E.TEC YEARBOOK

Legal Challenges of Technology

School of Law - University of Minho
2023

EDITOR
Sónia Moreira

E.Tec Yearbook

Legal Challenges of Technology

JusGov - Research Centre for Justice and Governance
School of Law - University of Minho

2023

TITLE
E.Tec Yearbook - Desafios Jurídicos da Tecnologia

EDITOR
Prof.ª Doutora Sónia Moreira

AUTHORS
Ana Flávia Messa | Célia Dias Pereira | Everton Luiz Zanella | Levy Emanuel Magno
Luís Manuel Pica | Mário Filipe Borralho | Mercília Pereira Gonçalves
Sofia Travassos Alcaide | Tomàs Gabriel García-Micó

DATE
December 2023

PUBLISHERS
JusGov - Research Centre for Justice and Governance (www.jusgov.uminho.pt)
University of Minho - School of Law (www.direito.uminho.pt)

DESIGN AND TYPESET
Mariana Teixeira

COVER
Photo by Andrea De Santis on Unsplash

ISSN
2184-707X

Publication funded by the Portuguese National Funding Agency (FCT) under project UIDB/05749/2020.

TABLE OF CONTENTS

PREFACE

Welcome to the sixth E-Tec Yearbook!

In 2023, our Law School celebrates its 30th anniversary. Considering the occasion, the theme cuts across all of E-Tec's thematic strands: "Legal Challenges of Technology". Thus, the call for this publication established for this year the exploration of the legal problems arising from technological innovations, especially digital transformation, artificial intelligence and robotics, and their repercussions on Industry 4.0, Health Law and Governance.

As usual, the texts presented here denote the multidisciplinary nature that research into these areas entails: we find reflections on the use of Artificial Intelligence in Medicine and Agriculture, on its repercussions on Family and Children's Law and Civil Liability Law, on the use of new technologies in Registry Law, etc.

We would like to thank the authors for their generosity and hard work, as well as Dr Mariana Teixeira, who helped us with the graphic editing of the book. On the other hand, these thanks would not be complete without a word of recognition to the Law School of the University of Minho, in the person of its President, Professor Cristina Dias, for the unconditional support she always gives to JusGov's initiatives, and to the JusGov Board, in the person of Professor Maria Miguel Carvalho, who always encourages us to move forward in our role, which is to investigate and disseminate the results of our research, sharing legal science with all those who are interested in it.

Braga, December 2023.

Sónia Moreira
Coordenadora

PREFÁCIO

Bem-vindos ao sexto Yearbook do E-Tec!

Neste ano de 2023, a nossa Escola de Direito celebra 30 anos. Considerando a efeméride, o tema é transversal a todos os eixos temáticos do E-Tec: "Desafios Jurídicos da Tecnologia". Assim, a call desta publicação deu conta de que se visava explorar os problemas jurídicos decorrentes das inovações tecnológicas, especialmente a transformação digital, a inteligência artificial e a robótica, e as suas repercussões na indústria 4.0, no Direito da Saúde e na Governação.

Como é habitual, os textos que ora se apresentam denotam o carácter multidisciplinar que a investigação sobre estas áreas implica: encontramos reflexões sobre a utilização de Inteligência Artificial na Medicina e na Agricultura, sobre as suas repercussões no Direito da Família e Menores e no Direito da Responsabilidade Civil, sobre o uso das novas tecnologias no Direito Registral, etc.

Não podíamos deixar de veicular o nosso agradecimento aos autores, pela sua generosidade e trabalho, e ainda à Dr.ª Mariana Teixeira, que nos acompanhou na edição gráfica da obra. Por outro lado, estes agradecimentos não estariam completos sem uma palavra de reconhecimento à Escola de Direito da Universidade do Minho, na pessoa da sua Presidente, a Professora Cristina Dias, pelo apoio incondicional que sempre presta às iniciativas do JusGov, e à Direção do JusGov, na pessoa da Prof.ª Doutora Maria Miguel Carvalho, que sempre nos incentiva a seguir em frente no papel que nos cabe e que é o de investigar e divulgar o resultado da nossa investigação, partilhando a ciência jurídica com todos aqueles que nela tenham interesse.

Braga, dezembro de 2023.

Sónia Moreira

Coordenadora

INFILTRAÇÃO VIRTUAL NO DIREITO BRASILEIRO

Ana Flávia Messa[1]
Everton Luiz Zanella[2]
Levy Emanuel Magno[3]

Resumo: No presente artigo, interessa-nos destacar e enfatizar reflexões construtivas sobre como o instituto de infiltração de agentes constitui uma ferramenta de fundamental importância no campo de produção de elementos de convicção que possa levar a responsabilização de crimes praticados não só no âmbito das Organizações Criminosas (Lei 12.850/13), como também na Lei de Drogas

[1] Doutora em Direito Público pela Universidade de Coimbra. Doutora em Direito Público pela Universidade de São Paulo. Mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Membro da Academia Paulista de Letras Jurídicas. Membro do Conselho Científico da Academia Brasileira de Direito Tributário. Membro do Conselho Editorial da *International Studies on Law and Education*. Professora da Graduação e Pós-Graduação da Universidade Presbiteriana Mackenzie. Investigadora integrada na equipa do JusGov (no âmbito das atividades do JUSLAB) da Universidade do Minho.

[2] Doutor em Direito Processual Penal e Mestre em Direito Penal, ambos pela Pontifícia Universidade Católica de São Paulo. Professor da Faculdade de Direito e Membro do Conselho de Ensino, Pesquisa e Extensão (CEPE) da Universidade Presbiteriana Mackenzie. Professor na Graduação, Mestrado e Doutorado da Faculdade Autônoma de Direito (FADISP). Professor e membro do Conselho Curador do CEAF-ESMP (Centro de Estudos e Aperfeiçoamento Funcional – Escola Superior do Ministério Público). Professor convidado dos cursos de Pós-Graduação da Escola Paulista de Direito e da Escola Paulista da Magistratura. Parecerista do Conselho Internacional de Estudos Contemporâneos em Pós-Graduação – CONSINTER (Juruá Editorial).

[3] Mestre em Direito Processual Penal pela Pontifícia Universidade Católica de São Paulo. Doutorando pela Universidade Presbiteriana Mackenzie. Professor de Pós-Graduação da Universidade Presbiteriana Mackenzie e do Centro Universitário FIG-UNIMESP. Professor há 30 anos de Direito Penal e Direito Processual Penal. Integrou o Ministério Público do Estado de São Paulo por 28 anos, o Setor de Recurso Especial e Extraordinário da Procuradoria-Geral de Justiça, o Gabinete do Procurador-Geral de Justiça como coordenador do Centro de Apoio às Promotorias Criminais do Estado de São Paulo. Oficiou na Escola Superior do Ministério Público, na qual é professor. Aposentou-se em 3 de março de 2020, passando a advogar na área penal e no campo da improbidade administrativa.

(Lei 11.343/06), na Lei de Lavagem de Dinheiro (Lei 9.613/98) e no Estatuto da Criança e do Adolescente (Lei 8069/90), seja na forma física ou virtual.

Palavras-chave: Tecnologia; Infiltração; Organização criminosa; Criminalidade virtual.

Abstract: In this article, we are interested in highlighting and emphasizing constructive reflections on how the agent infiltration institute constitutes a fundamentally important tool in the field of producing elements of conviction that can lead to the accountability of crimes committed within the scope of Criminal Organizations (Law n.º 12.850/13), the Drug Law (Law n.º 11.343/06), the Money Laundering Law (Law n.º 9.613/98) and the Child and Adolescent Statute (Law n.º 8069/90), either in the physical or the virtual form.

Keywords: Technology; Infiltration; Criminal organization; Cybercrime.

1. Dimensão tecnológica da pós-modernidade[4]

Na pós-modernidade, constatam-se mudanças qualitativas que exigem uma reformulação dos esquemas teóricos com os quais se apreendem e transmitem os fenômenos jurídicos[5] e a atuação estatal, descobrindo novos horizontes de análise.

Sob esse prisma, pode-se afirmar que a teoria política e jurídica enfrenta atualmente uma crise de legitimidade, já que as novas condições institucionais e culturais no cenário sócio-político contemporâneo tornaram obsoletos os fundamentos do direito e a eficácia do agir político-administrativo. Dentre o que Hespanha[6] denominou com acerto, "... não se pode ignorar que estamos hoje perante um direito realmente diferente daquele para o qual foi construída a dogmática jurídica corrente".

Com efeito, face ao descompasso entre a realidade contemporânea e o instrumental jurídico-político criado para os séculos XIX e XX, surge a necessidade de refletir sobre como o direito penal enfrentará os novos desafios.

---

[4] Tópico fundamentado na obra *Transparência, Compliance e Práticas Anticorrupção na Administração Pública* de Ana Flávia Messa (Editora Almedina, 2019).

[5] "...o Direito, entre as outras ciências sociais, tem o caráter distintivo do ser, como a língua, não só parte integrante mas também espelho integral da vida social" (Gabriel Tarde, *Les Transformations du Droit*, Paris, Berg, 1994).

[6] Antônio Manuel Hespanha, *Pluralismo Jurídico e Direito Democrático*, São Paulo, Annablume Editora, 2013.

Na sociedade atual do século XXI[7], afigura-se com nitidez um ambiente de riscos, incertezas[8] e mudanças significativas, *inclusive* de paradigmas[9] construídos pela modernidade ocidental[10], trazendo novos ares em sua organização e valores, com repercussão imediata no âmbito do Direito, provocando reflexões e a necessidade de posturas novas diante de opções e variações num contexto de complexidade e dinamicidade.

Após um período caracterizado na crença do progresso e nos ideais iluministas, vive-se a partir da segunda metade do século XX numa condição histórica pós-moderna[11] de incertezas e riscos, com a desconstrução de princípios e valores construídos na modernidade e ausência de projeto do futuro. A realidade atual é regida por uma narrativa do inconstante[12] combinada com a evolução tecno-

---

7 "O século XXI será recordado na História da Humanidade como o século da mudança, do perigo iminente, do 'choque' das civilizações, da insegurança colectiva, da desconfiança do 'outro', das injustiças praticadas, da Guerra do Iraque e, principalmente, dos trágicos atentados terroristas ocorridos a 11 de setembro de 2001, nos Estados Unidos, a 11 de março de 2004, em Espanha, e a 7 de julho de 2005, em Londres." (José Noronha Rodrigues, «A Política Exterior e de Segurança Comum», *Scientia Ivridica. Revista de Direito Comparado Português e Brasileiro*, Tomo LVIII, n.º 317, janeiro/março 2009, Universidade do Minho, Portugal).

8 "Científico é o saber que se sabe precário, que não se julga absoluto, que sabe ter de expor com plausibilidade a fundamentação de tudo que se afirma. Leis científicas, por definição, são temporárias. Serão refutadas. A refutação só prova que determinadas teses foram científicas enquanto foram críveis, plausíveis, para nós". (Menelick de Carvalho Netto e Guilherme Scotti, *Os direitos fundamentais e a (in) certeza do direito: a produtividade das tensões principiológicas e a superação do sistema de regras*, Belo Horizonte, Fórum, 2011).

9 Paradigmas são instrumentos de compreensão da realidade, gerados num contexto histórico, científico e social, que possibilitam previsibilidade no sentido de funcionamento e planejamento da vida das pessoas em sociedade. Os paradigmas jurídicos são construções teóricas estruturantes que funcionam como padrão ou modelo ordenador das relações sociais. Com a evolução e as novas exigências, os paradigmas construídos transformam-se em insatisfações teóricas, pois o pensamento jurídico tem por finalidade reduzir a incerteza do direito. A conscientização e a concretização dos paradigmas jurídicos permitem a compreensão da realidade e do sistema jurídico, gerando a possibilidade de análise crítica com debates e sugestões, características de um processo evolutivo. É caminhar de um conhecimento de regulação para um conhecimento por emancipação.

10 Eduardo Carlos Bianca Bittar, «O direito na pós modernidade», *Revista Sequência*, n.º 57, dezembro 2008, pp. 131-152.

11 "Na noção de uma não-história é que o pensamento pós-moderno procura se estabelecer enquanto ruptura com o moderno." (Philadelpho Menezes, *A Crise do Passado*, São Paulo, Experimento, 1994); "O pós-moderno sem dúvida traz ambiguidades. É isso que ele propõe: **a prudência como método, a ironia como crítica, o fragmento como base e o descontínuo como limite** [...]" (Nicolau Sevcenko, *O enigma pós-moderno*, in Roberto Cardoso de Oliveira (org.), *Pós-modernidade*, Campinas-SP, Editora da UNICAMP, 1987).

12 "O rótulo genérico abriga a mistura de estilos, a descrença no poder absoluto da razão, o desprestígio do Estado. A era da velocidade. A imagem acima do conteúdo. O efêmero e o volátil parecem derrotar o permanente e o essencial. Vive-se a angústia do que não pode ser e a perplexidade de um tempo sem verdades seguras. Uma época aparentemente pós-tudo: pós-marxista, pós-kelseniana, pós-freudiana." (João Maurício Adeodato, *Ética & Retórica. Para uma teoria da dogmática jurídica*, São Paulo, Saraiva, 2009, p. 353).

lógica, a revolução digital e a globalização, no contexto de transição[13] e busca de nova estrutura social.

Dentre as mudanças ocorridas no cenário jurídico nos últimos tempos, a atuação do Estado Garantidor[14], a emergência de uma quinta[15] ou até sexta[16] geração dos direitos fundamentais, a globalização, a constitucionalização dos ramos do direito, a valorização dos direitos fundamentais, destaca-se o desenvolvimento das tecnologias de informação e comunicação[17].

O desenvolvimento tecnológico fazendo parte das dinâmicas sociais, bastante peculiar à perspectiva do progresso técnico, é possível afirmar, com a chegada dos computadores, e principalmente com a internet, que estamos vivendo numa realidade em que o fluxo de mensagens e imagens entre as redes passou a ser o ingrediente básico nas relações sociais, revelando a configuração de uma sociedade tecnológica marcada pelo avanço da tecnologia de informação, uma verdadeira sociedade de informação. Desde os anos 90 estamos a viver numa era da digitalização de informações e uma automatização das indústrias.

Assim como smartphones e redes sociais oferecem uma conectividade muito além de qualquer coisa que poderíamos imaginar, os robôs estão começando a demonstrar capacidades físicas, Inteligência Artificial (IA) e habilidades cognitivas muito acima de nossas expectativas.

---

[13] "O mundo é 'um' em certo sentido, mas radicalmente cindido por desigualdades de poder em outro. E um dos traços mais característicos da modernidade é a descoberta de que o desenvolvimento do conhecimento empírico não nos permite, por si mesmo, decidir entre diferentes posições de valor" (Anthony Giddens, *As Conseqüências da Modernidade*, São Paulo: Edunesp, 1991).

[14] "...há quem fale de Estado 'Pós-Social', visto que o Estado deixa de ser o Estado Providência (o Estado Social de Serviço Público) e, sem regressar ao Estado Liberal, se transforma, nas áreas econômicas e sociais num Estado de Garantia (ou 'Estado Garantidor') que regula, orienta, incentiva as atividades privadas, designadamente e com especial intensidade aquelas que prosseguem interesses gerais ou colectivos." (José Carlos Vieira de Andrade, *Lições de Direito Administrativo*, Coimbra, Coimbra Editora, 2011, p. 22).

[15] Paulo Bonavides "destaca a paz como um direito de quinta geração que legitima o estabelecimento da ordem, da liberdade e do bem comum na convivência dos povos. Segundo ele, a concepção da paz no âmbito da normatividade jurídica onfigura um dos mais notáveis progressos já alcançados pela teoria dos direitos fundamentais" (Paulo Bonavides, «O direito à paz como direito fundamental da quinta geração», *Revista Interesse Público*, Belo Horizonte, Ed. Fórum, 1999, v. 8, n.º 40, novembro/dezembro 2006). Outros defendem que a biotecnologia e a informática fazem parte dos direitos de quinta geração (Auricelia do Nascimento Melo, *Liberdade de expressão: um direito fundamental na concretização da democracia*, Fortaleza, Premius, 2009).

[16] Zulmar Fachin e Deise Marcelino da Silva, *Acesso à água potável: direito fundamental de sexta geração*, São Paulo, Millennium editora, 2010, p. 74.

[17] José Antonio Dominguez Luis, «El derecho de información administrativa: información documentada y transparencia administrativa», *Civitas: Revista Española de Derecho Administrativo*, Madrid, n. 88, outubro/dezembro 1995.

2. Tecnologia e sociedade: sociedade de informação[18]

A tecnologia é parte integrante da vida do homem e da sociedade, funcionando como ferramenta para o desenvolvimento da civilização. Insere-se num processo histórico não linear, atua como canal de expressão da cultura das sociedades e serve como instrumento transformador das formações sociais[19].

Fala-se em interação entre sociedade e tecnologia, como um processo impreciso, e de conteúdo heterogêneo, associado à determinação das técnicas de que dispõe um grupo social em qualquer fase histórica de seu desenvolvimento, e ao surgimento de comportamentos, valores e atitudes adaptáveis aos estágios evolutivos referentes aos momentos tecnológicos[20].

Fator de organização social, instrumental de produtividade e/ou competitividade, aplicação de conhecimentos ou atividade humana em que se busca a solução de problemas práticos, a tecnologia exerce influência decisiva na sociedade, seja trazendo benefícios à humanidade com o conforto proporcionado pelos diver-

---

[18] Tópico fundamentado na obra *Transparência, Compliance e Práticas Anticorrupção na Administração Pública* de Ana Flávia Messa (*cit.*).

[19] Milton Vargas, *Para uma filosofia da tecnologia*, São Paulo, Alfa Omega, 1994; Glaucia da Silva Brito, *Educação e Novas Tecnologias: um re-pensar*, Curitiba, Ibpex, 2008; Steven Johnson, *Cultura da interface: como o computador transforma nossa maneira de criar e comunicar*, Rio de Janeiro, Jorge Zahar, 2001; Álvaro Vieira Pinto, *O conceito de tecnologia*, Rio de Janeiro, Contraponto, v. 1, 2005, p. 20; "o valor da tecnologia não está nela em si mesma, mas depende do uso que fazemos dela". (Juliana Côrrea, «Novas tecnologias de informação e da comunicação: novas tecnologias de ensino e aprendizagem», in Carla Viana Coscarelli (org.), *Novas tecnologias, novos textos, novas formas de pensar*, Belo Horizonte, Autentica, 2002); Tereza Fachada Levy Cardoso, «Sociedade e Desenvolvimento Tecnológico: Uma Abordagem Histórica», in Mírian P. S. Zippin Grinspun (org.), *Educação Tecnológica: Desafios e Pespectivas*, São Paulo, Cortez, 2001; Estéfano Vizconde Veraszto, *Projeto Teckids: Educação Tecnológica no Ensino Fundamental*, Dissertação de Mestrado, Campinas, Faculdade de Educação, UNICAMP, 2004.

[20] "As tecnologias são produzidas e apropriadas de formas diferenciadas, a partir de dinâmicos processos socioeconômicos, culturais e políticos específicos. Uma tecnologia influencia fenômenos sociais e é marcada por eles, em um complexo movimento histórico de reciprocidades, usos, inovações, desvirtuamentos e disputas" [Gilberto Ribeiro De Mello, *Estudos de Prática de Governança Eletrônica: instrumento de controladoria para tomada de decisões na gestão dos Estados Brasileiros*, São Paulo, USP, 2009, 187 f., Tese (Doutorado em Ciências Contábeis) – Programa de Pós-Graduação em Ciências Contábeis, Faculdade de Economia, Administração e Contabilidade, Universidade São Paulo, São Paulo, 2009].

sos aparatos e dispositivos técnicos, seja com os riscos da evolução tecnológica resultante em lucros, interesses e diversas questões sociais, éticas e políticas[21].

É neste contexto do progresso tecnológico e do seu impacto social que na história da humanidade, desde o início da civilização, é possível detectar movimentos ou eras tecnológicas, ou seja, épocas na evolução histórico-social do homem marcadas pelo predomínio de um tipo de tecnologia[22]. O desenvolvimento tecnológico da humanidade pode ser classificado em quatro eras: industrial, elétrica, eletrônica e da informação.

A sociedade de informação[23] foi introduzida como paradigma de sociedade a partir das décadas de 60/70 do século passado, difundindo-se no final do século XX e, no processo, adquirindo características de uma sociedade em que as tecnologias de informação e comunicação têm alta penetrabilidade e a interatividade passa a ser o ingrediente básico das comunicações. Essa inovada designação com que se identifica uma sociedade "pós-industrial" adquire um sentido próprio no campo da organização geopolítica, por apontar o surgimento de um novo paradigma técnico-social onde a informação tornou-se recurso estratégico em todos os setores da atividade humana[24].

No contexto da sociedade de informação, os avanços da microeletrônica permitiram o desenvolvimento das tecnologias de informação e comunicação e o surgimento da era eletrônica, fatores que condicionam a exigência de um momen-

---

[21] Gerd Schienstock, «Technology policy in the process of change. Changing paradigms in research and technology policy?», in Georg Aichholzer e Gerd Schienstock (eds.), *Technology Policy. Towards an Integration of Social and Ecological Concerns*, Vol. 52 in the series de Gruyter Studies in Organization, 1994; Brian Wynne, «Redefining the Issues of Risk and Public Acceptance», *Futures*, February 1983; Mario Bunge, *Treatise on basic philosophy, v.7: Philosophy of science and technology*, Dordrecht, Reidel, 1985; Carl Mitcham, *Thinking through technology. The path between engineering and philosophy*, Chicago, The University of Chicago Press, 1994; Arnold Pacey, *The Culture of Technology*, Cambridge, MA, MIT Press, 1983; Marília Gomes de Carvalho, «Tecnologia e Sociedade», in João A. S. L. Bastos (org.), *Tecnologia e Interação*, Coletânea "Educação e Tecnologia", PPGTE-CEFET, Curitiba, CEFET-PR, 1998, p. 01; Walter Antonio Bazzo, *Ciência, Tecnologia e Sociedade: e o contexto da educação tecnológica*, Florianópolis, Ed. da UFSC, 1998; Amílcar Herrera *et al.*, *Las Nuevas Tecnologías y el Futuro de América Latina*, Siglo XXI, México, 1994; Martin Heidegger, *Introdução à Metafísica*, São Paulo, Piaget, 1987.

[22] José Ortega y Gasset, *Meditação da técnica*, Rio de Janeiro, Livro Ibero Americano Limitada, 1963.

[23] A sociedade de informação pode ser vista como uma revolução da informação ocorrida na história da humanidade após a invenção da escrita, livro escrito e impressão, ou como paradigma construído em função da dependência da tecnologia e da ciência, como sequência conceitual ao longo do eixo da produção e dos tipos de conhecimento utilizados (Daniel Bell, *O advento da Sociedade Pós-Industrial: uma tentativa de previsão social*, trad.: Heloysa de Lima Dantas, São Paulo, Editora Cultrix, 1973, p. 25; Krishan Kumar, *Da Sociedade Pós-Industrial à Pós-Moderna: Novas Teorias sobre o Mundo Contemporâneo*, Rio de Janeiro, Jorge Zahar Editor, 1997, p. 21).

[24] José de Faria da Costa, O Papel do Provedor de Justiça e o acesso à Informação Pública, disponível em: https://www.provedor-jus.pt/documentos/O_papel_do_Provedor_de_Justica_e_o_acesso_a_Informacao_Publica-10_11_15_Montevideu.pdf [acesso em 10/01/2016].

to histórico-cultural mais aberto e potencializado pela difusão, disseminação e transmissão de informações para todos e por todos[25].

Na era eletrônica, ancorada nas novas tecnologias digitais, surge um novo ambiente de informação e comunicação, com transmissão global, velocidade ímpar e subversão dos fatores de tempo e espaço, que propicia novas formas de sociabilidade, influenciando no relacionamento entre o público e o privado. É o ciberespaço[26], termo citado por William Gibson no romance *Neuromancer*, entendido como um espaço de comunicação aberta que surge da interconexão mundial de computadores.

A era eletrônica, especialmente com o surgimento da internet, propicia a invasão no corpo da vida comunitária de uma nova identidade social baseada na ampliação da informação como papel de moeda globalizante, criando a *sociedade em rede* e uma *cidadania eletrônica* ou *cibercidadania*[27].

---

[25] "A capacidade de criar, difundir e usar conhecimento e informação é cada vez mais o principal fator para o crescimento econômico e a melhoria da qualidade de vida" (OCDE, OCDE SCIENCE, *Technology and Industry Scoreboard 1999*, Benchmarking Knowledge-based Economies, OCDE, 1999); Eric Hobsbawm, *O Novo Século (Entrevista a Antônio Polito)*, São Paulo, Companhia das Letras, 2000.

[26] Parece-nos útil delimitar o âmbito do ciberespaço em dois aspectos: a) aspecto subjetivo: ele designa os seres que navegam e alimentam o universo das redes digitais; dentro do aspecto subjetivo do ciberespaço, os seres que se utilizam desse espaço se identificam como identidades nômades sem corpo, sem simultaneidade de presença, apenas em solidão coletiva. Nesta linha, há um universo complexo e dinâmico de interações de sujeitos que transitam no ambiente virtual com discursos, práticas e imagens que passam a influenciar a conformação social; b) aspecto objetivo: ele designa o conteúdo que abrange um universo oceânico de informações com base numa infraestrutura material da comunicação digital. Ao lado da socialização, o ambiente virtual proporciona intercâmbio intenso de informações e imagens, especialmente com o advento da internet e o desenvolvimento da web (Pierre Levy, *Cibercultura*, São Paulo: Editora 34, 1999; René Lysloff, «Musical life in Softcity: in internet ethnography», in René Lysloff e Leslie Gay (orgs.), *musica and technoculture*, Middletown, Wesleyan University Press; Anthony Giddens, *Modernidade e identidade*, trad.: Plínio Dentizien, Rio de Janeiro, Jorge Zahar, 2002).

[27] Alketa Peci, Octavio Penna Pieranti e Silvia Rodrigues, «Governança e New Public Management: convergências e contradições no contexto brasileiro», in *XXXI Encontro da ANPAD*, Rio de Janeiro, 2007; Alvin Toffler, *A terceira onda*, Rio de Janeiro, Record, 1997; Luiz Akutsu e José Antonio Gomes de Pinho, «Sociedade da informação, accountability, e democracia delegada: investigação em portais de governo no Brasil», *Revista de Administração Pública*, Rio de Janeiro, v. 36, n. 5, setembro/outubro 2002, pp. 723-745; Fernando do Nascimento Lock, *Transparência da gestão municipal através das informações contábeis divulgadas na internet*, 111f. (Dissertação – Mestrado em Gestão Pública para o Desenvolvimento do Nordeste) – Universidade Federal de Pernambuco, Recife, 2003; Jorge José Baros de Santana Junior, *Transparência fiscal eletrônica: uma análise dos níveis de transparência apresentados nos sites dos poderes e órgãos dos Estados e do Distrito Federal do Brasil*, 176 f. (Dissertação – Mestrado em Ciências Contábeis) – Programa Multinstitucional e Inter-regional de Pós-graduação em Ciências Contábeis, Recife, 2008; Manuel Castells, *A sociedade em rede*, São Paulo, Paz e Terra, 1999.

3. Criminalidade virtual: o instituto da infiltração de agentes

Surge na realidade dos países uma sociedade de informação mediatizada e universalizada. Na década de 80, já ocorreram fraudes em caixas eletrônicos e cartões magnéticos. Já na década de 90 entramos no auge da convergência entre informática e telecomunicações e a generalização de serviços informáticos no cotidiano da sociedade.

É neste ambiente virtual ou ciberespaço, meio heterogêneo e transfronteiriço, que, a partir da digitalização da informação, com o potencial da interatividade, podemos perceber uma maior acessibilidade da informação à sociedade. Essa abordagem proporcionada pelas novas características e desenvolvimento das tecnologias de informação e comunicação, com a partilha fácil, veloz e em escala mundial de dados, reflete sobre toda a sociedade, *inclusive* na expressão da cidadania e na atuação da Administração Pública[16].

Na perspectiva da criminalidade, a sociedade de informação traz uma ampliação no universo de disseminação de informações, com novas e crescentes ameaças cibernéticas, colocando em risco a Administração Pública e a sociedade. Surge o criminoso virtual, especializado no cometimento de crimes digitais[28].

Fator agravante é a dificuldade na configuração do papel do direito no desenho normativo do ciberespaço. Cerca de duas décadas decorridas após a 'libertação' da internet, o desenvolvimento e a dimensão transnacional das redes electrónicas de comunicação continuam a suscitar a questão da regulação jurídica do espaço digital.

O desenvolvimento tecnológico é um dos fatores que faz surgir novos riscos, que adquirem dimensão social, com maiores impactos. Nesse sentido, a delinquência informática aparece configurada como um fenômeno social relacionado aos novos riscos. A criminalidade informática é apontada pela doutrina como ilícito complexo, decorrente da sociedade de risco. Neste contexto, surge a infiltração de agentes, como um dos meios operacionais para a prevenção e repressão de ações da criminalidade virtual.

A primeira aparição do tema deu-se no âmbito da Lei 9.034/95, que dispôs sobre a utilização de meios operacionais para a prevenção e repressão de ações praticadas por organizações criminosas, prevendo em seu art. 2.º, V, a "infiltração

---

[28] Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (Fabrízio Rosa, *Crimes de Informática*, Campinas, Bookseller, 2002).

por agentes de polícia ou de inteligência, em tarefas de investigação, constituída pelos órgãos especializados pertinentes, mediante circunstanciada autorização judicial"[29].

A Lei 9.034/95 ingressou no ordenamento jurídico trazendo certo desconforto no âmbito de sua aplicabilidade, pois ainda que se propusesse a estabelecer no introito os meios de repressão de ações praticadas por organizações criminosas, restou estabelecido no seu art. 1.º (texto original), que regularia meios de prova e procedimentos investigatórios que versassem sobre crime resultante de ações de **quadrilha ou bando**. Somente com a aprovação da Lei 10.217/01 alterou-se a redação do referido art. 1.º, permitindo-se a aplicação "sobre ilícitos decorrentes de ações praticadas por quadrilha ou bando ou organizações ou associações criminosas de qualquer tipo". Ainda assim, perdeu-se a oportunidade legislativa de se estabelecer conceito certo e determinado de organização criminosa.

Por sua vez, o Decreto Presidencial 5.015, de 12 de março de 2004, inseriu no sistema normativo a Convenção das Nações Unidas contra o Crime Organizado Transnacional, fixando o conceito de grupo criminoso organizado como sendo "grupo estruturado de três ou mais pessoas, existente há algum tempo e atuando concertadamente com o propósito de cometer uma ou mais infrações graves ou enunciadas na presente Convenção, com a intenção de obter, direta ou indiretamente, um benefício econômico ou outro benefício material"[30].

Passou, então, a persecução criminal pelos órgãos competentes a atuar no campo repressivo com base no conceito de organização criminosa trazido pelo referido decreto presidencial, entendendo-se majoritariamente, até aquele momento, que os contornos jurídicos de organização criminosa poderiam ser extraídos sem maiores dificuldades da Convenção das Nações Unidas sobre Crime Organizado, e incorporado no direito interno.

Entretanto, no Colendo Supremo Tribunal Fedral (C. STF), apreciando caso especificamente concreto, no qual utiliza o conceito dado pelo referido decreto, firmou-se entendimento de que o crime de quadrilha não se confundiria com organização criminosa, e que até aquele momento se encontrava sem definição jurídica no ordenamento pátrio[31].

---

[29] O referido instrumento somente foi inserido no texto original pela Lei 10.217/01, que adicionou o inciso V.

[30] Art. 2.º, "a", do Decreto Presidencial 5.015/2004.

[31] "TIPO PENAL – NORMATIZAÇÃO. A existência de tipo penal pressupõe lei em sentido formal e material. LAVAGEM DE DINHEIRO – LEI N.º 9.613/98 – CRIME ANTECEDENTE. A teor do disposto na Lei 9.613/98, há a necessidade de o valor em pecúnia envolvido na lavagem de dinheiro ter decorrido de uma das práticas delituosas nela referidas de modo exaustivo. LAVAGEM DE DINHEIRO – ORGANIZAÇÃO CRIMINOSA E QUADRILHA. O crime de quadrilha não se confunde com o de organização criminosa, até hoje sem definição na legislação pátria" (HC 96007, Rel. Marco Aurélio, 1.ª T., j. em 12/06/2012).

Com o advento da Lei 12.850/2013, passou-se a ter a inédita definição de organização criminosa como sendo "a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional"[32].

Além da incidência de aplicação da infiltração na hipótese de configuração de organização criminosa, tem-se também que se aplicará nas "infrações penais previstas em tratado ou convenção internacional quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente" (crimes à distância – internacionalidade), e em relação "às organizações terroristas, entendidas como aquelas voltadas para a prática dos atos de terrorismo legalmente definidos"[33].

E foi exatamente nessa *novel* legislação que se deu a regulamentação ordenada e específica do instituto da infiltração de agentes (arts. 3.º, VII, e 10 a 14, da Lei 12.850/13).

Veja-se que, embora o instituto da infiltração de agentes já estivesse previsto na Lei 11.343/06[34], não havia qualquer regulamentação concreta e específica sobre sua aplicabilidade.

Na sequência, a Lei 13.441, de 2017, estabeleceu a possibilidade de infiltração virtual de agentes de polícia na investigação de crimes contra a dignidade sexual de criança e de adolescente (Lei 8.069/90).

Ao final do relato histórico, tem-se que o denominado "pacote anticrime", veiculado pela Lei 13.964/19, inseriu no sistema normativo a infiltração virtual no âmbito da Lei 12.850/13 (organização criminosa), com a inclusão dos arts. 10-A a 10-D. A mesma Lei 13.964/2019 também incluiu o § 6.º ao art. 1.º da Lei 9.613/98, permitindo a infiltração de agentes para investigação de crime de lavagem de dinheiro, ainda que não haja organização criminosa.

Limita-se, pois, a incidência de aplicação do instituto de infiltração de agentes no campo das organizações criminosas (Lei 12.850/13), drogas (Lei 11.343/06), Estatuto da Criança e do Adolescente (Lei 8.069/90) e lavagem de dinheiro (Lei 9.613/98).

---

32 Art. 2.º, §1.º, da Lei 12.850/13.

33 Art. 1.º, §2.º, da Lei 12.850/13.

34 Art. 53. "Em qualquer fase da persecução criminal relativa aos crimes previstos nesta Lei, são permitidos, além dos previstos em lei, mediante autorização judicial e ouvido o Ministério Público, os seguintes procedimentos investigatórios: I - a infiltração por agentes de polícia, em tarefas de investigação, constituída pelos órgãos especializados pertinentes; (...)".

Tem-se, pois, na legislação, o instituto de infiltração de agentes no modo **físico** (no qual o agente infiltrado imerge pessoalmente, ou seja, fisicamente, no seio da organização criminosa) ou **virtual** (realizada através da internet, redes sociais, *chats*, grupos de mensagens etc., na qual o agente não se infiltra fisicamente entre os criminosos, mas sim por meio de um perfil falso na rede mundial de computadores).

4. Aspectos gerais da infiltração de agentes

4.1. *Conceito*

Passando-se ao estudo específico do instituto, tem-se como infiltração de agentes um **meio** (instrumento) de obtenção de **elementos de convicção** com o objetivo de propiciar a formação de convicção da autoridade policial e do membro do Ministério Público acerca de fatos tidos por criminosos.

Diz-se elementos de convicção, pois, nos termos do art. 155 do Código Penal, prova do ponto de vista técnico só pode assim ser considerada quando submetida ao contraditório e ampla defesa[35].

A Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo) conceitua infiltração de agentes como uma **técnica especial de investigação criminal** que tem por fim específico a obtenção da prova, "a fim de combater eficazmente a criminalidade organizada"[36].

"Por meio desta técnica especial, um agente policial (chamado de agente infiltrado) infiltra-se, física ou virtualmente, na organização criminosa, como se dela fosse membro, para buscar informações e colher elementos relevantes para apurar os fatos, como, por exemplo, saber quem são seus líderes, quais as tarefas executadas por cada um dos membros e as sedes utilizadas para os negócios escusos, entre outros"[37].

4.2. *Momento de aplicação*

O art. 10 da Lei 12.850/13 dá a entender pela possibilidade de utilização do instituto da infiltração de agentes em qualquer fase da persecução criminal. Com efeito, a Lei prevê, em seu art. 10, o uso do instrumento a requerimento do Mi-

---

[35] Art. 155. "O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas."

[36] Art. 20 da Convenção de Palermo, que se refere à vigilância eletrônica e às "operações de infiltração".

[37] Everton Luiz Zanella, *Infiltração de agentes e o combate ao crime organizado: análise do mecanismo probatório sob o enfoque da eficiência e do garantismo*, 2.ª ed., Curitiba, Juruá, 2020, p. 229.

nistério Público, exigindo-se manifestação do delegado de polícia quando requerido em sede de inquérito policial, extraindo-se, a *contrario sensu*, que, quando solicitada na fase judicial, não haveria necessidade de parecer da autoridade policial.

