UNIVERSIDADE CATÓLICA PORTUGUESA

Responsabilidade dos Programadores de Sistemas de Inteligência Artificial

Patrícia Isabel Silva Ribeiro

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2024

UNIVERSIDADE CATÓLICA PORTUGUESA

Responsabilidade dos Programadores de Sistemas de Inteligência Artificial

Patrícia Isabel Silva Ribeiro

Orientador: Professor Doutor Nuno Sousa e Silva

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2024

Resumo

Este estudo pretende investigar a responsabilidade dos programadores de sistemas de IA, uma vez que assistimos à integração da IA em diversas áreas da sociedade. Com o avanço surge questões éticas, legais e sociais relativamente ao desenvolvimento, implementação e uso desses sistemas. Assim, o objetivo é compreender os desafios legais e éticos que se enfrenta, analisando a responsabilidade que recairá sobre o programador que os incumpre. Para tal, investiga-se os meios que existem ao dispor do lesado, sejam de fonte legal ou diretrizes éticas. Destaca-se a preocupação com a transparência e explicabilidade, assim como a privacidade e segurança. Valores que o programador deve ter em conta quando concebe ou implementa um sistema IA. É importante que qualquer criador assuma as responsabilidades pelas suas criações e, para tal, urge uma colaboração entre especialistas em ética, legisladores e programadores para enfrentar os desafios emergentes e promover uma IA confiável e sustentável.

Palavras-chave: Sistema de IA; Diretrizes éticas; Programação ilícita; Responsabilidade civil contratual; Responsabilidade civil extracontratual; Responsabilidade civil do produtor.

Abstract

Given our reliance on AI in recent years, this study aims to investigate the responsibility of AI developers. With innovation comes ethics, legal and social questions regarding the development, implementation and use of these systems. Our goal is to understand the legal and ethic challenges that we face, by analysing the responsibility that will fall on the programmer who fails to comply with them. To this end, the means available to the injured party are investigated, whether from a legal source or ethical guidelines. The concern with transparency and explainability stands out, as well as privacy and security. Values that the programmer must take into account when designing or implementing an AI system. It is important that any creator takes the responsibility for their creations, to this end, collaboration between ethicists, policymakers and developers is urgently needed to address emerging challenges and promote reliable and sustainable AI.

Keywords: AI System; Ethical guidelines; Ilicit programming; Contractual civil liability; Non-contractual civil liability; Producer's civil liability.

Índice

Lista de siglas e abreviaturas

Ac. – Acórdão;

Art. – Artigo;

CC – Código Civil;

CE – Comissão Europeia;

CP – Código Penal;

CT – Código do Trabalho;

DL – Decreto-Lei;

DI – Direito Internacional;

DPD – Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à responsabilidade por produtos defeituosos (COM(2022) 495 final, 2022);

DRIA – (COM(2022) 496 final, 2022) Directive of the European Parliament and of the Council on Adapting Non-contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive);

GPAN IA – Grupo de Peritos de Alto Nível sobre a IA;

IA – Inteligência Artificial;

P. – página(s);

PE – Parlamento Europeu;

Proc. – Processo;

RCR – Proposta de Regulamento de Ciber-Resiliência (COM(2022) 454 final, 2022);

RIA – Proposta de Regulamento de Inteligência Altificial (2021/0106(COD), 2024);

SS. – Seguintes;

TJUE – Tribunal de Justiça da União Europeia;

UE – União Europeia.

Introdução

Temos assistido a uma crescente evolução tecnológica, sendo que isto se reflete no nosso dia-a-dia, com a aplicação de sistemas de inteligência em equipamentos que acabam por substituir o ser humano nas suas tarefas[1]. A IA veio para ficar e, dessa forma, desafiar os atuais quadros jurídicos que tutelam os lesados destes equipamentos tecnológicos.

O programador deve pensar em redundâncias[2], quando não o faz, quer seja por negligência consciente, quer seja por negligência inconsciente, a consequência é a produção de danos, logo, os programadores devem-se precaver desta possibilidade e adicionar redundâncias, para que não haja só uma fonte de verdade. Se ele não o fez, então coloca-se a questão de saber em que medida podemos civilmente responsabilizá-lo? Isto porque, a sua omissão ou, muitas vezes, a sua ação incompleta (com falhas) leva a danos graves para o lesado, que devem ser ressarcidos. Outras vezes, pelas caraterísticas de uma IA, esta acaba igualmente por produzir danos.

Então, é necessário entender qual o papel que o programador no sistema de IA. Ao longo da criação do sistema de IA temos vários programadores envolvidos, cada um fica responsável por uma tarefa. No fundo, uma equipa de programadores pode-se traduzir no seguinte: um *frontend*, que trata da parte visual do produto e necessita de estar a par desse mesmo produto (*qual o seu objetivo?; como pretende operar no mercado?*), mas já não tem o total conhecimento de como são executadas as tarefas de um *backend*, que está encarregue da lógica do produto, e, vice versa, porque o *backend* deve ter o conhecimento de como vai ficar a imagem do produto final, mas não sabe como foi realizado o projeto a nível estético.

Imaginemos que calha de faltar uma peça na construção do sistema e dessa forma o produto não cumpre aquilo que prometeu, causando danos, a pergunta que aqui colocamos é se temos ao nosso dispor instrumentos legais que consigam responsabilizar os programadores que, no fundo, são a mente por detrás do processo de desenvolvimento de um sistema de IA? Tendo em conta as características da IA, em que medida podem ser responsabilizados? Com as novas apostas da UE no estabelecimento de um quadro de

[1] A aplicação desta inteligência pode-se ver em sistemas de reconhecimento voz, como é caso dos assistentes pessoais (a Siri, a Alexa, o Assistente Google, entre outros), em sistemas de reconhecimento facial como forma de autenticação, e, aquele que será o maior exemplo, o ChatGPT.

[2] A redundância é manter o produto operacional mesmo que alguma coisa falhe.

harmonização de responsabilidade civil relativo à IA, será que conseguimos, numa cadeia de transmissões, chegar àqueles que efetivamente desenvolvem e criam o sistema de IA causador de danos.

No fundo, quando ocorre um facto danoso gerado por um sistema de IA, existem várias esferas a quem o podemos imputar: a montante temos o produtor, em segunda linha o utilizador e a jusante o beneficiário[3]. Neste trabalho pretendemos olhar, principalmente, para o produtor, que é onde, normalmente, se encontram os programadores, quer eles estejam incorporados numa pessoa coletiva (isto é, sejam trabalhadores de uma empresa que desenvolva sistemas IA), quer constituam uma pessoa singular[4].

Neste sentido devemos atender ao que se entende por IA e se existem princípios normativos ou éticos aplicáveis aos programadores de sistemas IA, e qual a sua vinculatividade. Em linha com esses instrumentos, analisaremos se existe programação que possa ser considerada ilícita, para depois vermos as vias de responsabilidade que existem ao nosso dispor para responsabilizá-los.

[3] (Silva N. S., 2019), p. 693.
[4] É difícil isto acontecer, porque isso exigiria muito trabalho sobre uma só pessoa

Capítulo I – Considerações Iniciais

1.1 Noção de IA

Assistimos à tendência cada vez mais crescente da incorporação da IA nas mais variadas tarefas do nosso dia e a vantagem, comparativamente ao ser humano, é que a IA não se cansa (não precisa de pausas) [5]. Neste âmbito, precisamos de compreender o que é um sistema de IA, as suas características e qual a intervenção humana.

Facilmente se qualifica a IA como a aptidão da máquina para realizar tarefas e/ou reproduzir capacidades que são habitualmente estritas do ser humano[6] (raciocínio, autoaprendizagem, capacidade de adaptação do comportamento ao ambiente envolvente, planeamento e criatividade[7]). No fundo, a IA executa tarefas que, normalmente, requerem a ativação de centros cerebrais complexos do ser humano[8] para as executar, tais como a perceção visual, reconhecimento de voz, tomada de decisões e tradução de linguagens, entre outros. A máquina pode substituir o ser humano, mas também pode ficar aquém dele ou até superá-lo. Vejamos, a IA é altamente eficiente se houver padrões definidos e respostas com um grande nível de consenso, em contrapartida, não será tão eficiente se as respostas que lhe foram requisitadas contiverem um grande nível de abstração[9].

A definição de IA é difícil de encontrar, porque estamos num mundo tecnológico em constante inovação. Uma definição mais detalhada diz que a IA é um software ou um programa de computador com capacidade de aprendizagem e utiliza-a para tomar decisões. Os programadores destes sistemas escrevem um código que os capacita para ler imagens, texto, vídeos ou áudio e aprender com isso[10]:

Ademais, o sistema pode possuir algoritmos com *artificial neural network* com capacidade de analisar dados do mesmo modo do cérebro humano. Ou, podem ser desenvolvidos algoritmos com capacidade de aprendizagem a partir de dados introduzidos (que pode ou não pode ser o programador), e assim o algoritmo aprende a fazer uma previsão com base em padrões e inferências por parte de alguém[11].

---

[5] (Rouhiainen, 2019), p. 3.
[6] (Russell & Norvig, Artificial Intelligence: A modern approach, 2010)
[7] (Parlemento Europeu, 2020), consultado a 23/01/2024.
[8] Veja-se o exemplo de (Surden, 2019), p. 1307, em que enuncia que o ser humano quando joga xadrez desbloqueia um conjunto de capacidades cognitivas superiores, assim como quando faz traduções de linguagem ou conduz.
[9] (Surden, 2019), p. 1321 a 1326.
[10] (Rouhiainen, 2019), p. 2 e 3.
[11] (WolfeWicz, 2023), E (Janiesch, Zschech, & Heinrich, 2021) e (Rouhiainen, 2019), p. 5 a 7.

Enquanto o primeiro exige por parte do programador um maior esforço *a priori*, uma vez que lhe cabe a ele criar as camadas que vão ser capazes de fazer com que o sistema funcione de acordo com aquilo que é suposto, posteriormente, na sua atuação não é necessário qualquer tipo de intervenção, pois o próprio sistema aprenderá com os seus erros. No segundo tipo de casos, não há uma programação explícita por parte do programador, mas existe uma intervenção humana para que seja tomada a decisão.

Em 2018, a CE defendeu que a IA se tratava de sistemas que apresentassem um comportamento inteligente, que, de acordo com o ambiente onde estão inseridos, tomam decisões, com um certo nível de autonomia, para atingir o objetivo proposto, sendo que poderia estar puramente confinado ao *software* ou ser integrado em dispositivos físicos (*hardware*).[12]

Assim, a par da autonomia, temos a racionalidade, que, tendo em conta o ambiente no qual está inserido, ele é capaz de recolher, interpretar e processar as informações recebidas através dos seus sensores, e, depois de devidamente racionalizado/processado, toma aquela que será a melhor decisão para atingir o objetivo[13].

Na versão original do RIA a definição limitava o sistema de IA a um *software,* desenvolvido de acordo com as técnicas listadas, que com um determinado número de *inputs* (definidos pelo ser humano), é capaz de gerar *outputs* como conteúdo, previsões, recomendações ou decisões que afetem o ambiente onde eles interajam.[14]

Esta definição é um pouco redutora, uma vez que apenas abrange o *software* e não faz menção ao *hardware*[15], por isso, talvez o uso da expressão *machine-based system* fosse uma melhor opção, uma vez que abarca ambas as realidades[16].

Tendo isto em conta, o GPAN IA entende que os sistemas de IA tanto englobam o *software* como o *hardware* concebido pelo ser humano e atuam tanto no mundo físico

[12] (COM(2018) 237 final, 2018), p. 1.

[13] (Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, 2019), p. 1.

[14] Nos EUA, e com algumas semelhanças pela primitiva definição apresentada pela CE, veja-se a secção 3, alínea b), do *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (disponível em (THE WHITE HOUSE, 2023)).

[15] Facilmente compreendemos que esta seria uma técnica que poderia ser utilizada pelos produtores de sistemas IA, isto é, criar máquinas que contenham uma IA tão básica que não se enquadraria na definição do RIA e, consequentemente, não lhe eram aplicadas as suas normas.

[16] (Floridi, 2023), p. 5.

como no digital, percecionando o ambiente através da aquisição de dados, interpretando, raciocinando, processando e decidindo para alcançar o objetivo a que se propõem[17].

