta para distinguir a conservação generalizada e indiferenciada de metadados, de conservação similar do conteúdo das comunicações, no que diz respeito à natureza da ingerência sobre o núcleo essencial do direito à privacidade. O tribunal de Luxemburgo – e, por extensão, o Tribunal Constitucional – deveria, assim, ter seguido o caminho hermenêutico adotado no acórdão *Schrems I*, relativamente a legislação norte-americana que concedia às autoridades públicas acesso generalizado ao conteúdo de comunicações eletrónicas.¹⁰⁵

6. Considerações finais

Nos Acórdãos n.º 403/2015, de 27 de agosto, e n.º 464/2019, de 18 de setembro, o Tribunal Constitucional bloqueou tentativas sucessivas para conceder, aos serviços de informações da República (SIS e SIED), acesso a metadados conservados

⁹⁹ Acórdão *Schrems II*, considerando 172.

¹⁰⁰ Acórdão *Quadrature du Net*, considerando 142.

¹⁰¹ Acórdão *Tele2 Sverige* considerandos 100-101.

¹⁰² *Idem*, considerando 99.

¹⁰³ Acórdão *Big Brother Watch and Others v. United Kingdom*, 25 de maio de 2021, 58170/13, 62322/14 e 24960/15, considerando 363.

¹⁰⁴ David Cole, “We kill people based on metadata”, *New York Review of Books*, 10 de maio de 2014, <https://www.nybooks.com/online/2014/05/10/we-kill-people-based-metadata/>.

¹⁰⁵ Acórdão *Schrems I*, considerando 94.

preventivamente pelos fornecedores de serviços ao abrigo da Lei dos Metadados.¹⁰⁶ Mas será razoável acreditar que os serviços de informações, pela natureza das suas funções, não acederam *ilicitamente* àqueles metadados? Não há dúvidas de que foi esse o caso das autoridades de investigação criminal, no que concerne a dados conservados ao abrigo da Lei n.º 41/2004, de 12 de julho, e da Lei n.º 32/2008, de 17 de julho, desde a prolação, pelo Tribunal de Justiça, dos acórdãos *Digital Rights e Tele2 Sverige*.

A passividade da Comissão Europeia, que ignorou pedidos para iniciar processos por infração contra os Estados-Membros que não revogaram legislação nacional de implementação da diretiva relativa à conservação de dados,¹⁰⁷ conjugada com uma falha sistémica de todos os atores nacionais relevantes no plano administrativo, legislativo e judicial (incluindo o próprio Tribunal Constitucional), permitiu a perpetuação, na ordem jurídica portuguesa, da conservação preventiva, generalizada e indiferenciada, de metadados até meados de 2022.

Ainda a poeira da histórica decisão do Tribunal Constitucional não tinha assentado quando o Governo apresentou proposta de alteração à Lei n.º 41/2004, de 12 de julho, em que, por um lado, atribuía acesso às autoridades de investigação criminal a dados conservados para fins de faturação e, por outro lado, exigia que os fornecedores de serviços de comunicações conservassem dados desnecessários (*e.g.* endereços de protocolo IP) para esse propósito específico.¹⁰⁸ Esta foi uma vã tentativa de fazer a quadratura do círculo, redefinindo, de forma encapotada, a finalidade de uma base de dados criada com o propósito de proteger direitos dos consumidores.¹⁰⁹ Se aprovada, não teria, com elevada certeza, sobrevivido a fiscalização preventiva da constitucionalidade entretanto prometida pelo Presidente da República.¹¹⁰

Em última instância, com efeito, caberá sempre ao Tribunal Constitucional conter derivas securitárias, contrárias ao direito constitucional da União Europeia, que ameaçam o direito fundamental dos titulares dos dados a esperar que as suas comunicações e os dados a elas relativos permaneçam anónimos.¹¹¹

¹⁰⁶ Acórdão do Tribunal Constitucional n.º 403/2015, de 27 de agosto, processo n.º 773/15, e Acórdão do Tribunal Constitucional n.º 464/2019, de 18 de setembro, processo n.º 26/18.