Trata-se, contudo, de questão bastante polêmica, que causa intensas divergências na doutrina, surgindo duas importantes correntes.

A primeira delas sustenta que a infiltração pode ocorrer em qualquer etapa da persecução. É a posição de Guilherme Nucci[38] e Renato Brasileiro de Lima[39]. Ela se baseia na leitura do art. 10 e reforça seu argumento a partir da leitura do art. 53, I, da Lei 11.343/2006, a qual permite, explicitamente, a infiltração de agentes "em qualquer fase da persecução penal", isto é, tanto na fase investigativa como na fase processual.

A segunda posição defende que o instituto da infiltração se limita à fase de investigação. São partidários desta tese Bittencourt e Busato[40]; Sanches e Pinto[41]; e Gonçalves e Baltazar Junior[42]. Esta corrente se ampara no art. 12, § 2.º, da Lei 12.850/2013, que estabelece: "os autos contendo as informações da operação de infiltração acompanharão a denúncia do Ministério Público". Ora, se os autos que formalizam a medida seguirão em conjunto à peça inicial acusatória, é porque necessariamente deve ser realizada na fase investigativa.

Adotamos neste artigo a segunda posição, ou seja, de que a infiltração de agentes se limita à fase investigativa. Primeiro, porque sua natureza é essencialmente investigatória. Segundo, porque ela é, expressamente, uma prova subsidiária às demais e não complementar (art. 10, § 2.º, da Lei). Neste aspecto, não seria razoável o Ministério Público oferecer denúncia com base em elementos colhidos no inquérito policial (os quais já foram suficientes para a ação penal) e, durante o processo, entender necessária a infiltração de agentes por ser a única forma de comprovar o crime. Ademais, se a infiltração de agentes fosse permitida na fase judicial, a partir de pedido do Ministério Público, seria necessário formar-se um incidente processual sigiloso (já que o sigilo da medida é indispensável para seu sucesso), o que, a nosso ver, desrespeitaria o contraditório

---

38 Guilherme de Souza Nucci, *Organização criminosa*, 2.ª ed., Rio de Janeiro, Forense, 2015, p. 86.

39 Renato Brasileiro de Lima, *Legislação especial criminal comentada*, 2.ª ed., Salvador, Juspodivm, 2014, p. 569.

40 Cezar Roberto Bittencourt e Paulo César Busato, *Comentários à Lei de Organização Criminosa: Lei 12.850/2013*, São Paulo, Saraiva, 2014. p. 162.

41 Rogério Sanches Cunha e Ronaldo Batista Pinto, *Crime organizado – comentários à nova lei sobre o crime organizado – Lei 12.850/2013*, Salvador, Juspodivm, 2014, p. 99.

42 Victor Eduardo Rios Gonçalves e José Paulo Baltazar Junior, *Legislação penal especial – esquematizado*, São Paulo, Saraiva, 2015, p. 712.

e a ampla defesa (pois a operação de infiltração de agentes – que pode perdurar meses – obviamente ocorreria sem o conhecimento da defesa técnica).

Com relação à infiltração virtual no âmbito da Lei 8.069/90 (Estatuto da Criança e do Adolescente), a Lei 13.441/2017 corrige o equívoco da Lei 12.850/2013 e expressamente autoriza o procedimento apenas na fase da persecução investigatória: "a infiltração de agentes de polícia na internet com o fim de **investigar** os **crimes** (...)."[43].

4.3. *Competência e legitimidade*

Trata-se de meio de obtenção de elementos de convicção **sujeito à reserva exclusiva da jurisdição**, não só porque sujeitou a implementação da pretensão à autorização judicial, bem como pela complexidade real do instituto de infiltrar agentes em organização criminosa, com os riscos inerentes da atuação.

Do ponto de vista de **competência**, não há qualquer observação específica quanto ao juízo natural para análise da medida de infiltração, podendo ser o magistrado identificado por intermédio do uso do critério de distribuição (quando houver mais de um juiz igualmente competente), como também por juízes que cuidam exclusivamente de medidas judiciais sujeitas à reserva da jurisdição no âmbito da persecução criminal investigatória, tendo-se como exemplo os juízes que integram o D.I.P.O[44].

E, sobre a fixação de juízes para atuação na fase da persecução criminal investigatória, o C. STF entendeu como constitucional esse modelo de divisão de tarefas. A propósito, "(...) há precedentes do STF que admitem a divisão de tarefas entre juízes que atuam na fase de inquérito e na fase da ação penal"[45].

Observamos que a Lei 13.964/2019 inseriu no sistema processual penal brasileiro o "juiz de garantias" (art. 3.º-B), o qual será competente para analisar a representação policial ou o requerimento ministerial de infiltração realizados na fase investigativa, porquanto se trata de um meio de obtenção de prova que restringe direitos fundamentais do investigado (art. 3.º-B, XI, "e"). Contudo, a implantação do juiz de garantias foi cautelarmente suspensa, por prazo indeterminado, pelo Colendo STF, em decisão liminar tomada nas ADINs 6.298, 6.299, 6.300 e 6.305.

Tem **legitimidade** para postular a medida de infiltração de agentes a autoridade policial e o membro do Ministério Público.

---

[43] Art. 190-A da Lei 8.069/90 – não negritado no original.

[44] Departamento de Inquéritos Policiais – situado no fórum criminal Complexo Judiciário Ministro Mário Guimarães, estabelecido no bairro da barra funda, capital de São Paulo.

[45] STF, HC 126536/ES, rel. Min. Teori Zavascki, j. em 1/3/2016.

Quando a lei fala em **autoridade policial**, deve se compreender como legitimado para postulação aquele que, dentro da musculatura policial brasileira[46], integra a polícia federal, ou a polícia civil dos Estados e do Distrito Federal, na qualidade de **delegado de polícia**[47].

4.4. *O agente infiltrado*

Na definição adequada de Renato Brasileiro de Lima, "o agente infiltrado é introduzido dissimuladamente em uma organização criminosa, passando a agir como um de seus integrantes, ocultando sua verdadeira identidade, com o objetivo precípuo de identificar fontes de prova e obter elementos de informação (...)"[48].

Há de ser feita uma distinção entre a condição agente de ***inteligência*** e agente ***infiltrado***. Na primeira hipótese, a atuação do agente está voltada para coleta de dados e informações com finalidade **preventiva** e estratégica; na segunda, a infiltração se dá com finalidade **repressiva**, com uso dos dados e informações para efeito concreto de levar a efeito a persecução criminal. A utilização de dados obtidos por agente de inteligência, para fim de persecução penal, não pode ser tida como válida, pois confunde-se com a atuação de agente de infiltrado que depende de autorização judicial[49].

Igualmente, não se pode confundir o agente infiltrado com o "agente policial disfarçado", figura criada pela Lei 13.964/2019, que a insere no corpo do Estatuto do Desarmamento e da Lei de drogas*:*

"Art. 17, § 2.º, da Lei 10.826/2003: Incorre na mesma pena quem vende ou entrega arma de fogo, acessório ou munição, sem autorização ou em desacordo com a determinação legal ou regulamentar, a agente policial disfarçado, quando presentes elementos probatórios razoáveis de conduta criminal preexistente".

---

[46] Art. 144. "A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: I - polícia federal; II - polícia rodoviária federal; III - polícia ferroviária federal; IV - polícias civis; V - polícias militares e corpos de bombeiros militares; VI - polícias penais federal, estaduais e distrital".

[47] Art. 2.º, § 1.º, da Lei 12.830/13 – "Ao delegado de polícia, na qualidade de autoridade policial, cabe a condução da investigação criminal por meio de inquérito policial ou outro procedimento previsto em lei, que tem como objetivo a apuração das circunstâncias, da materialidade e da autoria das infrações penais".

[48] Renato Brasileiro de Lima, *Legislação especial criminal comentada*, 4.ª ed., Salvador, Juspodivm, 2016, p. 571.

[49] "Habeas corpus. 2. Infiltração de agente policial e distinção com agente de inteligência. 3. Provas colhidas por agente inicialmente designado para tarefas de inteligência e prevenção genérica. Contudo, no curso da referida atribuição, houve atuação de investigação concreta e infiltração de agente em grupo determinado, por meio de atos disfarçados para obtenção da confiança dos investigados. 4. Caraterização de agente infiltrado, que pressupõe prévia autorização judicial, conforme o art. 10 da Lei 12.850/13. 5. Prejuízo demostrado pela utilização das declarações do agente infiltrado na sentença condenatória. 6. Viabilidade da cognição em sede de habeas corpus. 7. Ordem parcialmente concedida para declarar a ilicitude dos atos da infiltração e dos depoimentos prestados. Nulidade da sentença condenatória e desentranhamento de eventuais provas contaminadas por derivação" (STF, HC 147837, Rel. Min. Gilmar Mendes, 2ª T., j. em 26/02/2019).

"Art. 18, parágrafo único, da mesma Lei: Incorre na mesma pena quem vende ou entrega arma de fogo, acessório ou munição, em operação de importação, sem autorização da autoridade competente, a agente policial disfarçado, quando presentes elementos probatórios razoáveis de conduta criminal preexistente."

"Art. 33, § 1.º, IV, da Lei 11.343/2006: vende ou entrega drogas ou matéria-prima, insumo ou produto químico destinado à preparação de drogas, sem autorização ou em desacordo com a determinação legal ou regulamentar, a agente policial disfarçado, quando presentes elementos probatórios razoáveis de conduta criminal preexistente".

Destarte, havendo conduta criminosa pré-existente – tráfico de armas e tráfico de drogas –, o indivíduo que vender ou entregar arma ou droga ao agente policial disfarçado será penalmente responsabilizado pelo ato. Trata-se de uma figura semelhante ao "**agente encoberto**", previsto em ordenamentos jurídicos de países estrangeiros[50]. É um agente que não chega a se infiltrar, não tem envolvimento prévio[51] e não ganha a confiança da organização, praticando apenas alguns atos investigativos. Nas palavras de Joaquim Delgado, o "agente meramente encoberto" é aquele que, nas suas atividades rotineiras de policial, investiga um determinado crime mediante a ocultação de sua condição (de policial), mas sem se utilizar de técnicas de infiltração[52].

O referido professor espanhol distingue o "agente meramente encoberto" (encoberto ou disfarçado) do "agente encoberto infiltrado" (agente infiltrado), que é aquele que imerge na estrutura de grandes organizações criminosas e que passa a conviver em meio aos criminosos, praticando as mesmas atividades dos investigados, podendo fazer a infiltração sem ou com identidade falsa (este último o autor chama de "agente encoberto infiltrado com identidade falsa", destinado às infiltrações mais complexas)[53].

O agente policial disfarçado é definido por Rogério Sanches Cunha, Ronaldo Batista Pinto e Renee do Ó Souza como: "Aquele que, ocultando sua real identida-

---

[50] A legislação portuguesa estabelece que "consideram-se acções encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro actuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade" (Lei 101/2001, art. 1.º, n.º 2). O site da Procuradoria-Geral Distrital de Lisboa, nas notas de comentários ao artigo, cita entendimento jurisprudencial que diferencia o agente encoberto do infiltrado, sendo este último "o agente de polícia ou agente por si comandado que se insinua nos meios em que se praticam crimes, com ocultação da sua qualidade, de modo a ganhar a confiança dos criminosos, com vista a obter informações e provas contra eles" (disponível em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=89&tabela=leis, acesso em 21/04/2023).

[51] Neste sentido, as lições do autor português Manuel Augusto Alves Meires, *O Regime das Provas Obtidas pelo Agente Provocador em Processo Penal*, Coimbra, Almedina, 1999, pp. 163-164.

[52] Joaquin Delgado, *Criminalidad Organizada*, J.M. Bosch Editor, 2001, pp. 46-48.

[53] *Ibidem*.

de, posiciona-se com aparência de um cidadão comum (não chega a infiltrar-se no grupo criminoso) e, partir disso, coleta elementos que indiquem a conduta criminosa preexistente do sujeito ativo. O agente disfarçado ora em estudo não se insere no seio do ambiente criminoso e tampouco macula a voluntariedade na conduta delitiva do autor dos fatos"[54].

4.5. *Direitos do agente infiltrado*

São direitos do infiltrado "recusar ou fazer cessar a atuação infiltrada, ter sua identidade alterada (Lei n.º 9.807, de 13 de julho de 1999), usufruir das medidas de proteção a testemunhas, ter seu nome, sua qualificação, sua imagem, sua voz e demais informações pessoais preservadas durante a investigação e o processo criminal, salvo se houver decisão judicial em contrário, e não ter sua identidade revelada, nem ser fotografado ou filmado pelos meios de comunicação, sem sua prévia autorização por escrito"[55].

Deferida a infiltração, e estabelecidos os limites judicialmente, o agente poderá ter de praticar crimes quando inexigível conduta diversa, respondendo pelos excessos praticados[56].

5. Infiltração virtual de agentes

5.1. *Infiltração virtual no Estatuto da Criança e Adolescente*

A Lei 13.441/2017 inseriu os arts. 190-A, 190-B, 190-C, 190-D e 190-E à Lei 8.069/1990 (Estatuto da Criança e do Adolescente), prevendo a "infiltração de agentes de polícia na internet, com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente".

Temos, assim, a possibilidade de que um policial oculte sua real identidade e ingresse (com perfil falso) em ambientes cibernéticos, com o objetivo de investigar delitos contra a dignidade sexual de criança e adolescente, obtendo provas de materialidade e autoria.

A infiltração virtual é prevista, igualmente, no ordenamento jurídico português, mais precisamente no art. 19 da Lei 109/2009, para fins de se investigar os *cibercrimes* por intermédio das ações encobertas (Lei 101/2001, alterada pelas Leis 60/2013 e 61/2015), aplicando-se, no que couber, "as regras previstas para a intercepção de comunicações" (art. 19, item 2)[57].

---

[54] *Crime organizado: comentários à Lei 12.850/2013*, 5.ª ed., 2020, p. 268.

[55] Art. 14 da Lei 12.850/13.

[56] Art. 13 da Lei 12.85013.

[57] http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis, acesso em 15/05/2020.

"Assim, tanto lá como cá temos a previsão de um mecanismo probatório que miscigenou a infiltração de agentes com a captação de dados telemáticos, já que regulamenta o ingresso virtual de um policial em meio a criminosos (como regra 'pedófilos'), ocultando sua real condição (de policial) através da criação de um falso perfil (*fake*)[58], para, com isso, obter a necessária prova dos delitos investigados, a qual será colhida a partir da interceptação do fluxo de comunicações em sistemas de informática e telemática"[59].

5.2. *Infiltração virtual na Lei do Crime Organizado*

A Lei 13.964/2019 ("pacote anticrime") acrescentou a infiltração virtual de agentes na Lei 12.850/2013, por meio dos arts. 10-A, 10-B, 10-C e 10-D. Tais dispositivos legais correspondem a um misto daquilo que já era previsto para a infiltração física (art. 10 da Lei 12.850/13) com as disposições atinentes à infiltração virtual prevista no Estatuto da Criança e do Adolescente.

O art. 10-A estabelece que será admitida a ação de agentes de polícia infiltrados na internet, obedecidos os requisitos do *caput* do art. 10, "com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas".

A finalidade será a investigação do crime de organização criminosa (art. 2.º da Lei 12.850/2013) e também os crimes praticados pela organização.

"Os requisitos trazidos pelo próprio art. 10-A são: demonstração da necessidade da medida (elemento de proporcionalidade); indicação do alcance das tarefas policiais (trata-se de um plano operacional da infiltração virtual[60]); indicação dos nomes ou apelidos das pessoas investigadas (pelo menos aqueles que já forem de conhecimento quando do momento do pleito); e, se possível, os dados

---

[58] Importante observar que o artigo 190-D da Lei 8.069/1990, acrescentado pela Lei 13.441/2017, permite que a identidade fictícia seja, com autorização judicial, registrada em bancos de dados públicos. Esta permissão legal é de grande relevância para dar maior credibilidade e segurança ao disfarce, já que o perfil falso poderia ser facilmente descoberto por criminosos que tenham um maior acesso a servidores públicos responsáveis pelos bancos de dados oficiais.

[59] Everton Luiz Zanella, *Infiltração de agentes e o combate ao crime organizado*…, *cit.*, p. 272.

[60] O plano operacional de uma infiltração virtual não precisa ser tão detalhado quanto o de uma infiltração física. Isto porque, na infiltração pela internet, o policial infiltrado não estará submetido a um constante perigo de vida, pois não estará na companhia real ("*in loco*") dos criminosos.

de conexão ou cadastrais[61] que permitam a identificação das pessoas que serão alvo da diligência"[62].

A infiltração virtual pressupõe a existência de indícios de infração penal de que trata o art. 1.º da lei do crime organizado, bem como a impossibilidade de obtenção de provas por outros meios. Embora o art. 10-A, § 3.º, se reporte ao art. 1.º, o tipo penal de organização criminosa está no art. 2.º. De qualquer maneira, a *ratio* da norma é permitir a infiltração no afã de investigar e obter prova de delitos cometidos por organização criminosa.

6. O procedimento de infiltração (física e virtual)

O procedimento de infiltração contará com reserva de **sigilo**[63] e tramitará em expediente separado de qualquer outra medida processual, ou dos autos principais, e o acesso restará restrito ao magistrado, ao Ministério Público e ao delegado de polícia.

A **violação** do **sigilo** importará na responsabilização criminal pelo crime previsto no art. 20 da Lei 12.850/2013[64].

Tratando-se de diligências em andamento, inexiste a possibilidade de acesso pela defesa, nos exatos termos da Súmula Vinculante n.º 14, do C. STF[65].

Na hipótese de representação policial, o Ministério Público deverá ser ouvido antes da deliberação acerca da medida.

Para deliberação positiva da infiltração, devem ser apontados indícios da **ocorrência de infração penal** (*fumus comissi delicti*) que permita o deferimento da medida, devendo ser observado o caráter subsidiário[66] do instituto, posto que incabível o deferimento se houver outra maneira de obtenção dos elementos.

---

[61] Os conceitos de dados de conexão e cadastrais também foram objeto da Lei 8.069/1990, com redação da Lei 13.441/2017. A Lei 13.850/2013, com o texto atualizado pelo pacote anticrime, também trouxe um conceito no art. 10-A, § 1.º, incisos I e II. *In verbis:* I - **dados de conexão**: informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão; II - **dados cadastrais**: informações referentes a nome e endereço de assinante ou de usuário autenticado para a conexão (a quem foi atribuído o endereço de IP ou código de acesso no momento da conexão).

[62] Everton Luiz Zanella, *Infiltração de agentes e o combate ao crime organizado*…, *cit.*, p. 278.

[63] Art. 10 da Lei 12.850/13.

[64] Art. 20. "Descumprir determinação de sigilo das investigações que envolvam a ação controlada e a infiltração de agentes: Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa".

[65] "É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, **já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária**, digam respeito ao exercício do direito de defesa" (negrito não constante do original).

[66] Art. 10, § 2.º, da Lei 12.850/13: "Será admitida a infiltração se houver indícios de infração penal de que trata o art. 1.º e se a prova não puder ser produzida por outros meios disponíveis".

A postulação policial ou do Ministério Público deverá apontar as **razões** pelas quais os elementos pretendidos não podem ser obtidos de forma diversa e deverão contar com "a demonstração da necessidade da medida, o alcance das tarefas dos agentes e, quando possível, os nomes ou apelidos das pessoas investigadas e o local da infiltração"[67].

A decisão judicial deverá ser "precedida de circunstanciada, motivada e sigilosa autorização judicial, que estabelecerá seus limites"[68], e se deferida será estabelecido o prazo de até 6 meses, permitindo-se prorrogações diante da comprovação da necessidade[69].

Com relação à **motivação circunstanciada**, imperioso destacar, por analogia, a "imprestabilidade do ato decisório que, desprovido de base empírica idônea, resume-se a fórmulas estereotipadas consubstanciadas em textos padronizados revestidos de conteúdo genérico – ausência de informações resultantes de prorrogações de interceptações telefônicas autorizadas por decisão destituída de fundamento substancial – precedentes"[70].

No âmbito da Lei 11.343/06 (drogas), observa-se a ausência de qualquer tipo de regulamentação expressa de aplicação do instituto da infiltração de agentes, devendo ser seguido o procedimento estabelecido na Lei 12.850/13, seja do ponto de vista físico ou virtual[71].

Recebida a denúncia ofertada pelo Ministério Público, dar-se-á o início da ação penal com o objetivo de avaliar a responsabilidade criminal do agente, seguindo-se o procedimento comum ordinário ou especial da Lei de Drogas.

Os elementos informativos obtidos *inaldita altera pars* decorrentes da infiltração de agentes (física ou digital) acompanharão a denúncia do Ministério Público, disponibilizando-se todo o conteúdo para fins de exercícios da ampla defesa e do contraditório diferido ou postergado (art. 5.º, inciso LV, da Constituição Federal do Brasil de 1988).

Importante anotar que, com a globalização e a evolução da tecnologia da informação, as infrações penais passaram a tomar conta da internet sob diversas formas.

---

[67] Art. 11 da Lei 12.850/13.

[68] Art. 10 da Lei 12.850/13.

[69] Art. 10, §3.º, da Lei 12.850/13.

[70] HC 129646 AgR, Rel. Celso de Mello, 2.ª T., j. em 03/10/2020.

[71] STJ, HC 190.426/MS, Rel. Min. Og Fernandes, 6.ª T., j. em 17/03/2011.

A internet é o conjunto de redes de computadores que, espalhadas por todas as regiões do mundo, consegue trocar dados e mensagens utilizando um ritual acessível a todos.

Observou-se, com o tempo, que cada vez mais foram sendo veiculados crimes de diversas ordens, *inclusive* contra crianças, especialmente no âmbito da dignidade sexual.

Dada a complexidade dessas investigações, a infiltração de agentes passou a ser permitida no âmbito da rede mundial de computadores. Assim, "a infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei[72] e nos arts. 154-A[73], 217-A[74], 218[75], 218-A[76] e 218-B[77] do Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal)" passou a ser permitida no âmbito do Estatuto da Criança e Adolescente[78].

Nesse contexto, a infiltração de agentes policiais mostra-se de importância diferenciada, ressaltando-se que "os órgãos de registro e cadastro público poderão incluir nos bancos de dados próprios, mediante procedimento sigiloso e requisição da autoridade judicial, as informações necessárias à efetividade da **identidade fictícia** criada"[79].

Destaca-se que, na hipótese de infiltração no âmbito do Estatuto da Criança e do Adolescente: "não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial."[80].

Na hipótese de infiltração virtual prevista na Lei de Organização Criminosa, serão permitidas prorrogações "mediante ordem judicial fundamentada e desde que o total não exceda a 720 (setecentos e vinte) dias e seja comprovada sua necessidade"[81].

---

[72] Infrações penais relacionadas à pedofilia.

[73] Invasão de dispositivo informático.

[74] Estupro de vulnerável.

[75] Corrupção de menores.

[76] Satisfação da lascívia.

[77] Favorecimento da prostituição de criança ou adolescente ou de vulnerável.

[78] Art. 190-A da Lei 8.069/90.

[79] Art. 190-D da Lei 8.069/90.

[80] Art. 190-A, III, da Lei 8.069/90.

[81] Art. 10-A, §4.º, da Lei 12.850/13.

BREVES REFLEXÕES SOBRE O IMPACTO DA INTELIGÊNCIA ARTIFICIAL NO ORDENAMENTO JURÍDICO PORTUGUÊS: O INCONTORNÁVEL ALARGAMENTO DA RESPONSABILIDADE OBJETIVA?

Célia Dias Pereira[1]

Resumo: No contexto atual em que vivemos, somos diariamente confrontados com notícias sobre a Inteligência Artificial, nomeadamente os feitos atingidos pelos avanços da ciência, os seus benefícios, mas também os riscos envolvidos. Além disso, é notório que a nossa sociedade tende a ser cada vez mais dependente das ferramentas tecnológicas e digitais. Perante esta incontornável realidade, o Direito é novamente desafiado, todavia, com a particularidade de estas transformações se desenrolarem quase à velocidade da luz e de os seus efeitos serem deveras impactantes. De entre as diversas matérias jurídicas chamadas ao centro desta discussão, as questões inerentes à responsabilidade civil são talvez uma das mais sensíveis, gerando-se no interior dos juristas inquietações quanto à suficiência do respetivo instituto jurídico, designadamente em termos de adequação e eficácia dos mecanismos legais consagrados para tutela dos indivíduos perante violações decorrentes de sistemas dotados de Inteligência Artificial.

Palavras-chave: Inteligência Artificial; Responsabilidade civil; Responsabilidade objetiva.

Abstract: In the current context in which we live we are confronted daily with news about Artificial Intelligence, namely the achievements reached by the advances in science, its benefits, but also the risks involved. Moreover, it is notorious that our society tends to be increasingly dependent on technological and

[1] Assistente Convidada na Escola de Direito da Universidade do Minho. Investigadora do JusGov – Centro de Investigação em Justiça e Governação. Doutoranda em Ciências Jurídicas Privatísticas. Advogada.

digital tools. Faced with this unavoidable reality, Law is once again challenged, however, with the particularity that these transformations take place almost at the speed of light and their effects are quite impactful. Among the various legal matters called to the centre of this discussion, the issues inherent to civil liability are perhaps one of the most sensitive, generating within the jurists concerns about the sufficiency of the respective legal institute, particularly in terms of adequacy and effectiveness of the legal mechanisms devoted to the protection of individuals against violations arising from systems endowed with Artificial Intelligence.

Keywords: Artificial Intelligence; Civil liability; Strict liability.

1. Considerações introdutórias

A temática deste artigo centra-se na viabilidade das atuais normas da responsabilidade civil consagradas no ordenamento jurídico português em face das relevantes mutações com que a sociedade se depara, fruto da crescente expansão e afirmação da Inteligência Artificial (IA). Sem prejuízo de todas as demais questões que se colocam no panorama jurídico, igualmente pertinentes, por questões de delimitação do objeto do presente artigo, pretendemos cingir esta singela análise à específica questão colocada que, por si só, já é bastante profunda, com vários eixos e pontos de estudo que, naturalmente, não será esta a sede própria para os abordar na sua plenitude e com a exaustividade que merecem.

Hoje, mais do que nunca, ouvimos todos os dias falar em IA; hoje, mais do que nunca, a IA penetra na esmagadora maioria das atividades e tarefas que desempenhamos; hoje, mais do que nunca, o Mundo está ciente de que o progresso que poderemos alcançar está intimamente associado ao uso que é feito da IA e à maximização das suas potencialidades; mas hoje, mais do que nunca, estamos alertados para os desafios que serão colocados em todos os setores da vida em sociedade, desde a economia, passando pelos aspetos sociais até às relações pessoais; e hoje, mais do que nunca, começamos a ter uma maior consciência dos perigos que daí podem advir, caso a utilização da IA não ocorra em condições de segurança, transparência e respeito pelos princípios e valores estruturantes de um Estado de Direito Democrático.

1.1. *O 'recente' fenómeno da IA*

Feito este breve introito, ficamos com a sensação de que a IA está ligada a um fenómeno recentíssimo surgido nos últimos anos. Acontece que, no seio da co-

munidade científica, o conceito de IA remonta à década de cinquenta[2], sendo entendida como "a program that is able to mimic or re-create the thought processes demonstrated by the human brain"[3] ou "um ramo da engenharia informática que tenta replicar as funcionalidades do cérebro humano de forma eletrónica"[4], como "a capacidade de aprender, por um lado, e a capacidade de resolver problemas a partir de informação que foi obtida com essa aprendizagem, por outro"[5].

O conceito de IA não é estanque, nem tão-pouco é consensual e, por conseguinte, torna inviável dispormos de uma definição uniforme. Invocamos *supra* uma ou outra possível definição a título meramente exemplificativo, não querendo com isso transmitir que aquelas definições devem ser adotadas em detrimento de outras. Na medida em que falamos de um conceito cuja essência reside na ciência, na tecnologia e no digital e cujo conteúdo se vai moldando em função dos desenvolvimentos que aí vão sendo alcançados, cremos que as tentativas pela busca de uma definição fechada serão inglórias e que ganharemos muito mais se procurarmos reunir as suas principais características através de uma conjugação de todos os contributos que nos vão sendo fornecidos por aqueles que se dedicam ao estudo da IA.

Ora, desde que surgiu pela primeira vez o termo IA que tem vindo a ser desenvolvida investigação científica nesse âmbito, ainda que nem sempre a um ritmo regular, com períodos mais intensos e outras fases menos produtivas[6]. Por isso, e apesar de o fenómeno da IA se ter generalizado nos tempos mais presentes, em grande medida devido à cobertura dos *media*, que contribuiu significativamente para que o assunto se tornasse acessível ao conhecimento do comum dos cidadãos, não será rigoroso falar de IA como algo recente reportado, no máximo, à última década.

Contudo, é inegável que a IA se apresenta a todos nós numa roupagem distinta daquela que assumiu nos seus primórdios, pois impõe-se que não se ignore ou relativize que a sociedade de hoje não é a mesma de há umas décadas: correntemente deparamo-nos com fenómenos como a globalização, a internacionali-

---

[2] Arlindo Oliveira, *Inteligência Artificial*, Ensaios da Fundação Francisco Manuel dos Santos, Lisboa, Fundação Francisco Manuel dos Santos, 2019, p. 51.

[3] Woodrow Barfield e Ugo Pagallo, *Advanced Introduction to Law and Artificial Intelligence*, Edward Elgar Publishing, 2020, p. 1.

[4] Vítor Palmela Fidalgo, «Inteligência artificial e direitos de imagem», in Manuel Lopes Rocha e Rui Soares Pereira (coords.), *Inteligência Artificial & Direito*, Reimp. 2020, Almedina, 2020, p. 138 (pp. 137-146).

[5] Dário Moura Vicente, «Inteligência artificial e iniciativas internacionais», in Manuel Lopes Rocha e Rui Soares Pereira (coords.), *Inteligência Artificial & Direito*, Reimp. 2020, Almedina, 2020, p. 93 (pp. 93-105).

[6] Arlindo Oliveira, *Inteligência Artificial*, *cit.*, pp. 51-58.

zação, a interconectividade e a digitalização. Sem nos querermos antecipar nas nossas considerações, afirmamos apenas que é este particular contexto que faz com que olhemos para ela com outro cuidado, que lhe confiramos outra preponderância e que, consequentemente, coloquemos este assunto na ordem do dia.

Assim sendo, importa perceber um pouco melhor o que está na origem da ampla atenção que atualmente tem sido dada pelas mais diversas entidades, instituições e sujeitos em torno da IA.

1.2. *O impacto singular da IA na sociedade*

O *'boom'* de IA – se assim o podemos designar – que parece que estamos a experienciar na primeira pessoa desenrola-se num contexto muito específico e particular que marcará a História, entroncando-se, por sua vez, num outro fenómeno que tem vindo a ser apelidado de Indústria 4.0 ou Quarta Revolução Industrial[7].

É precisamente esta confluência de fatores e processos ímpares que geram e explicam o impacto que a IA está a provocar nos mais variados setores da sociedade e que adjetivamos como singular. E, de facto, ele é único, ele é distinto. Por isso é que estamos numa nova era que se demarca das anteriores, também elas transformadoras. No entanto, a Quarta Revolução Industrial será, certamente, mais do que transformadora e tende a ser considerada como disruptiva. Mas, afinal, o que é que ela traz de tão diferenciador?

O passado ficou marcado pela Revolução Agrícola e por três Revoluções Industriais que desencadearam transformações profundas nos setores produtivo e social, desde os progressos ao nível de recursos básicos e essenciais, nos transportes, nas linhas de produção, evoluindo para a produção em série e nos demais meios de comunicação até se alcançar a evolução tecnológica e digital com os computadores e a internet[8]. Ora, seguindo este fio condutor, o nosso primeiro impulso é concluir que os esforços da ciência vão no sentido de dar continuidade ao desenvolvimento tecnológico conseguido na última Revolução Industrial,

---

[7] Acerca deste conceito, a título meramente exemplificativo, *vide* Klaus Schwab, *A Quarta Revolução Industrial*, Levoir, 2019, e «The Fourth Industrial Revolution: What it means and how to respond», in *World Economic Forum*, 2016, pp. 1-9, disponível em https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ [consultado em 24/07/2023]; Klaus Schwab e Nicholas Davis, *Moldando a Quarta Revolução Industrial*, Levoir, 2019; Nicholas Davis, «What is the Fourth Industrial Revolution?», in *World Economic Forum*, 2016, pp. 1-13, disponível em https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/ [consultado em 24/07/2023].

[8] Revisitando estes períodos históricos, *vide* Arlindo Oliveira, *Inteligência Artificial*, *cit.*, pp. 31-35; Iván Mateo Borge, «La robótica y la inteligencia artificial en la prestación de servicios jurídicos», in Susana Navas Navarro (dir.), *Inteligencia Artificial. Tecnología Derecho*, Tirant to Blanch, 2017, p. 126; Klaus Schwab, *A Quarta Revolução Industrial*, *cit.*, pp. 9-11; Klaus Schwab e Nicholas Davis, *Moldando a Quarta Revolução Industrial*, *cit.*, pp. 25 e 26.

elevando os patamares de sofisticação e complexidade dos mecanismos e aparelhos que são colocados ao nosso dispor. Nada de errado quanto a isto. Aliás, é uma evidência. Porém, é mais do que isso e é exatamente por essa razão que se justifica demarcar o presente do passado mais recente pelo reconhecimento de uma nova Revolução Industrial.

Assim sendo, a Quarta Revolução Industrial distingue-se das anteriores, em particular da sua antecessora, porque interliga as diferentes tecnologias existentes numa simbiose entre as tecnologias industriais e as tecnologias de informação que aliadas à permanente conectividade num sistema em rede possibilitam a produção e a transmissão de dados a uma velocidade quase instantânea. Acresce que as tecnologias de hoje são cada vez mais sofisticadas em resultado do crescente investimento na inovação e no desenvolvimento de técnicas mais avançadas, como as de *machine learning* e *deep learning*[9]. Ora, é esta confluência de fatores que confere um impacto sem precedentes a esta Revolução Industrial e rompe com todos os paradigmas consolidados.

Todavia, os cientistas não deixam de reconhecer 'pontos fracos' aos sistemas dotados de IA, além de que permanece acesa entre a comunidade científica a discussão em torno do alcance que a evolução tecnológica poderá atingir, especialmente se será possível atingir o estágio da designada 'singularidade tecnológica', e o período de tempo que teremos de aguardar por novos e incomparáveis avanços. No conjunto das limitações que vão sendo apontadas, ressaltamos a rigidez dos sistemas, relativamente pouco adaptáveis, a dificuldade de comunicarem em linguagem natural, a capacidade diminuta para realizarem satisfatoriamente tarefas que envolvam o processamento de perguntas e imagens complexas e não estruturadas, bem como os grandes entraves perante ambientes não controlados e imprevisíveis, uma vez que o seu bom desempenho se revela em tarefas repetitivas e específicas. Em bom rigor, a IA do presente não adota comportamentos inteligentes, tão-só aparenta que as suas decisões são inteligentes. Os sistemas atuais não são dotados de emoções, empatia, criatividade e imaginação, que fazem parte integrante do ser humano. Por força destas e outras condicionantes, a IA (ainda) não está apta, pelo menos nas condições ideais, a lidar com conceitos

[9] Aludindo a estas noções, *vide* Pedro Domingos, *A Revolução do Algoritmo Mestre – Como a Aprendizagem Automática Está a Mudar o Mundo*, 9.ª ed., Reimp. 2019, Manuscrito, 2019, pp. 19-32; Harry Surden, «*Artificial* intelligence and law: an overview», *Georgia State University Law Review*, Vol. 35, 2019, pp. 1311-1316 (pp. 1305-1337), disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3411869 [consultado em 24/07/2023]; Woodrow Barfield e Ugo Pagallo, *Advanced Introduction to Law and Artificial Intelligence*, *cit.*, pp. 14-16.

abstratos, que carecem de valoração ou interpretação e com situações que se afastam de estruturas formais, exatas e objetivas[10].

Sem prejuízo das limitações que os sistemas de IA continuam a apresentar e que, diríamos nós, fazem parte do processo natural do progresso científico, é em virtude da conjugação de todos os elementos e características identificadas que a IA se eleva a um patamar nunca antes alcançado capaz de gerar mutações estruturantes com repercussões inéditas e transversais. Posto que, não constituindo a IA uma novidade, compreende-se que se tenha vindo, hodiernamente, a encará-la numa outra perspetiva: as atenções direcionam-se para esta temática, partilha-se um sentimento generalizado de que este é um assunto realmente importante e estamos mais sensibilizados para as questões delicadas que se levantam e que causam incontornavelmente preocupação.

É, portanto, uma enorme janela de oportunidades com duas variantes paralelas: ao abrir-se, tanto poderá fomentar o crescimento económico e o progresso social, como apresenta uma série de riscos e desafios, retirando a sociedade e, por inerência, o Direito que a regula, da sua zona de conforto.