Em 2023, foi aprovada pelos países membros da OCDE uma versão revista da definição de sistema de IA. Assim, um sistema de IA constitui um sistema baseado na máquina que, por objetivos explícitos ou implícitos, é capaz de gerar outputs, como decisões que influenciam o ambiente físico e virtual.[18] Esta é uma definição mais curta comparativamente àquela que foi apresentada anteriormente pela OCDE[19], mas, dessa forma, não corre o risco de ser excessiva ou conter imprecisões técnicas, visto que quanto mais longa e exaustiva for, menos capacidade terá de se adaptar ao desenvolvimento.

O RIA foi alvo de revisões e a versão final optou pela expressão *machine-based system* e *physical or virtual environments*, que acabam por serem mais amplas. Acrescenta-se, que não se faz referência a uma lista, mas antes diz-se que os sistemas são desenvolvidos para operar com uma variedade de níveis de autonomia e apresentam adaptação após a sua implementação. Com as alterações demonstra-se a aproximação à definição proposta pela OCDE. Pode trazer uma desvantagem que é a expressão *for explicit or implicit objectives*, visto que não se determina o que se entende por objetivos explícitos ou implícitos.

Após as revisões[20], esta é a definição de sistema de IA consagrada no RIA:

> *'AI system' is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*.

Em jeito de síntese, quanto mais autónomo e afastado da intervenção humana estiver, mais difícil será de se poder traçar um quadro de responsabilidade, uma vez que não necessitam de intervenção (apesar de a mesma poder ser feita) e não temos a quem possamos imputar os danos decorrentes deste sistema. Mas não será por isso que

[17] (Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, 2019), p. 6.

[18] (Russell, Perset, & Grobelnik, Updates to the OECD's definition of an AI system explained, 2023).

[19] Ainda se consegue encontrar esta definição no livro *Artificial Intelligence in Society,* disponível *online* em https://www.oecd-ilibrary.org/sites/eedfee77-en/1/1/5/index.html?itemId=/content/publication/eedfee77-en&_csp_=5c39a73676a331d76fa56f36ff0d4aca&itemIGO=oecd&itemContentType=book, consultado a 20/01/2024).

[20] Para estas e outras diferenças das versões do RIA veja-se (União Europeia, 2024).

deixaremos de tentar criar um quadro de responsabilidade direcionado a "alguém", até porque a UE opta por não atribuir personalidade jurídica à IA[21]. Como, aliás, podemos ver próprias definições vão no sentido de que ser humano tem, pelo menos, o mínimo de controlo, quando muito, foi este que desenvolveu e criou o sistema[22].

1.2 Contraponto entre *soft law* e *hard law*

No âmbito da IA, foram surgindo nos últimos tempos vários instrumentos[23] que tentam incentivar a que se cria um quadro de seguro para utilizadores e fornecedores. A este propósito, cumpre compreender se esses instrumentos que vão começando a surgir para regular a IA têm caráter vinculativo.

O art. 38.º do Estatuto do Tribunal Internacional de Justiça enuncia as fontes de DI[24]. Este elenco está longe de ser um elenco taxativo, e até nem é cabalmente defendido que essas sejam as principais fontes[25].

Uma realidade que é discutida a propósito das fontes de DI é a chamada *soft law*. Esta realidade encontra-se numa zona cinzenta, sendo que compreende os instrumentos internacionais que, não sendo por si vinculativos, acabam por conter, de forma implícita, uma objetividade que leva a que os sujeitos internacionais os cumpram. Tem grande relevo, porque incentiva a que se forme Direito, mas não tem vinculatividade e é insuscetível de resolver conflitos internacionais[26].

São exemplos de atos que dão origem a *soft law* as declarações feitas em conferências internacionais, resoluções parlamentares e declarações políticas, códigos de conduta, declarações que contêm princípios, livros brancos, diretrizes e recomendações de organizações internacionais ou comités de direitos humanos. Este tipo de instrumentos exprimem uma concordância dos intervenientes relativamente a uma certa matéria, uma

[21] Veja-se ((2020/2014(INL)), 2020). Também alguma doutrina não considera que deva ser atribuída à IA uma personalidade jurídica, ou porque não reúne as características para que se ficcione ser uma pessoa ou porque ao entender que o robot dotado de IA constituí uma pessoa em sentido jurídico, estaríamos a retirar ao ser humano a sua pessoalidade, a este propósito (Barbosa, Inteligência Artificial, E-Persons e Direito: Desafios e Perspetivas, 2020), do qual transcrevemos "(…) *por maior que seja a capacidade de raciocínio algorítmico de um robot, faltar-lhe-ão sempre as outras componentes essenciais da inteligência humana, como seja a dimensão dos sentimentos. E faltará sempre ao robot, acrescentamos nós, a dimensão espiritual e da alma* (…)", p. 66. No mesmo sentido (Matos, 2020).

[22] Ver (Floridi, 2023), p. 6 e 7 que abordam com mais detalhe o a expressão "*for a given set of human-defined objectives".*

[23] Veremos mais à frente no ponto 2.1.

[24] (Gouveia, 2017), p. 143 e ss.

[25] Veja-se (Miranda, 2016) p. 42 e ss. e (Gouveia, 2017), p. 140.

[26] (Machado, 2013), p. 139.

espécie de compromisso sem vinculação jurídica, acresce que isto é vantajoso porque regras rígidas acabam por restringir a atuação internacional[27].

No fundo, a *hard law* corresponde a um conjunto de obrigações legais vinculativas, mais concretas e exigentes em termos de interpretação e implementação. Em contrapartida, a *soft law* será mais flexível e menos vinculativa[28].

Uma vez que a h*ard law* representa a adoção de obrigações vinculativas, o seu incumprimento representa custos, seja por causa das sanções, seja por causa da reputação internacional que fica ferida, visto que esse sujeito, nas próximas relações que estabeleça, é visto como alguém de pouca confiança. Adicionalmente, tendo um instrumento que seja em certa medida rígido, torna-se difícil que ele se adapte às novas realidades que possam surgir sobre o tema[29].

Quanto à *soft law*, apesar de haver uma ideia de compromisso – quanto mais não seja um compromisso de boa-fé –, não passa de algo que pode ou não ser adotado nas jurisdições internas e, muitas vezes, não possui nos seus textos meios de resolução de litígios em caso de incumprimento[30]. Além de que, se o instrumento jurídico não for vinculativo, é mais provável os sujeitos venham-se a comprometer de forma mais profunda, com disposições mais pormenorizadas, uma vez que não precisam de se preocupar com a fiscalização das obrigações a que se vinculam[31].

A *soft law* assume grande relevo nos domínios internacionais em que seja muito difícil obter o consenso de vários Estados, uma vez que existe uma preocupação generalizada, mas não estão reunidos os requisitos para se formar consenso[32]. Devidamente compreendida trata-se de uma técnica complementar à regulação jurídica, quando seja impossível obtê-la. Ao mesmo tempo, serve de complemento, na medida em que cria o ambiente adequado para que se obtenha consenso[33].

---

[27] Sobre um maior aprofundamento sobre os custos que a *hard law* acarreta, em particular para a soberania dos Estados, ver (Abbot & Snidal, 2000).

[28] (Abbot & Snidal, 2000), p. 421 e 422.

[29] (Shaffer & Pollack, 2010), p. 719.

[30] (Boyle, 1999), p. 909.

[31] Sobre as vantagens e desvantagens de *hard law* e de *soft law* veja-se (Shaffer & Pollack, 2010), p. 717 a 721.

[32] Veja-se os exemplos de casos em que inicialmente se optou por um instrumento de *soft law* e este conduziu à conclusão de um tratado sobre a matéria, em (Boyle, 1999), p. 905 e 906.

[33] (Abbot & Snidal, 2000), p. 423.

No fundo, tal como acontece noutras matérias[34] em que existe uma falta de consenso alargada, no que toca à IA grande parte dos instrumentos avançados são em grande medida de *soft law,* visto que os diferentes Estados têm reservas quanto à sua possível regulamentação e preferem não se fechar num texto serrado.

Assim, dependendo da matéria que esteja em questão, os sujeitos internacionais podem optar[35] ou então criar instrumentos de ambas, complementando-se.

Capítulo II – Regras da Responsabilidade Civil aplicáveis aos programadores

2.1 Manual de boas práticas para programadores?

O crescente desenvolvimento da IA é acompanhado por constantes apelos à ética. Nessa medida, nos últimos anos, reúnem-se princípios e diretrizes que tentam consciencializar os programadores, preparando-os para uma possível responsabilidade

No âmbito dessas diretrizes, os aspetos da responsabilidade, da explicabilidade, da privacidade[36] e da justiça são os mais abordados. Mas também, valores como a robustez e segurança tendem a ser implementados pelos programadores.

Em 2018, vários especialistas que incorporam o *Center for AI and Digital Policy*, depois de uma grande investigação, emitiram um conjunto de diretrizes, a *Universal Guidelines for IA*[37], com doze os princípios que constituem a base para outros.

Apesar de não terem caráter vinculativo, elucidam os programadores das práticas que devem ou não ter quando estão a desenvolver um sistema de IA.

Em 2019, os países membros da OCDE assinaram pela primeira vez um conjunto de princípios relativos a uma IA inovadora e de confiança[38]. Comparativamente à anterior, esta enuncia que os sistemas de IA devem ser desenvolvidos de forma robusta, segura e protegida ao ponto de que, com a uma utilização normal, ou uma utilização previsível ou até mesmo incorreta, funcionem de modo adequado e não representem um risco de segurança excessivo. Aqueles que criam sistemas de IA devem ter uma acrescida atenção,

[34] Por exemplo, o ambiente e os direitos humanos.
[35] (Shaffer & Pollack, 2010), p. 716.
[36] Neste contexto, Google, Microsoft e Facebook lançaram o "AI Fairness 360", a "Ferramenta What-If", "Facets", "fairlern.py" e "Fairness Flow", respetivamente.
[37] (Universal Guidelines for AI, 2023)
[38] (OECD/LEGAL/0449, 2019)

pela especial perigosidade que um sistema de IA envolve, devem ter em conta todas as variantes. Apesar de ser um bom instrumento, é apenas uma recomendação, logo não é juridicamente vinculativa e os Estados que a assinam apenas se comprometem a tentar fazer aquilo que está ao seu alcance para as implementar.

Posto isto, vários Estados começaram a desenvolver as suas iniciativas para criar uma IA de confiança[39]. Na UE, o GPAN IA desenvolveu o *Guia de Orientações Éticas* para uma IA de confiança. Este defende que deve ser respeitado a autonomia humana, a prevenção de danos, a equidade e a explicabilidade. Estes são direitos fundamentais consagrados nos instrumentos legais, logo é obrigatório o seu cumprimento. Mas, este grupo desenvolveu uma análise destes princípios legais, incorporando-os numa componente ética.

Assim, assegura-se a capacidade de decisão do ser humano – que está munido de todos os conhecimentos – quando interage com um sistema de IA, sendo que este um sistema seguro, que tente não criar danos ou, pelo menos, não os agravar. [40]

Tendo como base os princípios enunciados e aproximando daquilo que foi desenvolvido pela OCDE, o GPAN IA elabora uma lista de requisitos, para que possa ser concretizada uma IA de confiança, que cumpra o propósito de estar ao serviço do ser humano[41]. Assim, ao longo de todo o ciclo de vida do sistema de IA deve ser assegurada: a ação e a supervisão humana; solidez técnica e a segurança em geral; a privacidade e governação dos dados; a transparência; a diversidade, não discriminação e equidade; bem-estar social e ambiental; e, por fim, existir a responsabilização, quer *a priori* com a avaliação dos algoritmos, dados e processos de conceção por parte de auditores internos ou externos antes de ser lançado no mercado, quer *a posteriori* com quadros de responsabilização.

Esta lista de requisitos não pretende ser algo meramente formal, e sim, colocada em prática pelos técnicos ao longo de todo o seu ciclo de vida[42].

---

[39] Veja-se nos EUA o *National Institute of Standards and Tecnology*. Também grandes empresas norte-americanas do setor, face aos entraves que se impôs no Congresso, decidiram avançar com o *Frontier Model Forum* (consulte-se: https://www.frontiermodelforum.org/updates/announcing-the-frontier-model-forum/).