¹⁰⁷ Parlamento Europeu, Relatório sobre a situação dos direitos fundamentais na União Europeia – Relatório anual para os anos 2018-2019, 2019/2199(INI), 19 de novembro de 2020, considerando 32.

¹⁰⁸ Proposta de Lei n.º 11/XV/1, aprovada pelo Conselho de Ministros a 26 de maio de 2022.

¹⁰⁹ Comissão Nacional de Proteção de Dados, Parecer 50/2022, 21 de junho de 2022.

¹¹⁰ Joana Morais Fonseca, “Marcelo vai pedir fiscalização preventiva da nova lei dos metadados ao Tribunal Constitucional”, *Eco*, 18 de maio de 2022.

¹¹¹ A tentativa parlamentar de reintroduzir a conservação generalizada e indiferenciada de dados através da inclusão de algumas alterações à Lei dos Metadados foi considerada inconstitucional no Acórdão do Tribunal Constitucional n.º 800/2023, de 4 de dezembro, processo n.º 1130/2023. Uma subsequente iniciativa parlamentar levou à adoção da Lei n.º 18/2024, de 5 de fevereiro, ainda não objeto de fiscalização pelo Tribunal Constitucional.

Desafios de cibersegurança no fenómeno da transição digital na Europa

*Henrique Santos**

1. Sobre a cibersegurança

Os anos recentes têm revelado a cibersegurança como um pilar essencial do desenvolvimento tecnológico.¹ Mas também tem revelado alguns paradoxos relacionados, como fica evidente em alguns estudos sobre o mercado de trabalho na área.² Primeiro, todos acham que é indispensável, mas o investimento (sobretudo em termos de educação e treino) é praticamente residual. A razão não é estranha ao facto de não existir um retorno de investimento, porque na verdade a cibersegurança não dá lucro (exceto, evidentemente, para as empresas que prestam serviços de cibersegurança). Em boa verdade, porque a cibersegurança, por definição, obriga a impor algum tipo de restrição na funcionalidade, tem impacto negativo na atratividade de um produto de TIC e, conseqüentemente, no lucro.

Outro facto interessante é a evidência do foco de investimento em cibersegurança, para as organizações que o fazem (por opção, ou por via regulamentar).

Nestes casos, como revelam alguns estudos, aplicam cerca de oitenta por cento do seu orçamento de cibersegurança na deteção de incidentes. Isto apesar de a grande parte dos profissionais afirmarem que a aposta deveria ser na prevenção e na resiliência, sempre com a consciência que iremos aprender a conviver com estes incidentes, como, aliás, tem acontecido com muitos outros desenvolvimentos tecnológicos.³

Um último paradoxo resulta da evidência que o melhor profissional de cibersegurança é impercetível. Com efeito, se esse profissional for bastante competente, será capaz de detetar a larga maioria dos incidentes e/ou reduzir o impacto daqueles que não é possível impedir. Uma consequência deste paradoxo é uma menor atratividade de profissionais para estas funções. Numa realidade em que a procura de profissionais para as TIC, em geral, é enorme, dadas as restrições desta área específica essas limitações são ainda maiores.⁴

* Professor na Escola de Engenharia da Universidade do Minho, ALGORITMI Research Centre/LASI, Braga.

¹ Saqib Saeed, *et al.*, “Digital transformation and cybersecurity challenges for businesses resilience: issues and recommendations”, *Sensors*, vol. 23, no. 15 (2023): 6666.

² ISC2, “2024 ISC2 Cybersecurity workforce study”, 31 de outubro de 2024, <https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study>.

³ Agnė Srėbaliūtė, “Best practices on cybersecurity budget allocation: a research-based guide”, *NordLayer* 30 de agosto de 2024, <https://nordlayer.com/blog/best-practices-cybersecurity-budget-research-guide>.