2. Os desafios jurídicos colocados pela IA em sede de responsabilidade civil

Partindo das considerações prévias sobre as quais nos debruçámos até então, chegados aqui, cumpre identificar os principais desafios jurídicos desencadeados pela utilização da IA no que toca à responsabilidade civil. Assumindo o compromisso de apresentar uma reflexão que, embora curta, seja consistente e com o mínimo de substância, não poderemos abordar as demais matérias jurídicas de natureza bastante variada em relação às quais o ordenamento jurídico é colocado à prova.

Em traços gerais, os potenciais problemas que equacionamos irão colocar-se, de forma direta ou indireta, de modo mais ou menos acentuado, em todos os pressupostos nos quais se funda o instituto da responsabilidade civil. Seja porque poderemos identificar mais do que um facto relevante e, correlacionado com isso, uma concorrência de causas; seja porque poderemos deparar-nos com condicionantes ao nível das tradicionais variantes da ilicitude consagradas no artigo 483.º, n.º 1, do Código Civil (CC) e a situação concreta, por exemplo, nos condu-

[10] Arlindo Oliveira, *Inteligência Artificial*, *cit.*, p. 57; Harry Surden, *«Artificial intelligence and law: an overview»*, *cit.*, pp. 1321-1326; Parlamento Europeu, «Artificial intelligence: How does it work, why does it matter, and what can we do about it?», *Study Panel for the Future of Science and Technology*, EPRS - European Parliamentary Research Service, junho de 2020, p. 17 (pp. 1-66) disponível em https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf [consultado em 08/10/2023].

za aos designados danos puramente patrimoniais; seja porque haja danos e eles não resultem de uma conduta culposa; seja porque a determinação da extensão dos danos não se afigure clarividente[11], entre outros.

Ademais, teremos ainda de ter presentes as dificuldades que surgirão também ao nível da prova. Por força dos traços característicos dos sistemas de IA, como a autonomia e a imprevisibilidade fruto das capacidades de aprendizagem e de interação com o ambiente, a par da elevada sofisticação do seu funcionamento, torna-se de difícil acesso ao comum dos indivíduos cumprir cabalmente com o ónus da prova dos pressupostos da responsabilidade civil, em especial da culpa e do nexo de causalidade[12]. Assim, a reconstrução do próprio processo decisório pode ser impercetível pela opacidade que caracteriza os sistemas de IA e, ainda, num patamar mais extremo, quando os próprios sistemas de IA se desviam da programação inicial praticando atos e apresentando resultados que fogem do controlo do ser humano. As dificuldades no acesso aos elementos probatórios poderão ser agravadas pelos meios dispendiosos para os obter que, certamente, não estarão ao alcance da esmagadora maioria dos lesados, sem devermos descurar a possibilidade da obtenção desses elementos ser mesmo inviável.

São, pois, certos elementos típicos dos sistemas de IA que estão na origem destas problemáticas e que não podem ser desvalorizados. Um primeiro ponto essencial prende-se com a urgência em encontrar procedimentos que contribuam para a transparência das tecnologias de IA, cujo modo de operar é de tal modo opaco que torna bastante complicado o rastreamento das decisões tomadas pelos sistemas de IA. Aliado a isto é comum a existência de uma multiplicidade de intervenientes em toda a cadeia do processo, já ele por si só complexo, o que significa que a imputação de responsabilidade a um determinado sujeito não se afigurará

---

[11] Procurando encontrar os critérios mais adequados para a delimitação dos danos e, por conseguinte, para a determinação da obrigação de indemnização, reflexões vertidas no panorama geral da responsabilidade civil, mas que seguramente nos poderão ser úteis em cenários relacionados com a IA, *vide* Ana Mafalda Castanheira Neves de Miranda Barbosa, «Entre a ilicitude e o dano», *Revista de Direito da Responsabilidade*, Ano 1, 2019 (pp. 1-44), e *Danos – Uma leitura personalista da responsabilidade civil*, Principia, 2018.

[12] A problemática em torno do nexo de causalidade no seio da IA é uma realidade cada vez mais próxima que vem adicionar uma nova vertente à abordagem deste pressuposto da responsabilidade civil. No entanto, a complexidade na sua aferição sempre esteve presente, em termos generalizados e não somente agora neste contexto específico, e daí ser uma das temáticas que despertou e continua a despertar mais estudo na nossa doutrina. Ainda assim, pela especial dedicação a esta matéria, destacamos Ana Mafalda Castanheira Neves de Miranda Barbosa, «Do nexo de causalidade ao nexo de imputação», in Margarida Paz, Gabriela Cunha Rodrigues e Patrícia Costa (coords.), *Novos olhares sobre a responsabilidade civil – Jurisdição civil*, Coleção Formação Contínua, Ed. atualizada setembro 2019, CEJ, outubro 2018 (pp. 39-80); e *Responsabilidade civil extracontratual: Novas perspetivas em matéria de nexo de causalidade*, Princípia, 2014.

uma tarefa fácil. Por vezes, poderá não ser possível identificar todos os potenciais responsáveis por nos depararmos com um processo repartido em diversas fases – conceção, produção, testagem, colocação no mercado, comercialização, utilização –, cada uma delas com diferentes intervenientes, aos quais competem funções e deveres de natureza distinta, o que pode levar a que, a final e em face do tempo decorrido, percamos o rasto a algum deles. Outras vezes, estando identificados os eventuais responsáveis, poderemos esbarrar no estabelecimento do nexo de causalidade entre a conduta concreta e a produção dos danos pelo facto de, na maior parte das vezes, as diferentes atuações dos vários sujeitos estarem interligadas e não ser tecnicamente claro qual ou quais a(s) conduta(s) relevante(s) para a produção dos danos, uma vez que têm sido reconhecidas limitações em termos de explicação do funcionamento dos sistemas de IA.

Além disso, havendo várias causas a concorrer para a ocorrência dos danos, a definição daquela(s) que foi(ram) preponderante(s) pode igualmente revelar-se deveras complicada. A aferição da responsabilidade enquadra-se num contexto tecnológico, no qual os dados e os elementos técnicos são quase sempre, se não sempre, imprescindíveis para descortinar as falhas existentes, sendo certo que a generalidade dos lesados carece desses conhecimentos especializados e que também não serão de fácil acesso.

Referimo-nos a falhas e, ao fazê-lo, tendemos a fazer a associação com a adoção de um comportamento culposo. Efetivamente, podemos deparar-nos com situações danosas que advêm de um erro humano: existência de um defeito na conceção prevista no regime de responsabilidade do produtor, um incumprimento por parte do programador, a falta de atualizações, um errado emprego por parte do utilizador, entre outros. E também aqui as adversidades na aferição dos preenchimentos dos pressupostos da responsabilidade civil podem fazer-se sentir pelas particularidades dos sistemas de IA. Mas, e quando não se vislumbra culpa? Como dissemos, os sistemas de IA tendem a ser dotados de cada vez mais sofisticação no seu desempenho pelo aprimoramento das capacidades de autonomia, interação e aprendizagem. Portanto, se a conduta que está na origem do dano é o resultado de uma decisão tomada pela máquina dotada de IA para a qual não estava programada e não há qualquer desconformidade e/ou violação de deveres por parte de qualquer um dos responsáveis pelos sistemas de IA, a quem se irá imputar a obrigação de indemnizar?

Por outro lado, o facto de lidarmos com sistemas que envolvem uma permanente conectividade e que estão sujeitos a constantes atualizações técnicas e informáticas são fatores que geram incerteza quanto ao *modus operandi* das ferramentas de IA. Funcionamento pautado por uma imprevisibilidade acrescida derivada das próprias capacidades da nova geração de máquinas dotadas de IA que, sendo

do ponto de vista científico uma manifestação de inovação tecnológica, suscita receios no que toca à perda de controlo humano[13].

Nessa medida, é inevitável ponderar se as atuais normas de responsabilidade civil que vigoram no nosso ordenamento jurídico são ou não suficientes para dar resposta adequada ao conjunto de potenciais situações danosas que irão emergir com o acentuado uso da IA e com a disponibilização de sistemas altamente sofisticados e complexos. É notório que as mutações que estão a ocorrer na sociedade vão desaguar numa tendência de alargamento das esferas de riscos até então não perspetivadas e, por conseguinte, sem a correspondente previsão legal, pelo menos pensada propositadamente para esse tipo de situações. É o nosso instituto da responsabilidade civil tal como está consagrado suficientemente elástico para abarcar estas novas realidades geradoras de danos decorrentes do uso da IA e, sendo-o, assegurará uma tutela eficaz dos direitos e interesses dos lesados? Ou terá o legislador de intervir? E, colocando-se este último cenário, em que moldes o fará?

2.1. *A posição da União Europeia*

Em face das problemáticas referenciadas, desde sensivelmente 2017 que a IA está na agenda da União Europeia (UE) como uma das temáticas centrais para o mercado único europeu, agora, na sua dimensão digital. Os estudos, as análises, os debates e as reflexões têm sido abundantes com a criação de grupos de trabalhos especializados a dedicarem-se em exclusivo às matérias ligadas à IA e os resultados começam a ser visíveis, pese embora estas iniciativas ainda sejam a ponta do icebergue. É certo que a UE ainda não se encontra num estádio de execução de medidas e implementação de procedimentos e regras legais, contudo, algumas conclusões começam a ganhar forma e, principalmente, denota-se vontade dos órgãos competentes em regular a IA.

Revisitando os passos que já foram sendo dados a este nível por parte da IA, destacamos que, inicialmente, a UE demonstrou abertura para a atribuição de personalidade jurídica aos entes dotados de IA mediante a criação de uma ca-

[13] Estas problemáticas têm vindo a ser apontadas pela generalidade da doutrina. A título meramente exemplificativo, *vide* Ana Mafalda Castanheira Neves de Miranda Barbosa, «O futuro da responsabilidade civil desafiada pela inteligência artificial: as dificuldades dos modelos tradicionais e caminhos de solução», *Revista de Direito da Responsabilidade*, Ano 2, 2020, pp. 280-284 (pp. 280-326); Arlindo Oliveira, *Inteligência Artificial*, *cit.*, pp. 95-99; Klaus Schwab e Nicholas Davis, *Moldando a Quarta Revolução Industrial*, *cit.*, p. 167; Pedro Domingos, *A Revolução do Algoritmo Mestre – Como a Aprendizagem Automática Está a Mudar o Mundo, cit.*, pp. 311 e 312.

tegoria jurídica de personalidade eletrónica[14]. Na Resolução do Parlamento Europeu 2015/2103 (INL)[15], além da hipótese de criação de um regime de seguros obrigatórios e de fundos de compensação, a UE defendia um estatuto jurídico específico para os entes autónomos mais sofisticados, a fim de serem considerados pessoas eletrónicas. Esta posição foi alvo de fortes críticas que contribuíram para ditar a sua reversão, entre as quais evidenciamos razões de cariz ético sustentadas no princípio da dignidade da pessoa humana, capacidades e características que por enquanto não estão presentes nos sistemas de IA, inviabilizando uma equiparação com o ser humano, a impossibilidade de emitir um juízo de imputação a estes entes, conexionada com a falta de autoconsciência e de intencionalidade e, ainda, a ausência de um fim específico que legitime um enquadramento semelhante às pessoas coletivas[16].

Mais tarde, no início de 2020, a Comissão Europeia apresentou o Livro Branco sobre a IA, o qual tinha como notas principais: (i) trazer a IA para o centro das preocupações da UE, por se constatar a sua relevância para a integridade do mercado único europeu; (ii) aproveitar os benefícios da IA como uma fonte altamente rentável para a prosperidade dos Estados-Membros em termos de ganhos de eficiência e produtividade, reforço da competitividade, melhoramento do

---

[14] Na doutrina podemos encontrar certos autores que não excluem este posicionamento, *v.g.*: Robert van den Hoven van Genderen, «Do We Need New Legal Personhood in the Age of Robots and AI?», in Marcelo Corrales, Mark Fenwick e Nikolaus Forgó (editors), *Robotics, AI and the Future of Law*, Springer, 2018, pp. 42 e ss. (pp. 15-55), admite que poderá ser desejável a criação de uma categoria *sui generis* para certos *robots* autónomos; Samir Chopra e Laurence F. White, *A Legal Theory for Autonomous Artificial Agents*, University of Michigan, 2011, pp. 145-151 e 171-182, assentam a atribuição de personalidade jurídica na característica da autonomia destas máquinas ao ponto de permitir associá-la a intenções. Outros autores, como Ugo Pagallo, *The Law of Robots - Crime, Contracts and Torts*, Springer, 2013, pp. 103-106 e 162-170, propõem que os entes dotados de IA não sejam entendidos como pessoas, mas como agentes no quadro contratual. São, assim, encarados como *e-servants* materializando-se a responsabilidade do utilizador da máquina na constituição de um *peculium* digital inspirado na antiga figura do *peculium* dos escravos romanos.

[15] De 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52017IP0051 [consultada em 24/07/2023].

[16] Cfr., entre nós, algumas dessas vozes: Ana Mafalda Castanheira Neves de Miranda Barbosa, «Responsabilidade civil por danos causados pela inteligência artificial: uma cronologia europeia», *Revista de Direito da Responsabilidade*, Ano 3, 2021, pp. 504-509 (pp. 497-518); Dário Moura Vicente, «Inteligência artificial e iniciativas internacionais», *cit.*, pp. 102 e 103; Henrique Sousa Antunes, «Inteligência artificial e responsabilidade civil: enquadramento», *Revista de Direito da Responsabilidade*, Ano 1, 2019, (pp. 139-154); Sónia Moreira, «IA e robótica: a caminho da personalidade jurídica?», in A. Sofia Pinto Oliveira e Patrícia Jerónimo (coords.), *Liber Amicorum Benedita Mac Crorie*, Vol. II, Uminho Editora, 2022, pp. 545-549 (pp. 537-550), disponível em https://ebooks.uminho.pt/index.php/uminho/catalog/book/105 [consultado em 24/07/2023].

bem-estar dos cidadãos e promoção da inovação tecnológica e das competências digitais; (iii) ajustamento e melhoramento do quadro legislativo vigente devido às especificidades da IA; (iv) reconhecimento da necessidade de intervenção do legislador na projeção de um quadro regulamentar comum que confira fiabilidade e segurança jurídica como resposta aos riscos relacionados com a IA, nomeadamente quanto aos direitos fundamentais, à segurança e à responsabilidade; (v) classificação dos sistemas de IA baseados no risco segundo a aplicação de critérios previamente definidos[17].

Foi mais recentemente, na Resolução do Parlamento Europeu 2020/2014 (INL)[18], que a UE afastou a consagração de personalidade eletrónica, ao deixar escrito no seu n.º 7 a passagem que transcrevemos: "Observa que todas as atividades, dispositivos ou processos físicos ou virtuais operados por sistemas de IA podem, do ponto de vista técnico, ser a causa direta ou indireta de danos ou prejuízos, contudo são quase sempre o resultado de alguém que construiu, utilizou ou interferiu com esses sistemas; observa, a esse respeito, que não é necessário conferir personalidade jurídica aos sistemas de IA".

Deste modo, a solução apresentada direcionou-se para a consagração de responsabilidade civil objetiva do operador de um sistema de IA de alto risco e os restantes casos serem regulados pela responsabilidade baseada na culpa com uma configuração agravada e assente numa presunção de culpa. Defendeu ainda como vias de solução plausíveis e mais adequadas a criação de regras de transparência, segurança e controlo dos mecanismos dotados de IA, a par da criação de seguros de responsabilidade civil obrigatórios e fundos de compensação[19].

Adicionalmente, foi elaborada Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à adaptação das regras de responsabilidade civil extracon-

---

[17] Comissão Europeia, Livro Branco sobre a IA: uma abordagem europeia virada para a excelência e a confiança, 19 de fevereiro de 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52020DC0065 [consultado em 24/07/2023].

[18] De 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime de responsabilidade civil aplicável à IA, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020IP0276 [consultada em 24/07/2023].

[19] Considerandos J e K da Resolução do Parlamento Europeu 2020/2014 (INL), de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime de responsabilidade civil aplicável à IA e considerandos 14, 21 e 22 do seu anexo, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020IP0276 [consultada em 24/07/2023]. Os moldes em que as propostas apresentadas foram esboçados na Resolução não ficaram isentos de críticas, tendo sido apontadas fragilidades, nomeadamente quanto à opção pela diferenciação dos sistemas de IA para efeitos de aplicação do regime da responsabilidade objetiva, bem como ao nível da demarcação do conceito de ilicitude, da determinação dos danos indemnizáveis e nos limites máximos de indemnização estabelecidos – cfr. Henrique Sousa Antunes, «A responsabilidade civil aplicável à inteligência artificial: primeiras notas críticas sobre a Resolução do Parlamento Europeu de 2020», *Revista de Direito da Responsabilidade*, Ano 3, 2021, pp. 5-15 (pp. 1-22).

tratual à IA por se entender que "as atuais regras nacionais de responsabilidade, em especial em matéria de responsabilidade culposa, não se adequam ao tratamento de ações de indemnização por danos causados por produtos e serviços assentes em IA. (…) As características específicas da IA, incluindo a complexidade, a autonomia e a opacidade (o denominado efeito de «caixa negra»), podem dificultar ou tornar proibitivamente oneroso para as vítimas a identificação da pessoa responsável e a prova dos requisitos necessários a uma ação de indemnização bem-sucedida"[20]. Nesse conspecto, a referida Diretiva será aplicável a ações de indemnização de direito civil extracontratual por danos causados por um sistema de IA, sempre que tais ações sejam intentadas ao abrigo de regimes de responsabilidade culposa, destacando-se a consagração de uma presunção de causalidade ilidível (que estará condicionada a um juízo por parte do Tribunal da dificuldade excessiva de cumprimento do ónus probatório quando estejam em causa ações relativas a sistemas de IA que não integrem a categoria de risco elevado), devendo a culpa ser provada nos termos gerais.

No momento atual, foi aprovada pelo Parlamento Europeu a Proposta de Regulamento IA do Parlamento Europeu e do Conselho[21], o qual será aplicável aos fornecedores, utilizadores, distribuidores, importadores e fabricantes de sistemas de IA (excluindo os que sejam desenvolvidos ou usados exclusivamente para fins militares). Dos aspetos tratados nesta Proposta de Regulamento, salientamos que a mesma mantém a lógica dos documentos antecedentes no que concerne ao critério do risco, distinguindo entre sistemas de IA de risco inaceitável, de risco elevado e de risco baixo ou mínimo, além de estabelecer uma lista de práticas

[20] Diretiva Responsabilidade da IA, 2022/0303 (COD), de 28 de setembro de 2022, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52022PC0496 [consultada em 24/07/2023]. A proposta em causa rege-se pela proporcionalidade, seguindo uma abordagem faseada: numa primeira fase, as medidas cingem-se ao ónus da prova através da consagração de uma presunção ilidível; numa segunda fase, visa-se a reavaliação da necessidade de medidas mais rigorosas ou abrangentes tendo em consideração a futura evolução tecnológica.

[21] 2021/0106 (COD), de 21 de abril de 2021, que estabelece regras harmonizadas em matéria de IA e altera determinados atos legislativos da União, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021PC0206 [consultada em 24/07/2023]. Os objetivos traçados a alcançar neste quadro regulamentar são: "garantir que os sistemas de IA colocados no mercado da União e utilizados sejam seguros e respeitem a legislação em vigor em matéria de direitos fundamentais e valores da União; garantir a segurança jurídica para facilitar os investimentos e a inovação no domínio da IA; melhorar a governação e a aplicação efetiva da legislação em vigor em matéria de direitos fundamentais e dos requisitos de segurança aplicáveis aos sistemas de IA; facilitar o desenvolvimento de um mercado único para as aplicações de IA legítimas, seguras e de confiança e evitar a fragmentação do mercado".

absolutamente proibidas (por, por exemplo, violarem direitos fundamentais)[22], elencar os requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado[23] e respetivas obrigações, prever as obrigações de transparência quanto a determinados sistemas de IA[24] e criar um Comité Europeu para a IA.

Desta forma, avizinha-se no futuro próximo desenvolvimentos mais precisos ao nível da regulamentação europeia em matéria de IA. Os moldes exatos em que tal será feito e quando em concreto teremos regras em vigor são uma incerteza não só devido ao próprio funcionamento dos órgãos europeus e a todo o procedimento que a criação de Direito da UE tem de obedecer, mas também por se tratar de uma temática sensível e complexa, o que tenderá a prolongar todo o processo.

Apesar das condicionantes que possam existir, cremos que aquilo que de mais positivo podemos retirar é o facto de a UE estar a desenvolver esforços no sentido de marcar posição mundial quanto às questões associadas à IA e de ter traçado como um dos seus objetivos ser pioneira na regulamentação jurídica da IA.

3. As eventuais soluções vertidas no ordenamento jurídico português

Ante os desafios que vislumbramos *supra* será conveniente explorar algumas das hipóteses legais da responsabilidade civil para, posteriormente, estarmos minimamente seguros na nossa avaliação acerca da suficiência e adequação das normas vigentes para os casos específicos que advêm da utilização de sistemas dotados de IA.

3.1. *O Direito constituído*

Focando-nos na responsabilidade civil extracontratual, no nosso ordenamento jurídico, o instituto da responsabilidade civil assenta, por excelência, na culpa,

---

[22] Incluem-se aqui "práticas com potencial significativo para manipular as pessoas por meio de técnicas subliminares que lhes passam despercebidas ou explorar as vulnerabilidades de grupos específicos", a "classificação social assente na IA para uso geral por parte das autoridades públicas" e a "utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública".

[23] A Proposta prevê duas categorias principais de sistemas de IA de risco elevado: sistemas de IA concebidos para serem utilizados como componentes de segurança de produtos que estão sujeitos a uma avaliação da conformidade *ex ante* por terceiros; outros sistemas de IA autónomos com implicações em matéria de direitos fundamentais que são explicitamente mencionados no anexo III.

[24] Estão em causa sistemas que i) interagem com seres humanos, ii) são utilizados para detetar emoções ou determinar a associação com categorias (sociais) com base em dados biométricos, iii) geram ou manipulam conteúdos («falsificações profundas»).

de acordo com o princípio geral vertido no artigo 483.º, n.º 1, do CC, deixando expressamente determinado que a responsabilidade civil que prescinda da culpa é excecional e está dependente de previsão legal, conforme estipula o artigo 483.º, n.º 2, do CC[25].

Como sabemos, cabe ao lesado o ónus da prova dos factos constitutivos do seu direito de indemnização, pelo que lhe compete a demonstração do preenchimento no caso concreto dos pressupostos que fazem nascer a obrigação de indemnizar na esfera jurídica do lesante. Todavia, o legislador não deixou de facilitar parte deste ónus quando consagrou presunções de culpa mediante a verificação de certas circunstâncias, em particular no caso de danos causados por coisas, animais ou atividades, nos termos do artigo 493.º, n.º 1 e n.º 2, do CC.

No que concerne à responsabilidade objetiva[26], destacamos a responsabilidade do comitente, prevista no artigo 500.º do CC, a responsabilidade por danos causados por animais, vertida no artigo 502.º do CC, e a responsabilidade resultante de acidentes causados por veículos, consagrada no artigo 503.º do CC. Noutros

---

[25] Sobre o instituto da responsabilidade civil a doutrina é vasta, pelo que as referências indicadas não passam de uma pequena amostra do estudo que tem vindo a ser feito neste conspecto. Cfr. Ana Mafalda Castanheira Neves de Miranda Barbosa, *Lições de responsabilidade civil*, Principia, 2017; Fernando de Sandy Lopes Pessoa Jorge, *Ensaio sobre os pressupostos da responsabilidade civil*, Reimp., Almedina, 1995; Heinrich Ewald Horster, «Esboço esquemático sobre a responsabilidade civil de acordo com as regras do Código Civil», in António Cândido de Oliveira (coord.), *Estudos em comemoração do d*écimo *aniversário da Licenciatura em Direito da Universidade do Minho*, Almedina, 2004 (pp. 323-338); Inocêncio Galvão Telles, *Direito das Obrigações*, Reimp. da 7.ª ed., Coimbra Editora, 2010; João de Matos Antunes Varela, *Das obrigações em geral*, Vol. I, Reimp. 2022, Almedina, 2017; Jorge Ferreira Sinde Monteiro, «Rudimentos da responsabilidade civil», *Revista da Faculdade de Direito da Universidade do Porto*, A. 2, 2005 (pp. 349-390), e *Estudos sobre a responsabilidade civil*, Almedina, Coimbra, 1983; José Alberto Rodriguez Lorenzo Gonzalez, *Direito da responsabilidade civil*, *Quid Iuris*, 2017; Manuel A. Carneiro da Frada, *Teoria da confiança e responsabilidade civil*, Reimp. da ed. de fevereiro de 2004, Almedina, 2018, e *Direito Civil, responsabilidade civil: o m*étodo do *caso*, Reimp., Almedina, 2010; Mário Júlio Almeida Costa, *Direito das Obrigações*, Reimp. 2022 da 12.ª ed. revista e atualizada, Almedina, 2010.

[26] Abordando esta modalidade, nomeadamente algumas das situações tipificadas na lei como fonte de responsabilidade civil objetiva, indicamos a título ilustrativo algumas obras: Ana Mafalda Castanheira Neves de Miranda Barbosa, «Responsabilidade civil por ato de terceiro: Entre a culpa, o risco e a confiança», *Revista de Direito da Responsabilidade*, Ano 3, 2021 (pp. 1038-1084), e *Estudos a propósito da responsabilidade objetiva*, Principia, 2014; Maria da Graça Trigo, *Responsabilidade civil delitual por facto de terceiro*, Coimbra Editora, 2009; Nuno Manuel Pinto Oliveira, «Responsabilidade objetiva», in Jorge Ferreira Sinde Monteiro (coord.), *Responsabilidade Civil – II Seminário dos Cadernos de Direito Privado*, N.º especial 02, CEJUR – Centro de Estudos Jurídicos do Minho, 2012 (pp. 107-121).

diplomas legais é de suma importância a responsabilidade decorrente de produtos defeituosos, regulada pelo Decreto-Lei n.º 383/89, de 6 de novembro[27].

Numa tentativa de transpor as normas apontadas para potenciais situações de responsabilidade civil por danos causados por máquinas dotadas de IA, sempre que o dano for causado por uma conduta culposa, ou seja, sempre que fique demonstrado que houve uma violação de regras e/ou deveres impostos ao sujeito responsável pelo sistema de IA, culminando tal violação numa conduta culposa, as regras da responsabilidade civil por factos ilícitos, à partida, darão resposta igualmente satisfatória para estes casos específicos comparativamente com as demais situações geradoras da obrigação de indemnizar. Nesta sede, uma questão delicada que se poderá colocar será quando, por força das especificidades da IA, a demonstração da culpa não seja de fácil alcance. Aqui, poderá chamar-se à colação as presunções de culpa acima identificadas, hipótese que poderá não satisfazer totalmente como explicaremos no ponto *infra*.

Produzindo-se danos, mas inexistindo culpa de qualquer um dos intervenientes na cadeia relacionada com o sistema de IA, teremos de nos socorrer da responsabilidade fundada no risco. Neste âmbito, as situações que porventura poderão ser mais pacíficas dizem respeito, em primeiro lugar, à responsabilidade civil pelos acidentes causados por veículos, cujos pressupostos são suscetíveis de serem aplicados aos veículos autónomos com recurso a uma interpretação atualista dos mesmos[28]. Em segundo lugar, relativamente aos danos provocados por defeitos dos sistemas de IA que se enquadrem na aceção do regime da responsabilidade do produtor, a responsabilidade civil será devidamente aferida com base nas normas deste específico diploma, pese embora não se rejeite a necessidade de o

---

[27] Para uma análise mais detalhada sobre este diploma legal, *vide* Henrique Sousa Antunes, «Responsabilidade civil do produtor: Os danos ressarcíveis na era digital», *Revista de Direito da Responsabilidade*, Ano 1, 2019 (pp. 1476-1485); João Calvão da Silva, *Responsabilidade civil do produtor*, Almedina, 1990; Jorge Morais Carvalho, «Responsabilidade objetiva do produtor: Uma mão cheia de muito pouco», *Vida Judiciária*, N.º 197, setembro-outubro 2016 (pp. 28-29); Juliana Campos, «A responsabilidade civil do produtor pelos danos causados por robôs inteligentes à luz do regime do Decreto-Lei n.º 383/89, de 06 de novembro», *Revista de Direito da Responsabilidade*, Ano 1, 2019 (pp. 700-730); Mota Pinto e Calvão da Silva, «Responsabilidade civil do produtor», *O Direito*, A. 121, N.º 2, abril-junho 1989 (pp. 237-312); Vera Lúcia Paiva Coelho, «Responsabilidade do produtor por produtos defeituosos. "Teste de resistência" ao DL n.º 383/89, de 6 de novembro, à luz da jurisprudência recente, 25 Anos volvidos sobre a sua entrada em vigor», *Revista Eletrónica de Direito*, N.º 2, junho de 2017 (pp. 1-54).

[28] Partilhamos o entendimento defendido por Sónia Moreira, «Veículos autónomos – Propostas de solução no âmbito da responsabilidade civil», in Sónia Moreira e Pedro Miguel Freitas (coords.), *Inteligência Artificial e Robótica: Desafios para o Direito do século XXI*, Gestlegal, 2022, pp. 135-141 (pp. 127-150).

mesmo ser revisto, como aliás já tem sido reclamado[29], a fim de dar uma resposta mais conveniente a determinadas situações que não decorrem necessariamente das questões que agora se levantam com a IA, mas que se poderá aproveitar tal intervenção para também as abranger no melhoramento do regime jurídico.

Quanto às restantes situações plausíveis de serem resolvidas por via da responsabilidade objetiva, as dúvidas já se colocam afincadamente. Aponta-se a norma do artigo 500.º do CC como uma via de solução, responsabilizando-se, na qualidade de comitente, o utilizador da máquina dotada de IA, sendo esta entendida como comissário[30]. Antecipamos que este cenário nos causa muitas reservas, como veremos de seguida.

3.2. *O Direito a constituir?*

Efetivamente o nosso ordenamento jurídico confere um conjunto diversificado de soluções legais para a problemática da responsabilidade civil[31]. Todavia, esta aparência de adequação e suficiência na resposta legal a estas questões fica beliscada quando pensamos em todas as particularidades que revestem as potenciais situações de responsabilidade civil pelo uso de IA. Apontadas as principais especificidades dos sistemas de IA e as implicações mais relevantes que eventualmente as mesmas poderão ter ao nível da imputação da responsabilidade

---

[29] Nesse sentido, *vide* Ana Mafalda Castanheira Neves de Miranda Barbosa, «O futuro da responsabilidade civil desafiada pela inteligência artificial: as dificuldades dos modelos tradicionais e caminhos de solução», *cit.*, pp. 318-322; Henrique Sousa Antunes, «Responsabilidade civil do produtor: Os danos ressarcíveis na era digital», *cit.*, pp. 1478, 1482 e 1483; Juliana Campos, «A responsabilidade civil do produtor pelos danos causados por robôs inteligentes à luz do regime do Decreto-Lei n.º 383/89, de 06 de novembro», *cit.*, pp. 718-720 e 730. No seio da própria UE, a porta à revisão da Diretiva 85/374/CEE do Conselho, de 25 de julho de 1985, relativa à responsabilidade decorrente dos produtos, mantém-se entreaberta, sendo que já em 2020, no considerando 9 do Anexo da Resolução do Parlamento Europeu 2020/2014 (INL), de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime de responsabilidade civil aplicável à IA, se aludia à possível revisão da mesma.

[30] Ana Mafalda Castanheira Neves de Miranda Barbosa, «O futuro da responsabilidade civil desafiada pela inteligência artificial: as dificuldades dos modelos tradicionais e caminhos de solução», *cit.*, pp. 291 e 324; José Alberto Rodriguez Lorenzo Gonzalez, «Responsabilidade por danos e Inteligência Artificial (IA)», *Revista de Direito Comercial*, 2020, pp. 97-104 (pp. 69-111); Nuno Sousa e Silva, «Inteligência artificial, *robots* e responsabilidade civil: o que é diferente?», *Revista de Direito Civil*, Vol. 4, N.º 4, Coimbra, 2019, p. 705 (pp. 691-711).

[31] Para uma perspetiva histórica da evolução do instituto da responsabilidade civil no nosso ordenamento jurídico, a nível doutrinário, legislativo e jurisprudencial, e que nos poderá elucidar acerca dos pontos mais sensíveis do nosso sistema e que requerem, porventura, uma reflexão e reformulação, *vide* José Carlos Brandão Proença, «A responsabilidade civil extracontratual nos 50 anos de vigência do Código Civil: Um olhar à luz do Direito contemporâneo», *Revista de Direito da Responsabilidade*, Ano 1, 2019 (pp. 245-311).

civil, dificultando a aferição dos seus pressupostos, parece-nos que será natural a busca por soluções, no mínimo, diferenciadas.

Ora, o primeiro obstáculo com o qual o direito constituído se depara diz respeito ao potencial campo alargado de danos provocados pela utilização de sistemas de IA sem que tal implique uma conduta culposa, ou seja, sem que consigamos preencher o requisito da culpa. Nestes casos, é ponto assente que a responsabilidade subjetiva não poderá operar, abrindo caminho para a aplicação da responsabilidade civil objetiva.

E ainda que se recorra às presunções de culpa, como as previstas no artigo 493.º do CC, o resultado final poderá ser infrutífero, pois o lesante terá, à partida, facilidade em ilidir a presunção, demonstrando que observou os procedimentos e deveres aos quais estava adstrito e/ou que os danos se verificariam independentemente de haver culpa. Isto porque, relembre-se, a probabilidade de os danos decorrerem da autonomia e autoaprendizagem da máquina sem que se vislumbre uma ação ou omissão culposa de qualquer um dos intervenientes na cadeia produtiva é bastante elevada nas situações em que se utiliza a IA nos níveis de sofisticação que estão projetados para o futuro próximo. Além disso, poderá questionar-se a existência de um dever de vigilância que, demonstrado inexistir no caso concreto, afastará a aplicação das presunções de culpa assentes em tal dever, assim como algumas objeções poderão ser apontadas no que toca ao conceito de perigosidade, isto é, se realmente a generalidade dos sistemas de IA são suscetíveis de configurar uma atividade perigosa à luz do artigo 493.º, n.º 2, do CC.

Por outro lado, a hipótese de aplicação do artigo 500.º do CC também poderá revelar-se inviável caso se siga a posição maioritária que afasta a atribuição de personalidade jurídica às máquinas dotadas de IA. Partindo-se da ideia de que os sistemas de IA não são entes jurídicos, surge automaticamente a questão da imputação do evento lesivo, na medida em que a responsabilidade do comitente pressupõe a responsabilidade do comissário (a máquina), o que, por sua vez, implica dispor de discernimento para entender as suas condutas e as consequências das mesmas, sendo capacitado para emitir um juízo de valor sobre os próprios comportamentos.

Posto isto, uma via de solução possível poderá passar pela criação de uma norma semelhante à responsabilidade objetiva do artigo 502.º do CC, prevista para os danos causados por animais, de forma a responsabilizar aqueles que utilizam os sistemas de IA, usufruindo das suas vantagens, pelos danos que estas máquinas causarem. Obviamente que a ideia de 'perigo especial' teria de ser pensada e concretizada, tendo em vista a delimitação do círculo de danos para não extrapolar a *ratio* da responsabilidade objetiva e, por inerência, não alargar desmesuradamente o âmbito da responsabilidade civil que prescinde de culpa.

Numa perspetiva mais cautelosa e não avançando de imediato para a criação de uma norma de responsabilidade objetiva que abranja a generalidade dos sistemas de IA, uma segunda opção poderá consistir numa intervenção cirúrgica e faseada através da criação de normas específicas de responsabilidade baseada no risco com um âmbito de aplicação claramente balizado, consoante as áreas onde a IA passe a desempenhar um papel ativo e onde a ocorrência de danos se revele mas gritante. Ou seja, a nova regulamentação poderá seguir uma linha de intervenção mais sectorial e especializada, incindindo gradualmente nas atividades onde a IA se for revelando mais impactante à medida do tempo e, consequentemente, a intervenção do legislador também seja mais premente, colmatando as lacunas que surjam ou, preferencialmente, projetando os setores de atividade onde as mesmas poderão surgir mais rapidamente.

Por fim, não podemos deixar de mencionar uma hipótese que vem sendo equacionada, ainda que não o seja explicitamente e que esteja longe de ser perfilhada por um núcleo considerável de doutrinários e juristas, e que consiste numa regulação ampla por via da previsão de uma cláusula geral de responsabilidade objetiva. As interrogações acerca dos moldes em que a responsabilidade civil objetiva está configurada no nosso ordenamento jurídico não são de hoje, sendo perfeitamente natural que o questionamento surja atendendo à longevidade do nosso CC. Porém, garantidamente que as circunstâncias presentes fazem-no ecoar com mais intensidade e aceleram a abordagem de novas perspetivas e entendimentos, em particular um cenário de alteração estrutural e mais profunda do nosso instituto da responsabilidade civil.