[40] Os sistemas de IA devem ser concebidos para aumentar, complementar e capacitar as competências cognitivas, sociais e culturais dos seres humanos (European Commission, Directorate-General for Communications Networks, 2019), p. 15.

[41] (European Commission, Directorate-General for Communications Networks, 2019), p. 6.

[42] (European Commission, Directorate-General for Communications Networks, 2019), p. 26.

Por fim, numa vertente mais prática, cumpre ainda mencionar que se avança com a ideia da criação de indicadores de qualidade de serviço para avaliar os testes, o treino dos algoritmos, a funcionalidade, o desempenho, a usabilidade, a fiabilidade, a segurança e a manutenibilidade[43]. Uma outra boa iniciativa também foi avançada pelo IEEE *standards association*, que pretende igualmente treinar e capacitar os auditores para priorizar a ética.[44]

Apesar de existirem vários instrumentos que tentam nortear a criação e implementação de um sistema de IA, não há nada que se possa assumir como *legis artis*. No fundo, fornecem um quadro para uma utilização ética e responsável de IA, mas continua a ser uma escolha dos mesmos. Assim, podemos não ter um código deontológico, mas assistimos à criação de diretrizes baseadas na ética que deve ser adotada.

2.2 Programação ilícita vs. Programação lícita

Aquilo que o programador de IA faz é criar algoritmos avançados, para os incorporar em *softwares*. Geralmente, não se trata apenas de um único programador, mas sim uma equipa e, se estamos a falar das grandes empresas tecnológicas, são várias equipas a trabalhar no mesmo projeto (cientistas de dados, engenheiros de *softwares,* especialistas de *machine learning/deep learning*, designers do produto, designers gráficos, matemáticos ou estatísticos e especialistas dos testes e do controlo de qualidade). Assim o produto deve ser testado e avaliado, para que o sistema de IA possa ser tido como preciso e confiável. A verdade é que este *dever ser* nem sempre é algo tido em consideração, uma vez que isto implica gastos que nem todas as empresas conseguem suportar.

Muitas vezes, estando as empresas cientes que têm determinados objetivos para cumprir, podem pedir aos seus programadores para contrariem normas legais ou éticas[45]. Os programadores são levados a criar o seu código, e, por diversos motivos, como, por exemplo, o medo de perder o emprego, não questionam as intenções que estão por detrás

[43] (European Commission, Directorate-General for Communications Networks, 2019), p. 27. Depois de sujeito a *feedback*, foi produzida uma lista de avaliação final, *The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment*. Este documento está disponível em: https://op.europa.eu/en/publication-detail/-/publication/73552fcd-f7c2-11ea-991b-01aa75ed71a1.

[44] Para uma avaliação do efeito prático destas iniciativas veja-se, por exemplo, Hagendorff, T. The Ethics of AI Ethics: An Evaluation of Guidelines, *Minds & Machines*, 30 (2020), 99–120. (disponível online: https://doi.org/10.1007/s11023-020-09517-8).

[45] Veja-se o caso diretor geral da Volkswagen foi condenado a sete anos de prisão, por ter mandado criar um algoritmo que fazia com que o carro detetasse quando estava a ser testado, cumprindo as normas impostas, mas, na verdade, não as cumpria (disponível em: https://observador.pt/2017/12/16/dieselgate-poe-mais-um-na-prisao-schmidt-foi-condenado/).

do desenvolvimento desse produto[46]. No fundo, quando um programador aceita determinado projeto, deve estar ciente das responsabilidades que sobre si recaem, pois ele tem uma posição de poder em relação ao lesado, visto que será possivelmente a última linha de proteção contra práticas ilegais.

Nos termos do art. 128.º, n.º 1, alínea e), CT, o trabalhador deve cumprir as ordens e instruções do empregador, desde que não sejam contrárias aos seus direitos ou garantias. No entanto, é considerada uma desobediência legítima se estiver em causa a prática de um crime, isto é, constitui causa de exclusão de ilicitude, nos termos do art. 31.º, n.º 2, alínea c) do CP conjugado com o art. 36.º, n.º 2 do CP. Assim, tudo aquilo que lhe seja pedido que leva à prática de um crime, o programador tem o direito a recusar, uma vez que o dever de obediência hierárquica cessa.

As dúvidas surgem quando à partida não lhe foi pedido para desenvolver um sistema ilegal, mas o intuito final era que esse sistema levasse à prática de um crime ou a produção de danos.

Há algumas jurisdições que avançam que é ilegal a criação de *software* destinado a cometer crimes, por exemplo, a lei penal alemã no art. 202c do StGB[47]. Posteriormente, o tribunal constitucional alemão[48] esclareceu que esta lei só deve ser utilizada contra programas que apenas têm como propósito a prática de um ato criminoso, deixando de fora todos os outros programas que, para além de poderem ser usados de forma ilegal, também podem ser usados para fins legítimos. Portanto, quando estamos perante um *malware,* que constituem as situações em que o objetivo do programa são fins maliciosos[49], então pode o programador ser punido[50].

[46] Por exemplo, o testemunho de Bill Sourour que se arrependeu de ter criado este *website*, porque escreveu o código sem pensar nas consequências do mesmo, acabando por levar à morte de uma pessoa (disponível em: https://www.freecodecamp.org/news/the-code-im-still-ashamed-of-e4c021dff55e).

[47] https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1962

[48] https://www.bundesverfassungsgericht.de/entscheidungen/rk20090518_2bvr223307.html

[49] Um *malware* consiste num *software* desenvolvido especificamente para perturbar, danificar e conquistar o acesso ao computador sem ter autorização para tal.

[50] Por exemplo, nos EUA, um programador de um *malware* foi punido com pena de prisão por ter contribuído e incentivado ao *hacking*, veja-se: FBI. (05 de jul. de 2018). *Prolific Malware Developer Responsible for Countless Computer Intrusions*. Consultado a 05 de jan. de 2024. Disponível em: https://www.fbi.gov/news/stories/malware-creator-sentenced-070518.

Curiosa é também a legislação espanhola neste tema, uma vez que os criadores de *malware* não estão abrangidos pela proteção conferida pela *Ley de Propiedad Intelectual*, veja-se o seu art. 96.º, n.º 3[51].

Para além de normas legais que devem ser respeitadas, o programador tem de ter em consideração possível ética exigida. Com esta nova realidade, apesar de começar a tentar criar regulamentação, as considerações éticas avançadas no ponto anterior ficam-se pela *soft law,* o que faz com que não sejam vinculativas, podendo os programadores ter liberdade para desenvolver.

Por outro lado, é habitual que as grandes empresas criem códigos de conduta, para que se compreenda as práticas que são ou não são admitidas na empresa e, principalmente, prevenir qualquer tipo de discriminação[52]. Apesar de também não ter valor vinculativo, é bastante útil para perceber quais os valores que determinada empresa valoriza.

Isto posto, podemos concluir que constituirá programação ilícita tudo aquilo que é criado com o objetivo de praticar algum ilícito, provenha ele da base legal ou da base ética. Isto não é "preto no branco", há uma grande mancha cinzenta que será difícil de podermos considerar que constitui programação ilícita. Aqueles casos em que questionamos se, apesar do programador ter criado o sistema com ambas as vertentes, o facto de o utilizador ter usado o programa para fins ilegais, poderá ser considerado programação ilícita.

2.3 Delimitação do quadro da responsabilidade civil contratual, do delitual e da responsabilidade laboral

2.3.1 Responsabilidade laboral vs. Responsabilidade Civil

Se foi o concreto programador a produzir o dano e este está incorporado numa empresa, então recairá sobre uma responsabilidade laboral ou civil?

A responsabilidade laboral está ligada ao vínculo existente entre empregador e trabalhador, enquanto a responsabilidade civil está ligada à obrigação de reparar danos de

[51] https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930#a96 , "Artículo 96. Objeto de la protección. 1. (…) 3. La protección prevista en la presente Ley se aplicará a cualquier forma de expresión de un programa de ordenador. Asimismo, esta protección se extiende a cualesquiera versiones sucesivas del programa así como a los programas derivados, salvo aquellas creadas con el fin de ocasionar efectos nocivos a un sistema informático.

Cuando los programas de ordenador formen parte de una patente o un modelo de utilidad gozarán, sin perjuicio de lo dispuesto en la presente Ley, de la protección que pudiera corresponderles por aplicación del régimen jurídico de la propiedad industrial."

[52] (Kerkhove, 2019)

terceiros. Assim sendo, a responsabilidade civil é mais lata que a responsabilidade laboral, porque se aplica em diversos contextos da vida em sociedade.

A relação laboral é complexa e, nessa medida, questões ligadas aos acidentes de trabalho, às doenças profissionais e ao assédio, como causam vicissitudes no vínculo laboral, merecem um tratamento separado da responsabilidade civil dita geral. Há uma preocupação do legislador[53] em criar um ambiente laboral saudável e seguro. Aliás, foi o Direito do Trabalho que impulsionou à evolução do instituto geral da responsabilidade civil, para que, posteriormente, surgisse responsabilidade independente de culpa[54]. Aqui o risco são os perigos inerentes à atividade profissional, assim como o risco de ter trabalhadores a seu cargo.

Para além desta responsabilidade laboral pelo risco que recai sobre o empregador, cumpre deixar nota da natureza das sanções disciplinares, que, apesar do desentendimento quando à sua substância[55], são uma forma de reação do credor (empregador) ao incumprimento por parte do devedor (trabalhador).

Todos os danos que não caibam dentro do âmbito desta responsabilidade laboral, devem ser ressarcidos com recurso aos mecanismos gerais da responsabilidade civil e, no fundo, em resposta à pergunta de que responsabilidade se deve convocar, tudo depende do impulsionador, se o lesado for um terceiro será a responsabilidade civil, se for o próprio empregador então poder-se-á traçar o caminho na responsabilidade laboral.

2.3.2 Responsabilidade civil delitual vs. Responsabilidade civil contratual

A responsabilidade civil pode assumir duas modalidades, uma é a responsabilidade contratual ou obrigacional e a responsabilidade extracontratual ou delitual.

[53] A nível internacional podemos apontar como exemplo: Convenção n.º 17 de 1925, da Organização Internacional do Trabalho, sobre a reparação dos desastres no trabalho, ratificada para a nossa ordem jurídica através do DL n.º 16/586, de 09/03/1929; Convenção n.º 18 de 1925, da Organização Internacional do Trabalho, sobre a reparação dos desastres no trabalho, ratificada para a nossa ordem jurídica através do DL n.º 16/586, de 09/03/1929. Entretanto, com a UE, surgiram muitos mais instrumentos de proteção do trabalhador. A nível nacional a proteção conferida em matéria de acidentes de trabalho surgiu com a Lei n.º 83, de 24/07/1913, que estabelece o direito à assistência clínica, medicamentos e indemnização para os operários e empregados vítimas de acidente de trabalho. Posteriormente, após uma grande evolução legislativa, temos a Lei n. ° 100/97, de 13 de setembro, regulamentada pelo DL n. ° 143/99, de 30 de abril e pelo DL n. ° 248/99, de 2 de julho.

[54] (Ramalho, 2023), p. 796 e 797,

[55] (Martinez, 1999), p. 657, entende que se trata de um remédio civil. Já (Ramalho, 2023), p. 673 e (Cordeiro, Manual de Direito do Trabalho, 1991), p. 749, entende que como têm um caráter conservatório ou extintivo do vínculo laboral, devem ser qualificadas de tipo punitivo e não ressarcitório.

Apesar de no plano teórico parecer simples a sua distinção, na prática, torna-se difícil, pois o mesmo facto lesivo pode desencadear ambas as responsabilidades. O regime que o legislador consagrou diverge, aliás veja-se pela própria sistematização do nosso CC, os arts. 483.º e ss. tratam da responsabilidade extracontratual, enquanto a responsabilidade contratual é tratada pelos arts. 798.º e ss. relativos ao não cumprimento das obrigações.

A responsabilidade contratual resulta da violação de um direito de crédito ou obrigação em sentido técnico[56], pressupõe à partida uma relação entre o lesado e o lesante e a obrigação de indemnizar surge por incumprimento do dever de prestar. Em contrapartida, a responsabilidade extracontratual abrange os restantes casos, ou seja, quando está em causa a violação de deveres ou vínculos jurídicos de caráter geral[57], mas, entre lesado e lesante, não existia uma relação intersubjetiva. Assim, a responsabilidade extracontratual pressupõe a violação de direitos absolutos ou de interesses protegidos pela lei através de normas de proteção, ainda que sejam objeto de tutela através do reconhecimento de um direito subjetivo[58].