⁴ Digital Guardian, “Cyber Security investments: experts discuss detection vs. prevention”, 26 de setembro de 2016, <https://www.digitalguardian.com/blog/cyber-security-investments-experts-discuss-detection-vs-prevention>.

2. Sobre a evolução das TIC

Nesta secção será apresentado um breve resumo da evolução tecnológica do que hoje designamos por TIC. O objetivo é realçar a lógica dessa evolução e justificar os impactos no contexto da cibersegurança e do Estado de Direito. Há pouco mais de meio século, com os primeiros computadores construídos, havia poucos centros de computação no mundo, sendo operados e usados por poucos profissionais e para resolver alguns problemas muito específicos. Não obstante o potencial desta tecnologia, as limitações inerentes à sua capacidade de utilização eram limitadas e inibidoras do negócio.

A partir daqui temos uma série de tecnologias que foram emergindo, sempre com vista a uma massificação da sua utilização: a começar pelo *time-share*, que era uma forma de utilizar remotamente, mas dentro do mesmo edifício, aqueles mesmos sistemas informáticos; depois, rapidamente vieram as redes de computadores e os sistemas distribuídos, que permitiram utilizar os mesmos sistemas mas já fora dos edifícios; e, finalmente, os computadores e dispositivos pessoais que, basicamente, repartiram a informação colocando-a em dispositivos no local de trabalho de cada um dos utilizadores, ou mesmo dispositivos móveis. Em paralelo desenvolveram-se conceitos como o de Computação Ubíqua, que procuraram vulgarizar esta tecnologia, introduzindo-a em todos os setores de atividade, fazendo crescer este mercado que hoje tem um peso na economia mundial. Por isso mesmo, reconhece-se que hoje este é um fenómeno imparável. Finalmente, a convergência das tecnologias, sobretudo as tecnologias de comunicação sem fios, permite que hoje já quase ninguém se preocupe com que tecnologia de dados está a utilizar. O mundo está interligado, com acesso a serviços de base digital, em qualquer lugar e a qualquer hora.⁵

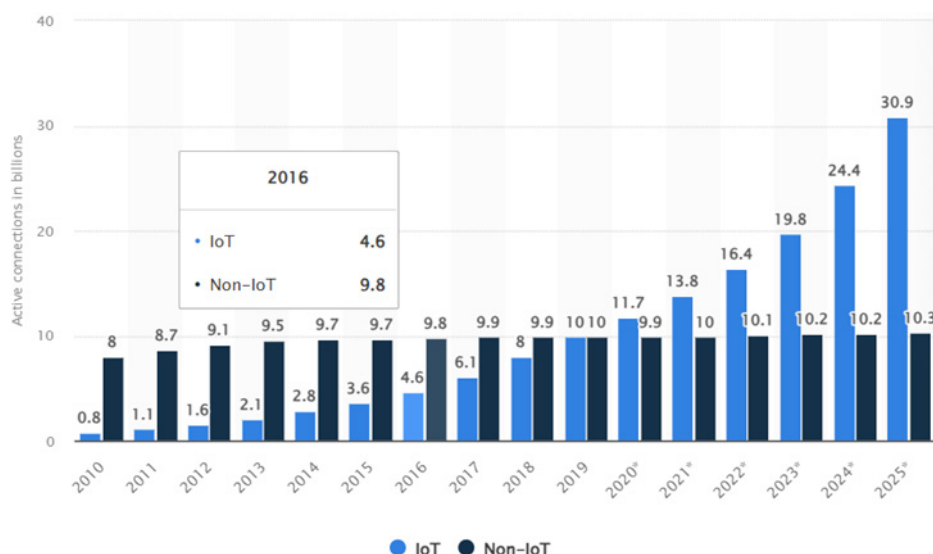
Nesta linha de evolução emergiu um outro conceito com um potencial impacto considerável: a *Internet of Things* (IoT).⁶ Criado numa perspetiva muito tecnológica, este paradigma é, frequentemente, ligado aos “pequenos” dispositivos que passaram a poder ser integrados no ciberespaço. Esses dispositivos têm uma capacidade limitada e, por isso, não são habitualmente considerados como muito relevantes. No entanto, há alguns desenvolvimentos paralelos e que mudam radicalmente a forma como interagimos com estas tecnologias: por um lado, a criação de protocolos *Machine-to-Machine* (M2M), que basicamente permitem que as máquinas comuniquem entre si implementando serviços digitais dedicados;⁷ por outro lado, o crescimento exponencial do número de máquinas presentes no ciberespaço e que ultrapassou, já em 2018, o número de seres humanos, como se evidencia na Figura 1.⁸