Somos solidários na partilha dos receios que esta opção acarreta, desde logo, por ser a mais radical de entre todas as hipóteses em discussão. Contudo, também reconhecemos que o momento atual é o mais propício ao estudo e reflexão desta mudança no conjunto de normas que regulam a responsabilidade civil. Sem margem para dúvidas que as mutações que se fazem sentir na sociedade e na interação com as mais variadas atividades, emergentes do contexto atual de alto desenvolvimento tecnológico e digital, conduzem ao alargamento das esferas de riscos e exigem repensar os modelos de imputação de responsabilidade civil.

Estamos longe de apresentar uma opinião formada quanto à melhor escolha a seguir, mas perspetivamos convictamente que as mudanças no ordenamento jurídico não passarão certamente à margem das possibilidades aqui explanadas.

4. Breves conclusões

Terminamos esta excursão apenas com a certeza de que a IA, para além de já fazer parte do nosso presente, no futuro próximo, vai assumir um papel fulcral em todos os setores socioeconómicos com transformações profundas e que, nessa medida, o Direito terá de intervir. Quanto a tudo o resto, é uma incógnita…

Olhando à nossa volta dispomos de informação factual e objetiva que nos permite concluir que a IA está na ordem do dia, formando-se uma atmosfera transversal de consciencialização da sua importância pelo impacto positivo e negativo que poderá ter e, por isso, constatando-se um misto de sentimentos de oportunidade para o crescimento económico e para o progresso social, mas também de preocupação e receios com os riscos inerentes à sua utilização.

A discussão está já a decorrer, desde a simples conversa de café, aos *media* até às mais altas instâncias institucionais e governamentais; o estudo, a análise, a reflexão, o desenvolvimento de iniciativas, a apresentação de propostas e medidas também já estão a desenrolar-se. Portanto, o caminho está a ser feito, ainda que esteja longe de estar terminada esta árdua jornada onde o Direito será um dos vetores-chave para lidarmos com a IA de forma segura, transparente, adequada, equilibrada e em conformidade com os princípios estruturantes de um Estado de Direito Democrático. A grande dúvida reside em encontrarmos a fórmula certa para obtermos o ponto ótimo entre o incentivo e aposta no investimento na inovação tecnológica, de um lado, e a regulação jurídica das ferramentas e sistemas de IA, cuja intervenção é aconselhável que se guie pelo princípio da proporcionalidade, do outro.

Em sede de responsabilidade civil, parece-nos que, mais cedo ou mais tarde, será inevitável reajustar as normas vigentes. Não defendemos uma intervenção radical, pelo contrário, cremos que a base do nosso instituto jurídico deverá manter-se intacta e que os princípios fundamentais que regem a responsabilidade civil deverão continuar a orientar o legislador. No entanto, a circunstância de a IA estar a ganhar uma dimensão nunca antes vista com um impacto generalizado e não circunscrito a determinadas áreas é um reflexo da sociedade atual: uma sociedade inovadora, digital, globalizada, permanentemente conectada onde as esferas de risco tendem a alargar-se. O funcionamento da sociedade de hoje é indiscutivelmente distinto da sociedade do passado com base na qual se construíram as normas da responsabilidade civil. O Direito molda-se às alterações sociais, económicas, políticas, histórias e outras, construindo-se e reconstruindo-se sem ignorar as necessidades da sociedade em cada tempo, lugar e contexto.

Assim sendo, na nossa modesta perspetiva, as alterações em matéria de responsabilidade civil passarão não só pela consagração de presunções de culpa e do

nexo de causalidade e/ou pela facilitação do ónus da prova destes pressupostos em determinadas circunstâncias, como também pelo alargamento do tipo de sinistros sujeitos a seguro de responsabilidade civil obrigatório e pela criação de fundos de compensação como elementos complementares a uma indemnização integral dos danos. Porém, estamos convictos de que será ao nível da responsabilidade civil pelo risco que as modificações serão mais significativas com a ampliação do seu campo de aplicação ou até mesmo com a consagração de uma cláusula geral de responsabilidade objetiva, a fim de se conseguir abranger as situações danosas decorrentes do uso da IA nas mais variadas áreas e de se dar uma resposta eficaz que ultrapasse os problemas ao nível da imputação de responsabilidade nestes específicos casos.

O futuro nos dirá se assim será.

O AGRO-AUTÓMATO E A QUARTA REVOLUÇÃO AGRÍCOLA: BREVE RECENSÃO DOS ENSAIOS DE SISTEMAS DE RESPONSABILIDADE CIVIL NO SEIO DA AGRICULTURA ARTIFICIALMENTE INTELIGENTE

Luís Manuel Pica[1]
Mário Filipe Borralho[2]

Resumo: Os sistemas de inteligência artificial estão tendencialmente a "galgar" terreno no quotidiano. A sua utilização é variável, podendo, *inclusive*, ser utilizada no seio de atividades mais rústicas e tradicionais como é a agricultura. A sua capacidade de antecipação e/ou predição de acontecimentos futuros são uma capacidade cada vez mais acolhida que permite aos agricultores otimizar e maximizar os recursos disponíveis. Estes novos agricultores (agro-autómatos) ganham um novo estatuto de modernização, mas esta evolução não é despiciendo de riscos e perigosidades. É que, não obstante as inegáveis vantagens, não se poderá deixar de referir que os riscos inerentes à otimização e aos novos métodos de agricultura suscitam palpitações que são assinaláveis, pelo que se impõe o estabelecimento de um quadro garantístico normativo suficientemente eficiente e capaz de acautelar os novos perigos emergentes.

[1] Doutor em Ciências Jurídicas Públicas pela Escola de Direito da Universidade do Minho; Investigador do JUSLAB, grupo de investigação do JusGov (Centro de Investigação em Justiça e Governação), e do Centro de Estudos Avançados em Direito Francisco Suárez – CEAD; Professor Adjunto Convidado no Instituto Politécnico de Beja; Professor Auxiliar Convidado na Faculdade de Direito da Universidade Lusófona de Lisboa e no Instituto Superior Manuel Teixeira Gomes (Portimão).

[2] Licenciado em Solicitadoria e em Direito; Mestrando em Direito pela Faculdade de Direito da Universidade de Lisboa; Assistente Convidado do Instituto Politécnico de Beja.

Palavras-chave: Agro-autómato; Responsabilidade civil; Agricultura; Inteligência artificial.

Abstract: Artificial intelligence systems are tending to gain ground in everyday life. Their use is variable, and they can even be used within more rustic and traditional activities such as agriculture. Their ability to anticipate and/or predict future events is an increasingly welcomed capability that allows farmers to optimize and maximize available resources. These new farmers (agro-automates) are gaining a new modernization status, but this development is not without risks and dangers. Notwithstanding the undeniable advantages, the risks inherent in optimization and new farming methods have raised significant concerns, and a sufficiently efficient regulatory framework must be established to safeguard against the new dangers that are emerging.

Keywords: Agro-automation; Civil liability; Agriculture; Artificial intelligence.

1. Introdução

A inteligência artificial atrai interesses e holofotes diariamente. A sua relevância, utilidade prática e as preocupações que são levantadas com a mesma tornam o tema tão falado, na sociedade comum, na imprensa, ou nas instituições nacionais e internacionais.

Esta relevância não é despicienda de sentido e lógica, pois veja-se que a inteligência artificial está presente no nosso quotidiano. Desde a simples utilização de um *smartphone* para indicação do caminho mais rápido a determinado destino, a utilização de uma aplicação para cultivo de plantas ou a própria utilização de sistemas no âmbito da agricultura sustentável, designadamente com a utilização de sistemas inteligentes para indicação de previsões de quantidades de adubos e fertilizantes a utilizar, criação de esquemas e expedientes para determinar a melhor forma de plantação ou de utilização de meios e recursos disponíveis.

É nesta utilização variada que as repercussões podem, também elas, ser variadas. Falamos de repercussões factuais e jurídicas como, por exemplo, os erros que podem derivar da utilização destes sistemas inteligentes. E, nestes casos, como regular estas situações? Se somos impelidos a afirmar que a regulamentação da inteligência artificial está a ser considerada a vários níveis, certo também será dizer que, até à data, a tónica tem sido colocada nas questões relacionadas com a responsabilização dos atos praticados por estes sistemas inteligentes, designadamente, por via do instituto da responsabilidade civil. Mas poderão ser equacionadas outras soluções? Como deverá o Direito intervir para regular a utilização destes sistemas inteligentes e quais os perigos que podem surgir dos mesmos?

Procuraremos, com as presentes considerações, tecer algumas notas sobre a utilização da inteligência artificial no seio da nova agricultura, as suas potencialidades, benefícios e vantagens, bem como dotar o leitor de algumas premissas ao nível da tutela e proteção jurídica até à data dispensadas a todos aqueles que tenham conexão com os impactos dos sistemas de inteligência artificial, assim como de eventuais soluções e ideias até aqui identificadas.

2. Um conceito (aproximado) de inteligência artificial

Numa primeira abordagem ao tema objeto de estudo, dir-se-á que o conceito de "inteligência artificial" tem alavancado interesses e debates, suscitando a curiosidade recente de investigadores, docentes, instituições públicas e privadas, organizações, etc. Poderia, contudo, pensar-se que estamos perante uma realidade utópica própria de ficção científica. Mas, longe disto, cabe-nos, em primeiro lugar, restringir o conceito e (tentar) definir o que é a inteligência artificial. Isto porque um estudo que se anseia científico não pode deixar de pressupor (ainda que de forma breve) uma aproximação ao objeto do nosso estudo (reservando sempre a dificuldade de delimitação conceptual[3]). Por isso, impõe-se uma delimitação conceptual do que se deve entender por *inteligência artificial*, a qual deve ser entendida unicamente para efeitos de enquadramento sistémico ao estudo que nos propomos alcançar.

Na realidade, quando falamos em *inteligência artificial* (aplicada ao setor económico, político, administrativo ou na própria agricultura), somos impelidos, desde logo, a afirmar que estamos perante um conceito de imitação da capacidade cognitiva humana. Em termos simples, criar uma máquina capaz de imitar o ser humano, com vista à sua utilização a fim de cumprir os interesses deste. Mas uma abordagem desta natureza não poderá socorrer-se de uma delimitação simplista e redutora da realidade. Isto porque, quando falamos em *inteligência artificial*, suscita-se, desde logo, uma *inteligência maquinal* representada por pré-resultados identificados previamente pelo produtor e cujo aglomerado constitui

[3] Philip Glass, «Datenschutzrecht für künstliche Intelligenz in der öffentlichen Verwaltung», in *Datenschutz Rechtliche Schnittstellen*, Zurich, Dike, 2023, p. 179, disponível em https://digitalcollection.zhaw.ch/bitstream/11475/26659/2/2023_Widmer_Datenschutz-rechtliche-Schnittstellen_Dike.pdf [consultado em 25/07/2023].

um algoritmo que é utilizado pelo sistema informático[4]. Com base na representação de conhecimentos específicos e no processamento de conhecimentos, os algoritmos efetuam o reconhecimento de padrões, as instruções de controlo/ação e o processamento de problemas para atingir o resultado previamente determinado[5]/[6].

Falamos, nestas situações, numa extensão de *inteligência artificial fraca*, que funciona dentro dos limites da programação. Daí que se coloque em crise a verdadeira natureza de *inteligência*, pois estamos na presença de uma mera reprodução de conclusões. Com efeito, é na chamada *inteligência artificial forte* que se encontra o desenvolvimento mais profícuo da inteligência artificial. Esta organiza-se e desenvolve-se de forma autónoma após uma fase inicial com base numa programação específica, utilizando posteriormente métodos de aprendizagem automática e clássicos como as redes neuronais artificiais preditivas utilizadas como procedimentos complexos de resolução de problemas.

---

[4] O termo "algoritmo" refere-se a instruções de ação claramente estruturadas que não são inicialmente descritas como artificialmente inteligentes. Em termos metafóricos, são como "receitas culinárias" e outros processos de dedução lógica. Assim, um algoritmo é definido como qualquer instrução de ação não ambígua que é utilizada para resolver certos problemas em passos individuais definidos. O momento da inteligência artificial não está no algoritmo, mas no modelo que é implementado pelo algoritmo. Assim, um sistema algorítmico não tem necessariamente de ter funções artificialmente inteligentes. Como referimos noutra sede, "falamos de sistemas de inteligência artificial que procuram a recolha de dados pessoais e a sua leitura massiva, através de máquinas pensantes (*selbst denkende Maschinen*), e pelos quais resultam a atuação em conformidade com a simulação de comportamentos humanos através de condutas programáticas previamente delimitadas (*Simulation menschlichen Verhaltens durch Maschinen*)". Cfr. Luís Manuel Pica, *A inteligência artificial no Direito Tributário: Fundamentos e Limites Constitucionais*, Coimbra, Almedina, 2023, p. 32.

[5] Christian Würschinger, «Künstliche Intelligenz – Zwischen Wunsch und Wirklichkeit», *Wirtschaftsinformatik & Management*, vol. 12, n.º 2, 2020, p. 86.

[6] Seguindo esta ideia, a Proposta de Regulamento sobre Inteligência Artificial da União Europeia consagra, no seu artigo 3.º, n.º 1, que um *sistema de inteligência artificial* é "um programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage" (ainda que para efeitos da presente proposta). Proposta de Regulamento do Parlamento Europeu e do Conselho, COM(2021), da Comissão Europeia, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN [consultado em 06/07/2023].

Por último, socorremo-nos das considerações tecidas pelo Grupo de Peritos em inteligência artificial da OCDE[7], o qual delimitou uma definição aberta e tecnologicamente neutra de *inteligência artificial*. De acordo com a OCDE, os sistemas de inteligência artificial são: i) sistemas baseados em máquinas capazes de fazer previsões, gerar recomendações ou influenciar o seu ambiente real ou virtual no âmbito de objectivos definidos por seres humanos; ii) sistemas que utilizam dados de entrada conceptualmente necessários, gerados por seres humanos ou máquinas, para percecionar ambientes reais ou virtuais e transformá-los em modelos estatísticos; iii) quando aplicados a novos dados, são finalmente capazes de formular opções e informações para ações com base nesses modelos, utilizando a dedução de modelos. Ao fazê-lo, estes sistemas têm diferentes graus de autonomia.

Já o Conselho da Europa formula esta questão de forma um pouco mais abstrata no seu estudo sobre a viabilidade e os possíveis elementos de um quadro jurídico para o desenvolvimento, a conceção e a utilização de sistemas de inteligência artificial no que diz respeito à proteção dos direitos humanos, à democracia e à realização do Estado de Direito[8]. A inteligência artificial é aqui definida como a descoberta de padrões e tendências em grandes conjuntos de dados, utilizando para o efeito métodos estatísticos. Através dela, algoritmos inteligentes permitiram o reconhecimento de imagens e sons, a racionalização de produtos e serviços e grandes ganhos de eficiência na realização de tarefas complexas. Foi o aparecimento de sistemas de *big data*, constituídos por grandes memórias, grandes quantidades de dados e processadores rápidos, que, na sequência do aparecimento da *world wide web*, acelerou o desenvolvimento de novos métodos de desenvolvimento de algoritmos com base nos quais podem ser criados e treinados modelos probabilísticos.

Com base no referido, importa concluir com a seguinte ideia: *mais que uma verdadeira "inteligência", devemos considerar a existência de uma máquina instrumentalizada aos objetivos do ser humano, a qual é destinada à análise sequencial de dados e informações para reprodução dos resultados identificados previamente*[9]. Como resultado, não se procurará uma substituição do ser humano, mas sim um instrumento destinado à concretização dos seus objetivos. Assim, deixam-se de lado questões éticas (cujo sentido e teor não se negligencia nem se menospreza), mas procuraremos conceber um estudo jurídico direcionado à aplicabilidade da

---

[7] Oecd, *Artificial Intelligence in Society*, OECD Publishing, Paris, 2019, disponível em https://doi.org/10.1787/eedfee77-en [consultado em 25/07/2023].

[8] Ad Hoc Committee on Artificial Intelligence, *Feasibility Study*, CAHAI (2020)23, n.º 4, 2020, disponível em https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da [consultado em 25/07/2023].

[9] Luís Manuel Pica, *A inteligência artificial no Direito Tributário*…, *cit.*, p. 29.

inteligência, designadamente no que concerne ao domínio da prática agrícola e as repercussões jurídicas que a mesma poderá ter.

3. Um novo paradigma de agricultura: a agricultura digital, a (semi-)automatização e o agro-autómato

Como deixámos presente no ponto antecedente, a inteligência artificial dificilmente poderá ser concebida como um ente autónomo e subjetivamente relevante. Pelo contrário, devemos entender a inteligência artificial enquanto instrumento criado e utilizado pelo e para o ser humano, sendo um seu instrumento afeto aos seus próprios interesses. Enquanto instrumento capaz de reproduzir as condutas programadas pelo seu criador, procura-se atingir e concretizar os desideratos do seu utilizador, sendo a sua instrumentalidade e os interesses finalísticos o seu meio e fim. E será por via desta instrumentalidade que não se poderá desconsiderar a falta de autonomia da inteligência artificial.

Enquanto instrumento potencializador dos interesses do seu criador e do seu utilizador, não se poderá deixar de identificar a panóplia de áreas e domínios onde a sua aplicabilidade será determinante. Isto porque as tecnologias digitais em geral, e a inteligência artificial em particular, estão, cada vez mais, a penetrar nos vários domínios da sociedade e da economia, sendo exemplo inequívoco a sua utilização na produção agrícola.

Pense-se, por exemplo, que a inteligência humana e a inteligência artificial interagem e complementam-se mutuamente nas várias produções agrícolas, desde a horticultura, passando pela fruticultura e viticultura, até à cultura de cereais. A inteligência artificial assume-se cada vez mais como incontornável aliada no processo de *decision-making* no domínio da agricultura, nomeadamente, com vista a uma atividade agrícola com maior produtividade e sustentabilidade, com maior proteção do consumidor e menor impacto ambiental, sendo diversas as manifestações da sua *vis* transformadora:

i) Gestão das culturas e das colheitas: *robots* dotados de inteligência artificial e de sensores e mecanismos dedicados podem efetuar tarefas de "agricultura inteligente" como a plantação, a colheita e a poda com precisão e eficiência, recolher dados sobre a composição do solo, os níveis de humidade e a saúde das plantas, permitindo aos agricultores otimizar a utilização de fertilizantes[10], bem como avaliar os níveis de nutrientes, o equilíbrio do pH e outros parâmetros de saúde

[10] Jennifer Clapp; Sarah-Louise Ruder, «Precision Technologies for Agriculture: Digital Farming, Gene-Edited Crops, and the Politics of Sustainability», *Global Environmental Politics*, vol. 20, n.º 3, 2020, p. 49, disponível em https://direct.mit.edu/glep/article/20/3/49/95048/Precision-Technologies-for-Agriculture-Digital.

do solo, orientando os agricultores para práticas ótimas de gestão do solo[11]; a inteligência artificial permite a condução autónoma de tratores e outro equipamento agrícola, assim libertando trabalhadores de tarefas rotineiras e/ou que representem risco para a vida humana[12]; os algoritmos de inteligência artificial são capazes de proceder à análise de dados de sensores do solo e de previsões meteorológicas, interpretando dados com vista à otimização dos programas de irrigação e à conservação dos recursos hídricos[13], prevendo padrões climáticos e ajudando a planear as variações sazonais[14]; as plataformas alimentadas por inteligência artificial podem oferecer recomendações personalizadas de plantação, rotações de culturas ou práticas de gestão de pragas com base em condições agrícolas específicas[15];

ii) Gestão de pragas e de doenças: a inteligência artificial tem sido implementada enquanto estratégia votada ao controlo e à gestão de doenças e de pragas (*v.g.*, infestações de insetos) que afetem as culturas, designadamente, pela análise de imagens ou de dados fornecidos por sensores com vista a identificar sinais dessas doenças ou pragas[16]. Deste modo, propicia uma atempada ministração de tratamentos, bem como uma maior eficácia na identificação, controlo e eliminação de pragas, designadamente, através da utilização de dispositivos dotados de inteligência artificial aptos a identificar níveis de infestação de pragas e propor

---

[11] Manojit Chowdhury; Rohit Anand, «AI-Driven Agricultural Robotics: Advancements and Applications», *Agriculture & Food: E-Newsletter*, vol. 5, n.º 7, 2023, p. 420, disponível em https://www.researchgate.net/publication/371964537_AI-Driven_Agricultural_Robotics_Advancements_and_Applications.

[12] Vincenzo Barrile *et al.*, «Experimenting Agriculture 4.0 with Sensors: A Data Fusion Approach between Remote Sensing, UAVs and Self-Driving Tractors», *Sensors*, vol. 22, n.º 20, 2022, p. 7916, disponível em https://www.mdpi.com/1424-8220/22/20/7910.

[13] André Glória *et al.*, «Management for Sustainable Irrigation Systems Using Internet-of-Things», *Sensor*s, vol. 20, n.º 5, 2020, p. 1404, disponível em https://www.mdpi.com/1424-8220/20/5/1402.

[14] Bogdan Bochenek; Zbigniew Ustrnul, «Machine Learning in Weather Prediction and Climate Analyses—Applications and Perspectives», *Atmosphere*, vol. 13, n.º 2, 2022, p. 187, disponível em https://www.mdpi.com/2073-4433/13/2/180.

[15] J. Schöning; M.L. Richter, «AI-Based Crop Rotation for Sustainable Agriculture Worldwide», in *Global Humanitarian Technology Conference (GHTC)*, 2021, p. 142, disponível em https://www.researchgate.net/publication/356678115_AI-Based_Crop_Rotation_for_Sustainable_Agriculture_Worldwide.

[16] A. Kamilaris; F. X. Prenafeta-Boldú, «Deep Learning in Agriculture: A Survey, Computers and Electronics», *Agriculture*, vol. 147, 2018, pp. 70-90, disponível em https://www.sciencedirect.com/science/article/abs/pii/S0168169917308803.

soluções específicas no seu combate[17], seja pela via da utilização de pesticidas ou de inimigos naturais (caso em que a inteligência artificial terá por função a determinação da solução mais eficiente, bem como das quantidades e zonas a ser aplicada, de modo a reduzir o impacto ambiental da operação[18]), os quais podem ser implementados pelo recurso a *drones* dotados desses mecanismos de deteção e de eliminação[19];

iii) Identificação e gestão de ervas daninhas: os algoritmos de inteligência artificial podem identificar e diferenciar entre plantas cultivadas e ervas daninhas invasoras, permitindo medidas de eliminação – ou de controlo e gestão – destas[20]. Utilizando a aprendizagem automática da inteligência artificial (reconhecimento de imagem), um *robot* de monda reconhece as ervas daninhas em relação às culturas (*v.g.*, cereais, algodão, milho, etc.), permitindo a sua eliminação;

iv) Controlo de qualidade dos produtos agrícolas: os sistemas de inteligência artificial podem inspecionar a qualidade dos produtos agrícolas e proceder à sua classificação com base em atributos como o tamanho, a cor e a maturação[21], garantindo a consistência da qualidade alimentar;

v) Organização de cadeias de abastecimento e de fornecimento, gestão de inventário: os algoritmos de inteligência artificial podem desempenhar uma importante função na previsão de rotas de transporte, na gestão da cadeia de abastecimento (desempenhando tarefas de gestão de inventário, tais como moni-

---

[17] K. D. Jyothi; M. S. R. Sekhar; S. Kumar, «Applications of Statistical Machine Learning Algorithms in Agriculture Management Processes», in *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, Solan, India, 2021, p. 237.

[18] Ana Cláudia Teixeira *et al.*, «A Systematic Review on Automatic Insect Detection Using Deep Learning», *in Agriculture*, vol. 13, n.º 3, p. 714, disponível em https://www.mdpi.com/2077-0472/13/3/713.

[19] Fernando H. Iost Filho *et al.*, «Drones: Innovative Technology for Use in Precision Pest Management», *Journal of Economic Entomology*, vol. 113, n.º 1, 2020, p. 1, disponível em https://academic.oup.com/jee/article/113/1/1/5666881?login=false.

[20] Jonas Anderegg *et al.*, «On-farm evaluation of UAV-based aerial imagery for season-long weed monitoring under contrasting management and pedoclimatic conditions in wheat», *Computers and Electronics in Agriculture*, vol. 204, 2023, pp. 2-3, disponível em https://www.sciencedirect.com/science/article/pii/S0168169922008663.

[21] I. H. Hadfi; Z. I. Mohd Yusoh, «Banana Ripeness Detection and Servings Recommendation System using Artificial Intelligence Techniques», *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 10, n.º 2-8, 2018, pp. 83-87, disponível em: https://jtec.utem.edu.my/jtec/article/view/4464.

torização de *stocks*, de expedições e entregas) e de fornecedores (avaliando preços em vigor no mercado, qualidade e prazos de entrega)[22];

vi) Agrofinanças e avaliação de riscos: os sistemas de inteligência artificial podem proceder à avaliação de riscos financeiros (tais como catástrofes naturais, eventos geopolíticos, flutuações do mercado e outros eventos que possam causar interrupções de abastecimento ou fornecimento)[23], bem como fornecer recomendações para investimentos agrícolas e apólices de seguro.

Dito isto, somos impelidos a afirmar que a inteligência artificial revela-se como um sistema de assistência que possibilita aos agricultores o aumento da eficiência dos recursos disponíveis, os quais permitem a concretização de rácios de eficácia desejados[24] e a concretização de desideratos imediatos e mediatos, designadamente:

a) Através da utilização de sistemas de inteligência artificial aplicados à agricultura, consegue-se atingir desideratos que são afetos à disponibilidade direta dos meios utilizados na agricultura, designadamente, uma racionalização de meios e um aumento na eficiência da produção agrícola. Através destes meios atinge-se uma majoração na atividade produtiva e uma agricultura mais sustentável e economicamente mais rentável;

b) Contudo, não se poderá desconsiderar, também, a concretização de interesses mediatos. Através da adoção por métodos mais adequados, segundo critérios ecológicos mais eficazes e com uma racionalização de meios, consegue-se, por exemplo, diminuir os riscos de impactos ambientais indesejados, tais como poluição dos solos, dos ecossistemas ou do meio ambiente, os quais poderiam resultar em impactos negativos gerais. O controlo da atividade agrícola é, portanto, maior quanto aos impactos que poderiam surgir por via de trabalhos descontrolados, pouco planeados e baseados em critérios puramente cognitivos, tradicionais e culturais.

---

[22] H. Min, «Artificial intelligence in supply chain management: theory and applications», *International Journal of Logistics: Research and Applications*, vol. 13, n.º 1, 2010, pp. 13-39, disponível em https://www.tandfonline.com/doi/epdf/10.1080/13675560902736537?needAccess=true&role=button.

[23] Cosimo Magazzino, «The Inextricable Link Among Climate Change, Pandemic, Migrations, and Geopolitics: How Artificial Intelligence Can Help Us - The Inextricable Link Among Climate Change, Pandemic, Migrations, and Geopolitics: How Artificial Intelligence Can Help Us», in José Alberto Benitez-Andrades *et al.* (coord.), *Global Challenges for a Sustainable Society: EURECA-PRO The European University for Responsible Consumption and Production*, Springer, Suíça, 2023.

[24] A título de exemplo, consegue-se uma maior eficiência na produção agrícola quando existe uma conversão de trabalhos considerados "fastidiosos" e "tendenciosos", transferindo-os para a máquina com vista a melhorar os critérios de eficácia pretendidos (*v.g.* controlo e análise de dados, regas temporalmente necessárias, gestão de pragas, etc.).

Porém, não afirmamos, com isto, que os agricultores são substituídos por sistemas de inteligência artificial. Os agricultores não se tornam supérfluos no seu trabalho, mas operam com estruturas de trabalho e qualificações alteradas com base na sua própria experiência prática. A medida em que a utilização da inteligência artificial apoiará a produção agrícola no futuro depende também da confiança e da aceitação dos agricultores. Por isso, são fatores importantes para uma utilização sustentável a existência de um quadro jurídico eficaz e, ainda, de sistemas de segurança direcionados à eficiência económica e ecológica. Isto aplica-se não só à organização e gestão agrícola otimizada pela inteligência artificial, mas também, em particular, à criação de animais e ao cultivo de vários produtos agrícolas.

4. A responsabilidade dos atos praticados pelos "agro-autómatos" e o ressarcimento dos danos causados

4.1. *Ponto de partida*

Atenta a demonstrada simbiose entre a inteligência artificial e a agricultura, e como posteriormente se voltará a secundar, não podemos deixar de referir a necessidade de regulação da inteligência artificial e dos atos praticados por estes sistemas em utilização. Neste domínio, colocam-se vários problemas jurídicos. Por exemplo, o que acontece se um sistema de inteligência artificial praticar atos desconformes com a vontade do seu utilizador (p.e., a inteligência artificial apanha não só morangos vermelhos, mas também todos os verdes e amarelos, o que significa uma perda considerável de lucro para o agricultor)? Quem será o responsável pelos danos[25]? Outra questão que tem suscitado inúmeros problemas e questões (e também inúmeros estudos doutrinários) reside nos chamados "resultados tecnicamente inaceitáveis" da inteligência artificial. Nos casos mais extremos, falamos daquelas decisões que são erradamente praticadas porque o sistema inteligente se baseou em características erradas e não é possível encontrar com exatidão o motivo da decisão.

Com efeito, vários problemas se levantam no que diz respeito aos ilícitos praticados por estes sistemas de inteligência artificial:

i) *Complexidade*: multiplicidade de atores nos ecossistemas digitais e multiplicidade de componentes digitais – *hardware*, *software*, serviços;

[25] Mafalda Miranda Barbosa, «O futuro da responsabilidade civil desafiada pela inteligência artificial: as dificuldades dos modelos tradicionais e caminhos de solução», *Revista de Direito Civil*, vol. 2, Almedina, 2020, p. 290.

ii) *Opacidade*: a opacidade dos procedimentos decisórios tomados pela inteligência artificial gera aquilo que é designado por caixas negras (*blackbox*), nomeadamente por via do sistema de autoaprendizagem do algoritmo[26]. Por via desta "aprendizagem" vai-se tornando cada vez mais difícil prever o comportamento de um produto apoiado pela inteligência artificial, o momento em que o algoritmo aprendeu erroneamente ou o momento disruptivo do algoritmo originário[27];

iii) *Abertura*: atualizações ou melhorias constantes no sistema de inteligência artificial tornam-no imprevisível, sendo que essas atualizações podem ser controladas por *updates* manuais por via da interação com outros sistemas ou fontes de dados;

iv) *Autonomia:* intimamente conexa com a questão da abertura, os atos praticados pela inteligência artificial carecem de um controlo humano constante. Isto porque uma das características matriciais da inteligência artificial é a sua autonomia, praticando atos com menos necessidade do ser humano, o que levará a questões (éticas, mas, também, jurídicas) de imputabilidade e de legitimidade pelos atos praticados;

v) *Dependência de dados*: outra das preocupações que não pode ser despicienda é a dependência de informações externas, pois os dados de utilização não estão pré-instalados na inteligência artificial, nem são passíveis de antevisão pelo programador do algoritmo utilizado pelo mesmo. Estes dados – que servem de *inputs* para o funcionamento da inteligência artificial – acabam por ser gerados, ou comunicados, a partir do exterior, pelo que se tornará necessário um maior controlo e cuidado nos mesmos;

---

[26] O dinamismo do algoritmo traz consigo a sensibilidade de a própria inteligência artificial decidir sobre decisões, pelo que o *iter* cognitivo que levou à emanação do ato poderá revelar-se cada vez mais difícil e reduzido, segundo o quadro de previsibilidade e de catalogação do algoritmo inicialmente programado. Fernando Serrano Antón, «Fiscalidad y Robótica: funcionalidades disruptivas en el Derecho tributario», in *Fiscalidad e Inteligencia Artificial: Administración Tributaria y Contribuyentes en la era digital*, Thomson Reuters Aranzadi, p. 52.

[27] "Resulta, igualmente difícil, a delimitação de um critério coerente de imputação de responsabilidade algorítmica, quando os *updates* do *software* utilizados pela administração forem realizados segundo critérios fornecidos por entidades terceiras e que não têm qualquer ligação com o produtor originário do produto. Da articulação mencionada, não se consegue determinar se a lesão ocorreu em virtude do algoritmo modificado ou, por porventura, se se deve à programação originária operada no sistema de inteligência artificial, implicando uma problemática adstrita ao desenvolvimento concreto do algoritmo utilizado e que se desencadeia segundo um dinamismo que complexifica a determinação funcional daquela e a identificação concreta do ato zero". Luís Manuel Pica; *Mário Filipe Borralho*, «A personificação dos autómatos? A eclosão de uma nova arquitetura jurídica derivada da inteligência artificial», in *E.Tec Yearbook – Industry 4.0: Legal Challenges*, Braga, 2022, p. 46, disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/81488/1/E-TEC_2022_Yearbook.pdf [consultado em 22/07/2023].

vi) *Vulnerabilidade*: especial suscetibilidade a violações da cibersegurança devido à abertura e complexidade subjetiva (sujeitos em rede) e objetiva (dados de acesso aberto) dos ecossistemas digitais.

Se pensarmos nestes riscos inerentes à inteligência artificial, percebemos que os riscos identificados *supra* podem ser repercutidos na "agricultura inteligente"[28]. Isto porque se a utilização de sistemas de inteligência artificial causar ferimentos pessoais, danos materiais ou danos ambientais, coloca-se a questão de saber a quem deve ser imputado o ato danoso[29] e, consequentemente, sobre quem recai a obrigação de indemnização.

Vejamos, assim, algumas ideias e (possíveis) soluções.

4.2. *A (necessidade de) adaptação dos institutos jurídicos de responsabilidade civil*

Os problemas até aqui identificados levam-nos a uma conclusão já assumida: a regulação dos sistemas de inteligência artificial, nomeadamente naquilo que respeita à imputação pelos seus atos, deverá ser feita por via dos institutos de responsabilidade civil. Por conseguinte, não assumimos a tese de uma *antropomorfização* que resulte numa "independência" ou "autonomização" dos sistemas inteligentes e, consequentemente, na imputação a estes[30]. Nem tampouco a "perversão" das normas de Direito Societário para permeabilização dos sistemas de inteligência artificial. Pelo contrário, a natureza maquinal e silogista bem como a sua instrumentalidade aos desideratos e desejos do ser humano suscitam logo

---

[28] "A proposta também tem ligações indiretas ao Pacto Ecológico Europeu. As tecnologias digitais, em especial, incluindo a IA, são um fator essencial para alcançar os objetivos de sustentabilidade do Pacto Ecológico em muitos setores diferentes (incluindo os cuidados de saúde, os transportes, o ambiente e a agricultura)", disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52022PC0496&from=EN [consultado em 22/07/2023].

[29] Pense-se, por exemplo, se animais de criação, como galinhas ou porcos, forem feridos durante a alimentação automatizada; se um sistema de gestão da saúde animal controlado pela inteligência artificial não reconhecer as doenças dos animais ou administrar a medicação errada; se forem aplicados fertilizantes ou pesticidas, de forma pouco adequada ou em doses indevidas, durante o processo de colheita; se a faixa marginal de água não for respeitada ou se os limites de aplicação forem ultrapassados, ou se toda a (futura) exploração agrícola 4.0 entrar em colapso devido a um ataque cibernético.

[30] "A sua ligação a bases de dados e as interconexões aos demais dados pessoais que lhe permitem alterar o algoritmo originário programado pelo homem são factos que não lhe conferem autonomia cognitiva e um substrato humano suficientemente sólido e dignificante para a designada antropomorfização". Luís Manuel Pica; *Mário Filipe Borralho*, «A personificação dos autómatos? A eclosão de uma nova arquitetura jurídica derivada da inteligência artificial», *cit.*, p. 32.

que a imputação seja feita na pessoa deste último[31]. Duas são as razões: (i) a sua instrumentalidade face aos desideratos do seu utilizador (ii) e que o sistema inteligente é produto do ser humano e existe por e para si.

Neste sentido, veja-se que, inicialmente, o Parlamento Europeu defendeu a tese da *antropomorfização*, nomeadamente pela ascensão de um *tertium genus* correspondente à criação de uma nova categoria de pessoa ("pessoa eletrónica"), cujo regime seria suficientemente robusto e sólido, podendo ser, inclusive, integrado como um instituto jurídico *ex novo*, alterando o estatuto jurídico das pessoas vertido no Código Civil[32].

Contudo, uma solução tão arrojada não pode ser levianamente aceite e introduzida num sistema jurídico (ou conjunto deles). Os conhecidos estudos sobre ordenação normativa exigem que a regulação de qualquer conduta social seja estudada, cuidada e previsivelmente atendível num quadro de razoabilidade e de segurança. E, perante uma novidade cujos contornos são ainda (muitos deles) desconhecidos, o legislador é impelido a refletir, a academia a estudar as possibilidades e os órgãos legiferantes obrigados a prever as hipóteses sobre a sua inserção e enquadramento num sistema jurídico[33].