Apesar do legislador tentar estabelecer alguma coincidência, há diferenças importantes entre as duas[59]. Nomeadamente, o regime da responsabilidade contratual mostra-se mais favorável ao lesado, visto que está consagrada uma presunção de culpa no art. 799.º, n.º 1 do CC. Por seu turno, na responsabilidade extracontratual cabe ao lesado provar a culpa[60] nos termos gerais (art. 487.º, n.º 1 e art. 342.º, n.º 1 do CC).[61]

É consensual o entendimento que a tutela contratual é aquela que, em regra, favorece mais o lesado na sua pretensão indemnizatória, uma vez que a indemnização é pelo "interesse positivo". Compreende-se que exista uma proteção acrescida do lesado no âmbito da responsabilidade contratual, pois, aquilo que se aspira é a recuperação financeira do lesado pela lesão patrimonial que sofreu em virtude da violação contratual[62].

---

[56] (Costa, Direito das Obrigações, 2009), p. 539

[57] (Costa, Direito das Obrigações, 2009), p. 540

[58] Ac. do Tribunal da Relação do Porto, de 08/02/2021 (relator: Eugénia Cunha), proc. n.º 274/17.8T8AVR.P1, *in* www.dgsi.pt.

[59] Para uma parte da doutrina estão em causa diferenças da própria natureza (Moreira, 1925), p. 117 e ss, (Andrade, 1992), p. 21, (Telles, 1989), p. 58 e 211 e ss., (Varela, 2000), p. 518 ss. 520, nota (1)), (Pinto C. A., 1982), p. 426 e ss., (Monteiro, 1983), p. 8-9 e João Calvão Da Silva, Cumprimento, p. 146 e ss. Para outra parte, apenas a responsabilidade extracontratual é fonte de obrigações ((Leitão, 2016), p. 281 e 282).

[60] Salvo as exceções previstas nos arts. 491.º, 492.º, n.º 2 e 493.º do CC.

[61] Além desta, existem diferenças relativamente aos prazos de prescrição e os pressupostos exigidos para a responsabilização por atos de terceiros. Veja-se (Costa, Direito das Obrigações, 2009), p. 545.

[62] (Costa, O concurso da responsabilidade civil contratual e da extracontratual, 1998), p. 555-565.

2.4 Possíveis caminhos de responsabilidade

2.4.1 Via contratual[63]

No âmbito da responsabilidade aplicada à IA, os contratos podem desempenhar um papel muito importante, na medida em que ajudam a definir obrigações que ambas as partes se comprometem, assim, a sua responsabilidade pode-se ver delimitada. Aquele que vende um determinado produto, vincula-se, que ele possuía determinadas características e qualidades que previamente garantiu[64].

A vantagem da responsabilidade contratual é a possibilidade que atribuí às partes de, mediante as obrigações contratualizadas, ser-lhe imputada a devida responsabilidade em caso de violação[65]. Assim, a falta de cumprimento das obrigações contratuais leva a responsabilização pelo prejuízo causado ao credor[66].

Ora, se cabe ao devedor executar a prestação, então, quando não cumpre, está a frustrar não só o credor, mas também o ordenamento jurídico que atribuiu legitimidade àquele dever[67]. Desta forma, surge uma nova obrigação, a obrigação de indemnizar. Neste sentido, a indemnização compreende a diferença entre a situação patrimonial do lesado e a que ele teria se não tivessem existido danos[68], logo abrange danos emergentes e lucros cessantes.

Estando em causa um contrato de compra e venda e a coisa seja vendida com vícios, poder-se-á equacionar o regime da compra e venda de coisas defeituosas[69].

Por último, a responsabilidade contratual deixa de fora as situações em que os danos sejam causados a terceiros e não exista culpa na conceção ou desenvolvimento do sistema de IA. E, no âmbito dos sistemas de IA, muitas vezes, não está em causa uma falta ou um

---

[63] (Correia, 2019).

[64] A título de exemplo veja-se o caso da Volvo, onde informou que (apesar de não esclarecer os contornos) assumiria a responsabilidade proveniente de um acidente causado pelo seu modo autónomo (veja-se Noticias ao Minuto (07 de out. de 2015). "*Volvo assume a responsabilidade se um dos seus carros autónomos bater"*. Consultado a 13 de fev. de 2024, de Tech ao Minuto: https://www.noticiasaominuto.com/tech/464625/volvo-assume-a-responsabilidade-se-um-dos-seus-carros-autonomos-bater).

[65] Ac. do Tribunal da Relação de Lisboa, de 16/06/2011, proc. n.º 1429/06.6TBALQ.L1-8, *in* www.dgsi.pt.

[66] Cfr. art. 798.º do CC.

[67] (Cordeiro, Tratado de Direito Civil II, Direito das Obrigações, Tomo III, 2010), p. 391.

[68] (Faria J. R., 2023), p. 336.

[69] Para explicações sobre o seu regime veja-se (Silva J. C., Compra e Venda de Coisas Defeituosas, (Conformidade e Segurança), 2008).

atraso de cumprimento, mas antes uma prestação realizada com vícios, defeitos ou irregularidades, não existindo uma relação contratual.

2.4.2 Via delitual

Responsabilidade civil do produtor

Com a grande facilidade de acesso a bens de consumo, o consumidor torna-se um alvo fácil. Assim, um outro caminho é a via da responsabilidade civil do produtor que tem como objetivo proteger o consumidor em caso de os produtos serem defeituosos.

No âmbito desta via, iremos tratar da responsabilidade civil do produtor, que é regulada a nível da UE pela Diretiva do Conselho 85/374/CEE, de 25 de julho de 1985, trasposta para o nosso ordenamento jurídico pelo DL n.º 383/89, de 6 de novembro.

Do art. 1.º da DPD não se consegue entender se o objetivo é que a responsabilidade continue no campo do risco, mas, se olharmos para o art. 9.º, n.º 1 e o art. 10.º, n.º 1, é possível extrair o princípio da responsabilidade objetiva dos operadores económicos, uma vez que o demandante não necessita de provar a culpa, apenas lhe cabe a prova do defeito do produto, do dano sofrido e do nexo causalidade, assim, a responsabilidade não depende de culpa. Além disso, quando se elenca as causas de isenção ou de exclusão da responsabilidade, conclui-se que nesse elenco a possibilidade de isenção se não existir culpa, logo a culpa não constitui pressuposto para a aplicação deste regime.

Isto posto, trataremos a responsabilidade civil do produtor, com especial ênfase na DPD, uma vez que esta vem trazer importantes alterações à Diretiva 85/374/CEE, com o objetivo de incorporar os desafios que são colocados pela IA.

A UE estabeleceu regras comuns em matéria de responsabilidade decorrente dos produtos defeituosos, com o objetivo de eliminar as divergências entre os Estados-Membros, conferindo uma proteção harmonizada aos consumidores[70].

Assim, não vai importar se o produtor adotou as medidas adequadas e necessárias, se respeitou as regras de segurança ou se atuou com dolo ou negligência[71], pois será responsabilizado independentemente de culpa.

[70] (Parlamento Europeu, 2020)
[71] (Pereira, 2023), p. 221.

Esta proteção iniciou-se com a Diretiva da Responsabilidade dos Produtos[72], mas, depois de ter sido alvo de uma análise profunda[73], entendendo-se que havia lacunas no domínio das tecnologias digitais emergentes, porque os conceitos da primitiva Diretiva não eram claros diante de determinados desafios que a economia digital moderna coloca.

Neste seguimento surge a DPD, que procura assegurar que este novo quadro reflita a natureza e os riscos dos produtos digitais, imputando responsabilidade a quem a tem[74].

Deste modo, surgem grandes inovações, mas destaquemos as que poderão ter mais impacto para a vida dos lesados, nomeadamente o tipo de danos que abrangidos[75], que na DPD[76] podem ser os danos resultantes de morte ou lesão corporais (incluindo danos à saúde psicológica clinicamente reconhecidos), estragos a quaisquer bens da sua redistribuição (exceto o próprio produto defeituoso), um produto danificado por um componente defeituoso desse produto e os bens utilizados exclusivamente para fins profissionais. Também se considera como danos a perda ou a corrupção de dados que não sejam utilizados exclusivamente para fins profissionais, uma vez que se reconhece cada vez mais importância ao valor dos ativos intangíveis[77]. Relativamente aos danos não patrimoniais remete-se para os diversos Estados-Membros a sua compensação.

No fundo, pretende estabelecer um nível máximo de harmonização[78], consagrando meios de responsabilidade dos operadores económicos por danos sofridos por pessoas singulares por produtos defeituosos[79].

Para que o lesado possa socorrer da sua proteção é necessário que preencha o conceito de produto e de operador económico.

---

[72] Diretiva 85/374/CEE do Conselho, de 25 de julho de 1985, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros em matéria de responsabilidade decorrente dos produtos defeituosos, que é transposta para ordem jurídica portuguesa pelo DL n.º 383/89, de 6 de novembro.

[73] (COM(2020) 65 final, 2020) e (European Commission, Directorate-General for Justice and Consumers, 2019)

[74] (SWD(2022) 317 final, 2022)

[75] Ver art. 4.º (6) da DPD.

[76] Anteriormente, no art. 8.º do DL n.º 383/89 não se abrangia os danos puramente patrimoniais. Para mais desenvolvimentos sobre o facto de não se contemplar os danos económicos puros, veja-se (Silva J. C., Compra e Venda de Coisas Defeituosas, (Conformidade e Segurança), 2008), p. 215 e ss. Além disso, os danos patrimoniais inferiores a 500€ não eram passíveis de indemnização na Diretiva anterior e agora suprime-se esta regra e prolonga-se o período durante o qual os fabricantes são responsáveis por um produto defeituoso, depois de o colocarem no mercado (Considerando (43) DPD).

[77] Cfr. Considerando (16) DPD.

[78] Cfr. art. 3.º da DPD.

[79] Cfr. art. 1.º da DPD.

Relativamente ao conceito de produto, a DPD enuncia no art. 4.º (1), que constituiu produto os bens móveis, mesmo que integrados noutro bem móvel ou num bem imóvel, incluindo o software. No art. 3.º, n.º 1 do DL n.º 383/89, entende-se por produto "qualquer coisa móvel, ainda que incorporada noutra coisa móvel ou imóvel". Havia quem entendesse que na definição de produto se compreendia este tipo de produtos digitais[80].

Encontramos a definição de coisa no art. 202.º do CC, mas não é uma definição rigorosa[81] e conta com algumas críticas[82]. Pelo que, podemos definir as coisas em sentido jurídico como aquilo que tenha utilidade, individualidade e seja suscetível de apropriação[83]. Neste sentido, o *software* deve ser considerado uma coisa, uma vez que tem autonomia, pois é apto a realizar o fim a que se destina. A acrescer, possibilita a apropriação exclusiva por uma pessoa em concreto e tem a aptidão para satisfazer necessidades ou interesses humanos[84]. Deste modo, já devia ser considerado produto.

Para não haver dúvidas, vem-se expressamente consagrar que o *software* é um produto quer seja colocado no mercado como um produto autónomo, quer esteja incorporado noutros produtos[85]. Além disso, os operadores económicos podem ainda ser responsabilizados pelos componentes defeituosos[86].

---

[80] (Silva J. C., Responsabilidade Civil do Produtor, 1990), p. 613. Também em (Silva J. C., Compra e Venda de Coisas Defeituosas, (Conformidade e Segurança), 2008), p. 185, o mesmo autor justifica que o *software* aterial e incorpórea). No mesmo entender Henrique Sousa Antunes em (Antunes, 2019), p. 1478, afirma que tendo em conta era digital atual é necessário rever o conceito de coisa para a disciplina da responsabilidade civil do produtor e os conteúdos digitais partilham com as coisas corpóreas uma existência sensorial.

[81] Há bens que são suscetíveis de serem objeto de relações jurídicas, mas não são coisas em sentido jurídico, como é o caso das pessoas, das prestações, dos modos de ser ou bens da própria personalidade. (Pinto C. A., 1999), p. 339.

[82] Sobre o tema veja-se (Mendes, 1979), p. 165 e ss.