⁵ Henrique M. Santos, *Cybersecurity: a practical engineering approach* (Boca Raton: CRC Press, 2022).

⁶ Fadele Ayotunde Alaba, *et al.*, “Internet of Things security: a survey”, *Journal of Network and Computer Applications*, vol. 88 (2017): 10-28. <https://doi.org/10.1016/j.jnca.2017.04.002>.

⁷ Ala Al-Fuqaha *et al.*, “Internet of Things: a survey on enabling technologies, protocols, and applications”, *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4 (2015): 2347-2376. doi: 10.1109/COMST.2015.2444095.

⁸ Lionel Sujay Vailshery, “IoT and non-IoT connections worldwide 2010-2025”, *Statista* 6 de setembro de 2022, <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/>.

Figura 1. Evolução do número de dispositivos interligados no ciberespaço

Fonte: <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/>, ver nota de rodapé 8.

No contexto do crescimento deste fenómeno IoT, entre diversas evoluções, registou-se a capacidade para explorar os Ambientes Inteligentes que, nas duas últimas décadas, têm vindo a estudar e experimentar soluções de redes de sensores com algoritmos de gestão inteligente de operações, sobretudo para o apoio à decisão e previsão.⁹ A IBM cunhou este mundo novo como sendo instrumentalizado, interligado e inteligente.¹⁰

Podemos (e devemos) encarar o futuro admitindo a existência de biliões de dispositivos, interligados e a interoperar. A cibersegurança desse ciberespaço é fundamental para garantir a “*correta*” operação desses dispositivos que, cada vez mais, se vai imiscuir no nosso espaço físico tradicional. Até aqui tínhamos privacidade em casa com redes chamadas privadas. Tínhamos uma série de benefícios na utilização diária que, através de tecnologias como as *Virtual Private Networks* (VPNs), ou outras sob controlo direto do ser humano, permitia proteger-nos minimamente, nomeadamente no que respeita à privacidade.¹¹

A União Europeia, na sua estratégia de transição digital, vem apontar alguns princípios fundamentais. A cibersegurança e a proteção pessoal (ou *safety*) aparecem, naturalmente, como pilares desejáveis. A questão fundamental é tentar perceber se esses pilares estão efetivamente a ser construídos, ou se apenas existem na conceção.¹²

3. O papel das normas e da regulamentação

Admitindo que existe esta nova realidade digital, vamos ainda admitir que existe, também, uma identidade digital (efetivamente existe ou, pelo menos, pode ser caracterizada) e que, muitas vezes, corresponde a uma identidade de um ser humano, muito embora essa independência seja quase radicalmente defendida

⁹ Diane J. Cook, *et al.*, “Ambient intelligence: technologies, applications, and opportunities”, *Pervasive and Mobile Computing*, vol. 5, issue 4 (2009): 277-298. <https://doi.org/10.1016/j.pmcj.2009.04.001>.

¹⁰ Sam Palmisano, “A smarter planet: the next leadership agenda”, 6 novembro de 2008, https://www.ibm.com/ibm/ideasfromibm/za/en/smarterplanet/20081106/sjp_speech.shtml.

¹¹ Henrique M. Santos, *Cybersecurity: a practical engineering approach*.