Com efeito, as soluções apresentadas recentemente têm deixado à margem esta solução inicialmente ensaiada, procurando soluções sistemicamente consolidadas e segundo uma ordenação já conhecida com os institutos jurídicos vigentes nos sistemas jurídicos. Por isso, a solução proposta tem vindo a apontar para a criação de um regime jurídico de imputação de responsabilidade aos produtores e utilizadores de sistemas de inteligência artificial, adaptando os regimes de

---

[31] Florent Thouvenin; Markus Christen; Abraham Bernstein; Nadja Braun Binder; Thomas Burri; Karsten Donnay; Lena Jäger; Mariela Jaffe; Michael Krauthammer; Melinda Lohmann; Anna Mätzener; Sophie Mützel; Liliane Obrecht; Nicole Ritter; Matthias Spielkamp; Stephanie Volz, *Positionspapier: Ein Rechtsrahmen für künstliche Intelligenz*, DSI 2021, disponível em https://www.zora.uzh.ch/id/ eprint/211386/ [consultado em 26/07/2023].

[32] António Pinto Monteiro, «'*Qui facit per alium, facit per se'* — Será ainda assim na era da robótica?», in *Direito e Robótica*, Coimbra, Centro de Direito do Consumo, Faculdade de Direito da Universidade de Coimbra, 2020, p. 13.

[33] Como referimos noutra sede, "bem vistas as coisas, não podemos deixar de referir que a ordenação do Direito obriga o legislador a consagrar medidas coerentes e direcionadas à regulação pacífica e sistémica das matérias pretendidas". Luís Manuel Pica; Mário Filipe Borralho, «A personificação dos autómatos? A eclosão de uma nova arquitetura jurídica derivada da inteligência artificial», *cit.*, p. 33.

responsabilidade civil já existentes[34]. Esta tese evidencia-se, principalmente, com a Comunicação 2021/206, a qual aprova uma Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União[35], bem como por via da proposta de Diretiva para a Responsabilidade Civil extracontratual adaptada à Inteligência Artificial (Proposta n.º 2022/0303 (COD)[36]), e de uma proposta de Diretiva para a Responsabilidade decorrente de Produtos Defeituosos (Proposta n.º 2022/0302 (COD)[37]). Por via das referidas propostas procurou-se: i) assegurar que as vítimas de danos causados por produtos de inteligência artificial beneficiam da mesma proteção que os consumidores de qualquer outro produto – debatendo-se com o problema da distribuição de responsabilidade no que a estes produtos respeita; ii) reduzir as dúvidas na atribuição de responsabilidade direta na utilização empresarial; iii) uniformizar e harmonizar legislação a nível europeu, de forma a prevenir discrepâncias entre os sistemas jurídicos dos Estados-Membros da União Europeia.

A ideia proposta parte, fundamentalmente, dos três diplomas enunciados, sendo que a Proposta de Regulamento para a Inteligência Artificial, de 21 de abril de 2021, distingue vários níveis de risco na utilização de sistemas de inteligência

[34] "As atuais regras nacionais de responsabilidade, em especial em matéria de responsabilidade culposa, não se adequam ao tratamento de ações de indemnização por danos causados por produtos e serviços assentes em IA". Proposta de Diretiva para a Responsabilidade Civil em assuntos de Inteligência Artificial (Proposta n.º 2022/0303 (COD)), disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52022PC0496&from=EN [consultado em 22/07/2023].

[35] Nas palavras do Parlamento Europeu e do Conselho, esta proposta "estabelece regras harmonizadas para o desenvolvimento, a colocação no mercado e a utilização de sistemas de Inteligência Artificial na União na sequência de uma abordagem proporcionada baseada no risco. Propõe-se uma definição inequívoca e preparada para o futuro de «inteligência artificial». Algumas práticas de Inteligência Artificial particularmente prejudiciais são proibidas, uma vez que violam os valores da União, e são propostas restrições e salvaguardas específicas relativamente a determinadas utilizações de sistemas de identificação biométrica à distância para efeitos de manutenção da ordem pública. A proposta estabelece uma metodologia de análise de riscos sólida para definir sistemas de Inteligência Artificial de «risco elevado» que criam riscos significativos para a saúde e a segurança ou para os direitos fundamentais das pessoas. Esses sistemas de Inteligência Artificial terão de cumprir um conjunto de requisitos obrigatórios horizontais para uma Inteligência Artificial de confiança e seguir procedimentos de avaliação da conformidade antes de poderem ser colocados no mercado da União. Os fornecedores e os utilizadores desses sistemas também estão sujeitos a obrigações previsíveis, proporcionadas e claras para garantir a segurança e o respeito da legislação em vigor que protege os direitos fundamentais ao longo de todo o ciclo de vida dos sistemas de Inteligência Artificial".

[36] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52022PC0496&from=EN [consultado em 22/07/2023].

[37] Disponível em https://eur-lex.europa.eu/resource.html?uri=cellar:b9a6a6fe-3ff4-11ed-92ed-01aa75ed71a1.0011.02/DOC_1&format=PDF [consultado em 22/07/2023].

quando repercutidos os efeitos na esfera jurídica dos destinatários. Para além disso, exige-se que os sistemas de inteligência artificial sejam concebidos e desenvolvidos com capacidades que permitam o registo automático de eventos ("registos") enquanto o sistema de inteligência artificial de risco elevado estiver em funcionamento (cfr. artigo 12.º, n.º 1, da Proposta de Regulamento sobre Inteligência Artificial). Entende-se esta obrigatoriedade, pois procura prevenir-se situações de obscuridade decisória, designadamente naquilo que a doutrina considera como *blackbox*[38]. Por via dos registos de atos praticados atinge-se um nível de rastreabilidade que permite identificar o funcionamento do sistema de inteligência ao longo do seu ciclo de vida, percorrendo todo o *iter* decisório do sistema de inteligência artificial[39]. Concebe-se que "os sistemas de IA [Inteligência Artificial] de risco elevado devem ser concebidos e desenvolvidos de tal modo, incluindo com ferramentas de interface homem-máquina apropriadas, que possam ser eficazmente supervisionados por pessoas singulares durante o período de utilização do sistema de IA" (interpolado nosso)[40]. Em termos sistémicos, dir-se-á que a supervisão humana deve procurar prevenir ou minimizar os riscos para a saúde, a segurança ou os direitos fundamentais que possam surgir quando um sistema de inteligência de risco elevado é usado em conformidade com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsíveis, em especial quando esses riscos persistem apesar da aplicação das condicionantes impostas legalmente.

Todos estes institutos clássicos de responsabilidade civil são inegavelmente ricos e a sua bondade é inquestionável. Todavia, não se nega que os mesmos carecem de respostas face às características dos sistemas de inteligência artificial. Ou seja,

---

[38] "É que, como já referimos, a problemática da blackbox ou 'caixa negra' corresponde à impossibilidade de a Administração Tributária justificar o motivo e os fundamentos da decisão emanada pelos sistemas de inteligência artificial por si utilizados nas atividades de gestão fiscal. A capacidade de aprendizagem e de mutação do algoritmo - que permite a sua transformação constante, com base nas decisões, nos atos praticados por esta, e, também, na fácil alteração manual do mesmo -, conduz-nos à sua incompreensão intermédia na atuação, tornando muito difícil determinar o porquê de o algoritmo utilizado pela inteligência artificial adotar aquela determinada decisão". Luís Manuel Pica, *A inteligência artificial no Direito Tributário*…, *cit.*, p. 188.

[39] "Dir-se-á que estamos perante um verdadeiro princípio norteador que permite aos sujeitos envolvidos conhecer o teor das decisões e dos atos praticados pelos sistemas inteligentes, dotando-os de informações necessárias sobre todos os momentos, atos, procedimentos e meios utilizados e adotados por estes". Luís Manuel Pica; *Mário Filipe Borralho*, «A personificação dos autómatos? A eclosão de uma nova arquitetura jurídica derivada da inteligência artificial», *cit.*, p. 34.

[40] Proposta de Regulamento sobre Inteligência Artificial do Parlamento Europeu e do Conselho, o qual estabelece regras harmonizadas em matéria de Inteligência Artificial (COM(2021) 206 final (2021/0106), disponível em https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_1&format=PDF [consultado em 22/07/2023].

colocam-se as mesmas questões derivadas dos institutos de responsabilidade civil existentes, designadamente na complexidade de atores nos ecossistemas digitais e na multiplicidade de componentes digitais – *hardware*, *software*, serviços; na opacidade dos procedimentos decisórios tomados pela inteligência artificial; no caráter aberto das atualizações ou melhorias constantes no sistema de inteligência artificial; na autonomia dos mesmos; na dependência de dados e da qualidade dos mesmos; e na vulnerabilidade a que os sistemas de inteligência artificial estão expostos.

É na senda destes problemas (não negamos que não se tratará de um diploma exaustivo e que dê resposta a todas estas problemáticas) que a Proposta de Regulamento sobre Inteligência Artificial intenta convergir na convocação de um instituto de responsabilidade civil próprio e adequado às especificidades da inteligência artificial. A evolução de um instituto jurídico capaz e adequado *às vicissitudes próprias* pretende instituir um conjunto de medidas garantísticas dimensionadas temporalmente num momento prévio e preventivo, bem como num momento posterior dimensionado à "reposição" factual em caso de eventuais danos. Entende-se que os sujeitos devem encontrar nos procedimentos ditos "inteligentes" um fundamento cognitivo que lhes permita conhecer o *iter* decisório. E este conhecimento apenas será possível se forem instituídas medidas informativas, registais e de armazenamento de informação sobre as várias dimensões que são adotadas no procedimento de decisão. Para além disto, este registo e conhecimento permitir*ão* aferir o momento concreto em que o comportamento desviante ocorreu e, consequentemente, permitir*ão* imputar à pessoa autora do ato danoso a responsabilidade e a obrigação de indemnização que daí deriva.

Contudo, denota-se que o regime legal pretendido na mencionada proposta de regulamento europeu é profundamente personalista, pois centra a sua tutela no ser humano e nos eventuais danos causados a este. A dimensão personalista perspetiva que o instituto jurídico da responsabilidade civil desenvolvida centra a sua atenção na esfera jurídica individual e privatística do ser humano. Deixa-se, assim, interesses difusos e que genericamente constituem direitos (fundamentais) que obedecem (e merecem) também a uma tutela não individual e generalizada. A abordagem aos direitos difusos, como por exemplo o direito à saúde e ao meio ambiente, *é deixada ao sector privado*, passando a gestão destes direitos a ser individualizada pelos utilizadores da inteligência artificial.

Isto porque a tendência do jurista é a de, em caso de uma inovação ou realidade *ex novo*, legislar e criar um regime jurídico próprio às necessidades em ascensão. Deixa-se de lado a adaptação de regimes existentes ou a análise casuística

da legislação existente para adequar às necessidades então emergentes[41]. Mas, em certos casos, a melhor maneira de conhecer o direito adequado aplicável a atividades especializadas é consultar as regras gerais já existentes e vigentes no ordenamento jurídico.

Por isso, *não podemos deixar de considerar o próprio regime jurídico da responsabilidade por danos ambientais, aprovado pelo Decreto-Lei n.º 147/2008, de 29 de julho. Consagra* o citado diploma legal uma verdadeira responsabilidade civil derivada dos danos ambientais[42], bem como às ameaças iminentes desses danos, causados em resultado do exercício de uma qualquer atividade desenvolvida no âmbito de uma atividade económica, independentemente do seu carácter público ou privado, lucrativo ou não. Falamos de uma verdadeira i) responsabilidade objetiva, na qual quem, em virtude do exercício de uma atividade económica enumerada no anexo iii do citado decreto-lei, ofender direitos ou interesses alheios por via da lesão de um qualquer componente ambiental é obrigado a reparar os danos resultantes dessa ofensa, independentemente da existência de culpa ou dolo; e ii) de uma responsabilidade subjetiva suportada por quem, com dolo ou mera culpa, ofender direitos ou interesses alheios por via da lesão de um componente ambiental fica obrigado a reparar os danos resultantes dessa ofensa.

Todavia, questiona-se a efetividade que esse instituto poderá ter e se o mesmo será adequado para regular as atuações baseadas em sistemas de inteligência artificial. Será este instituto jurídico capaz de abranger todas as situações e complexidades derivadas das características próprias da inteligência artificial?

As principais dificuldades residem, por um lado, na não enumeração da atividade agrícola no seio das atividades ocupacionais constantes do anexo iii do mencionado decreto-lei e, por outro, na não consagração da exploração/prossecução dessa – ou de qualquer outra – atividade ocupacional através de sistemas de inteligência artificial, o que impede o funcionamento do regime de responsabilidade que, por prescindir da existência de dolo ou culpa, se apresenta mais garantístico

---

[41] Frank Easterbrook, *Cyberspace and the Law of the Hors*, The University of Chicago Legal Forum, 1996, pp. 207-216 [consultado em 22/07/2023].

[42] Segundo a alínea e) do n.º 1 do artigo 11.º do Decreto-Lei n.º 147/2008, de 29 de julho, consubstanciam danos ambientais: i) os danos causados às espécies e habitats naturais protegidos, considerando-se como aqueles que tenham "efeitos significativos adversos para a consecução ou a manutenção do estado de conservação favorável desses habitats ou espécies…"; ii) os danos causados à água, designadamente aqueles que "afetem adversa e significativamente: o estado ecológico ou o estado químico das águas de superfície, o potencial ecológico ou o estado químico das massas de água artificiais ou fortemente modificadas, ou o estado quantitativo ou o estado químico das águas subterrâneas…" ou "o estado ambiental das águas marinhas"; iii) os danos causados ao solo, definidos como "qualquer contaminação do solo que crie um risco significativo para a saúde humana devido à introdução, direta ou indireta, no solo ou à sua superfície, de substâncias, preparações, organismos ou microrganismos".

na reparação de danos resultantes da ofensa de direitos ou interesses alheios por via da lesão de um qualquer componente ambiental e, também, de danos ambientais, isto é, do regime de responsabilidade objetiva (previsto nos artigos 7.º e 12.º, n.º 1, do Decreto-Lei n.º 147/2008, de 29 de julho).

O enquadramento no aludido regime de responsabilidade objetiva somente pode ser operacionalizado através da decomposição casuística das várias vertentes que compõem a atividade agrícola, resultando dessa aproximação tipológica nele se incluírem os danos ambientais que resultem da utilização de sistemas de inteligência artificial no contexto, *v.g.*, da captação e represamento de águas (n.º 6), da libertação para o ambiente de produtos fitofarmacêuticos, pesticidas, agroquímicos e/ou de biocidas (n.º 7, al*íneas* c) e d)), da utilização de microrganismos geneticamente modificados ou da libertação deliberada para o ambiente de organismos geneticamente modificados (n.os 10 e 11), e ainda da gestão de resíduos agrícolas (não excecionados pelo artigo 2.º do Regime Geral da Gestão de Resíduos, publicado em anexo ao Decreto-Lei n.º 102-D/2020, de 10 de dezembro) (n.º 2, todos do anexo iii do Decreto-Lei n.º 147/2008, de 29 de julho).

Porém, a atividade agrícola não se esgota nessas atividades, sendo que todas as demais condutas ambientalmente danosas que não forem subsumíveis no aludido anexo iii encontram-se sob a égide da responsabilidade subjetiva, prevista nos artigos 8.º e 13.º do Decreto-Lei n.º 147/2008, de 29 de julho, da qual constitui pressuposto a alegação – e prova – do dolo ou da negligência de quem tenha causado danos ambientais em virtude do exercício dessas atividades ou uma ameaça iminente daqueles danos em resultado das mesmas. Acresce que, tratando-se de atividade não enumerada no aludido anexo iii do Decreto-Lei n.º 147/2008, de 29 de julho, e ante uma ameaça iminente de danos ambientais, o operador somente se encontra obrigado a adotar medidas de prevenção necessárias e adequadas "(…) se tiver agido com dolo ou com negligência"[43].

Neste sentido, o regime de responsabilidade civil implementado pelo Decreto-Lei n.º 147/2008, de 29 de julho, não se apresenta adequado para atingir o desiderato de absorver ou dar cobertura ao acréscimo de risco e externalidades negativas que a utilização de sistemas de inteligência artificial representa, no atual estágio evolutivo e no seio das atividades agrícolas, para o ambiente.

Destarte, e apesar da aplicabilidade dos modelos clássicos de responsabilidade civil existentes – que são tendencialmente cegos aos instrumentos através dos

[43] Manuel Gouveia Pereira, «A contaminação do solo resultante de passivos ambientais: (Des) enquadramento no Direito português», in Carla Amado Gomes; Rui Tavares Lanceiro (coord.), *Actas do Colóquio "Solos contaminados, riscos invisíveis"*, Lisboa, ICJP – Instituto de Ciências Jurídico-Políticas; CIDP – Centro de Investigação de Direito Público, 2020, p. 58, disponível em https://www.icjp.pt/sites/default/files/publicacoes/files/ebook_soloscontaminadosriscos_invisiveis_icjp_jun2020_0.pdf.

quais se produzem as condutas danosas –, as vicissitudes próprias dos entes artificialmente inteligentes exigem uma adaptação dos institutos que operam a aludida imputação de danos. Tal circunstância foi enfatizada pelas instâncias europeias, que sublinharam a necessidade de se estabelecer uma disciplina específica que permita dar uma resposta eficiente e coerente face à atuação potencialmente lesiva destes instrumentos mecanizados. Por isso, tem vindo a ser apresentado um conjunto de medidas que permitem o ressarcimento pelos danos causados e a responsabilização destes sistemas de inteligência artificial, designadamente através da criação de medidas e esquemas de seguros obrigatórios. Ou seja, as situações apresentadas em função da sua relevância para efeitos de imposição não podem deixar de comportar a adoção de instrumentos securitários que permitam a criação de fundos de garantia ou de compensação que se arrogam na subsidiação do mesmo para ressarcimento de eventuais danos causados.

4.3. *A personificação jurídica da inteligência artificial e a sua automatização enquanto ser eletrónico: o agro-automáto?*

Após termos enquadrado (brevemente) o regime jurídico próprio da responsabilidade ambiental e da proposta de regulamentação da inteligência artificial e da sua responsabilização, não podemos, sob pena de negligenciar uma fonte garantística possível, deixar de referir a tese da "comercialização dos autómatos".

A tese da "comercialização dos autómatos" tem vindo a ganhar grande destaque no seio da doutrina norte-americana[44], designadamente através da adaptação da estrutura jurídica dos Estabelecimentos Individuais de Responsabilidade Limitada e Sociedades Comerciais – estas constituídas sob o manto da unipessoalidade –, a qual poderá servir como arquétipo de regulação dos autómatos. Com isto procura-se aplicar o sistema de inteligência artificial a um centro jurídico de imputação de direitos e deveres que permita dar resposta às questões de responsabilização.

Neste domínio, se tomarmos por referência o Código Civil, distinguimos entre pessoas singulares e pessoas coletivas, tendo o legislador civilista sistematizado de forma autónoma, atribuindo-lhe vicissitudes próprias. Mas a sistematização do Código Civil exige-nos – em termos análogos ao que acontece no ordenamento jurídico alemão com o *BGB* – o recurso aos ensinamentos de Kant e Savigny[45]. A tese do indivíduo defendida por Kant exige-nos a assunção da ideia de que pessoas são centralizadas no "eu", sendo acompanhada pela sua dignidade. Tudo o que se afaste da sua dignidade e da importância dada ao ser

[44] Shawn Bayern, «The Implications of Modern Business–Entity Law for the Regulation of Autonomous Systems», *European Journal of Risk Regulation*, n.º 7, 2016, pp. 297-309.

[45] Sobre a sistematização e enquadramento histórico formulado por estes autores, cfr. Menezes Cordeiro, *Tratado de Direito Civil – Pessoas*, Coimbra, Almedina, 2007, pp.140 e ss.

humano pertencerá ao mundo das coisas[46]. Para além disto, as pessoas físicas agem livremente e de acordo com as normas morais que acham corretas. Pelo contrário, a tese sufragada por Savigny – cristalizada no nosso Código Civil – exige-nos a conceção da pessoa humana e física como elemento "substancial"[47]. Na esteira de Mota Pinto[48], a tese organicista existente no Código Civil sustenta a ideia de uma estrutura coletiva acompanhada de um substrato humano e/ou patrimonial, direcionando-os aos interesses coletivos e comuns ligados a uma função económico-social do instituto da personalidade coletiva[49]. À par destas, a pessoa humana e física pode criar centros de imputação que sirvam os seus propósitos e que sejam sujeitos de relações. As pessoas coletivas surgem assim como verdadeiras "ficções" criadas pelo e para o ser humano, servindo os seus propósitos e sendo instrumentais a estes. Como afirmámos num outro domínio, "daí que se atribua à pessoa física a característica de livre-arbítrio e de existência num contexto social, podendo atuar de forma livre e sendo matéria existente no mundo, enquanto as «pessoas jurídicas» são classificadas de forma negativa, isto é, são todas aquelas que não são pessoas físicas"[50].

Atenta a estrutura sistemática dos institutos preconizados, não podemos deixar de referir que a adoção desta tese resultará numa solução altamente complexa e de difícil aplicabilidade. Pense-se, por exemplo, nas questões que seriam levantas no âmbito do Direito Societário, designadamente sobre quem assumiria a posição de sócio e, portanto, quem iria exercer os direitos e deveres que este estatuto confere; ou quem iria exercer os poderes de direção e gestão. Por outro lado, o substrato humano que é elemento essencial nos centros de imputação de direitos dificilmente seria identificado[51].

---

[46] A fórmula do objeto (*Objektformel*) exige-nos um repúdio à equiparação do ser humano a uma máquina, a um objeto, ou a uma coisa. Com efeito, a "coisificação" do ser humano é contrária à conceção da dignidade da pessoa humana e consequentemente a violação da ideia de matricialidade que o mesmo assume num sistema social (e também jurídico). Jorge Reis Novais, *Princípios Estruturantes de Estado de Direito*, Coimbra, Almedina, 2021, pp. 13 e ss. Para maiores desenvolvimentos sobre a rejeição da equiparação, cfr. Luís Manuel Pica, *A inteligência artificial no Direito Tributário*…, *cit.*, 2023.

[47] Menezes Cordeiro, *Tratado de Direito Civil – Pessoas*, *cit.*, pp. 517 e ss.

[48] Carlos Mota Pinto, *Teoria Geral do Direito Civil*, 4.ª ed., Coimbra, Coimbra Editora, 2005, pp. 141 e ss.

[49] Desconsiderando a importância absoluta da personalidade jurídica enquanto centro de imputação de direitos e deveres. Cfr. Jorge Manuel Coutinho de Abreu, *Curso de Direito Comercial – Volume II – Das Sociedades*, 4.ª ed., Coimbra, Almedina, 2011.

[50] Luís Manuel Pica; *Mário Filipe Borralho*, «A personificação dos autómatos? A eclosão de uma nova arquitetura jurídica derivada da inteligência artificial», *cit.*, p. 30.

[51] Manuel de Andrade, *Teoria Geral da Relação Jurídica*, Coimbra, Almedina, 1997, p. 50.

Sem dificuldade se antevê que a integração de sistemas de inteligência artificial é dificilmente concebível enquanto estrutura jurídica, ou física, exclusivamente afeta aos interesses humanos. Podemos identificar diversos fundamentos, nomeadamente, os de que os sistemas de inteligência artificial inseridos em arquétipos análogos aos regimes coletivos ou de responsabilidade limitada não possuem uma direção efetiva pelo ser humano, nem, tampouco, estaremos sempre perante um verdadeiro interesse do ser humano, pois pode acontecer que a vontade seja a do ente artificial e não a do seu utilizador. É que não podemos esquecer a capacidade de mutação do algoritmo em que os interesses nele vertidos se desenvolvem para além do desiderato originário do programador e do utilizador. As mutações podem assim desenvolver uma vontade própria – alheia à vontade inicial seu utilizador –, desviando-se dos interesses iniciais que estiveram na origem da criação e da utilização do sistema de inteligência artificial. Pense-se novamente, por exemplo, que o sistema de inteligência artificial capta, através das redes digitais a que tem acesso, informação sobre determinado tipo de consumidores, obtendo a informação de que numa região longínqua são comercializados apenas morangos de determinada qualidade. Após esta aprendizagem, o sistema de inteligência artificial começa a realizar todos os atos destinados a produzir esses morangos concretos, que não são desejados pelos consumidores da região onde o utilizador os comercializa.

Pode-se afirmar que as problemáticas que se desenvolvem em torno desta solução são dificilmente concebíveis no seio dos ordenamentos de família germânica[52]. A conceção de patrimónios autónomos e/ou de centros de imputação de direitos suscitam sempre questões próprias afetas à "humanização" destes, ou à sua instrumentalidade aos interesses finalísticos associados. Consequentemente, a utilização da legislação vigente nestes ordenamentos jurídicos para enquadramento e regulação das condutas dos sistemas de inteligência artificial é, com o devido respeito, inadequada, redutora e disruptora em torno da dogmática própria destes sistemas artificiais. Isto porque é a própria legislação vigente que está concebida para regular uma dogmática concreta: os entes jurídicos afetos aos interesses do ser humano. A sua adaptação à regulação dos entes dotados de inteligência artificial é, assim, manifestamente insuficiente e impede a regulação de determinados aspetos concretos que se procura acautelar. Por isso, não podemos deixar de rejeitar a aplicabilidade deste regime jurídico de natureza especial, assumindo-se vital a construção de um instituto jurídico próprio e adaptado às vicissitudes próprias que caracterizam a atuação e utilização dos autómatos.

[52] Doris Forster; Janika Rieder, «Roboter als Rechtssubjekte – Der Streit um die E-Person», *Juridica Internacional*, vol. 30, 2021, pp. 32-39.

5. Conclusões

Embora se entenda os benefícios da inteligência artificial numa agricultura sustentável e cujos rácios de eficiência são bastante superiores a uma agricultura tradicional, não poderemos acolher a tese da "solução milagrosa" a todos os problemas que são colocados. Isto porque as melhoras significativas que são concretizadas não podem constituir fundamento perentório para acolher estes sistemas sem qualquer restrição e adequação sistémica. Não podemos deixar de referir que os sistemas são permeáveis a erros e que existem prejuízos e danos causados a pessoas, animais, plantas, terras ou ao próprio meio ambiente. E, perante um Estado de Direito responsável, o enfoque reclamado pela ciência jurídica não pode deixar de passar pela regulação e pelo equilíbrio de interesses. Mas, em primeiro lugar, se a convocação dos institutos clássicos de responsabilidade civil se mostra inegável, não poderemos deixar de referir que os mesmos são, ainda, insuficientes face às especificidades dos sistemas de inteligência artificial. Em segundo lugar, a novidade e o rápido desenvolvimento dos sistemas inteligentes determinam a necessidade de estudo prévio e de avaliação dos impactos que uma regulamentação iria ter.

Enfim, sendo certo que várias foram as reflexões tecidas ao longo do presente discurso, entendemos de todo conveniente terminar enfatizando o seguinte: a utilização dos sistemas de inteligentes não deve ser coartada, principalmente no seio de uma agricultura ecologicamente mais sustentável e eficiente, mas com os devidos cuidados e particular atenção aos atos potencialmente lesivos dos direitos e bens jurídicos alheios e que devem ser aqui tutelados.

REALIZAÇÃO DE ATOS NOTARIAIS POR VIDEOCONFERÊNCIA

Mercília Pereira Gonçalves[1]

Resumo: A simplificação digital dos atos notariais está associada a uma facilitação dos procedimentos em torno da digitalização. Os atos notariais são celebrados através de sessões de videoconferência, o que pressupõe uma verdadeira transformação digital, traduzindo uma inovação da atividade notarial. Ao longo deste artigo científico, abordaremos a celebração de atos notariais por videoconferência, numa perspetiva essencialmente notarial e exploraremos os aspetos peculiares do regime, ao abrigo do Decreto-Lei n.º 126/2021, de 30 de dezembro.

A análise do nosso tema será sucinta, na medida em que existe escassez de bibliografia sobre o presente tema. Desta forma, procuramos tratar fundamentalmente dos atos que podem ser realizados por videoconferência; da questão do agendamento; da junção de documentos; da videoconferência; da recusa da prática do ato notarial; do valor probatório dos atos realizados por videoconferência; do arquivo e acesso a documentos, das nulidades dos atos, bem como do tratamento de dados pessoais. Iremos expor também uma lista de procedimentos a utilizar pelos profissionais e um caso prático para ilustrar a situação dos atos à distância. Esperamos que o leitor obtenha um maior esclarecimento do regime jurídico existente e que possamos contribuir para uma boa reflexão na temática dos atos notariais, na égide da transformação digital. É do nosso pleno interesse contribuirmos ainda para a doutrina nacional em torno desta matéria.

Palavras-chave: Simplificação; Digital; Atos notariais.

Abstract: The digital simplification of notarial acts is associated with a streamlining of procedures through digitization. Notarial acts are celebrated through video conferencing, which presupposes a true digital transformation, reflecting an innovation in notarial activity. Throughout this scientific article, we will address

[1] Doutoranda em Ciências Jurídicas Privatísticas na Escola de Direito da Universidade do Minho. Bolseira de Investigação (FCT). Investigadora do JusGov – Centro de Investigação em Justiça e Governação na Escola de Direito da Universidade do Minho. Mestre em Direito dos Contratos e da Empresa pela Escola de Direito da Universidade do Minho. Licenciada em Direito pela Escola de Direito da Universidade do Minho.

the celebration of notarial acts by video conference, from a primarily notarial perspective, and explore the peculiar aspects of the regime under Decree-Law no. 126/2021, of December 30th.

Our analysis of the topic will be brief, given the scarcity of literature on this subject. Thus, we seek to address fundamentally the acts that can be performed by video conference; the scheduling issue; the attachment of documents; the video conference itself; the refusal to perform the notarial act; the evidentiary value of acts performed by video conference; the archiving and access to documents, the nullity of acts as well as processing of personal data. We will also provide a list of procedures to be used by professionals and a practical case to illustrate the situation of remote acts. We hope that the reader will gain greater clarity on the existing legal regime and that we can contribute to a good reflection on the topic of notarial acts, under the auspices of digital transformation. It is of our utmost interest to contribute to national doctrine on this matter

Keywords: Simplification; Digital; Notarial acts.

Introdução

Realização de atos notariais por videoconferência é o título dado ao presente trabalho. Neste campo, pretendemos esclarecer o leitor de que os atos notariais estão sujeitos a um fenómeno de transformação digital, dado que é utilizada a tecnologia digital em prol de soluções de problemas tradicionais.

Sobre esta matéria, tem especial interesse em Portugal, o Decreto-Lei n.º 126/2021, de 30 de dezembro, e com ele procuraremos fazer uma análise profunda, dada a escassez de bibliografia sobre o presente tema, pelo que faremos questão de contribuirmos para a doutrina nacional. O citado diploma estabelece o regime temporário aplicável à realização, através de videoconferência, de atos autênticos, termos de autenticação de documentos particulares e reconhecimentos que requeiram a presença dos intervenientes perante titulador ou profissional competente[2], oferecendo, na nossa opinião, idênticas garantias de certeza e segurança jurídica.

No presente escrito será abordado o tema da simplificação digital dos atos notariais, de maneira a introduzirmos um conceito por nós criado na doutrina nacional. A simplificação trata-se de uma forma de digitalização, mas a simplificação digital não constitui uma simplificação absoluta, nem resolve o problema, se não se eliminarem determinadas superfluidades ou dados excessivos na elaboração do ato notarial. Aqui procuraremos tratar sobretudo da correlação existente en-

[2] Abordaremos, em especial, a figura do notário, sem descurar outros agentes importantíssimos para o desenvolvimento da função notarial.

tre simplificação e digitalização, já que uma depende da outra e não abordar a pura simplificação em si mesma. O objeto do nosso trabalho relaciona-se, assim, com a área do direito digital e da tecnologia.

Ao longo deste trabalho procuraremos explorar as generalidades dentro da simplificação digital dos atos notariais; a celebração de atos por videoconferência; aspetos peculiares do regime e, dentro deste, abordar certas questões, tais como: quais os atos que podem ser efetuados por videoconferência?; o agendamento; a junção de documentos; a videoconferência propriamente dita; a recusa da prática do ato notarial; a assinatura; o valor probatório dos atos realizados por videoconferência; o arquivo e acesso a documentos, a nulidade dos atos e o tratamento de dados pessoais. Iremos expor também uma lista de procedimentos a utilizar pelos profissionais e um caso prático para ilustrar a situação dos atos à distância.

Dada a escassez de bibliografia sobre o presente tema, procuraremos analisar de forma profunda o regime do Decreto-Lei n.º 126/2021, de 30 de dezembro, contribuindo, assim, de forma inovadora para a doutrina nacional. É isso mesmo que pretendemos.

1. A simplificação digital dos atos notariais: generalidades

A simplificação digital dos atos notariais é um conceito que adotamos quando nos queremos referir à pura digitalização dos atos notariais. Falamos de pura digitalização no sentido em que os atos notariais são celebrados por via eletrónica e não em papel, o que traduz uma inovação da atividade notarial, inserindo o notário num contexto tecnológico.

Como órgão próprio da função notarial, o notário encara agora um período de novas tendências da atividade notarial e envereda por caminhos que conduzem a uma facilitação dos procedimentos até então utilizados. Designamos esta facilitação por simplificação. Há quem prefira outros termos, que são, até certo ponto, semelhantes, tais como: desmaterialização, desburocratização ou, até mesmo, desformalização. Somos da opinião de que a expressão mais correta para tratar este tema será a simplificação porque resume de forma sucinta a abolição de superfluidades ou dados excessivos na elaboração do ato notarial[3]. E é isso mesmo que acontece com a digitalização dos atos notariais, isto porque existe uma facilitação ao nível do procedimento adotado. As partes celebram de forma digital o seu contrato, evitando-se, assim, deslocações desnecessárias ao cartório.

O termo simplificação constitui uma forma de digitalização, dado que, quando está em causa a digitalização de um ato notarial, surge associada a ideia de que

[3] José Augusto Mouteira Guerreiro, *Temas de Registos e de Notariado*, Coimbra, Almedina, 2010, p. 520.

aquilo que se verificou foi uma facilitação nos procedimentos utilizados para a confeção do ato notarial. Mas, a simplificação absoluta não é gerada por uma revolução digital se não se eliminarem os dados excessivos. Assim, simplificação e digitalização estão numa "constante correlação", com dependência uma da outra[4].

2. Celebração de atos por videoconferência

Face à situação pandémica de COVID-19, começaram a utilizar-se cada vez mais meios à distância no setor público e no setor privado. Neste contexto, surge em Portugal o Decreto-Lei n.º 126/2021, de 30 de dezembro, que estabelece o regime jurídico temporário aplicável à realização, através de videoconferência, de atos autênticos, termos de autenticação de documentos particulares e reconhecimentos que requeiram a presença dos intervenientes perante conservadores de registos, oficiais de registos, notários, agentes consulares portugueses, advogados ou solicitadores, isto é, que requeiram a presença dos intervenientes, perante titulador ou profissional competente, oferecendo idênticas garantias de certeza e de segurança jurídica.

O presente Decreto-Lei tem a duração de dois anos (art. 15.º), findos os quais o Governo decidirá pela sua implementação ou não[5], tendo entrado em vigor a 4 de abril de 2022. Trata-se de uma ponderação intransigente, no sentido da qual se opta pelos novos meios tecnológicos ou pela clássica tradição. O recurso à videoconferência é facultativo (art. 6.º, n.º 1), ninguém pode ser obrigado a praticar atos à distância, podendo os interessados recorrer aos demais meios, legalmente previstos, de realização dos indicados atos. A videoconferência tem de abranger todos os participantes.

3. Aspetos peculiares do regime

3.1. *Quais os atos que podem ser efetuados por videoconferência?*

As escrituras públicas, procedimentos especiais de transmissão, oneração e registo de imóveis (Casa Pronta), procedimento de divórcio por mútuo consentimento, processo de separação de pessoas e bens por mútuo consentimento, procedimentos de habilitações de herdeiros com e sem registos, termos de autenticação de documentos particulares ou reconhecimentos presenciais e atos relativos a factos sujeitos a registo predial que respeitem a: factos jurídicos que determinem

---

[4] Mercília Pereira Gonçalves, *O Notário e a Atividade Notarial: Certeza e Segurança Jurídica*, Coimbra, Almedina, 2022, p. 215.

[5] Preâmbulo do Decreto-Lei n.º 126/2021, de 30 de dezembro.

a constituição, o reconhecimento, a aquisição, a modificação ou a extinção dos direitos de propriedade, usufruto, uso e habitação, superfície ou servidão; factos jurídicos que determinem a constituição ou a modificação da propriedade horizontal; promessa de alienação ou oneração de imóveis, se lhe tiver sido atribuída eficácia real ou a cessão da posição contratual emergente desse facto; hipoteca, sua cessão, modificação ou extinção, a cessão do grau de prioridade do respetivo registo e a consignação de rendimentos (art. 1.º, n.os 1 a 3).

São estes alguns dos atos notariais *online* que podem ser praticados à distância, num "clique", sem ser necessária a deslocação do cidadão à conservatória ou ao cartório notarial, simplificando-se, sem se colocar em causa, no nosso parecer, a certeza e a segurança jurídica.