[83] (Ascensão, 2000), p. 344.

[84] (Vasconcelos, 2015), p. 200.

[85] Considerando (12) DPD. A CE deixa claro que a IA é um produto para efeitos da DPD, veja-se a questão n.º 8 do site da Comissão Europeia, intitulado de "Questions and answers on the revision of the Product Liability Directive" (https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5791). Por outro lado, o DPD exclui do seu âmbito de aplicação o chamado *open source* ou *software* livre (considerando (13) DPD), o faz algum sentido, uma vez que para que haja desenvolvimento da área é, muitas vezes, com este tipo de códigos de acesso livre que os programadores aprendem, logo se este estivesse sujeito a responsabilização, poderia constituir um fator desencorajador. No entanto, duvida-se se esta questão não deveria estar incluída no corpo normativo e não apenas no considerando, de modo que ganhar vinculatividade ((Wagner, 2023) p. 14 e 15). Cabe àqueles que o utilizam verificar a existência de *bugs* ou deficiências de segurança, para que não recaia sobre si a respetiva responsabilidade ((Hacker, 2023), p. 11).

[86] Definição de componente consta do art. 4.º (3) DPD. Sobre as questões que se colocavam em relação à qualificação jurídica de produtos ou serviços de *software* tangíveis veja-se, por exemplo, (Bertolini, 2020), p. 57. e (Bruyne, Gool, & Gils, 2022).

Antes falava-se em "produtor", que corresponderia não só ao fabricante do produto, da parte componente ou de matéria-prima, mas também a quem se apresentava como tal pela aposição no produto do seu nome, marca ou outro sinal distintivo[87]. Estavam aqui abrangidos o produtor real[88], o produtor aparente[89] e o produtor presumido[90].

Em contrapartida, o regime da DPD segue o conceito de operador económico, de modo a haver harmonia entre os diplomas relativos à responsabilidade e o diploma em matéria de segurança dos produtos e da fiscalização do mercado da UE.

Assim, referimo-nos ao fabricante de um produto ou componente, o prestador de um serviço conexo, o mandatário, o importador, o prestador de serviços de execução ou o distribuidor[91]. Assiste-se a uma ampliação dos sujeitos, de modo a assegurar que existe sempre um operador económico, contra o qual possa ser intentada uma ação de indemnização.

Para perceber em que medida são responsáveis é necessário atender ao art. 7.º da DPD. Em primeira linha, cabe a responsabilidade ao fabricante ou ao fabricante de componente defeituoso, que são àqueles que desenvolve, fabrica ou produz ou manda projetar ou fabricar um produto, ou, ainda modificam um produto que já tenha sido colocado no mercado ou em serviço[92]. Para que estes sejam responsabilizados é necessário que a modificação *seja considerada substancial* e *caso seja efetuada em circunstâncias que escapam ao controlo do fabricante inicial*. No fundo, constituem situações de controlo os casos em que o fabricante (i) autoriza a integração, a interligação ou o fornecimento a terceiros de um componente, incluindo atualizações ou evoluções de *software* ou (ii) autoriza a modificação de um produto[93].

---

[87] Cfr. art. 2.º, n.º 1, DL n.º 383/89.

[88] Entenda-se como produtor real como aquele que participa na criação do produto, seja o fabricante do produto acabado, de uma parte componente ou de matéria-prima (Silva J. C., Responsabilidade Civil do Produtor, 1990), p. 546.

[89] Entenda-se por produtor aparente os distribuidores, as cadeias comerciais, os grossistas que aplicam nos produtos ou embalagem a sua marca, o nome, ou o símbolo distintivo da marca, apresentando o produto final ao consumidor, como próprio, quando na realidade é apenas um distribuidor (Pereira, 2023), p. 216.

[90] Sobre o produtor presumido, destaca-se o ponto 32 e 34 da decisão proferida pelo TJUE, de 7 de julho de 2022, no proc. C-264/21, onde claramente se enuncia que colocar no produto o nome, a marca ou outro sinal distintivo, aquele que se apresenta como produtor "dá a impressão de estar implicada no processo de produção ou de assumir a responsabilidade por essa produção", uma vez que torna o produto mais atrativo para o público, logo pode-se desencadear a sua responsabilidade.

[91] Cfr. art. 4.º (16) da DPD.

[92] Também o programador ou o produtor de *software*, incluindo os fornecedores de sistemas de IA são considerados fabricantes (Considerando (12) DPD).

[93] Cfr. art. 4.º (5) DPD.

Desta forma, se estiver em causa atualizações regulares realizadas depois do produto ser colocado em circulação, a solução deve ser a mesma. Só será doutra forma, se o conteúdo digital for fornecido por uma pessoa diferente do produtor, devendo, contudo, afirmar-se a responsabilidade do produtor se esta atualização do *software* for essencial para o seu funcionamento.

Porém, parece que se impõe que haja um efetivo consentimento da incorporação, não se basta com uma possibilidade técnica de integrar ou interligar, ou uma mera recomendação da utilidade para a marca ou ainda com a não proibição de certos serviços ou componentes conexos.

Portanto, quando um produto é substancialmente modificado e escapa ao controlo do fabricante inicial deve-se considerar que se trata de um produto novo, e, consequentemente, deverá ser responsável a pessoa que procedeu à modificação substancial enquanto fabricante de um produto modificado[94]. No entanto, podemos ter uma zona cinzenta quando estamos perante situações em que no processo de aprendizagem se realiza configurações personalizadas e estes tipos de modificações não se qualificam como modificações substanciais. A norma não esclarece se a autoaprendizagem pode ser qualificada como uma modificação substancial[95].

Em segunda linha, podem também ser responsáveis os fabricantes dos componentes[96] defeituosos que tenham determinado o defeito do produto final[97]. De facto, tendo em conta que, muitas vezes, o sistema tem um *software* integrado ou interligado a si, onde a sua ausência impede que o produto desempenhe alguma(s) das suas funções ou não cumpra o objetivo para qual foi desenvolvido, então, procurou-se responsabilizá-los nesta medida.

Em terceira linha, podem ser responsabilizados tanto o importador[98] como o mandatário[99] do fabricante, sempre que o fabricante esteja estabelecido fora da UE. Em quarta linha, também o prestador de serviços de execução[100] pode ser responsabilizado, cumpridos estejam os pressupostos. Em penúltima linha, o distribuidor[101], sempre que

[94] Considerando (29) DPD.
[95] (Dheu, De Bruyne, & Ducuing, 2022), p. 35 e 36.
[96] Veja-se o art. 4.º (3) DPD para compreender o que se entende por componente.
[97] Considerando (26) DPD.
[98] Definição de importador consta do art. 4.º (13) da DPD.
[99] Definição de mandatário consta do art. 4.º (12) da DPD.
[100] Definição de prestador de serviços em execução consta do art. 4.º (14) da DRIA.
[101] Cfr. art. 4.º (15) da DPD.

não seja possível identificar o fabricante, o importador, o mandatário ou o prestador de serviços de execução, desde que o lesado solicite a identificação. Por fim, pode também ser responsável qualquer prestador de encargos, sendo que é responsável pelos mesmos termos que o distribuidor do produto.

Compreendendo que o sistema de IA é considerado produto e o programador é considerado fabricante para efeitos desta DPD, cabe então atender àquilo que será considerado defeito para que possa ser aplicada.

A noção de defeito consta do art. 6.º da DPD, sendo que será defeituoso porque não oferece a segurança que o público em geral pode legitimamente esperar, tendo em conta todas as circunstâncias elencadas no n.º 1. Portanto, a qualidade defeituosa do produto está associada a uma ideia de segurança do produto[102] e não à aptidão ou idoneidade deste para cumprir o fim a que é destinado. Não se exige que o produto ofereça uma segurança absoluta, mas apenas a segurança que legitimamente se possa contar e não de acordo com as expectativas subjetivas do lesado, mas antes de acordo com a expectativa objetiva do público em geral.

Neste ponto, comparativamente ao quadro vigente, verifica-se apenas uma extensão da diretriz modificativa das circunstâncias, de modo a refletir a natureza dos produtos da era digital e a ideia de que o *software* ou os algoritmos subjacentes são concebidos por forma a evitar riscos. Importante destacar, *o efeito no produto de qualquer capacidade de continuar a aprender depois de ser posto em funcionamento*, o *efeito no produto de outros produtos que se possa razoavelmente esperar que sejam utilizados em conjunto com o produto* e os *requisitos de segurança dos produtos*[103] ou as *expectativas específicas dos utilizadores finais*.

No DL n.º 383/89, o produtor não seria responsabilizado se provasse que, tendo em conta os seus conhecimentos técnicos e científicos, *se pode razoavelmente admitir a inexistência do defeito no momento da entrada do produto em circulação*[104], ou seja, se

[102] Este teste de segurança pode ser desafiador, já anteriores pesquisas o mostraram, veja-se, por exemplo, C. Wendehorst, (2020) *Safety and Liability Related Aspects of Software*, Wendehorst/Duller, Safety and Liability Related Aspects of Software: Study commissioned by the European Commission (2020), p. 67-69.

[103] Deve-se fazer a ponte entre o DPD e normas contidas no art. 32.º do Regulamento Geral da Proteção de Dados, o art. 15.º do RIA e no RCR, que consagram normas de cibersegurança relevantes neste âmbito.

[104] Cfr. alínea b) do art. 5.º do DL n.º 383/89.

quando colocou o produto em circulação no mercado nada permitia detetar o defeito, tratando-se de um risco do próprio desenvolvimento.

Apesar de, muitas vezes, os danos provocados pela IA estarem ligados às suas características e não por um concreto defeito[105], esta afirmação, por si só, não pode constituir uma causa de exclusão da responsabilidade, uma vez que por detrás de toda a criação está o seu criador[106].

Concordamos que, todos os que integram a cadeia de produção e distribuição, devem ser responsabilizados pelos danos causados pelos produtos defeituosos que colocam no mercado, assim como devem continuar a ser responsabilizados se a qualidade defeituosa se ficar a dever a atualizações ou evoluções ou ainda se conter algoritmos de aprendizagem automática[107]. Somos da mesma opinião de Calvão Silva, pois cabe ao produtor a obrigação de vigiar e acompanhar aquele que é o desenvolvimento dos produtos que coloca no mercado[108].

A própria DPD vem consagrar que não deve ser excluída a responsabilidade no caso de risco de desenvolvimento, uma vez que para além de ser determinante o momento de colocação do produto no mercado, é também relevante se o fabricante mantém controlo sob o produto depois da sua colocação no mercado[109]. Não é o facto de a lesão ter resultado da instalação de uma atualização de segurança ou do autodesenvolvimento do *software* que irá impedir a qualificação do produto como defeituoso. Pelo contrário, a capacidade de continuar a aprender depois de ser posto em funcionamento e o momento em que o produto deixou de estar sob o controlo do fabricante, são agora momentos de ponderação muito relevantes.

Como seria de esperar, cabe ao lesado fazer a prova da qualidade defeituosa do produto, do dano sofrido e do nexo de causalidade entre qualidade defeituosa do produto

[105] (Barbosa, O futuro da responsabilidade civil desafiada pela inteligência artificial: as dificuldades dos modelos tradicionais e caminhos de solução, 2020), p. 288.

[106] Foi neste sentido, que o PE em (2020/2014(INL)), entendeu no ponto 7 que a opacidade, a conectividade e a autonomia podem dificultar a identificação de determinados resultados terem origem numa intervenção humana específica ou em decisões de conceção, mas, apesar disto, pode-se contornar isto atribuindo responsabilidade àqueles que criam, realizam a manutenção ou controlam os riscos associados.

[107] Considerando (37) DPD. E veja-se ainda o ponto [13] e [14] no relatório do (European Commission, Directorate-General for Justice and Consumers, 2019).

[108] Acrescenta ainda que se não o fizer, incorre em responsabilidade subjetiva por culpa provada (art. 483.º do CC) ou presumida do produtor médio (art. 493.º, n.º 2, CC) ou ainda, tendo em conta o produtor ideal, com base no risco. Veja-se (Silva J. C., Compra e Venda de Coisas Defeituosas, (Conformidade e Segurança), 2008)*)*, p. 210-211.