¹² Louis Brun, “The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity” (Diss. Mestrado, UCLouvain, 2018).

através da promoção de técnicas de anonimização, procurando promover a privacidade. Seja como for, seria desejável que essa identidade digital pudesse ser imputada da responsabilidade da sua operação no ciberespaço. A não o ser, a responsabilidade e consequência de atos maliciosos desencadeados por identidades digitais e que não possam ser factualmente ligadas a qualquer identidade humana, não poderá ser atribuída.¹³ Adicionalmente, o crescimento exponencial da IoT, aliado ao desenvolvimento de tecnologias de IA, começa a configurar um cenário complexo e com inúmeras vulnerabilidades e ameaças à cibersegurança e à segurança na utilização, acabando por aumentar, também exponencialmente, os incidentes de cibersegurança.¹⁴

A questão fundamental é saber se este segundo mundo que está a crescer debaixo dos nossos utensílios diários é ou não devidamente regulado. Mais ainda, estaremos a educar e treinar devidamente os seres humanos para conviver de forma racional, consciente e ética com este mundo e todos os desafios e perigos que encerra? Não será esta uma expectativa mais que legítima num Estado de Direito?¹⁵

Em Portugal, o Centro Nacional de Cibersegurança (CNCS), que depende do Gabinete Nacional de Segurança (GNS), é a entidade designada para se ocupar da cibersegurança. Para já, o seu maior esforço reside na procura de formas de adaptar e criar os recursos essenciais para aplicar a regulamentação europeia sobre o assunto e que, claramente, não cobre todas as vertentes das ciberameaças.¹⁶ Em suma, efetivamente estamos perante uma ameaça considerável, que é o mundo digital, e que não estamos a controlar devidamente, revelando um défice considerável. Mas esta linha de resposta revela ainda uma limitação importante, ao não conseguir acompanhar a velocidade com que o próprio desenvolvimento tecnológico acontece e, por conseguinte, das ameaças inerentes.

Uma alternativa para preparar a resposta reside numa utilização mais atenta de normas, ou standards.¹⁷ Uma norma, basicamente, é um documento que define um patamar mínimo de qualidade que é aceite por especialistas de diversos *players*. A *International Standardization Organization* (ISO) integra a larga maioria dos países e, através de uma rede de comissões técnicas nacionais, procura de alguma forma normalizar o bom uso das tecnologias (entre outras dimensões de atividade).

A cibersegurança foi já alvo de um considerável esforço de normalização. A ISO desenvolveu um conjunto alargado de normas, globalmente designado por família de normas ISO/IEC 27000. Os Estados Unidos têm também uma família de normas, a SP 800. A Europa tem ainda duas organizações específicas de normalização – *European Committee for Standardization* (CEN) e *European Committee for Electrotechnical Standardization* (CENLEC) – que, embora estejam bastante coladas à ISO, desenvolvem algumas normas específicas, sobretudo de natureza setorial. Alguns países, como o Reino Unido, também têm o seu articulado normativo.¹⁸

¹³ Nikhil Ghadge, “Digital identity in the age of cybersecurity: Challenges and solutions”, *London Journal of Research In Computer Science And Technology*, vol. 24, no. 1 (2024): 1–10.

¹⁴ Masike Malatji and Alaa Tolah, “Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI”, *AI and Ethics* (2024). <https://doi.org/10.1007/s43681-024-00427-4>.

¹⁵ Suzana Kraljić, “The right to education in a digital era”, in *Digital technologies and distributed registries for sustainable development: legal challenges*, ed. Larisa V. Sannikova (Springer, 2024), 135–153.

¹⁶ Damjan Fujs and Igor Bernik, “Analyzing cybersecurity strategies of the European Union: challenges and opportunities for public administration”, *Elektrotehniski Vestnik*, vol. 91, nos. 1-2 (2024): 8–20.

¹⁷ Adebola Folorunso, et al., “Security compliance and its implication for cybersecurity”, *World Journal of Advanced Research and Reviews*, vol. 24, no. 1 (2024): 2105–2121.