Como é óbvio, haverá sempre questões relacionadas com a certeza e segurança jurídica que aqui se possam levantar. Por isso, ao notário cabe-lhe a decisão de praticar o ato notarial à distância ou não, pelo que só quando tiver preenchido os pressupostos necessários à celebração à distância do ato notarial é que o notário pode autorizar o instrumento notarial[6]. Entendemos que a simplificação digital não coloca em causa o ideal de segurança jurídica, quando o notário ou outro titulador (como advogado ou solicitador) envereda pelo caminho desta simplificação, tem a plena certeza de que a segurança jurídica estará mais do que garantida, caso contrário, teria recusado a prática do ato notarial. No caso do notário, defendemos que este continua a ser o mesmo agente da função notarial que pratica as suas funções jurídicas, mas desta vez de forma inovadora, num contexto tecnológico e globalizado.

O recurso à videoconferência não vai ser possível para testamentos nem para atos que dizem respeito a alguns factos sujeitos a registo predial. Porém, o sistema brasileiro permite todo e qualquer ato notarial celebrado de forma eletrónica, incluindo os testamentos, constituindo atualmente uma realidade jurídica no Brasil[7]. Estudos mais antigos já apontavam para a possibilidade do testamento público digital no Brasil[8], mas foi com a situação pandémica de COVID-19 que o testamento público digital veio a ser implementado, através do Provimento n.º 100, de 26 de maio de 2020. Assim se garantiu a certeza e a segurança jurídica

---

[6] Neste sentido, João Ricardo Menezes, «Atos autênticos, por videoconferência. A perspetiva notarial», *CeNoR*, junho 2022 (sem páginas).

[7] Ana Luiz Nevares, «Testamento virtual: ponderações sobre a herança digital e o futuro do testamento», *Civilística.com*, a. 10, n.º 1, 2021, pp. 1-20.

[8] Como nota pertinente, em Espanha e França, já existe legislação para os testamentos públicos digitais. Neste sentido, Modesta Lorena Hernández Sánchez e Armando Adriano Fabre, «Testamento y herencia digital», *Enfoques Jurídicos*, n.º 4, julho/dezembro 2021, pp. 120-136.

do testamento público digital[9]. Os testamentos digitais foram tão enraizados no ordenamento jurídico brasileiro, que acabaram por se tornar um "costume"[10], não estando proibidos pelo Provimento n.º 100 ou por outra norma jurídica no sistema notarial brasileiro.

A nossa orientação é a de que a decisão do legislador não foi positiva. Conforme tivemos a oportunidade de nos pronunciarmos sobre esta matéria, "Há, de facto, que ter cautela em relação à matéria testamentária, mas proibi-la digitalmente, não. Consideramos que se o legislador português viesse a permitir o testamento público digital, o notário nesta sede deveria ser mais exigente ainda, mais prudente[11] e mais rigoroso na celebração do testamento público digital, pautando-se por critérios rígidos para a sua celebração, uma vez que estamos perante um ato singular e de natureza solene"[12]. Não diríamos melhor.

Perguntemo-nos pelo seguinte: Os testamentos públicos digitais são seguros?

Escrevemos pertinentemente que "estamos mais ou menos dentro do mesmo patamar ao nível da segurança jurídica"[13], referindo-nos em concreto à celebração do ato notarial presencial e à celebração do ato notarial de forma remota. Justificamos a nossa afirmação com base na ideia de que com a celebração do testamento público digital existe uma gravação da manifestação de vontade do testador, sendo certo que o procedimento acaba por se tornar seguro, dado que a gravação pode ser revista e, assim, constatar-se que a vontade das partes é correspondente à vontade real[14].

No que se refere à realização de atos por videoconferência, quais os requisitos de acesso para um notário?

- Atos praticados em território nacional

- Certificado profissional

- Configuração de entidade na plataforma (PAD)

---

[9] Ivanildo de Figueiredo Andrade de Oliveira Filho, *Forma de Declaração de Vontade na Internet: Do contrato eletrónico ao testamento digital*, Tese de Doutoramento, Recife, março 2014.

[10] Jorge José Lawand, *O testamento digital e a questão de sua validade*, São Paulo, Dialética Editora, 2021, p. 42.

[11] Sobre prudência notarial, veja-se Mercília Pereira Gonçalves, «A prudência notarial e a resolução antecipada de litígios», *CeNoR*, 2022 (sem páginas).

[12] Neste sentido, Mercília Pereira Gonçalves, «Testamento público digital: a proibição do legislador português», *Observador*, 2022 (sem página).

[13] *Idem*, *ibidem*.

[14] *Idem*, *ibidem*.

- Assinatura digital

- Computador com câmara, microfone, colunas e acesso à internet

- Navegador na internet

- Software de videoconferência

E quais os pressupostos de acesso para um cidadão?

- Autenticação da Chave Móvel Digital ou do Cartão de Cidadão (leitor de Cartão de Cidadão e respetivo PIN)

- Assinatura digital

- Computador com câmara, microfone, colunas e acesso à internet

- Navegador na internet

- Software de videoconferência

3.2. *Agendamento*

Os intervenientes podem requerer este serviço mediante agendamento (art. 5.º, n.os 1 e 5) ou junto de um profissional habilitado.

3.3. *Junção de documentos*

Podem, ainda, através da sua área reservada na plataforma, juntar documentos que se destinam a instruir o ato a realizar[15]. A mesma função tem os profissionais. O documento que titula o ato, ficheiro em formato pdf, é partilhado, lido e assinado na sessão de videoconferência[16].

3.4. *Videoconferência*

O participante pode fazer-se acompanhar de advogado ou solicitador para a celebração do ato notarial (art. 2.º, n.º 5), o que significa que estamos perante a presença de mais um jurista de qualidade na realização do ato notarial e, por isso, os níveis de segurança jurídica serão ainda maiores, sendo que a sessão é sempre gravada (art. 6.º, n.º 1), independentemente de estar o advogado do participante ou não. Os participantes não podem desativar, de maneira alguma, a captação de imagem ou som durante a sessão de videoconferência, sob pena de o procedimento ser interrompido pelo profissional (no caso em concreto, o notário) e não haver lugar à conclusão do ato. As sessões de videoconferência só se iniciam após o consentimento de todos os intervenientes (art. 3.º, n.º 1, alínea

[15] Cfr., ainda, art. 3.º, n.º 1, alínea a), e art. 4.º, n.º 5.

[16] Departamento de Gestão e Apoio Técnico-Jurídico aos Serviços de Registo, «Realização de atos por videoconferência – D.L 126/2021, de 30 de dezembro», IRN, dezembro de 2022, p. 11.

b)) para a verificação da sua identidade pelo profissional, terem feito a autenticação na plataforma informática e terem declarado conhecer as condições para a sua concretização.

Para se certificar de que os intervenientes agem de livre vontade e questionar se o ato é praticado em território nacional, o notário que conduzir a sessão solicita aos intervenientes que mostrem o espaço em seu redor. A leitura, explicação e assinatura dos documentos deverão realizar-se no mesmo dia, sob pena de nulidade (art. 6.º, n.º 8), cabendo ao profissional certificar-se de que o ato é conforme à real vontade dos intervenientes, devendo estes declará-lo de forma expressa antes da assinatura do documento (arts. 6.º, n.º 8, e 3.º, n.º 1, alínea e)). Deve também certificar-se de que o pagamento dos emolumentos, taxas ou impostos se encontra efetuado antes de concluir o ato[17]. No documento notarial deve ficar consignado que o mesmo foi realizado através de videoconferência, por aposição, da seguinte menção: "Ato realizado por videoconferência, nos termos do Decreto-Lei nº. 126/2021, de 30 de dezembro, para cuja gravação foi prestado o necessário consentimento"[18].

3.5. *Recusa da prática do ato notarial*

No que se refere à recusa da prática do ato, o profissional, neste caso, o notário, deve recusar a prática do ato que lhe seja requerido, se tiver dúvidas sobre:

a) A identidade dos intervenientes;

b) A livre vontade dos intervenientes para a prática do ato;

c) A capacidade dos intervenientes;

d) A genuinidade ou integridade dos documentos apresentados.

Mais, nomeadamente nos casos de falta de pagamento dos emolumentos, taxas e impostos devidos, de inexistência de assinatura digital ativa, de Cartão de Cidadão cancelado e de certificado digital revogado.

Os interessados não podem desativar, em circunstância alguma, a captação de imagem ou som durante a sessão de videoconferência, sob pena de o procedimento ser interrompido pelo notário e o ato não ser concluído. Da mesma forma, caso não se verifiquem as condições técnicas necessárias à boa condução do procedimento, designadamente nos casos de ocorrência de fraca qualidade de imagem, de condições deficientes de luminosidade ou som, ou de interrupções na transmissão do vídeo, o procedimento deve ser recusado ou interrompido (art. 7.º). O n.º 2 do art. 8.º do citado diploma impõe ao notário que, antes da

[17] *Idem*, p. 13.

[18] *Idem*, *ibidem*.

assinatura digital do documento, verifique a qualidade da gravação da sessão realizada, uma vez que se deve ter a clara perceção de tudo o que se passou durante a realização da videoconferência.

O objetivo fulcral destes artigos prende-se, essencialmente, com a garantia de que durante a sessão não existem quaisquer fatores externos que impossibilitem a "correta" e a "cabal" compreensão do ato por todos os intervenientes e inviabilizem a quem mais tarde se veja confrontado com a necessidade de visualizar a respetiva gravação ter a clara perceção do que se passou durante a sua realização[19]. Certos ruídos que possam existir durante a sessão, tais como, a circulação rodoviária e área ou execução de obras, contudo, não justificam a interrupção do ato, dado que não afetam a sua compreensão nem o conteúdo do mesmo[20].

3.6. *Assinatura*

O notário disponibiliza a versão final do documento na plataforma para assinatura, depois da leitura e explicação do ato e depois da aferição pelo oficial público de que o mesmo corresponde à vontade dos intervenientes (art. 8.º, n.º 1)[21].

A assinatura do documento é realizada de forma exclusiva com a utilização de certificado digital qualificado, nomeadamente, Cartão de Cidadão ou Chave Móvel Digital. Os participantes têm acesso ao documento através da plataforma, onde procedem à sua validação e assinatura, sendo certo que o procedimento é sistematicamente repetido quantas as assinaturas que forem necessárias. A assinatura com certificado digital do Cartão de Cidadão é feita fora da plataforma, devendo o participante efetuar *upload* do documento assinado para o sistema[22]. A respetiva assinatura eletrónica qualificada é aposta no documento elaborado pelo notário depois da recolha das assinaturas de todos os intervenientes e após verificada a qualidade da gravação da sessão (art. 8.º, n.º 2).

As gravações das sessões de videoconferência são arquivadas e guardadas por um período de 20 anos, podendo ser disponibilizadas aos intervenientes mediante decisão judicial (art. 9.º, n.ºs 1 a 5) ou ser solicitadas pelo próprio tribunal no âmbito de uma ação judicial de impugnação de ato praticado, tendente, nomeadamente, à declaração de nulidade ou anulabilidade do negócio celebrado. Assim se mostra fundamental que a gravação não apresente quebras ou ruídos

---

[19] *Idem*, p. 14.

[20] *Idem*, p. 15.

[21] *Idem*, p. 16.

[22] *Idem*, *ibidem*.

e esteja em boas condições técnicas, para que quem a esteja a visualizar tenha a clara perceção de tudo o que se passou na sessão de videoconferência[23].

3.7. *Valor probatório dos atos realizados por videoconferência*

Os atos autênticos, termos de autenticação de documentos particulares e reconhecimentos realizados ao abrigo do presente decreto-lei têm o mesmo valor probatório dos atos realizados presencialmente, desde que observados os pressupostos nele previstos (art. 12.º).

3.8. *Arquivo e acesso a documentos*

Neste contexto, salientamos que os documentos particulares autenticados que titulem atos sujeitos a registo predial e os respetivos documentos instrutórios, ainda que realizados por recurso à videoconferência, estão sujeitos a depósito eletrónico, nos termos previstos no art. 24.º do Decreto-Lei n.º 116/008, de 4 de julho.

Os restantes documentos realizados por videoconferência e respetivos documentos instrutórios são na mesma arquivados pelo respetivo profissional durante o período imposto por lei para os documentos lavrados em suporte de papel, não se dispensando o cumprimento de outras formalidades impostas por lei. Os documentos lavrados e respetivos documentos instrutórios podem ser consultados na plataforma informática por qualquer um dos intervenientes durante 30 dias após a realização do ato (art. 9.º, n.º 4).

Uma vez concluído o procedimento, o documento que formaliza o ato está disponível para consulta e *download* por todos os intervenientes durante o prazo de 30 dias. Esta disposição equivale à entrega de cópia eletrónica à luz do art. 8.º, n.º 4.

3.9. *Nulidades dos atos*

A preterição das formalidades instituídas pelo presente diploma determina a nulidade dos atos realizados ao seu abrigo (art. 13.º).

3.10. *Tratamento de dados pessoais*

Cada profissional é responsável pelo tratamento de dados pessoais que efetue no âmbito da realização de atos notariais através de videoconferência.

O IRN, I.P., enquanto entidade gestora da plataforma informática, é responsável pelo tratamento de dados pessoais que não sejam da responsabilidade dos profissionais.

---

[23] *Idem*, *ibidem*.

4. Procedimentos[24]

No final da sessão de videoconferência, o profissional pode consultar a lista de procedimentos a observar na realização do ato, devendo assinalar cada uma das etapas para visualização da seguinte. A referida lista visa apenas e tão-só auxiliar o titulador nos procedimentos a observar.

1) Verificar e comprovar a identidade dos participantes através de perguntas biográficas. A plataforma disponibiliza a informação obtida com a autenticação do participante (NIC, NISS, NIF), morada ou dados pessoais.

2) Verificar se a imagem facial dos participantes na videoconferência corresponde à imagem disponibilizada na plataforma após autenticação com Cartão de Cidadão ou Chave Móvel Digital.

3) Solicitar aos participantes que apresentem o seu documento de identificação em frente à câmara por forma a ser legível.

4) Solicitar que os participantes filmem o espaço físico circundante, por forma a garantir que estão num local que assegure uma participação consciente e de livre vontade e que quaisquer elementos externos perturbadores são previamente identificados.

5) Confirmar que todos os intervenientes optaram pela videoconferência como meio para a realização do ato e prestam o seu consentimento para a gravação audiovisual do mesmoe que em causa está ato praticado em território nacional.

6) Confirmar que os participantes têm os meios necessários para a realização de assinaturas digitais, nomeadamente leitor de Cartão de Cidadão e respetivos PINs de assinatura ou Chave Móvel Digital ativa.

7) Confirmar que todos os intervenientes estão devidamente informados sobre as condições necessárias para a realização da sessão.

8) Garantir que a câmara não é ocultada e que não é colocado fundo (*background*) e que a sessão decorre com qualidade e sem qualquer interrupção, tanto ao nível de áudio como de imagem.

9) Assegurar que a totalidade dos documentos está previamente disponível na aplicação, para consulta prévia por parte dos participantes.

10) Ler e apresentar, assegurando que todos os participantes visualizam, os documentos do ato.

---

[24] Elaboramos os seguintes procedimentos com base no documento referente ao Departamento de Gestão e Apoio Técnico-Jurídico aos Serviços de Registo, «Realização de atos por videoconferência…», *cit.*, pp. 21-22.

11) Questionar sobre o correto entendimento de todos os participantes sobre o decorrer da sessão.

12) Questionar sobre a vontade de todos os participantes.

13) Confirmar se o pagamento dos emolumentos, taxas ou custas se encontra efetuado antes de concluir o ato.

14) Verificar se os pagamentos entre os participantes, quando devidos, foram devidamente concretizados.

15) Garantir que estão realizadas as liquidações e cobranças de impostos relativos aos atos.

16) Configurar e validar a recolha de assinaturas dos participantes.

Na realização de qualquer ato através de videoconferência, o profissional deverá ainda ter em atenção os seguintes procedimentos:

- Informar os intervenientes que o documento que formaliza o ato e os respetivos documentos instrutórios podem ser consultados na plataforma informática, através da respetiva área reservada, até 30 dias após a realização da videoconferência.

- Verificar a qualidade da gravação da sessão, nomeadamente se a mesma não apresenta cortes ou interrupções na imagem e som suscetíveis de interferir com a correta e cabal apreensão do ato realizado e da livre vontade dos intervenientes.

- Proceder à assinatura eletrónica qualificada do documento que formaliza o ato realizado – para que sejam adicionados os atributos profissionais, a assinatura deverá ser efetuada localmente, ou seja, fora da plataforma.

5. Caso prático[25]

O António vai vender uma casa à Maria e o título vai ser feito à distância, por videoconferência, perante um profissional:

A Maria tratou da documentação da casa e contactou o notário para pedir o agendamento do ato, optando pela modalidade de atendimento à distância, por videoconferência, para a realização do título.

[25] Este caso prático foi disponibilizado por uma Notária, a quem agradecemos pela partilha do mesmo e apresentado em 10 de fevereiro de 2023, no Porto, nas instalações do IRN.

a) Na plataforma de atendimento à distância, desenvolvida pelo IRN e acessível no endereço atendimento.justica.gov.pt, o profissional criou o ato "compra e venda" e geriu todo o processo, incluindo:

b) a identificação dos participantes: comprador e vendedor

c) a submissão de documentos para a assinatura digital dos participantes

d) o agendamento da sessão de videoconferência.

- Agendamento

O ato será agendado de acordo com a disponibilidade do profissional.

- Notificação

Após o agendamento da sessão, a Maria e o António receberam um *email* com os detalhes do agendamento, a informação sobre as condições do atendimento à distância e o *link* de acesso à plataforma atendimento.justica.gov.pt, onde se deverão autenticar com Cartão de Cidadão ou Chave Móvel Digital.

- Autenticação

A Maria acedeu ao endereço e autenticou-se com o Cartão de Cidadão, enquanto o António se autenticou com a Chave Móvel Digital.

Nas suas áreas reservadas, a Maria e o António visualizaram os detalhes do ato em que são participantes e acompanharam a evolução do processo.

No dia agendado, a Maria estará em Bragança, o António em Cuba e o/a profissional estará no balcão de atendimento único, em…

- Os participantes irão autenticar-se na plataforma atendimento.justica.gov.pt e entrar na sessão de videoconferência.

1. O profissional inicia a sessão e a gravação audiovisual é iniciada automaticamente:

a) Os Participantes entram na sessão, dando consentimento para a gravação audiovisual.

b) Quando todos os intervenientes estão visíveis na janela da videoconferência e audíveis, o profissional confirma a identidade dos participantes, assegurando-se que estão reunidas condições para a realização do ato.

c) O profissional lê o documento de compra e venda e os participantes visualizam o documento nos seus ecrãs.

d) O profissional solicita a assinatura dos participantes, de forma sequencial.

e) O comprador acede ao documento e assina digitalmente (com Chave Móvel Digital).

f) O vendedor acede ao documento e assina digitalmente (com Chave Móvel Digital).

g) O profissional acede ao documento e verifica se está corretamente assinado por todos os participantes.

2. O profissional encerra a sessão de videoconferência:

a) Verifica a qualidade da gravação e assina o título digitalmente.

b) Conclui o ato e os documentos ficam disponíveis na plataforma para todos os participantes durante 30 dias.

Conclusão

A simplificação digital dos atos notariais é uma noção que adotamos quando nos queremos referir à pura digitalização dos atos notariais. A pura digitalização dos atos notariais respeita aos atos lavrados de forma digital e não em papel, inserindo o notário num contexto tecnológico e globalizado. Assiste-se a um fenómeno de transformação da própria atividade notarial, exercida atualmente por vários agentes da função notarial, tais como, conservadores de registos, oficiais de registos, notários, agentes consulares portugueses, advogados ou solicitadores, nos termos elencados no art. 3.º do Código do Notariado, sendo que, como órgão próprio da função notarial, previsto no art. 1.º do Código do Notariado, referimo-nos, na maioria dos casos, somente ao notário e à sua atividade notarial, mas, como bem se sabe, não é a única autoridade a praticar atos notariais, aplicando-se a outras entidades já designadas anteriormente o Código do Notariado e ao que agora nos interessa também o Decreto-Lei n.º 126/2021, de 30 de dezembro que estudamos.

Simplificação constitui, assim, uma forma de digitalização, dado que, quando se presencia a digitalização de um ato notarial, ocorre desde logo uma facilitação dos procedimentos que são utilizados para a confeção do ato notarial. O cerne da recente digitalização dos atos notariais – atos que são, de acordo com a legislação em vigor, realizados por videoconferência – reside, no essencial, numa ponderação vista como prudente, rigorosa ou intransigente que coloca em cima da mesa a questão da prática do ato notarial à distância, ou seja, com a ausência física das partes ou com a presença física das mesmas. É precisamente ao profissional competente que cabe tomar uma decisão que tem em conta as circunstâncias do caso concreto, como, por exemplo, as condições técnicas, mas, para além disso, uma série de parâmetros que o diploma mencionado apresenta, mais propriamente,

no seu art. 7.º e que respeitam ao regime de recusa da prática de um ato notarial e que não faz nada mais do que reproduzir o próprio art. 173.º do Código do Notariado, aplicável desde sempre aos atos notariais na forma como até então os conhecíamos, em papel e com a intervenção física do agente da função notarial. Os pressupostos previstos nestas normas são nada mais nada menos do que os requisitos que o notário deve preencher na prática de qualquer ato notarial. Deste modo, o legislador prevê tacitamente esta exigência, embora não coloque nenhuma norma que faça referência à reflexão ou tomada de decisão. Esta é, portanto, a prática comum na realização de atos notariais por videoconferência e pensamos que é uma boa solução.

Por fim, renovamos a ideia de que somos da opinião de que a simplificação digital não coloca em causa o ideal de segurança jurídica porque, quando o notário opta pelo caminho da digitalização, tem a plena certeza de que a segurança jurídica se encontra ressalvada; se assim não fosse, teria recusado a prática do ato notarial no momento da sua reflexão. Terminamos com a seguinte afirmação: o notário é e continua a ser o mesmo agente da função notarial num quadro de inovação tecnológica.

A APLICABILIDADE DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL NO ÂMBITO DO DIREITO DA FAMÍLIA E DAS CRIANÇAS

Sofia Travassos Alcaide[1]

Resumo: Nos últimos anos, a população mundial tem assistido a um rápido desenvolvimento dos mecanismos dotados de inteligência artificial, que podem ser aplicados a uma multiplicidade de matérias e de contextos. Contudo, e ainda que vários autores se tenham já pronunciado acerca da eventual aplicabilidade de sistemas artificialmente inteligentes à resolução de litígios, tais estudos focam-se, especialmente, na eventualidade de o juiz humano ser substituído por decisões algorítmicas ou, por outro lado, na aplicação destes sistemas no contexto do direito penal. A verdade é que os estudos relativos à eventual aplicabilidade de sistemas de inteligência artificial no contexto do Direito da Família e das Crianças ainda não se encontra no cerne da discussão entre investigadores, relevando trazer esta temática à discussão, atenta a sensibilidade das matérias em crise. Certo é que, por forma a evitar que a tecnologia, uma vez mais, se adiante relativamente ao direito, é essencial iniciar investigação nesta matéria. Este artigo não pretende ser um estudo aprofundado da matéria e da tecnologia, servindo, antes, como ponto de partida para investigação futura, analisando propostas de sistemas de inteligência artificial já existentes neste ramo do direito, formulando-se algumas questões.

Palavras-chave: Inteligência artificial; Direito da Família e das Crianças; Resolução de conflitos em linha.

Abstract: In recent years, the world population has witnessed a rapid development of artificial intelligence mechanisms, which can be applied to a multitude of matters and contexts. However, although several authors have already commented on the possible applicability of artificially intelligent systems to dispute resolution, such studies focus in particular on the possibility of the human judge being replaced by algorithmic decisions or, on the other hand, on the application

[1] Docente Assistente Convidada na Escola de Direito da Universidade do Minho. Doutoranda em Ciências Jurídicas Privatísticas. Investigadora na Escola de Investigadores do JusGov – Centro de Investigação em Justiça e Governação. Advogada.

of these systems in the context of criminal law. The truth is that studies on the possible applicability of artificial intelligence systems in the context of family and children's law are not yet at the heart of the discussion among researchers, and it is relevant to bring this issue to the discussion, given the sensitivity of the matters in crisis. It is certain that, in order to prevent technology from once again getting ahead of the law, it is essential to initiate research on this matter. This article is not intended to be an in-depth study of the subject and technology, but rather to serve as a starting point for future research, analyzing proposals for artificial intelligence systems already existing in this branch of law, formulating some questions.

Keywords: Artificial intelligence; Family and Children's Law; Online dispute resolution.

1. Introdução

A problemática da inteligência artificial aplicada às decisões judiciais assumiu e assume especial relevância na última década, facto impulsionado pela competitividade mundial no que concerne ao seu desenvolvimento. A evolução dos mecanismos artificialmente inteligentes sofreu um grande avanço nos últimos anos, com a sua crescente utilização e disponibilização em todo o mundo. Certamente, qualquer um de nós possui um *smartphone* com reconhecimento de voz, ou mesmo um aspirador *robot* nas suas casas – de resto, considerado o primeiro grande sucesso comercial, em 2002, com o *iRobot Roomba Robotic Floorvac*, tendo o seu primeiro e único antecessor, o *Rug Warrior*, sido desenvolvido pelo *Massachusetts Institute of Technology (MIT) Artificial Intelligence (AI) Laboratory*, em 1989[2].

Com o crescente desenvolvimento da inteligência artificial, ainda que o seu percurso, desde as décadas 40-50 do século passado, tenha sido marcado por períodos considerados invernosos e outros considerados períodos dourados[3], com mais ou menos aposta financeira e, consequentemente, maior ou menor grau de desenvolvimento[4], ainda antes da década de 90 do século passado, introduziu-se a problemática dos sistemas de inteligência artificial aplicados às decisões judi-

[2] Joseph L. Jones, «Robots at the Tipping Point – The Road to the iRobot Roomba» [Online], in *IEEE Robotics & Automation Magazine*, Vol. 13, n.º 1, março 2006, p. 76, disponível em https://ieeexplore.ieee.org/abstract/document/1598056 [consultado em 28/07/2023].

[3] Raymond S. T. Lee, *Artificial Intelligence in Daily Life*, Singapura, 2020, pp. 22-28.

[4] Joseph L. Jones, «Robots at the Tipping Point – The Road to the iRobot Roomba», *cit.*

ciais[5]. A discussão em torno desta matéria, desde então, tem-se vindo a intensificar, com o crescente desenvolvimento de algoritmos e tentativas de reproduzir o processo de tomada de decisão por um juiz.

No presente artigo, pretende-se levantar algumas questões, analisando a aplicação de mecanismos artificialmente inteligentes a litígios relacionados com a jurisdição de família e crianças, sem que se procure apresentar soluções imediatas. Estas matérias, por serem do foro estritamente pessoal e, naturalmente, por influírem de forma mais intensa com questões ético-morais e, até, sentimentais, poderão levantar maiores questões no que concerne ao recurso a algoritmos rígidos, incapazes de apreender a inata sensibilidade humana.

2. O Desenvolvimento da Inteligência Artificial aplicada às Decisões Judiciais – Breve Resenha

Desde cedo se iniciaram estudos para aferir de que forma a inteligência artificial poderia ser útil na tomada de decisões judiciais. Ainda em 1989, Donald H. Berman e Carole D. Hafner afirmaram que o recurso à inteligência artificial poderia auxiliar na resolução da crise do sistema judiciário – que, à data, se considerava em "estado de crise", devido à morosidade na resolução dos litígios, à perda de confiança no sistema, aos custos elevados de acesso à justiça, considerando-se, mesmo, que os que dispunham de menores condições económicas se encontravam em condição de desproteção legal[6]. As autoras partem de um exemplo comum, de uma situação real relacionada com mediação imobiliária e defeitos de imóvel vendido, para analisar custos prováveis com a ação judicial, bem como todos os riscos que cada uma das partes na ação poderá correr, sendo necessário analisar jurisprudência, as normas existentes, ponderar o risco de ter um julgador ou um júri que possa ser mais sensível a uma ou outra posição. Defendem que o julgador não poderá ser substituído na tomada de decisão efetiva, mas que os sistemas de inteligência artificial poderão auxiliar na compilação de jurisprudência e normas relativas a cada matéria judicial, mas também se poderão desenvolver mecanismos que, de forma minimamente razoável, indiquem o sentido das decisões judiciais existentes mediante um certo tipo de crime, por

---

[5] Giovanni Sartor e L. Karl Branting, «Introduction: Judicial Applications of Artificial Intelligence», in *Judicial Applications of Artificial Intelligence*, E-book, 1998, p. 1, disponível em https://link.springer.com/book/10.1007/978-94-015-9010-5 [consultado em 28/07/2023].

[6] Donald H. Berman e Carole D. Hafner, «The Potential of Artificial Intelligence to Help Solve the Crisis in Our Legal System», in *Communications of the ACM*, Vol. 32, n.º 8, agosto 1989, p. 928, disponível em https://www.tud.ttu.ee/im/Ermo.Taks/IDK0310/Reading/p928-berman1.pdf [consultado em 28/07/2023].

exemplo, podendo auxiliar a existência de uma maior equidade na tomada de decisões[7].

Já na década de 90, autores como Giovanni Sartor e Karl Branting afirmavam que a substituição de um modelo judicial assente na discricionariedade dos juízes – que para produzirem as suas decisões judiciais desenvolvem um raciocínio, não só baseado em conhecimento jurídico altamente aprofundado, mas também na capacidade cognitiva e inteligência emocional – não pode ser sobrestimado[8], uma vez que a decisão judicial não é pura e somente técnica. Michele Taruffo, partindo da análise dos vários passos que uma decisão judicial comporta – entre os quais, a exposição por cada uma das partes no processo daquele que é o enquadramento ou os enquadramentos legais possíveis para determinada situação legal e fáctica, originando, pelo menos e desde logo, duas possibilidades distintas, às quais acresce(m) a(s) possibilidade(s) suscitada(s) pelo próprio juiz, especialmente quando tal poder lhe é atribuído, para culminar numa decisão acerca dos fundamentos legais e dos factos trazidos à discussão, de entre as variadas possibilidades e enquadramentos legais que pudessem ser aplicáveis ao caso concreto, devido ao facto de a mesma se apresentar como sendo a mais adequada, devendo o juiz formular a decisão e, partindo da mesma, expor toda a fundamentação que conduziu a determinado resultado, numa espécie de argumentação e contra-argumentação[9] –, afirma que tentar reduzir a um modelo lógico e rígido o processo de tomada de decisão de um juiz é praticamente impossível, atenta a sua complexidade, variabilidade, sem descurar a parte ético-moral da qual é naturalmente imbuída[10]. À época, e atendendo a estes fundamentos, Giovanni Sartor e Karl Branting concluíam que a inteligência artificial poderia ser útil ao sistema judicial, numa ótica de auxílio na produção de determinados documentos judiciais ou mesmo na análise de documentação e outro tipo de provas, permitindo uma maior rapidez na justiça e desonerando os juízes de determinadas tarefas, sem que, contudo, se pudesse substituir a figura do julgador e que a decisão, a final, fosse por este produzida[11].

Ainda que diversos autores na área legal tivessem afirmado que não era possível o desenvolvimento de algoritmos que reproduzissem, na íntegra, o processo de

---

[7] *Idem*, p. 937.

[8] Giovanni Sartor e L. Karl Branting, «Introduction: Judicial Applications of Artificial Intelligence», *cit.*, pp. 1-2.

[9] Michele Taruffo, «Judicial Decisions and Artificial Intelligence», in *Judicial Applications of Artificial Intelligence*, E-book, 1998, pp. 208-212, disponível em https://link.springer.com/book/10.1007/978-94-015-9010-5 [consultado em 28/07/2023].

[10] *Idem*, pp. 212-213.

[11] Giovanni Sartor e L. Karl Branting, «Introduction: Judicial Applications of Artificial Intelligence», *cit.*, p. 6.

tomada de decisão por um juiz, a verdade é que a tecnologia se desenvolveu, nas últimas décadas, no sentido de criar mecanismos auxiliares de resolução de litígios.

2.1. Da Resolução Alternativa de Litígios[12] à Resolução de Conflitos em Linha[13]

Os meios de resolução alternativa de litígios surgiram no âmbito de uma sociedade de consumo, pautada por uma crescente conflitualidade[14]. Em virtude do maior consumo nas mais diversificadas áreas de vida, também se verificou um maior consumo dos meios judiciais, por forma a resolver os litígios decorrentes do consumo propriamente dito, na área do crédito, de aquisição de bens e serviços, na área dos seguros e outros[15]. Estes meios foram desenvolvidos no sentido de desonerar os tribunais, criando-se instâncias alternativas, externas aos tribunais, com recurso a uma terceira figura imparcial, para se obter uma solução mais célere e menos onerosa[16].

Os sistemas de ODR, por sua vez, surgiram com os novos meios tecnológicos de comunicação, permitindo que as partes em litígio e até a entidade terceira independente, como seja o mediador ou árbitro, estejam em diferentes localizações geográficas[17]. O que distingue os ODR dos sistemas de RAL é que, nos primeiros, as partes encontram-se fisicamente distanciadas[18].

Nos sistemas de ODR, a tecnologia pode assumir um papel mais singelo, funcionando, tão-só, como meio de comunicação, ou poderá assumir um papel mais relevante e desenvolvido. É conforme esta sua especificidade que alguns autores

---

[12] Abreviadamente referidos como RAL ou ADR ("Alternative Dispute Resolution").

[13] Abreviadamente referidos como ODR ("Online Dispute Resolution").

[14] Fernando Manuel Martins Viana, *A resolução alternativa de litígios e as tecnologias de informação e comunicação – O caso particular da resolução de conflitos na Internet em Portugal e na UE*, Dissertação de Mestrado, Universidade do Minho, outubro 2015, pp. 27-28, disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/41173/1/Fernando%20Manuel%20Martins%20Viana.pdf [consultada em 29/07/2023].

[15] Catarina Frade, «A resolução alternativa de litígios e o acesso à justiça: A mediação do sobreendividamento», *Revista Crítica de Ciências Sociais*, n.º 65, maio 2003, p. 110, disponível em https://www.ces.uc.pt/publicacoes/rccs/artigos/65/RCCS65-107-128-Catarina%20Frade.pdf [consultado em 29/07/2023].

[16] Fernando Manuel Martins Viana, *A resolução alternativa de litígios e as tecnologias de informação e comunicação…*, *cit.*, p. 27.

[17] Francisco Andrade, Davide Carneiro e Paulo Novais, «A inteligência artificial na resolução de conflitos em linha», *Scientia Iuridica*, Tomo LIX, n.º 321, 2010, pp. 1-2, disponível em https://repositorium.sdum.uminho.pt/handle/1822/19388 [consultado em 29/07/2023].

[18] *Idem*, p. 2.

os enquadram em sistemas de ODR de primeira geração ou sistemas de ODR de segunda geração. Os primeiros são definidos como aqueles que preservam a pessoa como sendo "o elemento central no processo de planeamento e de tomada de decisão. (…) As ferramentas electrónicas serão utilizadas mas sempre vistas como meros instrumentos, sem autonomia e sem capacidade de desempenho de qualquer papel de relevo. O único objectivo da sua utilização será o de tornar mais fáceis e eficientes, para as partes, os processos de comunicação e de gestão da informação"[19].

Já a segunda geração de sistemas de ODR assume uma maior intervenção na resolução de litígios. Estes sistemas poderão mesmo substituir os intervenientes principais num litígio, isto é, atuarão no processo, representando-os, agindo como as partes e a própria entidade que assume a posição de neutralidade agiriam. Também poderão representar softwares que propõem soluções, até no âmbito do processo decisório[20]. Contudo, Francisco Andrade, Davide Carneiro e Paulo Novais assumem que, no que respeita ao desenvolvimento dos sistemas de ODR de segunda geração, estes são de mais difícil evolução, devido à complexidade de transformar o processo decisório que um julgador utiliza/desenvolve num software, não descurando a resistência da população relativamente à ideia de que poderá ser um sistema/algoritmo a tomar qualquer decisão referente à sua vida[21]. O entendimento relativo à dificuldade de desenvolver um *software* capaz de reproduzir o processo de decisão de um julgador humano, já referido *supra*, manteve-se inalterado entre o final da década de 80 e o ano de 2010, sendo este último o ano em que os autores referidos anteriormente assumiram tal entrave, relacionado com a evolução de sistemas de ODR de segunda geração.

São sistemas de ODR: sistemas multiagente, sistemas de apoio à decisão, raciocínio com informação incompleta, sistemas periciais (*expert systems*), representação do conhecimento, interfaces inteligentes, raciocínio baseado em casos[22]. Destes sistemas de ODR, são frequentemente utilizados no âmbito legal os sistemas periciais[23], que se caracterizam por serem sistemas de *software* que procuram replicar as capacidades humanas em determinada área de conhecimento. Estes sistemas periciais devem ser capazes de rececionar informação, analisá-la, desenvolver raciocínio e conhecimento e, sobretudo, tomar ou prever decisões tendo por base toda a informação previamente adquirida. Estes sistemas devem ser dotados de conhecimento prévio, o que poderá ser obtido através da compi-

[19] *Idem*, p. 5.

[20] *Idem*, pp. 6-7.

[21] *Idem*, p. 6.

[22] *Idem*, pp. 7-18.