[109] Veja-se o art. 10.º, n.º 2, alínea e), DPD.

e dano[110]. Todavia, tendo em conta que o lesado se encontra, muitas vezes, numa situação de desvantagem informativa relativamente os fabricantes, esta assimetria pode comprometer a repartição equitativa dos riscos (sobretudo em casos de complexidade técnica ou científica)[111], logo, entendeu o legislador europeu, que era necessário facilitar o acesso dos lesados aos meios de prova assegurando que esse acesso se deve limitar ao que é necessário/proporcional e que as informações confidenciais/segredos comerciais são protegidos nos termos do art. 8.º da DPD.

Além disso, pelas mesmas razões, entendeu também ser necessário reduzir o ónus da prova do demandante, desde que estejam preenchidas determinadas condições. Assim sendo, estabelece-se uma presunção de qualidade defeituosa do produto (presunção de facto) e uma presunção do nexo de causalidade entre a qualidade defeituosa do produto e dano em determinadas situações (presunção de direito).

Assim, nos termos do art. 9.º, n.º 2 da DPD presume a qualidade defeituosa do produto numa de três situações: (1) *caso o demandante não tenha cumprido a obrigação de divulgar os elementos de prova pertinentes que dispõe ao abrigo do art. 8.º, n.º 1* da DPD; (2) caso *o demandante estabeleça que o produto não cumpre os requisitos de segurança obrigatória estabelecidos no direito da União e no direito nacional*; (3) caso *o demandante estabeleça que o dano seja causado por uma falha manifesta do produto no decurso da sua utilização normal ou em circunstância normais*[112]. Estes últimos conceitos careceram de ser preenchidos pelo intérprete, pois o DPD não esclarece o que entende por "falha manifesta" ou "circunstâncias normais".

Adicionalmente, deve presumir-se o nexo de causalidade[113] sempre que se verifique que o produto defeituoso e os danos causados são de *natureza compatível com o defeito em questão.* Uma das vantagens está aqui, uma vez que no âmbito da IA pode ser extremamente difícil a prova do nexo de causalidade entre a falta de segurança que

[110] Cfr. art. 9.º, n.º 1 da DPD. Impende sobre o lesado o ónus de provar o dano, o defeito e o nexo de causalidade, visto que aquele *que invocar um direito cabe fazer a prova dos factos constitutivos do direito alegado* (cfr. art. 342.º, n.º 1 do CC).

[111] Cfr. Considerando (30) DPD.

[112] Perguntamos se quando se presume a qualidade defeituosa com base em determinadas obrigações que violaram ou com base na falha decorrente da utilização, não estaremos a cair numa responsabilidade baseada na culpa, uma vez que tanto no caso como noutro se viola certos padrões de conduta. (Hacker, 2023), p. 29 e 30.

[113] Cfr. art. 9.º, n.º 3, DPD.

ocorreu no sistema e que foi essa mesma que gerou o dano e não circunstâncias externas[114].

Contudo, para que demandante possa beneficiar da presunção exige-se a demonstração de que *o produto contribuiu para o dano* e que *é provável que o produto fosse defeituoso ou que a sua qualidade defeituosa seja uma causa provável do dano, ou ambos*. No fundo, é uma presunção sob certas condições.

Por último, caso o requente enfrente dificuldades excessivas de prova, a qualidade defeituosa e o nexo de causalidade também se presumem, mas, apenas se este demonstrar, com *provas suficientemente pertinentes,* que *o produto contribuiu para o dano* e é *provável que o produto fosse defeituoso ou que a sua qualidade defeituosa seja uma causa provável do dano*[115]. No fundo, terá de reunir em si conhecimentos técnicos para avaliar estas situações, mais difícil será se se tratar de um produto com elementos digitais ou sistemas *IoT*, visto que poderá ser trabalhoso encontrar a deficiência nos dados externos introduzidos para reunir provas pertinentes, por isso este ónus deveria recair sobre o operador económico[116].

A DPD consagra importantes alterações, de modo a proteger o lesado e colmatar algumas dificuldades, principalmente àquelas ligadas à prova, uma vez que para um lesado que não tenha conhecimento técnicos, provar um defeito ou o nexo pode ser particularmente difícil[117].

Apesar de tudo, estas presunções são ilidíveis[118], logo o demandado pode provar que aplicou todos os *standards* técnicos que a arte exigia, à data que o sistema foi colocado em circulação[119] e, até mesmo, nas consequentes atualizações. Além disso, o art. 10.º do DPD prevê meios de defesa para os operadores económicos, de modo, a equilibrar a

[114] Veja-se a título de exemplo a notícia da *Toyota Motor Corporation* que está disponível em https://www.cbc.ca/news/business/toyota-cleared-in-stuck-accelerator-crash-verdict-1.1959806 e https://www.washingtonpost.com/business/economy/toyota-reaches-12-billion-settlement-to-end-criminal-probe/2014/03/19/5738a3c4-af69-11e3-9627-c65021d6d572_story.html (consultado a 17/02/2024).
[115] Cfr. art. 9.º, n.º 3, DPD.
[116] (Koch & et alii, 2023), p. 9.
[117] (Bruin, 2016), p. 491.
[118] Cfr. art. 9.º, n.º 5, DPD.
[119] (Maia, 2021), p. 19.

balança e fazer com que estas presunções não signifiquem um desincentivo ao desenvolvimento[120].

Apesar de haver conceitos que carecem de preenchimento (seja pelo legislador nacional, seja pela doutrina ou jurisprudência) e dos requisitos de prova que são exigidos ao lesado poderem divergir em função do Estado-Membro onde é proposta a ação[121], este parece ser, dentro daqueles que existem, o caminho que melhor salvaguarda todas as posições.

Responsabilidade extracontratual adaptada à IA

Um outro quadro que pode ser equacionado em caso de danos causados por IA é a via delitual. Neste âmbito, foi apresentada a DRIA que sugere um caminho mais facilitado para o lesado, visto que, por exemplo, na nossa legislação, exige-se ao lesado a prova do facto ilícito e culposo levou ao dano[122].

Tendo em conta que a IA possui características como a opacidade, a autonomia e a complexidade, a consequência seria, muitas vezes, a incapacidade do lesado de prova, nomeadamente, do nexo de causalidade, visto que teria de se provar que aquele *input* executado por aquela pessoa originou aquele *output* causador de danos[123].

Sendo difícil a responsabilização quando esteja em causa um sistema IA, inevitavelmente, o consumidor não tem vontade de os utilizar, porque não confia neles. Assim, como a IA é um fenómeno que transcende as fronteiras nacionais, a UE entendeu que devia intervir e harmonizar esta matéria, de modo a estabelecer a segurança jurídica para o mercado em geral.

Diferenças relativamente a outros instrumentos

A DPD e a DRIA complementam-se no intuito de formar um regime de responsabilidade civil eficaz[124], sendo que a primeira exige a defeituosidade do produto

[120] Sobre a defesa como tentativa de ajudar no risco de não desenvolvimento, veja-se alguma doutrina que para os veículos automóveis já escrevia sobre isto, por exemplo, (Chatzipanagiotis & Leloudas, 2020).

[121] Veja-se a título de exemplo, Van Dam, C. (2013). *European tort law*. OUP Oxford. (disponível em: https://books.google.pt/books?hl=en&lr=&id=VjZpAgAAQBAJ&oi=fnd&pg=PP1&dq=C.+Van+Dam,+European+Tort+Law,+Oxford+University+Press,+2013&ots=5SU6alA3c5&sig=fYSsLPEo-Gftr3ugzwgiRgfBoHY&redir_esc=y#v=onepage&q=C.%20Van%20Dam%2C%20European%20Tort%20Law%2C%20Oxford%20University%20Press%2C%202013&f=false) o estudo que faz nesta matéria.

[122] Pressupostos retirados do art. 483.º, n.º 1, CC.

[123] Cfr. Considerando (3) DRIA.

[124] DRIA, p. 3.

e a segunda pressupõe a culpa. A ideia é que se assegure uma igualitária proteção dos lesados de danos causados por IA e dos lesados de danos causados por produtos em geral.

O DPD aplica-se a todos os produtos do mercado, inclusive ao *software* e a DRIA apenas se aplica à IA, mas ambas pretendem cumprir o objetivo enunciado. Por outro lado, a DRIA consegue ter um escopo mais alargado de direitos protegidos, nomeadamente, confere a proteção de direitos fundamentais, tais como a violação de privacidade ou discriminação.

Uma diferença importante é que enquanto a DPD implementa um quadro de harmonização máxima[125], a DRIA implementa um quadro de harmonização mínima, uma vez que os lesados podem invocar regras nacionais sempre que essas se mostrem mais favoráveis[126]. Consequentemente, esta harmonização mínima pode deitar por terra o objetivo da sua criação, isto é, continua a existir o perigo de fragmentação da responsabilidade entre os Estados-Membros levando a que possa consubstanciar um obstáculo à implantação da IA. Por outro lado, com a não harmonização máxima deixa uma margem de articulação que permite uma margem de flexibilidade para aprendizagem[127].

A par da complementaridade entre as duas, para compreender a DRIA, esta deve ser lida em conjunto com o RIA, nomeadamente, porque o art. 2.º, n.º (2) da mesma remete a definição de sistema de IA de risco elevado para o art. 6.º do RIA, tal como faz remissão da definição de fornecedor e utilizador para o mesmo diploma.

Divulgação de elementos de prova e presunção de incumprimento

Pormenorizando, no âmbito do RIA, quando estejam em causa sistemas de IA de risco elevado, são impostas aos operadores certas obrigações de diligência[128], sendo que

[125] De modo a ilustrar esta afirmação, veja-se o art. 3.º DPD. Adicionalmente, TJUE, Proc. C-183/00, María Victoria González Sánchez c. Medicina Asturiana ECLI:EU:C:2002:255 p. 23 e ss.; TJUE, Proc. C-52/00: Comissão das Comunidades Europeias/República Francesa ECLI:EU:C:2002:252 p. 13 e ss.; TJUE, Proc. C-154/00, Comissão/Grécia, ECLI:EU:C:2002:254 p. 9 e ss. Para mais esclarecimentos sobre a matéria, (Verheyen, 2018), p. 119 a 140.

[126] Ver Considerando (14) DPD.

[127] (Dheu, De Bruyne, & Ducuing, 2022), p. 16.

[128] Veja-se o RIA nesta matéria.

operador poderá constituir quer um fornecedor[129], quer um utilizador, quer um mandatário, quer um importador ou um distribuidor[130].

Tentando colmatar algumas das dificuldades de prova do lesado, no art. 3.º confere-se ao Tribunal, a pedido de um potencial demandante, a possibilidade de exigir do fornecedor[131] a divulgação de elementos de prova que sejam pertinentes sobre o sistema, mas apenas sobre aqueles que são considerados de risco elevado nos termos do RIA.

Pode-se criticar esta remissão da DRIA para o RIA, porque a categorização do RIA deixa de fora algumas realidades, nomeadamente, apesar dos veículos autónomos serem considerados sistemas de alto risco nos termos do art. 6.º, n.º 1 e 2 do RIA, estão isentos de todas as obrigações prevista nele[132]. Consequentemente, a presunção do art. 3.º da DRIA não é aplicável, constituindo uma oportunidade perdida, pois estes sistemas são tão propensos a causar danos como os outros.[133] Nesta medida, talvez uma remissão em bloco poderá não ser o melhor caminho.

Por outro lado, outras realidades (como os "modelos básicos" e as ferramentas de *open-source*[134]), têm em si implícito uma grande dificuldade de identificação dos riscos, pois fazem um pouco de tudo, torna-se difícil apurar todos os riscos, e, este trabalho extra acaba por ser um ponto contra a que estas empresas desenvolvam.[135]

Isto posto, olhando novamente para a letra do art. 3.º da DRIA, só opera esta ordem judicial se o potencial demandante *apresentar factos e elementos de prova suficientes para fundamentar a plausibilidade de uma ação de indemnização*[136] e se já tiver solicitado diretamente ao potencial demandado tendo este recusado o acesso às

[129] O fornecedor constitui a pessoa, seja ela singular ou coletiva, que desenvolve um sistema de IA ou que tenha um sistema de IA desenvolvido para colocar no mercado ou em forma de serviço sob o seu nome ou marca. Cfr. art. 3.º, n.º 2 do RIA.

[130] Cfr. art. 3.º, n.º 8 RIA.