¹⁸ Wenjia Wang, et al., “A survey of major cybersecurity compliance frameworks”, *2024 IEEE 10th Conference*

Apesar de todo esse esforço, o número de certificações em todo o mundo é muito reduzido. Muito particularmente em Portugal, o número de organizações que solicitaram certificações em cibersegurança é extremamente baixo, infelizmente.¹⁹ O gráfico apresentado na Figura 2 ilustra a distribuição das certificação da norma ISO/IEC 27001 – Gestão da Segurança da Informação –, uma das mais conceituadas nesta área, apenas incluindo os países com um número de certificações superior a 200 (do total dos 189 países sobre os quais existem dados, Portugal encontra-se na 37ª posição; no entanto, e mesmo à escala da dimensão do país, percebe-se que a preocupação é muito menor a partir dos cinco primeiro países, que apenas incluem a Itália, no que respeita à UE). Ainda no contexto da normalização, deve-se assinalar que o próprio uso da IA está a ser alvo de um esforço de normalização.

Falta, claramente, a vontade política de fazer utilizar estas normas, por exemplo, obrigando a que pelo menos os concursos públicos relacionados com tecnologias obrigassem a que os concorrentes demonstrem que os seus produtos ou serviços estão alinhados com estas normas. Apesar de parecer simples, esta solução tem limitações sobretudo relacionadas com o custo da certificação e que iria necessariamente afetar os preços. Por outro lado, não é de esperar que o setor privado seja pioneiro nesta matéria, já que não sendo obrigatória, a certificação é objetivamente vista como um custo – não esquecer que a cibersegurança, tal como anteriormente realçado, é considerada como um custo.²⁰

O custo do alinhamento com normas tem ainda um impacto adicional no Estado de Direito. Grandes empresas podem facilmente suportar esses custos, mas as pequenas não, gerando uma assimetria assinalável e facilmente reconhecida.

É ainda pertinente olhar aqui para a estratégia que a União Europeia tem vindo a assumir para responder a estes desafios. Primeiro, tivemos o *Cybersecurity Act* europeu, onde foi criada a ENISA, a Agência Europeia para a Cibersegurança. Esta agência suporta um modelo de certificação europeu, que já está aprovado. Procura aumentar a cooperação entre todos os Estados-Membros com mecanismos de resposta a incidentes, os chamados *Computer Security Incident Response Team* (CSIRT), ou *Security Operations Centre* (SOC), para os quais produziu documentação de suporte, tais como guias. Cada país na Europa terá um CSIRT (a medida já está implementada em todos os países, mesmo não existindo um mecanismo de fiscalização efetivo). Mais recentemente, a produção da diretiva NIS2 vem permitir a autoridade que controla cada CSIRT (no nosso caso é o CNCS) definir coimas, aplicadas a quem não cumpre com o que está preconizado – um mecanismo muito semelhante ao que foi criado com o RGPD.²¹