[23] Também referidos por Donald H. Berman e Carole D. Hafner, no artigo *supra* citado.

lação e introdução nos sistemas de software de casos similares e respetivas decisões. Além disso, estes sistemas deverão ser dotados de *machine learning*, isto é, capacidade de aprendizagem, podendo ser corrigidos e aperfeiçoados a todo o tempo pelos seus programadores[24].

Uma vez que já nos encontramos com algum conhecimento acerca do funcionamento dos sistemas de ODR, poderemos, agora, passar a analisar alguns exemplos da sua aplicabilidade, em casos de Direito da Família e das Crianças, em diversos ordenamentos jurídicos, em diferentes pontos do globo.

2.2. *A Aplicação de Sistemas de ODR no âmbito do Direito da Família e das Crianças*

Como se pôde analisar *supra*, aquando da análise do desenvolvimento da inteligência artificial no que respeita às decisões judiciais, desde cedo os autores que se debruçaram sobre a matéria puderam verificar pontos positivos, designadamente no que respeitava à possibilidade de compilação e cruzamento de dados, ainda que todos, ou pelo menos a grande maioria, fossem no sentido de que o julgador humano não poderia ser substituído, atenta a complexidade do seu processo de decisão – tendo posteriormente sido verificado, no contexto da análise dos sistemas de ODR, que não se afigurava fácil reproduzir tal processo de decisão em mecanismos de ODR.

Cumpre, antes de mais, referir que os sistemas de ODR, em especial os aplicáveis no âmbito do Direito da Família, têm sido vistos, mais recentemente, como positivos. É esse o entendimento de Darren Gingras e Joshua Morrison, ambos investigadores no Canadá, que realçam que o desenvolvimento da inteligência artificial aplicável aos sistemas judiciários não tem ido no sentido de eliminar os intervenientes humanos, mas antes no sentido de desenvolver plataformas de auxílio à resolução dos litígios, simplificando processos complexos[25].

Uma das vantagens que estes autores apontam é no âmbito do processo de divórcio e inventário, quando os clientes têm de reunir documentação diversa, referente aos bens que existam para partilhar, sejam eles os relativos a propriedades, contas bancárias, ativos financeiros e outros, reduzindo aquilo que foi uma vida em comum a meros números. Apontam os sistemas de inteligência artificial como sendo úteis para a análise desta documentação, simplificando o processo. Fazem ainda menção ao sistema de inteligência artificial designado como "Tone

---

[24] Francisco Andrade, Davide Carneiro e Paulo Novais, «A inteligência artificial na resolução de conflitos em linha», *cit.*, pp. 12-13.

[25] Darren Gingras e Joshua Morrison, «Artificial Intelligence and Family ODR», *Family Court Review*, Vol. 59, n.º 2, abril 2021, p. 228, disponível em https://onlinelibrary.wiley.com/doi/abs/10.1111/fcre.12569 [consultado em 30/07/2023].

Analyzing Software", que analisa o tom de voz, as palavras, o seu significado e a intenção com que são proferidas, acabando por fazer sugestões de adaptação da linguagem, no sentido de esta se tornar mais neutra e a ideia que se pretende fazer passar à parte contrária ser mais objetiva, diminuindo a crispação, tão comummente existente entre as partes nos processos de divórcio e subsequente partilha[26].

Referem, ainda, que os sistemas de ODR aplicados aos litígios de família, como sejam os que analisam e desenvolvem eventuais soluções para questões financeiras – que terão impacto na partilha –, os sistemas capazes de analisar indícios de violência doméstica, os mecanismos que auxiliam, como se referiu, na análise dos objetivos pretendidos pelas partes, ainda que sugerindo determinada forma de comunicação, permitem encurtar o tempo do litígio, ao passo que também possibilitam que as partes sejam mais focadas e objetivas na resolução dos seus diferendos[27]. Contudo, afirmam que se denota uma elevada relutância por parte de advogados e outros intervenientes jurídicos na utilização de sistemas de inteligência artificial no meio legal[28].

Este estudo é, contudo, pouco aprofundado, no que concerne à realização de experiências efetivas com recurso a sistemas de inteligência artificial no âmbito do Direito da Família, ainda que seja útil para demonstrar eventuais aplicações destes mecanismos na resolução de litígios familiares e sua utilidade. Procederemos à análise de alguns casos em que foram aplicados sistemas de ODR noutros países.

2.2.1. A Aplicação do Sistema Preditivo "Decision Tree Analysis"[29] em Taiwan

Com o objetivo de analisar quais os fatores determinantes para os julgadores em Taiwan atribuírem a custódia[30] dos filhos a um progenitor ou a outro, os investigadores aplicaram um sistema dotado de *machine learning* para investigar as decisões judiciais relativas à guarda das crianças decorrentes de processos de di-

[26] *Ibidem*.

[27] *Idem*, p. 229.

[28] *Idem*, p. 230.

[29] Em português, "Análise da Árvore de Decisão".

[30] De referir que, em Portugal, os termos "guarda" e "custódia" já não são legalmente aplicáveis, referindo-se o ordenamento jurídico português à regulação das responsabilidades parentais. No presente artigo, utilizam-se as expressões "custódia" e "guarda" por uma questão de fiabilidade face ao artigo em análise.

vórcio[31], tendo limitado o estudo aos casos em que ambos os progenitores eram taiwaneses e ambos tinham requerido a custódia dos filhos, entre 1 de janeiro de 2012 e 31 de dezembro de 2017, sendo também excluídos todos os processos em que um dos progenitores não se havia pronunciado e os referentes a casamentos transnacionais, escrutinando um total de 835 decisões, pelas quais se encontravam abrangidas 1290 crianças[32].

O estudo pôde concluir que os juízes consideram, em primeiro lugar, o progenitor que é apontado como o cuidador da criança. Em segundo lugar, se a mãe for a cuidadora principal ou se for a mãe e o pai em medidas similares, o sistema preditivo aplicado concluiu que os juízes terão em conta a escolha da criança. Contudo, mesmo que a mãe seja a principal cuidadora, se a criança escolher o pai, então a mãe tem probabilidades diminuídas de lhe ser atribuída a guarda total da criança[33]. Daqui se poderia inferir que os julgadores taiwaneses apresentam uma ligeira preferência pelos progenitores homens.

Contudo, nos casos reais, analisados ao longo de um período de seis anos, verificou-se que as mães têm uma superioridade considerável: 75% das mulheres ficou com a guarda total dos seus filhos. Os investigadores concluem que este estudo permite, de forma consistente, entender os padrões de decisão, o que deverá auxiliar advogados e as partes num litígio a avaliar as probabilidades de obterem a custódia dos seus filhos. Se for possível obter um juízo provável de decisão de forma antecipada, recorrendo a este software, então tal poderá conduzir a uma maior probabilidade de existir uma transação, diminuindo-se a litigiosidade[34].

2.2.2. O sistema mexicano "Expertius"

O sistema "Expertius" foi desenvolvido pelo Instituto de Investigação Jurídica e o Centro de Ciências Aplicadas e Desenvolvimento Tecnológico do México, em parceria com o Conselho Nacional de Ciência e Tecnologia e o Tribunal Superior

---

31 A necessidade do estudo em análise surgiu de uma alteração ao Código Civil de Taiwan. Até à alteração de 1996, o Código Civil de Taiwan estipulava que a guarda dos filhos seria, à partida, entregue ao pai, exceto em caso de acordo dos progenitores em sentido diverso ou em caso de decisão diversa do Tribunal. Em 1996, substituiu-se a preferência da figura paternal pelo princípio do superior interesse da criança.

32 Sieh-Chuen Huang, Hsuan-Lei Shao e Robert B Leflar, «Applying Decision Tree Analysis to Family Court Decisions: Factors Determining Child Custody in Taiwan», in *ICAIL'21: Proceedings of the Eighteenth International Conference on Artificial Intelligence and Law*, julho 2021, p. 258, disponível em https://dl.acm.org/doi/10.1145/3462757.3466076 [consultado em 30/07/2023].

33 *Idem,* p. 259.

34 *Ibidem*.

de Justiça do Estado de Tabasco[35]. Este sistema foi criado para auxiliar os tribunais na área de Direito da Família, especificamente nos casos relacionados com pedidos de pensão de alimentos. O sistema analisa se o requerente da pensão de alimentos necessita, efetivamente, da pensão de alimentos que requer e, bem assim, se preenche os pressupostos legais para o efeito. Em caso afirmativo, o sistema auxilia a determinar o montante de pensão de alimentos que deverá ser arbitrado[36]. Como afirmam Francisco Andrade, Davide Carneiro e Paulo Novais, "O sistema integra três módulos: o módulo tutorial, o módulo inferencial e o módulo financeiro. O módulo tutorial orienta o utilizador na realização de diferentes tarefas. O módulo inferencial avalia a prova de acordo com pesos que o utilizador atribui a cada meio de prova. Determina ainda quais os argumentos que prevalecem e quais os que são derrotados. Por fim, o módulo financeiro assiste o utilizador no cálculo do valor das pensões de acordo com critérios determinados". Trata-se, por tal, de um sistema capaz de representar o conhecimento, incluindo o conhecimento pericial[37].

Por tal, enquadra-se num dos sistemas de ODR referidos acima. Da sua breve descrição, podemos depreender que se trata de um sistema que retém conhecimento, auxilia o julgador e outros intervenientes processuais na tomada de decisão, contudo, não os substitui, pelo que, a final, a decisão será sempre do julgador, analisado o caso concreto e ponderada toda a prova carreada para o processo.

2.2.3. O sistema de apoio à decisão australiano "Family Winner"

Emilia Bellucci e John Zeleznikow produziram investigação no âmbito do Direito da Família australiano, centrando-se, em especial, no desenvolvimento de sistemas de suporte à negociação. Iniciaram tal investigação devido ao facto de terem verificado que os processos de negociação no âmbito familiar são complexos, designadamente por considerarem que o Direito da Família é um ramo que difere substancialmente de outros, pelos seguintes motivos: não existe um ganhador do processo, isto é, no final de um divórcio, ambas as partes terão uma parte dos bens que lhes serão adjudicados, por exemplo; na Austrália, há muitos casos de litigância neste ramo (cerca de 50 000 divórcios por ano); e, por regra, as partes num litígio de família têm de comunicar, no decurso do processo

[35] Enrique Cáceres Neto, «La Inteligencia Artificial Aplicada al Derecho como una nueva Rama de la Teoría Jurídica», *Anales de la Cátedra Francisco Suárez*, Vol. 57, janeiro 2023, pp. 68-69, disponível em https://revistaseug.ugr.es/index.php/acfs/article/view/26281 [consultado em 30/07/2023].

[36] Francisco Andrade, Davide Carneiro e Paulo Novais, «A inteligência artificial na resolução de conflitos em linha», *cit.*, p. 24.

[37] *Ibidem.*

ou mesmo após o seu término – ou, pelo menos, os tribunais incentivam a que tal suceda, sendo que, da nossa experiência, tal é motivado pela existência de filhos, por forma a que exista a mínima cordialidade, mas também porque se procura uma conciliação[38], ao invés de uma disputa judicial[39]. Em conformidade com outros autores e outras considerações que já se realizaram *supra*, também os autores agora em análise consideram útil o desenvolvimento de sistemas de ODR aplicados no âmbito do Direito da Família, que simplificarão os processos judiciais, tornando-os menos morosos e menos dispendiosos, além de possibilitarem que as partes envolvidas litiguem de forma mais saudável, atento o facto de serem processos naturalmente mais emocionais[40].

Os autores desenvolveram alguns sistemas, como o "Family Negotiator", o "Split-Up" e o "Adjusted Winner", que não iremos aqui analisar, pelo facto de o primeiro ter sido excluído por não ter sido comercialmente viável, o segundo não efetuar o processo de negociação propriamente dito[41] e o terceiro estar intimamente relacionado com o sistema "Family Winner", que assume maior relevância. O sistema "Adjusted Winner" foi desenvolvido tendo por base a teoria de jogos, segundo o qual as partes devem atribuir pontuação que reflita o quanto determinado bem é valioso para cada uma das partes. O último bem a partilhar, em regra, acaba por ser dividido pelas partes no litígio, seja fisicamente, seja vendendo e dividindo os proveitos do mesmo, conforme as circunstâncias e em consonância com a proporção que o sistema determinar[42].

Já o modelo "Family Winner", ainda que partindo, também, da lógica em que cada parte do litígio indica os bens a partilhar, a sua importância e como é que esses bens se poderão relacionar com outros, desagua numa solução distinta[43]. A partir daí, o sistema compila tudo o que foi arrolado pelas partes e realiza uma proposta da sua distribuição, sem descurar que a atribuição de um artigo a uma ou outra parte poderá fazer alterar as preferências de qualquer uma delas. Se as partes aceitarem a proposta, procede-se à divisão; caso contrário, "o sistema reinicia a negociação, artigo por artigo, começando pelos considerados menos discutidos", sendo que as partes devem separar os bens a partilhar em tantos

---

[38] Vejam-se as tentativas de conciliação consagradas no âmbito do Direito da Família português, designadamente no processo de divórcio (artigo 1779.º, n.º 1, do Código Civil português).

[39] Emilia Bellucci e John Zeleznikow, «Representations of Decision-making Support in Negotiation», *Journal of Decision Systems*, Vol. 10, 2001, p. 451, disponível em https://www.tandfonline.com/doi/abs/10.3166/jds.10.449-479 [consultado em 30/07/2023].

[40] *Idem*, pp. 451-452.

[41] *Idem*, pp. 455-458.

[42] *Idem,* p. 459.

[43] *Idem*, p. 466.

quantos possíveis, decompondo-os, sendo estes atribuídos paulatinamente, até que nenhum bem haja mais para partilhar[44]. Trata-se de um sistema complexo, aqui exposto de forma consideravelmente resumida, não se analisando com profundidade os mecanismos de inteligência artificial de que é dotado, apenas para dar a conhecer ao público a sua existência[45]. A verdade é que este sistema, partindo de um ponto de vista, à partida, neutro, propõe soluções de partilha racionais e lógicas, procurando, em simultâneo, fazer uma divisão justa e equitativa dos bens pelas partes.

3. Breves Considerações

Face aos mecanismos expostos, apresenta-se como praticamente indubitável assumirmos a importância e a facilidade que o desenvolvimento das novas tecnologias e, em particular, as artificialmente inteligentes, trouxeram à vida dos cidadãos em todo o mundo. Aliás, a sua utilidade e viabilidade foram, em alta medida, colocadas à prova com a pandemia da covid-19, que obrigou à aplicação de métodos alternativos de trabalho, desde o teletrabalho ao ensino *online*.

A resolução de litígios em linha, especialmente no âmbito do Direito da Família, será uma ferramenta útil, permitindo que as partes procurem encontrar consensos, alcançando um resultado mais rápido, mais cómodo e menos dispendioso, pois permitirá que os intervenientes possam nem encontrar-se no mesmo país, não deixando, no entanto, de solucionar os problemas comuns, a partir da intervenção de entidades imparciais, evitando-se o recurso aos tribunais. É neste sentido que também se têm pronunciado o American Law Institute (ALI) e o Instituto Internacional para a Unificação do Direito Privado (abreviadamente designado por UNIDROIT), que defende que os tribunais devem promover a conciliação das partes e, também, o recurso pelas mesmas aos meios de resolução alternativa de litígios, assim como a Assembleia Geral das Nações Unidas[46].

Analisando todos os mecanismos de ODR que têm sido colocados em experimentação, facilmente conseguimos cogitar a sua eventual aplicabilidade ao ordenamento jurídico português. Exemplificando: o sistema preditivo "Decision Tree Analysis" poderia ser útil como ferramenta de auxílio aos advogados que

---

[44] Francisco Andrade, Davide Carneiro e Paulo Novais, «A inteligência artificial na resolução de conflitos em linha», *cit.*, p. 26.

[45] De forma mais detalhada, Emilia Bellucci e John Zeleznikow, «Representations of Decision-making Support in Negotiation», *cit.*, pp. 466-475.

[46] Michael S. Coffee, «Cross-border issues associated with the use of online dispute resolution for international family law matters», *Family Court Review*, Vol. 59, n.º 2, abril 2021, pp. 211-212, disponível em https://onlinelibrary.wiley.com/doi/abs/10.1111/fcre.12568 [consultado em 30/07/2023].

atuam no âmbito do Direito da Família, por forma a poderem aconselhar os seus clientes, mas também aos mediadores[47]/[48], que com recurso a tal plataforma poderiam facilmente verificar, atendendo à jurisprudência e doutrina existentes, quais as probabilidades de cada uma das partes num eventual litígio de regulação de responsabilidades parentais, podendo melhor encaminhar o sentido das negociações entre as partes.

De igual forma, facilmente cogitamos a possibilidade de aplicação do modelo mexicano "Expertius" aos processos relativos a obrigação de alimentos, quer os devidos por pais a filhos – pois esta ferramenta sempre se afiguraria útil para sugerir um montante de pensão de alimentos a fixar, atendendo às especificidades concretas do caso e das partes –, da mesma forma que se afiguraria útil para averiguar o preenchimento dos pressupostos legais para que uma pensão fosse atribuída, por exemplo, pelo ex-marido à ex-mulher, sem prejuízo de este mecanismo ser sempre supervisionado pelo julgador e de a decisão caber apenas a este último, que sempre terá de verificar a efetiva obrigatoriedade de alimentos e qual a quantia adequada ao caso concreto.

Por último, também não se afigura tarefa árdua equacionar a aplicabilidade do sistema "Family Winner" aos processos de inventário, designadamente os decorrentes de processos de divórcio.

Indo um pouco mais longe, e ainda que, no presente artigo, não se evidenciem sistemas aplicados à matéria, parece possível, também, que sistemas preditivos possam ser aplicados aos processos de adoção. O processo de adoção, no ordenamento jurídico português, pauta-se pela existência de três fases: a fase preparatória, a fase de ajustamento e a fase final, conforme estatui o artigo 40.º do Regime Jurídico do Processo de Adoção[49]. É na fase de ajustamento que os organismos da Segurança Social ou da instituição particular autorizada avaliam as necessidades da criança em condição de adotabilidade e, avaliando os candidatos existentes por todo o país, procura fazer-lhe corresponder potenciais candidatos, procurando compatibilizar as condições do candidato a adotante e as necessidades da criança potencial adotanda. Seria, certamente, útil que um sistema preditivo, dotado de análise de situações reais, que tivessem desaguado ou não em processos

---

[47] A mediação encontra-se expressamente consagrada, no âmbito dos processos de divórcio, no artigo 1779.º do Código Civil português.

[48] Rossana Martingo Cruz, na sua obra *A Mediação Familiar como Meio Complementar de Justiça* (Almedina, 2018), aborda a utilidade da mediação como meio alternativo de resolução de litígios, especialmente no espetro do Direito da Família, que assume especificidades pessoais e emocionais, as quais se afigura útil salvaguardar através do menor recurso à litigância típica dos tribunais.

[49] Lei n.º 143/2015, de 8 de setembro, 1.ª Série, n.º 175, disponível em https://files.dre.pt/1s/2015/09/17500/0723207251.pdf [consultado em 31/07/2023].

de adoção efetivos, bem como de capacidade para analisar as características de potenciais adotantes e adotandos e sua eventual compatibilidade, pudesse realizar este tipo de procedimento, poupando recursos e tornando menos morosas estas tarefas, tornando, consequentemente, os processos de adoção mais céleres, sem prejudicar a segurança e certeza pelas quais se devem pautar. Obviamente, os juízos de probabilidade decorrentes do sistema deveriam ser verificados pelos técnicos especializados que, por regra, se encontram incumbidos de efetuar tais tarefas.

Os sistemas de inteligência artificial têm vantagens inegáveis e a sua utilidade no âmbito do Direito da Família e das Crianças é notória. A experiência de quem atua neste ramo do Direito é de que os litígios desta natureza são, não raras vezes, pautados por um comportamento hostil, de ressentimento e, muitas vezes, de vingança entre as partes. Tornando-se, consequentemente, um palco de rivalidade, onde, frequentemente, as crianças envolvidas nos litígios são vistas como meio de infligir dor à contraparte, funcionando como verdadeiras armas de arremesso.

A verdade é que os sistemas de ODR, que vieram adaptar e fazer evoluir os meios alternativos de resolução de litígios, são vantajosos, pois permitem que as partes não se vejam confrontadas num mesmo espaço, permitem o recurso a mecanismos que, com alguma razoabilidade, ajuízam as pretensões das partes, elucidando-as com maior racionalidade e objetividade – fatores que, em contextos de maior crispação, assumem maior relevância –, bem como permitem a obtenção de propostas de solução de forma pacífica e neutra – neutralidade, esta, que não raras vezes as partes colocam em causa relativamente aos julgadores em litígios judiciais, por considerarem que estes assumem uma maior simpatia por determinada parte do processo.

Estes sistemas comportam, contudo, riscos. Desde logo, a capacidade de *machine learning* de que muitos destes sistemas são dotados, como *supra* também se pôde aferir, sem prejuízo de os algoritmos que subjazem a tais sistemas poderem ser dotados de preconceitos. Se é certo que o erro humano existe, nos sistemas de inteligência artificial, o erro também não se encontra excluído[50] – não só porque a tecnologia é desenvolvida pela mão humana, mas também porque estas tecnologias podem desenvolver em sentido diverso do pretendido, o que naturalmente obrigará a um dever de sequela dos seus produtores ou programadores. É exatamente devido a estes riscos que a Comissão Europeia, na sua "Proposta de Regu-

[50] Lurdes Varregoso Mesquita e Rossana Martingo Cruz, «Algumas notas reflexivas sobre a carta portuguesa de direitos humanos na era digital: da proteção da criança ao uso da inteligência artificial em processos decisórios», *Fodertics 10.0 – Estudios sobre Derecho Digital*, junho 2022, pp. 773-774, disponível em https://www.comares.com/libro/fodertics-10-0_143750/ [consultado em 31/07/2023].

lamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial)", caracteriza os sistemas artificialmente inteligentes que procedam à aplicação da lei como sendo de risco elevado, conforme referido no Considerando 40 da proposta, bem como estabelece como princípio fundamental, no seu artigo 4.º-A, o "controlo e supervisão por humanos" dos sistemas de inteligência artificial[51].

Estas preocupações assumem maior relevância, no âmbito do Direito da Família e das Crianças, atenta a sua relação com os direitos fundamentais e a natural sensibilidade das matérias abrangidas.

4. Conclusão

O presente artigo, tendo como objetivo, essencialmente, analisar alguns dos estudos que têm vindo a ser efetuados no âmbito da inteligência artificial aplicada ao Direito da Família, e procurando averiguar a aplicabilidade real de sistemas preditivos no contexto de resolução de litígios neste específico ramo do direito, leva-nos a concluir pela utilidade e efetiva aplicabilidade de alguns mecanismos artificialmente inteligentes à resolução de querelas no contexto das referidas matérias.

Contudo, e atento o facto de estarem em causa direitos fundamentais, de também crianças serem visadas nestes litígios e, simultaneamente, o risco de uma excessiva confiança da humanidade nos sistemas de inteligência artificial e do seu desenvolvimento desregular, afigura-se essencial que estes sistemas atuem apenas como auxiliares na aplicação do direito, sendo devidamente "controlados e controláveis"[52], devendo caber sempre a decisão final a um juiz, a quem compita, igualmente, avaliar os resultados provenientes dos sistemas dotados de inteligência artificial.

O presente artigo, não tendo como finalidade formular propostas de solução ou de efetiva aplicação dos sistemas de inteligência artificial ao Direito da Família português, afigura-se como um estudo inicial da sua potencialidade, analisando as experiências que têm sido realizadas neste contexto, não descurando que os próprios investigadores na área tecnológica assumem a dificuldade de reprodu-

---

[51] Comissão Europeia, Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União, junho 2023, disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PT.html [consultada em 31/07/2023].

[52] Lurdes Varregoso Mesquita e Rossana Martingo Cruz, «Algumas notas reflexivas sobre a carta portuguesa de direitos humanos na era digital: da proteção da criança ao uso da inteligência artificial em processos decisórios», *cit.*, p. 778.

zir em algoritmos o processo decisório de um julgador humano, facto que deverá ser criteriosamente cuidado em futuros estudos de propostas de aplicação de sistemas preditivos neste ramo do direito.

SOFTWARE IN SURGICAL ROBOTS: WHEN INFORMATION MIGHT BE A PRODUCT

Tomàs Gabriel García-Micó[1]

Abstract: Product liability is one of the most well-known harmonised fields of EU law. It has provided, for closely 40 years, a way for consumers to obtain redress for damages suffered as a consequence of a defective product bought or used over them. On the one hand, such compensation can be obtained without proving that the manufacturer has acted negligently. But, on the other, the plaintiff has to establish the existence of a defect in the product and a causal connection between that and the damage. Even though, the Product Liability Directive has proved to be a good tool to obtain redress, a great deal of criticism has been thrown upon the Directive due to its lack of adaptability to modern times. Living in a century where technology evolves at a tremendous speed, the traditional distinction between «products» and «services» has become less useful and, at some point, artificial, as products today are combined with digital elements. This contribution focuses on the difficulties in the application of product liability law in a complex area, such as surgical robotics, where a movable good (a «product») combines with software (information, a «service»). In particular, it will be centered around when the software turns out to be hackable, and two main questions will be answered: is this software a «product» under the Product Liability Directive? If so, is defective the software that can be hacked?

Keywords: Software; Product liability; Hacking.

[1] Postdoctoral researcher in Civil Law (Universitat de Barcelona). Visiting Postdoctoral Researcher with the *Centro de Investigação em Justiça e Governação* (JusGov) at the *Escola de Direito* (*Universidade do Minho*). Contact: tggarcia-mico@ub.edu.

1. Introduction

We are now living in the era of Internet 4.0, of 5G, of the metaverse, as well as other interconnected technologies and more advanced systems marketed to make our lives easier. We can now access our medical records through mobile apps, or even we have smart houses that turn on lights or the air conditioning in summer by voice control. All these devices have something in common: software, a set of instructions, embedded or not to physical devices, that determine how a machine may act under specific circumstances. But undoubtedly, these advances have also their drawbacks: the fact that software may turn out to be defective and cause harm to its users. Here, is where people who suffered such damages will ask: what can I do? Whom can I sue? And, most importantly, under which grounds? Answering these questions is not easy at all. Software is intangible *per se*, it's just code that is written on a computer and, even though it would seem easy to consider that product liability law may have something to say, the application of such a regime requires that the damage has been caused by a «product». Therefore, the question that needs to be answered is: is software a product? The answer that I anticipate is, yes and no, depending on the case. To answer that question is, precisely, the aim of this contribution.

Software are different and diverse: it is not the same an application that we download and install on our mobile phones, or a microchip storing the operative system of our computer, or the chip that is embedded into a surgical robot and that makes the system to replicate, over the patient's body, the movements that a surgeon does with a set of joysticks located in a console. This latter scenario is the one in which I will be focusing on this contribution: the defective medical software embedded into the state-of-the-art in surgery: the Da Vinci surgical robot, manufactured by the American company Intuitive Surgical.

The question initially anticipated, about the qualification of the software as a product, would be partially solved with the Proposal of Directive,[2] which is still not officially approved,[3] and clarifies that software will be a product under the

[2] Proposal for a Directive of the European Parliament and of the Council on liability for defective products [COM(2022) 495 final, 2022/0302 (COD), the Proposal of Directive].

[3] First reading within the Council of the EU: https://eur-lex.europa.eu/procedure/EN/2022_302 and, as of October 9, 2023, the JURI and IMCO, as joint committee, adopted a report on the proposal for a new PLD, with the first trialogue taking place on October 14, 2023. According to the press statement resulting from this meeting, it was announced that the second trialogue is scheduled for December 14, 2023: https://www.europarl.europa.eu/committees/en/product/product-details/20230417CDT11482. The most recent amendments to the Proposal of Directive (A9-0291/2023) are accessible here: https://www.europarl.europa.eu/doceo/document/A-9-2023-0291_EN.html.

new Art. 4(1),[4] but this will only be a reality for products «placed on the market or put into service» after the date outlined in Art. 17(1) of the Proposal of Directive. But the research question of this contribution will remain unanswered for the thousands of products marketed before that date, and the Da Vinci is one of them.

1.1. *A short, but necessary, history of technology in surgery*

There has been a clear evolution in the medical field in the technical means used to perform surgeries on patients. Initially, surgeons needed to perform an incision all along the area in which they were going to operate (open surgery). Later, around 1960, surgeries were performed -and still are- by doing a small incision on the patient's body through which a laparoscope was introduced (laparoscopic surgery). Since the end of 1980, there has been an increasing trend in the use of surgical robots to assist surgeons in performing surgeries (robotic-assisted minimally-invasive surgery). The state-of-the-art of this latter is the Da Vinci surgical robot, which is not an example of artificial intelligence applied in medicine, but a master-slave system, where the robot physically installed in the litter of the operating room emulates (due to its embedded software) the movements that the surgeon does with a set of joysticks located in a console.

Just to show some relevant data, as of March 2023, more than 12 million surgeries have been performed with the assistance of this robot,[5] and the installed base is of 7,779 robots.[6] This increasing trend in the use of this surgical technology has given rise to the first legal procedures for damages suffered by patients in the course of a robotic-assisted minimally-invasive surgery performed with the Da Vinci. As of this moment, all the cases have been discussed in the United States of America. For this reason, it is of utmost importance, not just to discuss the legal implications of the not-so-future uses of artificial intelligence in medicine, but also to assess whether our current legal frameworks are fit to solve the problems that are already arising with non-AI technologies. It can be anticipated that current legal frameworks, even struggling, are fit for this purpose, but some modifications are necessary.

---

[4] «(1) 'product' means […] software».

[5] Gary Guthart, «Annual Shareholder Meeting 2023», available at https://isrg.intuitive.com/static-files/f5722e3a-5f2c-4864-b449-c8a90dc8e265 [consult. on 5/7/2023].

[6] Intuitive Surgical, «Investor Presentation. Q1 2023», available at https://isrg.intuitive.com/static-files/45f1021c-5658-4eb2-91bb-ad33417ffc6e [consult. on 5/7/2023].

1.2. *The liable subjects and ways to obtain redress*

(a) From the supply chain: the case of software

The Da Vinci robot is composed of hardware (the physical structure) and software (*vid. supra*), and therefore it is a product that needs to be manufactured. Assemblers (final manufacturers in terms of Art. 3.1 PLD[7]), or component manufacturers might be liable if a defect can be found in the product. If the defect is on the hardware, the applicability of the PLD cannot be doubted, but what if the source of the defect is software? In the case of modern products, we will see an evident trend where the source of damage is software,[8] not hardware.

(b) From notified bodies

The Da Vinci qualifies as a medical device under the MDR.[9] That means that before its commercialisation it needs to overcome a process called conformity assessment carried out by a notified body (Art. 52 MDR, in connection with Arts. 10.1, 19.1, 20.1, 20.5 MDR).[10] Conformity assessment is not, and shall not be equaled to, approval by a regulatory agency (*cfr.* with medicinal products[11]).[12] No regulatory agency intervenes in this process (unless it is the notified body of a Member State, something that is quite uncommon, but that constitutes the case in Spain). Whether the notified body is a private company, or a public administration (such as regulatory agencies) is only relevant for identifying the liability regime to be applied but does not change the fact that conformity assessment is not an official approval.

---

[7] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, Product Liability Directive, the PLD).

[8] Recital 12 of the Proposal of Directive.

[9] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017).

[10] According to the EU NANDO Database, to the date, up to 39 notified bodies have been officially appointed by the Member States. This information may be checked here: https://webgate.ec.europa.eu/single-market-compliance-space/#/notified-bodies/notified-body-list?filter=bodyTypeId:3,notificationStatusId:1,legislationId:34 [consult. on 7/7/2023].

[11] See Art. 6.1 of Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001) where it is clearly said that the approval by a regulatory agency is a «marketing authorisation», while the MDR does not includes any marketing authorisation.

[12] As most of the notified bodies are private companies.

Notified bodies -which are raised to gatekeepers- might be liable as they do have a duty of overseeing the medical devices they have positively assessed through audits, both announced and unannounced. Failing to perform these duties will make them liable for the damages suffered, for instance, by women who were implanted with deceitfully manufactured PIP breast implants.[13]

(c) From the authorised representative

The MDR regulates the «authorised representative», a company that is raised as a prerequisite for the marketing of medical devices in the European Union by manufacturers domiciled in a third State (Art. 11.1 MDR). The relationship between the authorised representative and the manufacturer is governed by the rules of the written mandate (Art. 11.3 MDR) and will entail the assumption by the former of functions of a representative nature. Furthermore, Art. 11.5 MDR extends the subjective scope of the PLD by making the authorised representative «legally liable for defective products under the same conditions as the manufacturer, and jointly and severally with the manufacturer». In other words, it places the authorised representative on the same level as the producer, without the need to resort to the other liable parties, or to the prior extrajudicial exercise of the claim against one of the suppliers to identify the specific importer in the European Union of the product, or the programmer of the potentially defective embedded software.

(d) From healthcare services providers

In Spain, health services are offered by public (National Health System, *Sistema Nacional de Salud*, the regional health services of the different autonomous communities) or by private means (most commonly, under the scope of healthcare insurance).[14] In Spain, according to the Health Ministry's data, close to 80% of

---

[13] All began with the ruling of the CJEU in Case C-219/15 *Elisabeth Schmitt v TÜV Rheinland LGA Products GmbH* [2017] ECLI:EU:C:2017:128, where the CJEU admitted that it was possible to find a notified body liable if they failed to comply with the duty of care that was imposed over them as entrusted of the conformity assessment of medical devices. In France, some rulings of the *Cour de cassation* have considered that TÜV Rheinland was liable for, precisely, failing to comply with its post-commercialisation obligations: rulings of 10.10.2018 (16-19.430, FR:CCASS:2018:C100615); and two of 25.5.2023 (21-23.257; FR:CCASS:2023:C100302; and 22-11.541, FR:CCASS:2023:C100301). In Germany, ruling of the *Bundesgerichtshof* of 27.2.2020 (VII ZR 151/18, NJW-RR 2020, 1514).

[14] According to the most recent data from UNESPA, there are a total of 10,292,344 people in Spain who are beneficiaries of health care insurance, which means, considering the population data from the INE, that 21.62% of the Spanish population is covered by these insurances. UNESPA, «Informe Estamos Seguros 2020», 2021, available at https://www.unespa.es/que-hacemos/publicaciones/informes-2021/ [consult. on 6/7/2023] and INE, «Cifras de Población (CP) a 1 de julio de 2022», 2022, available at: https://www.ine.es/prensa/cp_j2022_p.pdf [consult. on 6/7/2023].

the population attend the public health system when they need a specialist or surgery, while the remaining 20% opt to go to the private health system.[15]

The coexistence of public and private hospitals supposes that the subjects who are liable for damages are different, as well as the legal rules applicable to ascertain whether they are liable or not. In the case of private hospitals, we have the general tort law rules (Arts. 1902 CC[16] and ff), while in the case of the regional public health systems, their liability is regulated by the LRJSP.[17]

In the case of private hospitals, also the insurance company that provided the healthcare provider list might be liable. And always there is a recourse against the surgeon or the members of the medical staff to whom liability may be apportioned. Their liability will be based on the general rules of tort law. Given that these professionals are subject to an obligation of having insurance for civil liability, also the liability of this insurer will possibly be requested (Arts. 73-76 LCS,[18] and directly liable, under Art. 76.1 LCS). Their employers, the hospitals, will be directly liable both under the private law regime (Art. 1903 CC, *respondeat superior*), as well as in the public system (Art. 36.1 LRJSP, setting as a requirement to «enforce the patrimonial liability» for the harmed subjects to «directly demand compensation from the corresponding Public Administration»).

2. Software as a product

2.1. The concept of «product» in product liability law

According to Art. 2 PLD, the concept of «product» encompasses electricity, as well as any movable good, even when it is a component or part of another movable or immovable. There are some Member States that have made some noteworthy changes when transposing the PLD: Austria, Belgium and Estonia. In Austria and Belgium, not every movable good is a «product», but it is necessary that it is

[15] Ministerio de Sanidad, «Informe Anual del Sistema Nacional de Salud 2020-2021», 2022, available at: https://www.sanidad.gob.es/estadEstudios/estadisticas/sisInfSanSNS/tablasEstadisticas/InfAnualSNS2020_21/INFORME_ANUAL_2020_21.pdf, p. 26 [consult. on 7/7/2023]. It is also true that the trend since 2010 has been a greater, albeit discreet, rise of private medicine over public medicine. In 2010, the former accounted for 13.7% of consultations, in 2018 it accounted for 20%, and on 2020 for the 21.64%.

[16] Royal Decree of 14 July 1889 by which the Civil Code is published (Gaceta de Madrid 206, 25.7.1889, the CC).

[17] Act 40/2015, of October 1, of the Legal Regime of the Public Sector (BOE 236, 2.10.2015).

[18] Law 50/1980, of 8 October 1980, on Insurance Contracts (BOE 250, 17.10.1980, the LCS).

tangible (*bewegliche Sachgüter*, in Belgium;[19] and *bewewegliche körperliche Sache*, in Austria[20]).[21] In Estonia, software is expressly mentioned within the concept of «product».[22] In the other cases, we will need to analyse what is a movable good according to every Member State's civil legislation.