[131] Os pedidos de divulgação de elementos de prova só podem ser solicitados àqueles que têm obrigações estabelecidas no âmbito do art. 24.º ou 28.º, n.º 1 do RIA. Escusado será dizer que estes pedidos não podem ser dirigidos "a partes que não tenham obrigações por força do RIA e, por conseguinte, não tenham acesso aos elementos de prova". DRIA, p. 14.

[132] Esta conclusão extrai-se da conjugação do art. 2.º, n.º 2, do art. 84.º e do anexo II, secção B, n.º 2, 3, 6 e 7 do RIA.

[133] (Hacker, 2023), p. 9 e 10.

[134] Relativamente à definição de *open source,* corresponde a uma redistribuição gratuita de um código fonte, com a permissão de modificação, mas deve-se permitir a distribuição de *software* construído a partir do código fonte. Além disso, não é permitido que seja discriminatório e faça restrições ao seu uso. (Open Source Initiative (2006), The Open Source Definition, https://opensource.org/osd).

[135] (Hacker, 2023), p. 10 e 11.

[136] Cfr. art. 3.º, n.º 1 da DRIA.

informações necessárias[137], apesar de as ter à sua disposição[138][139]. O objetivo é que se identifique de forma clara os verdadeiros responsáveis e quais os elementos de prova relevantes para uma ação de indemnização, por outro lado, estes conceitos carecem de preenchimento.

Se o fornecedor ou utilizador não cumprirem a ordem do tribunal para a divulgação das informações necessárias, nesse caso, o tribunal presume o não cumprimento do dever de diligência pertinente[140][141]. Para promover a divulgação de informações relevantes[142] presume-se o incumprimento do dever de diligência[143].

Na verdade, continua a estar a cargo do demandante a prova dos factos e a prova de que existem suficientes indícios para fundamentar a ação, logo só se poderá aplicar a presunção, quando aqueles não cumprirem a obrigação de prestação de informações.

Além disso, a presunção não opera quando a informação fornecida é a de que não tomou a diligência necessária ou, mesmo tomando a diligência necessária, não consegue demonstrá-la, no fundo, apenas informa o demandante das medidas (insuficientes) que tomou. Assim, continua a ser o demandante quem tem de provar que a medida em concreto que era exigível e não foi adotada pelo demandado[144].

[137] Utiliza-se a palavra "necessárias", uma vez que esta obrigação de divulgação de evidências se limita ao necessário e proporcional para apoiar uma potencial reclamação ou um pedido de indemnização. Não ferindo assim o segredo comercial. Veja-se "limitar a divulgação ao mínimo necessário e evitar pedidos genéricos." DRIA, p. 14.

[138] Salienta-se que é necessário que o potencial demandante deve realizar todas as tentativas proporcionadas para obter as provas do potencial demandado (cfr. art. 3.º, n.º 2 da DRIA).

[139] Isto é diferente daquilo que vimos para o DPD, uma vez que nesse não é necessário que seja solicitado previamente ao demandado a divulgação de provas (veja-se art. 8.º, n.º 1, DPD). Em contrapartida, a DPD não confere a possibilidade de os tribunais poderem requerer a divulgação de provas (a favor desta inclusão, (Hacker, 2023), p. 18). Além disso, na DRIA esta possibilidade pode aplicar-se estejamos perante um potencial demandante ou já um demandado, enquanto a DPD parece indicar que esta apenas se aplica durante a instauração da ação.

[140] Há quem entenda que deveria ter sido consagrada uma inversão do ónus da prova e não uma presunção de ilicitude. Veja-se (Faria J. R., 2023), p. 81.

[141] Cfr. art. 3.º, n.º 5 da DRIA.

[142] Veja-se Considerando (21) DRIA.

[143] O dever de diligência é definido como a norma de conduta obrigatória (cfr. art. 2.º, n.º 9, DRIA). O mais adequado seria olhar para ele como um padrão de conduta, seja ele decorrente de um dever decorrente do negócio jurídico, da própria lei ou dado pela diligência do homem médio, tal como é estatuído no ordenamento jurídico português no art. 487.º do CC (Mello, 1989). No entanto, a DRIA parece apontar para que seja mesmo entendido como uma obrigação legal, uma vez que no art. 4, n.º 1, alínea a) se equipara a culpa ao incumprimento de um dever de cuidado. Esta questão pode, desta forma, criar fragmentações de interpretação deste conceito.

[144] (Faria J. R., 2023), p. 80.

Acrescenta-se que só deve ser desencadeada a presunção depois de recusado o pedido dirigido pelo tribunal, antes disso não se desencadeia a presunção de incumprimento[145].

Relativamente ao pressuposto da culpa, temos de compreender que tipos de culpa são abrangidos. Assim, a DRIA abrange o dano causado por um resultado ou pela incapacidade de produzir um resultado decorrente de um facto culposo de uma pessoa, deixando de fora os casos em que o dano é causado por uma avaliação humana seguida de uma ação ou omissão humana, tendo o sistema de IA apenas prestado informações ou aconselhamento que foram tidos em conta pelo interveniente humano em causa[146].

A ideia é que, nestes casos, como se consegue chegar ao ser humano, então não seria necessário ser consagrada estas presunções. Isto dá aso a críticas, pois, se no art. 29.º do RIA se exige que se implemente a supervisão aos sistemas de risco elevado, então esta restrição de que a DRIA só se aplica quando a tomada de decisão for automatizada poderá não fazer muito sentido. Deste modo, há quem entenda a presunção de incumprimento se deve aplicar mesmo que seja um ser humano a tomar a decisão final que conduziu a danos causados pelos resultados da IA[147].

Presunção de causalidade

Exceto no caso do art. 3.º, n.º 5 da DRIA, terá o lesado que demonstrar e provar as violações ao RIA. O que acaba por ser uma falha, uma vez a prova da culpa em sistemas de IA mais complexos é difícil de obter.

Tendo em consideração que em determinados sistemas de IA pode ser difícil determinar quais os *inputs* que foram relevantes para o resultado, no art. 4.º, n.º 1 da DRIA estabelece-se uma presunção ilidível do nexo de causalidade entre a existência de culpa do demandado (que compreende pelo menos a violação de um dever de diligência) e o resultado produzido ou a incapacidade do sistema de IA de produzir um resultado[148].

[145] Veja-se o Considerando (17) da DRIA.
[146] Cfr. Considerando (15) da DRIA.
[147] (Hacker, 2023), p. 13 e 14.
[148] Faz-se ressalva para art. 4.º, n.º 6, DRIA, uma vez que quando o demandado utiliza o sistema de IA no exercício de uma atividade pessoal e não profissional, a presunção só deve ser aplicada se *o demandado tiver interferido substancialmente nas condições de funcionamento do sistema de IA ou se o demandado tivesse a obrigação e a capacidade de determinar as condições de funcionamento do sistema de IA, mas não o tenha feito*. Compreende-se, visto que é necessário equilibrar os interesses das pessoas lesadas e dos utilizadores não profissionais.

No entanto, esta presunção só será aplicável se o demandante demonstrar que o demandado, nos termos do razoável, tem ao seu dispor elementos de prova e conhecimentos especializados suficientes para provar o nexo de causalidade[149].

No fundo, a presunção liga a culpa e a produção ou a falta de produção do resultado, deixando de fora o modo de determinação da culpa, a definição de existência ou inexistência de um resultado, a existência e extensão dos danos e o nexo de causalidade entre o resultado e o dano[150].

No que concerte à definição de causalidade, também não se avança com uma definição, aliás, tanto para a culpa, como para a causalidade e outros aspetos[151], remete para as regras nacionais[152].

Analisando as alíneas do n.º 1 do art. 4.º da DRIA, a presunção de causalidade só opera se forem cumpridos uns requisitos adicionais.

Primeiramente, o demandante precisa de demonstrar a culpa do demandado. Esta culpa deve pelo menos consistir no incumprimento de um dever de diligência destinado a proteger contra o dano ocorrido, esteja ele previsto em legislação europeia ou nacional[153]. Além disso, tendo em conta que o conceito de culpa não aparece harmonizado a nível europeu, podem os Estados-Membros, para além da violação do dever de diligência, determinar os contornos da mesma. Em contrapartida, se o incumprimento dos deveres de diligência não se destinarem a proteger diretamente os danos ocorridos, não se poderá aplicar esta presunção[154].

Em segundo lugar, o tribunal deve considerar razoavelmente provável que a falha tenha influenciado o resultado ou a incapacidade desse resultado, dependendo de uma avaliação casuística[155]. Apesar da DRIA esclarecer um pouco sobre aquilo que se entende como "razoável", caberá sempre uma avaliação subjetiva, levando a que possa ocorrer uma fragmentação em toda a UE.

---

[149] Cfr. art. 4.º, n.º 4 da DRIA.

[150] (Hacker, 2023), p. 20.

[151] Também os diferentes tipos de danos que dão origem a direitos de indemnização, a repartição da responsabilidade por vários infratores, a conduta que concorre para a origem do dano, o cálculo dos danos ou os prazos de prescrição são aspetos que a DRIA remete para cada Estado-Membro a sua regulação.

[152] Veja-se o Considerando (10) da DRIA.

[153] Pode este dever derivar de fonte jurisprudencial, visto que nem os considerandos nem a definição de "dever de diligência" impedem esta interpretação (Hacker, 2023), p. 21.

[154] Cfr. Considerando (22) da DRIA.

[155] Veja-se o Considerando (25) da DRIA.

Em terceiro lugar, o demandante apenas precisa de demonstrar que o resultado ou a incapacidade de produzir o resultado do sistema de IA causou danos. Esta questão é mais fácil, porque, em princípio, essas informações estão no seu domínio. Aliás, numa ação que não seja sobre um sistema IA já cabe ao lesado fazer a prova.

Após os requisitos gerais, no caso de a ação de indemnização ser intentada contra o fornecedor[156] de um sistema de IA de risco elevado, para que a presunção seja aplicada é necessário que ocorra a violação de requisitos específicos enumerados no RIA. Um fornecedor comete uma falha quando: (i) não cumpre o regime de governação de dados; (ii) o sistema não foi concebido e desenvolvido de modo a satisfazer a transparência; (iii) o sistema não foi desenvolvido de forma a permitir uma supervisão eficaz por parte de um humano; (iv) não foi criado de modo a atingir um nível adequado de precisão, robustez e segurança cibernética; (v) por último, o fornecedor não cumpre as obrigações que recaia sobre si de adotar medidas corretivas para repor a conformidade do sistema, ou proceder à retirada ou recolha do mesmo.[157]

Imaginemos que só depois de verificado o resultado é que se constata que se deveria ter cumprido um determinado tipo de obrigações. Por exemplo, existem obrigações de transparência, e, vamos supor que algumas dessas explicações só conseguem ser fornecidas após a verificação do resultado, isto dá origem a que presunção de causalidade não se aplique[158], uma vez que esta não abrange as obrigações que são geradas depois do resultado[159].

Uma outra situação é o caso de os sistemas de IA que produziram o resultado danoso não serem considerados pelo RIA como sistemas de risco elevado.

Nesses casos, a presunção de causalidade só é aplicável se o tribunal entender que é excessivamente difícil para o demandante provar a causalidade[160], sendo que isto deve ser aferido de acordo com as próprias características do sistema. Assim, tendo em conta

[156] Olhamos para o fornecedor uma vez que é este o sujeito que nos interessa no âmbito deste trabalho.

[157] Parece que no art. 4.º, n.º 2, DRIA estão em causa obrigações de meios, uma vez que exige que se deve ter "em conta as medidas tomadas" e não apenas os resultados (Dheu, De Bruyne, & Ducuing, 2022), p. 19 e 20.

[158] Está-se a falar dos casos em que os próprios fornecedores não conseguiriam fornecer aquelas informações, e, só após a produção do resultado é que se aperceberam que sobre si recaiam essas obrigações. Fora destes casos, estão as situações em que os desenvolvedores e criadores dos sistemas de IA ter-se-iam apercebido, se reunissem capacidades técnicas suficientes, que existia um problema e poderiam desenvolver um sistema de IA em conformidade e, mesmo assim, não o fizeram.

[159] (Hacker, 2023) considera isto um ponto fraco da DRIA, p. 24.