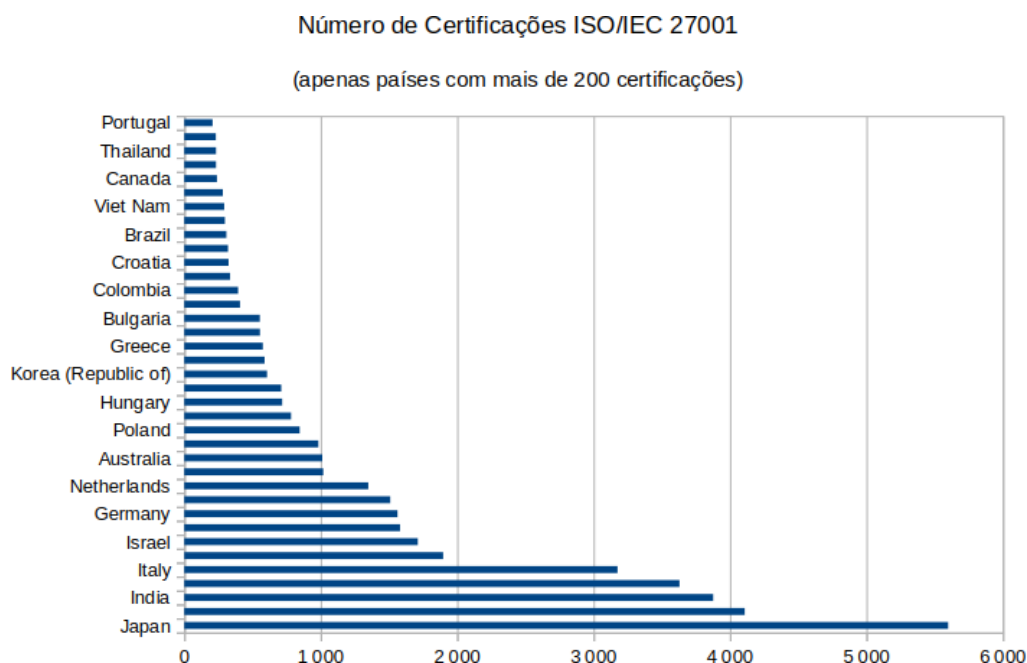
on *Big Data Security on Cloud* (BigDataSecurity) (2024): 23–34. [10.1109/BigDataSecurity62737.2024.00013](https://doi.org/10.1109/BigDataSecurity62737.2024.00013).

¹⁹ ISO, “The iso survey 2023”, 2023, <https://www.iso.org/the-iso-survey.html>.

²⁰ Geir Hørthe, “The importance of cyber security requirements: what you need to know”, *Nemko*, 25 de maio de 2021, <https://www.nemko.com/blog/is-cyber-security-mandatory>. See also Phil Robinson, “Why aren’t more businesses adopting security standards?”, *Cybersecurity Magazine*, 19 de maio 2023, <https://cybersecurity-magazine.com/why-arent-more-businesses-adopting-security-standards/>.

²¹ Adejoke T. Odebade and Elhadj Benkhelifa, “A comparative study of national cyber security strategies of ten nations”, March 2023, *arXiv* preprint arXiv:2303.13938. <http://dx.doi.org/10.48550/arXiv.2303.13938>.

Figura 2. Certificações da norma ISO/IEC 27001, extraídas dos dados fornecidos pela ISO



Fonte: elaboração própria, com base nos dados estatísticos fornecidos pela ISO.