2.2. Is it necessary that the movable good is tangible?

Doctrine (Spain and abroad) has been divided into two opposite positions about whether the concept of product in product liability law requires the movable good to be tangible or not. There has been a sector that has adopted an all-embracing approach and, therefore, has understood that it is irrelevant whether the good is corporeal or not.[23] Others have adopted a more restrictive approach, considering that «product» includes tangible goods, as well as incorporeal goods that can be apprehended or transported.[24]

---

[19] Art. 2 of the *loi relative à la responsabilité des produits défectueux* of 25 February 1991 (*Moniteur Belge* 1991-02-25/30, 22.3.1991).

[20] § 4 of the *Bundesgesetz vom 21. Jänner 1988 über die Haftung für ein fehlerhaftes Produkt* (BGBl. 95/1993).

[21] In Germany, the definition of «movible good» (*bewegliche Sache*) is linked to its corporeal nature (§ 90 BGB). See Gerhard Wagner, «Liability Rules for the Digital Age», *JETL*, vol. 13, issue 3, 2023, p. 200 (pp. 191-243).

[22] § 1063(1) *Võlaõigusseadus* (*Elektrooniline Riigi Teataja* I 2001, 81, 487).

[23] Joan Carles Seuba Torreblanca, «Capítulo III. Concepto de product», in Pablo Salvador Coderch and Fernando Gómez Pomar (eds.), *Tratado de responsabilidad civil del fabricante*, Cizur Menor, Aranzadi, 2008, pp. 111, 112 and 114 (pp. 105-133) and Mónica Navarro-Michel, «Vehículos automatizados y responsabilidad por producto defectuoso», *Revista de Derecho Civil*, vol. VII, issue 5, 2020, p. 181 (pp. 175-223).

[24] Santiago Cavanilla Múgica, «El Real Decreto Legislativo 1/2007 por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias», *Aranzadi civil*, issue 1, 2008, pp. 2133-2166. About this debate, it can further seen Simon Whittaker, «European Product Liability and Intellectual Products», *Law Quarterly Journal*, issue 105, 1989, p. 129 (pp. 125-ff); Jean-Paul Triaille, «The EEC Directive of July 25,1985 on liability for defective products and its application to computer programs», *Computer Law and Security Report*, issue 5, 1993, p. 218 (pp. 214-226); K. Alheit, «The applicability of the ED Product Liability Directive to Software», *Computer and Internatioanl Law Journal of Southern Africa*, issue 2, 2001, p. 200 (pp. 188-209); Daily Wuyts, «The Product Liability Directive – More than two Decades of Defective Products in Europe», *JETL*, vol. 5, issue 1, 2014, p. 5 (pp. 1-34); Chritoph Schmon, «Product Liability of Emerging Digital Technologies», *IWRZ – Zeitschrift für Internationales Wirtschaftsrecht*, issue 6, 2018, p. 255 (pp. 254-258); Bernhard A. Koch, «Product Liability 2.0 – Mere Update or New Version?», in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds.), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, Nomos, 2019, p. 105 (pp. 99-116), and Geraint Howells and Christian Twigg-Flesner, «Interconnectivity and Liability: AI and the Internet of Things», 2021, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3843134, p. 15 [consult. on 8/7/2023].

2.3. The case of software

(a) Software in the doctrine

The Cambridge Dictionary defines *software* as «the instructions that control what a computer does». This definition highlights a key feature of modern software: its intangibility since, in short, it is nothing more than information.[25] The debate shown above (2.2 *supra*) has been also maintained regarding the software (embedded vs. non-embedded software).[26] Not every software is the same, we need to distinguish between embedded software, which is incorporated within a tangible good (microchip or USB, for instance), and non-embedded software, which will be incorporated into a tangible good through a virtual process of downloading and installation.

A first doctrinal sector has defended the irrelevance of whether the software is integrated into a movable good, on the understanding that the treatment to be received by the manufacturers of one and the other should be the same, taking an all-embracing approach under the veil of the principle of technological neutrality.[27] Another has taken a clear position in favour of including embedded

[25] Jane Stapleton, «Software, Information and the Concept of Product», *Tel Aviv University Studies in Law*, issue 9, 1989, p. 150 (pp. 147-164); Jane Stapleton, *Product Liability*, London, Butterworths, 1994, p. 333; Marian Gili Saldaña, *El producto sanitario defectuoso en Derecho español*, Barcelona, Atelier 2008, p. 190, and Pedro Alberto de Miguel Asensio, *Derecho privado de Internet*, 6th edn., Navarra, Thomson Reuters, 2022, p. 205.

[26] The Commission, already in 1988, and not yet thinking of this second scenario, pronounced itself in favour of the inclusion of software in the definition of «product» of the PLD. See the written question No 706/88 by Mr. Gijs de Vries (LDR - NL) to the Commission of European Communities and the reply given by Lord Arthur Francis Cockfield, who was then the European Commissioner for Internal Market and Services: «Consequently, the Directive applies to software in the same way, moreover, that it applies to handicraft and artistic products» (OJEC C 114/42, 8.5.1989).

[27] Gerhard Wagner, «Produkthaftung für autonome Systeme», *Archiv für die civilistische Praxis*, vol 217, issue 6, 2017, p. 719 (pp. 707-765); Taivo Liivak, «Liability of a manufacturer of fully autonomous and connected vehicles under the Product Liability Directive», *International Comparative Justice*, vol. 4, issue 2, 2018, p. 181 (pp. 178-189), and Helmut Koziol, III Österreichisches Haftpflichtrecht, 3rd edn., Jan Sramek, 2020, pp. 453 ff.

software in the concept of a product.[28] They also consider that stand-alone software should also be included in the objective scope of the PLD, giving a teleological interpretation of the PLD since, they say, its purpose is none other than to protect consumers from damage caused by mass-produced products, and this would include software, except when it is developed according to the specific requirements of its recipient (bespoke software or custom software).[29] Also, a third

[28] Duncan Fairgieve, Geraint Howells, Peter Møgelvang-Hansen, Gert Straetmans, Dimitri Verhoeven, Piotr Machnikowski, André Janssen and Rainer Schulze, «Product Liability Directive», in Piotr Machnikowski (ed.), *European Product Liability. An Analysis of the State of the Art in the Era of New Technologies*, Cambridge, Intersentia, 2016, p. 17 (pp. 17-108); Jean-Sébastien Borghetti, «How can Artificial Intelligence be Defective?», in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds.), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, Nomos, 2019, p. 64 (pp. 63-76); Jean-Sébastien Borghetti, «Civil Liability for Artificial Intelligence: What Should its Basis Be?», *La Revue des Juristes de Sciences Po*, issue 17, 2019, p. 95 (pp. 94-102); Ernst Karner, «Liability for Robotics: Current Rules, Challenges, and the Need for Innovative Concepts», in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds.), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, Nomos, 2019, p. 119 (pp. 117-124), and Gerhard Wagner, «ProdHaftG § 2 Produkt», in Franz Jürgen Säcker (ed.), *Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB*, 8th edn., München, C.H. Beck, 2020, rn. 21.

[29] Cédric Coulon, «Du robot en droit de la responsabilité civile: à propos des dommages causés par les choses intelligentes», *Responsabilité civile et assurances*, issue 6, 2016, para 12; Jean-Sébastian Borghetti, «How can...», p. 64, and Jean-Sébastian Borghetti, «Civil Liability...», p. 95. In the US this position has been taken by courts in *Halstead v. United States*, 535 F. Supp. 782, 791 (D. Conn. 1982) and *Saloomey v. Jeppesen & Co.*, 707 F.2d 671, 676 (2d Cir. 1983). In Germany, this position was sustained back in the eighties in the case of contract law (contracts for the transfer of software). The BGH sustained a restrictive view focusing on whether the software (the data) was embedded into a tangible data carrier (the hardware). In Urt. v. 1987 – VIII ZR 314/86, NJW 1988, 406. In its Urt. v. 18.10.1989 – VIII ZR 325/88, NJW 1990, 320, the BGH faced a different case where it was not necessary to pronounce about whether a non-tangible software (because it was not contract law which was at stake, nor non-contractual liability) could or not be subject to sale. But, even though, the BGH considered that the good could be subject of a contract, not because the tangible data carrier (which was non-existent), but for the digital copy of the data which was done in the computer's hard disk. With the entry into force and the transposition of the PLD in Germany, it has been discussed whether if the hardware-linkage (*Hardwareanknüpfung*) theory sustained by the BGH back in the eighties should remain or not. For the debate, see Anne-Kathrin Müller, *Software als "Gegenstand" der Produkthaftung*, Baden-Baden, Deutscher Wissenschafts-Verlag, 2019, pp. 21-29.

position has been taken, a restrictive one that considers that non-embedded software will not be possibly subsumed in the definition of «product» of the PLD.[30]

Despite the divergence, what all these doctrinal sectors agree on is that software embedded in a complex product will always be a component of a product, as it is transportable by means of physical storage units, such as disks, USB devices or information storage chips. The differential issue, and one that does not present a problem for the purposes of this contribution, is precisely that of non-embedded or stand-alone software, the software that we download to our phones, for example, via applications. The all-encompassing thesis would consider it to be a product, while the restrictive thesis would not consider it as such. And the Proposal of Directive, if approved in the current state, will position with the all-embracing view and will make both non-embedded and embedded software a product covered by product liability law, except for free and open-source software, as defined in Recital 13 of the Proposal of Directive.

(b) Medical software

The issue of software as a product in the PLD has not, so far, been dealt with by the CJEU. However, there has been one case in which the CJEU ruled on whether or not a computer program «designed by its manufacturer to be used on human beings for the purpose of research into a physiological process without being

[30] Martin A. Hogg, «Liability for Unknown Risks: A Common Law Perspective», *JETL*, vol. 7, issue 2, 2016, p. 11 (pp. 1-32); Sebastian Rockstroh and Hanno Kunkel, «IT Sicherheit in Produktionsumgebungen», *MMR Zeitschrift für IT-Recht und Recht der Digitalisierung*, issue 2, 2017, p. 82; Gerald Spindler, «User Liability and Strict Liability in the Internet of Things and for Robots», in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds.), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, Nomos, 2019, p. 128 (pp. 125-143); Gerhard Wagner, «Robot Liability», in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds.), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, Nomos, 2019, pp. 41-42 (pp. 27-62); Tiago Sérgio Cabral, «Liability and artificial intelligence in the EU: Assessing the adequacy of the current Product Liability Directive», *Maastricht Journal of European and Comparative Law*, vol. 27, issue 5, 2020, p. 619 (pp. 615-635); Jan De Bruyne, Elias Van Gool and Thomas Gils, «Chapter 14. Tort Law and Damage Caused by AI Systems», in Jan De Bruye and Cedric Vanleenhove (eds.), *Artificial Intelligence and the Law*, Cambridge, Intersentia, 2021, p. 378 (pp. 359-404). In the US, the exclusion of non-embedded software has been justified for not being tangible [*America Winter v. G.P. Putnam's Sons*, 938 F.2d 1033, 1036 (9th Cir. 1991); *Am. Online, Inc. v. St. Paul Mercury Ins.*, 207 F. Supp. 2d 459, 467 (E.D. Va. 2002) and *Torres v. City of Madera*, No. 09–16573, 2005 WL 1683736, 46-49 (E.D. Cal. 2005)]; for being equated to professional services, and therefore they are not products [Michael D. Scott, «Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?» [2008] 67(2) *Maryland Law Review* 434-436; *La Rossa v. Sci. Design Co.*, 402 F.2d 937, 942 (3d Cir. 1968); *Lemley v. J & B Tire Co.*, 426 F. Supp. 1378, 1379 (W.D. Pa. 1977) and *Snyder v. ISC Alloys,* 772 F. Supp. 244, 250 (W.D. Pa. 1991)].

intended for a medical purpose» was a medical device within the meaning of Directive 93/42,[31] the predecessor of the MDR.[32]

As a basic principle, the CJEU recalled that software can be a medical device if «it is specifically intended by the manufacturer for one or more of the medical purposes set out in the definition of a medical device», and it is not sufficient that «they are used in a medical context».[33] The issue was that the purpose of the specific programme was identified in Art. 1.2(a), third indent of Directive 93/42 but «in the expression 'investigation of a physiological process', the medical purpose does not appear». Two interpretations could be drawn from the silence of Directive 93/42:

- The first, not expressly mentioned by the CJEU, according to which the intention of the Community legislator was not to attribute medical purposes to products for research into physiological processes.

- The second, is «to consider that the silence of the EU legislature on the matter is due to the fact that the medical purpose is inherent in the products in question».[34]

The CJEU concluded that this second is corroborated by a Commission guidance document (Meddev 2.1/1), which includes a chapter, under the heading Directive 93/42, whose «Article 1(1)(b) [...] explicitly states that medical devices are intended to be used for a medical purpose».[35] It also considers that the concept of medical device covers an object designed by its manufacturer to be used on human beings for the investigation of a physiological process only if it is intended for medical purposes. It, therefore, excludes sports equipment, for instance.[36] In accordance with the latter, it is therefore concluded that a computer program intended for primary medical use in the diagnosis or treatment of the patient will be a «medical device» and, according to some authors, a «product» in the terms of the PLD, by analogy.[37] This analogical application should be made with caution. The MDR defines a medical device expressly including software, whereas the PLD keeps silent on that by referring to the nature of the product as

---

[31] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993).

[32] Case C-219/11 *Brain Products GmbH and BioSemi VOF and otros* (ECLI:EU:C:2012:742) para 11.

[33] *BioSemi* paras 16-17.

[34] *BioSemi* para 23.

[35] *BioSemi* para 24.

[36] *BioSemi* para 31.

[37] Federica Giovanella, «Can 'Things' Be Defective Products? The Applicability of the Product Liability Directive to the Internet of Things», *SSRN*, 2022, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4023266 [consult. on 8/7/2023].

a movable good. Thus, not every medical device is a product within the meaning of the PLD.

(c) Information that may turn a product into defective: the principle of inherent characteristics

This question was raised in a recent ruling of the CJEU, on 10 June 2021.[38] The Krone case concerned the liability of the publisher of a newspaper (*Kronen-Zeitung*) in which a health advice section («*Hing'schaut und g'sund g'lebt*»), written by *Kräuterpfarrer Benedikt*, a member of a religious order and expert on medicinal herbs. In the column dated 31 December 2016, people with rheumatic pain were advised, after rubbing the affected area with fatty oil or lard, to put on a layer of horseradish for two to five «hours» -when he meant «minutes»-. A woman, the plaintiff of the case, followed the advice and after three hours she had to remove the ointment due to severe pain caused by a toxic skin reaction. Both the claim and the applicant's appeal were dismissed in their entirety, and she appealed to the Austrian Supreme Court (*Oberste Gerichtshof*), which referred the matter to the CJEU for a preliminary ruling.

The starting point of the CJEU is that health advice is information and, therefore, a service excluded from the scope of the PLD. But, according to the CJEU, a defective service -the information, the inaccurate health advice- may render the product into which it is incorporated -the newspaper- defective because of its inaccuracy if it relates to one of its inherent characteristics:

«In the present case, it must be observed that the service in question, namely the provision of inaccurate advice, is unrelated to the printed newspaper, which constitutes its medium. More specifically, that service does not concern either the presentation or the use of the latter. Therefore, that service is not part of the inherent characteristics of the printed newspaper which alone permit an assessment as to whether the product is defective».[39]

According to the CJEU, the health advice in question did not concern «the presentation and use» of the newspaper which constituted its medium. Thus, as the information was not one of the «inherent characteristics» of the product, the latter could not be considered defective because of the incorrectness of the information it contained. According to the CJEU, the opposite would cause the distinction drawn by the EU legislature between goods and services would be

[38] Case C-65/20*VI v. KRONE - Verlag Gesellschaft mbH & Co KG* (ECLI:EU:C:2021:471).

[39] *Krone* para 36.

blurred. Thus, the criterion that will govern this question is that of the assessment of the essentiality of the service -of the information-.[40]

Can we use the *Krone* case reasoning for the software case? Cautiously yes, as there is one important difference between the *Krone* case and the software case. In the case of software, not all are equal. There are, as we have seen, embedded and non-embedded. The *Krone* case is more like that of non-embedded software because, in short, the latter is only computer code that is installed in a device, but whose existence does not depend on a physical or tangible mechanism of incorporation (a pen drive, a microchip, etc.).

(d) Some medical software will be a product

Who is liable, then, if the information given by the robot to the doctor ends up causing harm to the patient through a diagnostic error or an incorrect determination of the course of treatment -by exceeding the recommended dosage or by not considering, for example, the patient's allergies- or the computer programme wrongly transmits the surgeon's commands to the Da Vinci from the master console to be executed on the patient? Is the software that gave that precise piece of information referring to an inherent characteristic of the product (hardware) that constitutes its support?[41]

My position, following the reasoning of *Krone*, is to conclude that the information may render the final product that constitutes its support defective if the specific piece of information is, therefore, essential for the functionality of the product (hardware). Is easier to reach that conclusion in the case of embedded software, due to the linkage between the software and hardware (*Hardwareanknüpfung*).

(e) The Da Vinci software is a product

In conclusion and applying the reasoning above to the case of the Da Vinci surgical system, there is no doubt that the hardware, its physical and tangible components -surgeon's console, tower, and the robotic arms with their removable components- are products within the scope of PLD. However, the fundamental question, which would be particularly relevant if the manufacturer of the robot's

---

[40] Christian Twigg-Fleser, «The Tale of the Grating Horseradish. Case Note on VI v KRONE-Verlag (Case C-65/20 VI)», *Journal of European Consumer and Market Law*, issue 6, 2021, p. 265 (pp. 262-266).

[41] It is irrelevant that the recommended course of treatment or diagnosis is not implemented directly on the patient by the hardware. A similar argument is made by Christian Twigg-Flesner, «The Tale…», p. 265. Twigg-Flesner starts by drawing the difference between mere information that is found in the newspaper, but does not affect in any way its functioning, whereas some digital contents are essential for the functioning of the product in which they are integrated, Twigg-Flesner gives the example of household appliances.

software were different from the final manufacturer, is whether the damage suffered by a patient operated on with the Da Vinci, because of a defect in the software that executes the movements made by the surgeon on the console, would be compensable under product liability law. I believe it would be, for the following reasons:

- First, because the software -the code in computer language, the service- of the Da Vinci does refer to its use, unlike in *Krone*, with the defective health advice: without the software that executes on the patient the movements that the surgeon performs on the console, the Da Vinci would remain a useless piece of steel, as it is this software that makes it work.

- Secondly, in this specific case, the difficulty associated with non-embedded software is resolved by the fact that it is a computer programme that is integrated into the hardware by means of a physical device, a tangible medium: the chip. Thus, there is no doubt that in line with the leading doctrine prior to *Krone*, embedded software is, without any doubt whatsoever, a product under the definition of the TR-LGDCU and the PLD.

- Thirdly, and as mentioned above, a teleological interpretation of PLD and, in particular, of its Art. 2, should lead to the conclusion that the aim of the Union legislator was to extend the objective scope of liability for defective products to intangible products, hence its express mention of electricity and, in the TR-LGDCU, also gas.

3. When the Da Vinci software will be defective?

The common core to answer this question can be summarised with one word: hacking.

3.1. Design defect: the potential risk of hacking

A design defect exists when the origin of the damage is not in the manufacturing phase, but in a previous state, even originally, in the very conception of the product. It is not a specific product that is defective, but all of them, because the design itself is defective. Thus, the most common consequence of the detection -judicial or extra-judicial- of a design defect is its withdrawal from the market, either before or after a court ruling declaring it defective.

The Da Vinci also has a very favourable risk-benefit ratio, as it has a very low rate of adverse events -0.6%[42]-, all of them linked to residual risks arising from man-

[42] Homa Alemzadeh, Jainshankar Raman, Nancy Leveson, Zbiginiew Kalbarczyk and Ravishankar K. Iyer, «Adverse Events in Robotic Surgery: A Retrospective Study of 14 Years of FDA Data», *PLoS ONE*, vol. 11, issue 4, 2016, pp. 3-7 (pp. 1-20).

ufacturing defects, those that the manufacturer, no matter how much diligence he employs and no matter how many controls he imposes, cannot eliminate, but only reduce their frequency. However, the Da Vinci has an embedded software: the computer programme that allows the movements made by the doctor to be executed on the patient from the surgeon's console. This software, like any other computer system, is susceptible to cyber-attacks.

Informatics scholarship has, in fact, studied the phenomena of cybersecurity risks[43] in the particular field of this contribution -teleoperated surgery-, and there is sufficient evidence as to the feasibility of these systems being attacked remotely by third parties.[44] The report prepared by Bonifaci et alii detected three sources of software risk: intention manipulation, intention modification and hijacking attacks.[45] Furthermore, it also highlighted how easy it was for an unknown third party to take control of the system and alter its correct functioning during the performance of a surgical procedure.[46] Additionally, it detected that these cybersecurity risks could be avoided and prevented at a low cost.[47] It is, therefore, necessary to decide whether the weakness of the software embedded into the Da Vinci, which makes it susceptible to unlawful interference by third parties, constitutes a design defect. The answer is already anticipated to be in the affirmative.

---

[43] As a risk of any interconnected device. See National Research Council y National Academy of Engineering, *Toward a Safer and More Secure Cyberspace*, Washington, D.C., The National Academy Press, 2007, p. 41.

[44] Tamara Bonifaci, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno and Howard Jay Chizeck, «To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robotics», 2015, available at https://arxiv.org/abs/1504.04339 [consult. on 9/10/2023].

[45] *Ibid.*, p. 2.

[46] *Ibid.*: "Our results, unfortunately, show that an attacker can easily and quite efficiently disrupt a surgical procedure".

[47] *Ibid.*, p. 9: "Thus the use of encryption and authentication has low cost and high benefits to telerobotic surgery, mitigating many analyzed attacks". In fields different from teleoperated surgery, see Alan Butler, « Products Liability and the Internet of (Insecure) Things: Should Manufacturers be Liable for Damage Caused by Hacked Devices?», *University of Michigan Journal of Law Reform*, Vol. 54, no. 4, p. 926 (pp. 913-930), and Bruce Schneier, «The Internet of Things is Wildly Insecure–And Often Unpatchable», in Wired, 6.1.2014, available at https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/#:~:text=6%3A30%20AM-,The%20Internet%20of%20Things%20Is%20Wildly%20Insecure%20%E2%80%94%20And%20Often%20Unpatchable,good%20way%20to%20patch%20them [consult. on 9/10/2023].

The risk of hacking is inherent to the Internet of Things and new technologies.[48] Using this technique, and exploiting a vulnerability in the system, a third party gains access to the system and hijacks it,[49] asking for a reward to restore its functionality; or taking control, with the consequent risk to the patient's safety, physical integrity, and life.[50] Based on this premise, patients cannot demand the Da Vinci's software be infallible and not possibly be affected by unlawful interference by third parties. Therefore, a product that can be hacked is not in itself defective. But what is legitimate to expect of the Da Vinci, and of any other software product, is that, if there is a risk of being hacked, the system:

- First, it lacks well-known vulnerabilities in terms of cybersecurity that would make it susceptible to such intrusions.

- Second, it should have early detection systems to detect the intrusion. That is, the software should be equipped with the ability to detect that a third party is attempting to gain access to the operation of the system. This is not technologically impossible. Any Smart TV can detect when a device is trying to establish contact with it via Bluetooth.

- Thirdly, a blocking device in case of hacking. In other words, the system would automatically be blocked when a third party gains access and takes control. Thus, with the system locked, the surgical team would only have to switch to open or laparoscopic surgery and proceed without any complications other than those of the surgical conversion.

To this end, there is an obligation on the manufacturer to employ whatever means are necessary to protect patients from such illegitimate intrusions. We are not talking about a hacker who takes control of a particular computer and prevents the user from accessing his files because, however annoying this may be for the affected person, it does not affect life and/or physical integrity. In this contribution, we deal with cases in which a third party accesses the software of a robot and is able to alter the dosage of the medication to be administered to the patient; or provides false information about the patient's clinical history so that the patient makes an erroneous medical decision; or makes the arms of the Da

[48] Mark Geistfeld, «A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation», *California Law Review*, issue 105, 2017, p. 1660 (pp. 1611-1694).

[49] Gillian Yeomans, *Autonomous Vehicles: Handing Over Control: Opportunities and Risks for Insurance*, *Lloyd's*, 2014, available: https://assets.lloyds.com/assets/pdf-autonomous-vehicles/1/pdf-autonomous-vehicles.pdf [consult. on 10/7/2023].

[50] According to the doctrine, courts would not have difficulties in considering liable the producer in cases where a person has died or suffered from severe injuries due to a software vulnerable to cyberattacks. Michael L. Rustad and Thomas H. Koenig, «The Tort of Negligent Enablement of Cybercrime», *Berkeley Technology Law Journal*, issue 20, 2005, p. 1578 (pp. 1553-1611).

Vinci work in the opposite direction to the orders given by the surgeon from the console. These are just examples, but they all have one thing in common: that the safety expectations are particularly high, as the CJEU held in the Boston case.[51]

If the caselaw of Spanish courts and the CJEU is analysed altogether, a defect can be defined in three different ways:

- First, the defect as the materialisation of an intrinsic risk of the product. For example, in the Boston case,[52] that the automatic defibrillator, as a consequence of the defect in the magnetic switch, was blocked and did not discharge when there was an alteration in the cardiac rhythm.

- Second, the defect as a lack of verification of intrinsic risks when it is required to do so in accordance with the state of science and technology, but without the materialisation of the risk. This is the defect of the Trilucent prostheses according to the judgment of the Civil Chamber of the Spanish Supreme Court of 9 December 2010.[53]

- Third, the presumption of defect due to the product belonging to a defective series or model. This is the case of Boston, too, but regarding the pacemakers.

If the defective nature of the product is verified, a design defect could be deemed to be present in the product, since it affects the very conception of one of its components: the embedded software that makes it work, the code that converts the doctor's orders into the movement that will replicate the Da Vinci on the patient.

3.2. Defective instructions or warnings

The information defect does not affect the product itself, but the instructions and warnings that the manufacturer provides on the product. In the case of the Da Vinci, the information publicly made available by the manufacturer,[54] is sufficiently complete to cover all the risks that have been materialised during sur-

---

[51] Cases C-503/13 and C-504/13 *Boston Scientific Medizintechnik GmbH contra AOK Sachsen-Anhalt – Die Gesundheitskasse and Betriebskrankenkasse RWE* (ECLI:EU:C:2015:148).

[52] Fn 50.

[53] ECLI:ES:TS:2010:7204. For a bit more of detail about this case, see Sonia Ramos González and Marian Gili Saldaña, «Comentario de la Sentencia del Tribunal Supremo de 9 de diciembre de 2010. También es defectuoso el producto que el fabricante pone en circulación sin haber realizado las comprobaciones suficientes sobre su toxicidad, aunque no haya causado daños a la salud de los consumidores», in Mariano Yzquierdo Toslada (dir.), IV *Comentarios a las sentencias de unificación de doctrina (Civil y Mercantil)*, Madrid, Dykinson, 2010, pp. 997-999 (pp. 975-1008).

[54] https://www.intuitive.com/en-us/about-us/company/legal/safety-information.

geries performed with this system.[55] Most of this risks have nothing to do with the embedded software, but with the hardware (the instruments used). I do not mean that it is expressly stated that the program can be affected by a computer virus, or that a third party can hack into it and take control of the robot, as we understand that such a level of detail would unnecessarily frighten patients who inquire about the Da Vinci.

It cannot be denied that the existance of this risk is well-known in the field of scientific literature[56] and, therefore, there is no reason to withheld this information to patients, who need to know about this important risk when weighing whether they prefer to be operated with this surgical system, or to trust in traditional, but analogic, surgical methods. It is further argued that the inclusion of a warning[57] about the inherent risk of any technological product being subject to hacking could satisfy the legitimate expectation of security,[58] so that a consumer on whom the Da Vinci is to be used could be fully aware that, like any software-dependent computer technology, a third party can access and take control of the system. If an event occurs in which the Da Vinci is hacked and this causes harm to the patient, the authorised representative could be held liable not only for a design defect, but also for an information defect.

This idea can be strongly defended taking into account the position of Spanish courts in this kind of cases. Spain has had the case of the Agreal -a drug legally commercialised between 1983 and 2005 to treat hot flashes and other disorders suffered by pregnant women- that was recalled as it was proved that there were some important secondary effects that would have been withheld by the producer of the drug. The Spanish Supreme Court considered that withholding relevant and known secondary effects was the source of the information defect, and or-

[55] According to Alemzadeh et alii (n 41), the adverse effects registered with the MAUDE database of the FDA were the following: system errors (536, 5%), video or image problems (275, 2.6%), broken or burned pieces that fell within the patient's body (1,557, 14.7%), arcing, sparking or charring of instruments (1,111, 11.5%); unintended functioning of the surgical instruments (1,078, 10.1%) and other unidentified causes (5,092, 47.9%).

[56] See ffnn 43-46.

[57] Such a warning may potentially exclude the risk of an information defect, but not the one of manufacturing or design defect that the product may present. In this sense, and with a view in US law, see Geistfeld (n 42) 1640.

[58] In US law, Geistfeld (n 42) 1639, 1658-9 excludes that a generic warning may be sufficient to exclude liability for an information defect.

dered compensation for the victims.[59] In the case of medical devices, we find the case of the Essure -a contraceptive mechanism which was implanted in one or both fallopian tubes and triggered an inflammatory reaction that occluded them by the resulting scar tissue- whose secondary effects brought to the suspension of the authorisation of commercialisation, and ended with the decision of the producer to end its commercialisation in every country, except in the United States. In Spain, the only case that reached the Courts has been solved by a lower court, that decided that the product presented an information defect.[60]

4. Can the authorised representative waive liability under Art. 7 PLD?

After a thorough review of all the Spanish caselaw involving product liability, I have detected that all manufacturers always invoke the same two exceptions to liability: Articles 7(d) and 7(e) PLD. We will see in this section that none of both exceptions to liability can properly succeed.

4.1. The inapplicability of the exception for compliance with mandatory regulations of Art. 7(d) PLD

This first exception has been linked to the fact that, prior to commercialise the product, manufacturers obtain a positive compliance assessment by a notified body, and they consider that this is sufficient to exclude liability.[61] That exception is not applicable for two reasons:

- First, Spain and other EU Member States, unlike in the US, do not have a pre-emption exception for specific medical devices that underwent an approval process by the regulatory agencies. Additionally, medical devices are not subject

[59] Rulings of the First Chamber of the Spanish Supreme Court of 17.6.2011 (ECLI:ES:TS:2011:4005), of 2.5.2012 (ECLI:ES:TS:2012:3662), of 6.6.2012 (ECLI:ES:TS:2012:3968), of 18.6.2013 (ECLI:ES:TS:2013:3334) and of 10.7.2014 (ECLI:ES:TS:2014:3433).
10.10.2018 (16-19.430, FR:CCASS:2018:C100615); and two of 25.5.2023 (21-23.257; FR:CCASS:2023:C100302; and 22-11.541, FR:CCASS:2023:C100301). In Germany, ruling of the *Bundesgerichtshof* of 27.2.2020 (VII ZR 151/18, NJW-RR 2020, 1514).

[60] Ruling of the Court of First Instance no. 2 of Orihuela, of 1.9.2021 (ECLI:ES:JPI:2021:1598).

[61] Ruling of the First Chamber of the Spanish Supreme Court, of 1.3.2021 (ECLI:ES:TS:2021:758). The Spanish Supreme Court needed to determine the statement of the producer, which succeded in the lower courts, according to which the hip prothesis cannot be defective as the «producer did underwent an important quality control and obtained the relevant european certifications and authorisations».

to approval by regulatory agencies. Both scholarship[62] and caselaw[63] agree in that conclusion. It would paradoxical that obtaining the CE conformity marking -in the case of medical devices- and the authorisation by a regulatory agency -in the case of drugs- would render the product as non-defective as, in the majority of cases, medical devices and defective products undergo controls prior to its commercialisation.

- Second, the MDR, nor any other legal rule imposes a specific design, but just requires the product to comply with some, rather generic, requirements, common to all products.

4.2. The inapplicability of the development risk defence of Art. 7(e) PLD

The development risk defence allows the manufacturer of a defective product that has caused damage to third parties to be exempted from liability where the state of knowledge at the time it was put into circulation was such that it was not possible to know of the existence of the defect. We will see that this exception could not be possibly applied to the cybersecurity -design- defects of the Da Vinci's software.

This particular risk has been studied in-depth, both in the field of teleoperated robots and outside,[64] and has found that they are systems susceptible to attack by third parties. The 2015 study identified in fn 63 state that there are three potential sources of risk for software: intention manipulation, intention modification and hijacking attacks. It also demonstrated the ease of third parties to break into the software and alter the correct functioning of a surgical procedure, as well as the low cost of preventing such cyber risks.

Therefore, and as mentioned above, the severity of the damage is different depending on the type of hacking involved, but the risk is the same and is known. Therefore, if a surgical robot were to be affected by the unlawful interference of a third party in its operation, the courts should not consider the development risk

---

[62] Pablo Salvador Coderch and Antoni Rubí Puig, «Capítulo VIII. Causas de exoneración de la responsabilidad. Apartado IV. Elaboración del producto conforme a normas imperativas existentes», in Pablo Salvador Coderch and Fernando Gómez Pomar (eds), *Tratado de responsabilidad civil del fabricante*, Cizur Menor, Aranzadi, 2008, pp. 578 and 581 (pp. 568-585).

[63] See the Spanish Supreme Court ruling referred in fn 60.

[64] Not in the field of surgical robotics: National Research Council and National Academy of Engineering, *Toward a Safer and More Secure Cyberspace*, The National Academy Press, 2005, p. 41. And in the field of teleoperated surgery: Tamara Bonaci, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno and Howard Jay Chizeck, «To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robotics», arXiv, 2015, available at: https://arxiv.org/abs/1504.04339 [consult. on 10/7/2023].

exception, as the risk is known, which is the only relevant factor for the purposes of this ground for exoneration.

5. Conclusions

I. The Da Vinci's software, as it is embedded into the hardware, will be a product in the terms of the PLD.

II. In the case of non-embedded software, only software that is essential for the functioning of the hardware in which it is installed, will possibly turn the latter into defective for its defective nature.

III. The Da Vinci's software can suffer from a design defect linked to cybervulnerability risks, that is, hacking if the conditions that have been explained above are fulfilled.

IV. Even though the producer of the Da Vinci provides complete information about the intrinsic risks of the product, does not offer any information as to the cybersecurity risks of the product.

That means that if the risk materialises, along with a claim for a design defect, also a claim for defective instructions may be filed against it.

V. As the cybersecurity risk is very well-known by the scientific literature, and it has been analysed in the field of teleoperated surgery, the defect could not be possibly exempted under Art. 7 PLD.

VI. Nonetheless the Proposal of Directive will include software as a product for the purposes of product liability law, it should be time for the EU legislator to rethink the usefulness of keeping the traditional distinction between product and service. In modern times, keeping such closed distinctions hampers legal certainty, as products are no longer what they traditionally were. A few years ago, before the new advancement in technologies, it was quite easy to classify a product as such (a pen, a wardrobe, an old car, etc.), but nowadays products and digital elements and services are intertwined, and a good example is Directive 2019/771. A proposal for the future would be that a new legal instrument at the EU level regulating product liability abandons the concept of a product as a movable good and adds the idea of Directive 2019/771: goods with digital elements.

VII. Additionally, two more ideas of the EU legislator included within the Proposal of Directive need to be highlighted and criticised, both related to the inclusion of «software», except for free and open-source software,[65] within the definition of product. The first one, the EU has lost its chance of distinguishing

[65] Recital 13 of the Proposal of Directive.

two realities that are completely different: the embedded and the non-embedded software. And the second, the broadening of the scope of the liability to any producer of products where a defective non-embedded software (a playing app, or a bank app) can be downloaded and cause damage to the user, for instance, as a consequence of an overheating of the central processing unit of the device. Not distinguishing between essential and non-essential non-embedded software is dangerous, as it may cause assemblers (the final manufacturers of a mobile phone, for instance) to be found liable for an app that they have not designed, and that caused the mobile to overheat and damage the user, even though, the mobile phone, as such, is not defective.

TITLE
E.TEC YEARBOOK - LEGAL CHALLENGES OF TECHNOLOGY

EDITORS
Prof.ª Doutora Sónia Moreira

AUTHORS
Ana Flávia Messa | Célia Dias Pereira | Everton Luiz Zanella | Levy Emanuel Magno | Luís Manuel Pica
Mário Filipe Borralho | Mercília Pereira Gonçalves | Sofia Travassos Alcaide | Tomàs Gabriel García-Micó

DATE
December 2023

PUBLISHERS
School of Law - University of Minho (www.direito.uminho.pt)
JusGov - Research Centre for Justice and Governance (www.jusgov.uminho.pt)

University of Minho
School of Law

JusGov
RESEARCH CENTRE FOR JUSTICE AND GOVERNANCE

fct Fundação para a Ciência e a Tecnologia