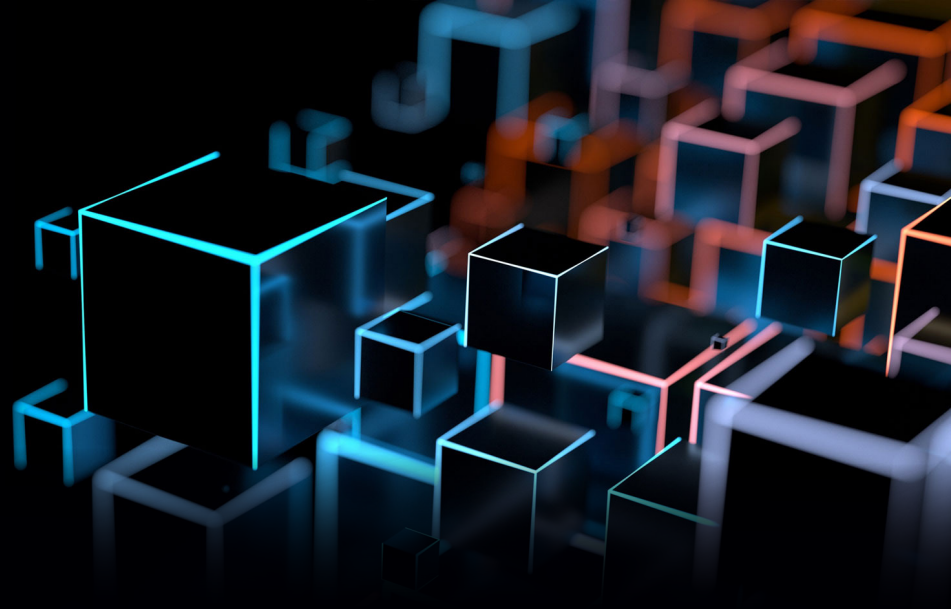
Não obstante estes esforços, há ainda questões em aberto: será pertinente a criação de um novo direito fundamental relacionado com o ciberespaço? Este mundo digital, que vai muito para além da IA, precisa ou não de ter mais articulados regulamentares e, sobretudo, como se poderá avaliar o seu impacto, sobretudo quando e se começar a ser um impedimento à competitividade das empresas? Se olharmos para o direito fundamental à segurança, que está contemplado no artigo 6.º do Carta dos Direitos Fundamentais da UE, a segurança atual no ciberespaço responde a estas exigências de uma vida digital?²² A segurança nesta área do digital é a mesma coisa? Na verdade, estamos a falar aqui de três coisas diferentes: segurança, enquanto a integridade e a disponibilidade da infraestrutura digital, focada em garantir que a “ferramenta” e a informação não é comprometida; isso inclui a confidencialidade da informação, que contribui para a privacidade, mas não é a mesma coisa, pois a privacidade é um direito de quem disponibiliza os dados; finalmente, temos a segurança na ótica de quem utiliza, relacionada com os eventuais danos resultantes para o utilizador – *safety*. Uma estrutura de resposta a incidentes como os CSIRTs que a Europa está a fazer é suficiente? Talvez ajude na resposta, mas e a prevenção? A prevenção assenta sobretudo na educação. Esta tem sido o parente pobre de todo o processo de transformação digital e, consequentemente, da cibersegurança. Se uma empresa vender um equipamento que tem defeitos, se a devida indicação, o que é muito frequente, no dia em que esse defeito for explorado e o equipamento for usado com impactos negativos em terceiros, a empresa vai ser responsabilizada?

²² Pier Giorgio Chiara, “Towards a right to cybersecurity in EU law? The challenges ahead”, *Computer Law & Security Review*, vol. 53, 105961 (2024).

4. Conclusões

O fenómeno habitualmente referido por transição digital revela uma dinâmica imparável. Segundo algumas estimativas, um terço do volume de negócios de todo o mundo já depende, direta ou indiretamente, desse fenómeno. Associado a essa evolução, as ciber ameaças e em particular o cibercrime, revelam-se como barreiras relevantes e que podem limitar substancialmente o potencial impacto daquele fenómeno.

A resposta dos Estados a estes problemas tem sido muito limitada. Os mecanismos que têm vindo a ser implementados focam-se maioritariamente na resposta, sobretudo baseada também em tecnologias, e muito pouco na prevenção. Mas o Estado atual revela assimetrias sociais assinaláveis, colocando em causa o chamado Estado de Direito. Os membros desta sociedade tecnologicamente transformada não todos iguais e se a capacidade para lidar com a tecnologia evidencia vulnerabilidades, também a capacidade para lidar com as tecnologias de cibersegurança revelam a mesma limitação. Na Europa, em particular, têm sido dados importantes nos domínios organizacional e da educação, que são importantes pilares na prevenção, em conjunto com os esforços de normalização, também acarinhados pelas agências europeias. No entanto, há ainda um longo caminho a percorrer.



E-book CitDig

**Centro de Excelência Jean Monnet em
Cidadania Digital & Sustentabilidade
Tecnológica**

**II Congresso Ibero-Americano sobre Direito e
Tecnologias Digitais subordinado ao tema “Estado
de direito e transição digital”**

Centro de Excelência Jean Monnet CitDig é financiado pelo Programa Erasmus+ (Project 101085242).
Mais informações: <https://citdig.direito.uminho.pt/pt/>.



Universidade do Minho
Escola de Direito



Co-funded by
the European Union