[160] Cfr. art. 4.º, n.º 5 da DRIA.

que precisa provar de que forma o sistema, quer seja por ação ou omissão humana, produziu determinado resultado ou foi incapaz de o produzir, então não lhe deve ser exigido que explique as características do sistema IA, nem a forma como estas dificultam a prova do nexo de causalidade[161].

Neste caso, exige-se a violação de um dever de diligência em geral, desde que seja destinado a proteger danos específicos.

A ideia é que se o sistema de IA acarreta um risco inferior, então o demandante terá sobre si mais exigências. No entanto, tal regra não fará sentido se estiver em causa um sistema que não seja de alto risco, mas comporte de igual forma um elevado nível de opacidade, havendo quem defenda[162] a extensão da presunção da causalidade nos mesmos termos dos sistemas de risco elevado.

Por último, a DRIA nada refere sobre os danos que possam ser causados pela implementação e utilização de um sistema de IA proibido ao abrigo do art. 5.º do RIA. Logo, quer os desenvolvedores que os colocam no mercado, quer os utilizadores que os implementam, devem ser responsabilizados pelos danos que se venham a verificar com o seu funcionamento[163].

2.5 Um apontamento sobre a Proposta de Regulamento Ciber-resiliência[164]

O RCR surgiu para aumentar a segurança com a utilização dos produtos na nova era digital, sendo que relativamente aos operadores económicos existem obrigações de segurança que devem ser cumpridas quando desenvolvem um produto.

Assim, no seu âmbito abrange produtos que contenham elementos digitais cuja intenção ou utilização razoavelmente previsível inclui, direta ou indiretamente, dados que se conectam a um dispositivo ou rede[165]. É uma definição ampla, de modo a incluir qualquer produto de *software*[166] ou *hardware,* assim como os seus componentes[167].

---

[161] Cfr. Considerando (28) da DRIA.
[162] (Hacker, 2023), p. 23 e 24.
[163] Nos moldes explicados por (Hacker, 2023), p. 25.
[164] Para mais desenvolvimentos sobre a matéria veja-se, por exemplo, Chiara, P.G. The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *Int. Cybersecur. Law Rev.* 3, 255–272 (2022). Disponível em: https://doi.org/10.1365/s43439-022-00067-6.
[165] Veja-se o art. 2.º, n.º 1, RCR.
[166] Fica apenas excluído deste âmbito o *software* como serviço e ainda o *software* livre ou de código aberto (veja-se o Considerando (9) e (10) do RCR). Como explica (Cabral, 2020), na p. 56, a IA pode ser fornecida como um serviço.
[167] Cfr. art. 3.º, (1), RCR.

Aquilo que existiam no âmbito da cibersegurança não incluía o *software* incorporado noutros produtos[168]. Assim, atualmente, se um sistema de IA é um *software* com capacidade de autoaprendizagem e autonomia, então, desde que lhe seja aplicável o RIA, poder-se-á equacionar a aplicação deste regime.

Isto posto, o RCR aplica-se a produtos com elementos digitais, sendo que estes vão ser agrupados em categorias e aqueles que são considerados produtos críticos são divididos em duas classes[169], em função do nível de risco que para a segurança cibernética representarem de acordo com a sua avaliação de conformidade[170], sendo certo que a segunda classe será aquela que representa um maior risco[171]. Desta forma, para os produtos que sejam considerados altamente críticos, é necessário que os fabricantes obtenham um Certificado Europeu de segurança cibernética para atestar a conformidade com os requisitos essenciais estabelecidos[172].

À semelhança do DPD, também RCR prefere a expressão "operador económico" que abrange fabricantes, distribuidores e importadores. Estes devem realizar uma avaliação dos riscos de acordo com a categoria do produto, em que o resultado dessa avaliação deve ser tido em conta no planeamento, conceção, desenvolvimento, produção, entrega e manutenção do produto no mercado, e a avaliação deve ser incluída na ficha técnica do produto[173]. Além destas, os arts. 10.º e ss. RCR preveem mais obrigações a cargo dos operadores económicos, sendo que vão divergir se estiverem causa produtos da classe I ou da classe II.

Assim, a disponibilização no mercado de produtos com elementos digitais pode ser realizada quando cumpra três condições gerais principais[174]: (i) tenham sido concebidos, desenvolvidos e produzidos de acordo com os requisitos considerados essenciais[175]; (ii) nos termos da condição de que sejam devidamente instalados, mantidos, utilizados ao fim a que se destinam ou sob condições que possam ser razoavelmente previstas e, quando aplicável atualizado; e (iii) os processos implementados pelo fabricante cumpram os requisitos essenciais estabelecidos[175].

---

[168] Veja-se os motivos que levaram à proposta em RCR e o Considerando (46) do RCR.
[169] Veja-se o Anexo III do RCR.
[170] Cfr. art. 6.º, n.º 4, RCR que remete para avaliação de conformidade do art. 24.º, n.ºs 2 e 3 RCR.
[171] Cfr. Considerando (26) do RCR.
[172] Cfr. art. 6.º, n.º 5, CRC.
[173] Cfr. art. 10.º, n.ºs 1, 2 e 3, RCR.
[174] Cfr. art. 5.º RCR.
[175] Veja-se o Anexo I, secção 1 e 2, RCR.

Relativamente à interação entre o RCR e o RIA temos o art. 8.º do RCR. Deste modo, produtos que caibam dentro do âmbito de aplicação do RCR e que sejam classificados como sistemas de IA de risco elevado pelo RIA, devem cumprir os requisitos estabelecidos no Anexo I do RCR. Estando cumpridos, o sistema de IA será considerado conforme segundo os requisitos de cibersegurança, na medida em que esses requisitos sejam abrangidos pela declaração de conformidade da UE[176].

Em contrapartida, o art. 43.º do RIA prevalece sobre as disposições do RCR[177]. No entanto, se um sistema de risco elevado é qualificado como um produto crítico pelo RCR, então está sujeito às regras de avaliação de conformidade do RCR[178]. Sintetizando, cabe às autoridades nacionais de fiscalização do mercado, designadas pelos Estados-Membros, realizarem a fiscalização do mercado quando estejam em causa produtos com elementos digitais nos termos do RCR. No entanto, se estiverem em causa sistemas de risco elevado com elementos digitais, as autoridades de fiscalização do mercado designadas para efeitos do RIA serão as autoridades responsáveis pela vigilância da atividade nos termos do RCR, ou seja, elas devem cooperar entre si[179].

De modo a assegurar o cumprimento efetivo das obrigações estabelecidas no RCR, cada autoridade terá em si o poder de impor ou solicitar a aplicação de multas administrativas[180].

[176] Cfr. art. 8.º, n.º 1, RCR.
[177] Cfr. art. 8.º, n.º 2, RCR.
[178] Cfr. art. 8.º, n.º 3, RCR.
[179] Cfr. art. 41.º, n.º 10, RCR.
[180] O RCR estabelece os limites máximos das multas pelo incumprimento das obrigações (Cfr. art. 53.º RCR).

Conclusão

Facilmente depreendemos que com todas estas propostas a UE tenta encontrar um equilíbrio entre aquilo que são as dificuldades dos lesados face às características inerentes a um sistema de IA. Isto porque, muitas vezes, o lesado é um leigo na área, por isso a UE cria presunções para facilitar a prova da defeituosidade ou da falha que ocorreu, mas fá-lo com alguma cautela, de modo a evitar que com a regulação se acabe com a inovação.

No fundo, a tendência da UE segue para a responsabilização de toda a linha de distribuição do sistema de IA, em especial, os desenvolvedores e criadores, uma vez que são estes aqueles que, em primeira linha, tiveram o controlo sob o sistema. Como vimos, podem responder por culpa se estiver em causa a violação de obrigações que constam dos documentos legais, mas também independentemente de culpa, no âmbito da responsabilidade do produtor.

Apesar de serem uma grande e importante iniciativa legislativa, existem importantes diferenças entre elas. Além disso, existem ainda conceitos nestas Propostas que necessitam de ser clarificados ou pelo legislador nacional (quando transpor as diretivas) ou pelo próprio intérprete.

Por estes e outros motivos, por isso há quem defenda que teria talvez sido mais eficaz optar por uma única via que harmonizasse toda a matéria em todos os países membros[181].

Em suma, defendemos que está certo o caminho no sentido de responsabilização dos operadores económicos, mas peca por ser tímido e pouco clarificador.

Tendo em conta os riscos dos sistemas IA, entendemos que seria preferível um quadro harmonizado, traduzido do seguinte modo: estando em causa sistemas de risco elevado (ou até mesmo sistemas proibidos), dever-se-ia aplicar um verdadeiro quadro de responsabilidade objetiva tal como previsto no nosso ordenamento para outro tipo de situações, onde se prescinde de qualquer tipo de culpa, uma vez que aqui está em causa o velho brocado *qui habet commoda ferre debet onera*, ou seja, quem coloca grandes riscos no mercado e retira benefício, deve ser responsável pelos danos; contrariamente, estando em causa sistema que não sejam categorizados de risco elevado, devem ser consideradas presunções ilidíveis de culpa e de causalidade, de modo a salvaguardar a continuidade da inovação e facilitar a busca de prova por parte do lesado. No fundo, um sistema de

[181] (Hacker, 2023), p. 29 a 33.

responsabilidade tendo em conta a categorização dos sistemas, ou seja, estando causa sistemas que não devem causar danos e que, se forem utilizados corretamente, não causam danos, deve ser aplicada a responsabilidade puramente objetiva, já quando estejam em causa sistemas que causem danos de forma inevitável devem enfrentar apenas presunções de culpa e causalidade.

Uma nota final para os chamados *foundation models* dependendo da utilização a que vai estar sujeita, ou seja, se for utilizado numa aplicação que não seja de risco elevado, deve ser aplicado o regime dos sistemas que não são de risco elevado, o mesmo se diga se estiver em causa a utilização numa aplicação considerada de risco elevado, deve-lhes ser aplicado o regime de responsabilidade dos sistemas de risco elevado.

Bibliografia

ABBOT, K. W., & Snidal, D. (2000). "Hard and Soft law in Internacional Governance". *International Organization, 54*(3), p. 421-456. Disponível em: https://www.jstor.org/stable/2601340

ANDRADE, M. A. (1992). *Teoria geral da relação jurídica* (reimp. 9ª ed., Vols. 2: Facto jurídico, em especial negócio jurídico). Coimbra: Almedina.

ANTUNES, H. S. (19 de nov. de 2019). "Responsabilidade civil do produtor: os danos ressarcíveis na era digital". *Revista de Direito da Responsabilidade* (Ano 1), p. 1476-1486. Disponível em: https://revistadireitoresponsabilidade.pt/2019/responsabilidade-civil-do-produtor-os-danos-ressarciveis-na-era-digital-henrique-sousa-antunes/

ASCENSÃO, O. (2000). *Direito Civil – Teoria Geral, I, Introdução, as pessoas, os bens* (2ª ed.). Coimbra: Coimbra Editora.

BARBOSA, M. M. (2020). "Inteligência Artificial, E-Persons e Direito: Desafios e Perspetivas". Em Instituto Jurídico Centro de Direito do Consumo, *Direiro e Robótica* (p. 57-90). Coimbra. Disponível em: https://www.fd.uc.pt/cdc/pdfs/rev_16_completo.pdf

_____. (31 de mar. de 2020). "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), p. 280-326. Disponível em: https://revistadireitoresponsabilidade.pt/2020/o-futuro-da-responsabilidade-civil-desafiada-pela-inteligencia-artificial-as-dificuldades-dos-modelos-tradicionais-e-caminhos-de-solucao-mafalda-miranda-barbosa/

BERTOLINI, A. (2020). *Artificial Intelligence and Civil Liability.* Study requested by the JURI committee. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf

BOYLE, A. (04 de out. de 1999). "Some Reflections on the Relationship of Treaties and Soft Law". *The International and Comparative Law Quarterly, 48*(4), p. 901-913. Disponível em: https://www.jstor.org/stable/761739

BRUIN, R. d. (2016). "Autonomous Intelligent Cars on the European Intersection of Liability and Privacy: Regulatory Challenges and the Road Ahead". *European Journal of Risk Regulation, 7*(3), p. 485-501. Disponível em: https://www.jstor.org/stable/24769968

BRUYNE, J., Gool, E., & Gils, T. (2022). *Tort Law and Damage Caused by AI Systems.* Disponível em: https://lirias.kuleuven.be/retrieve/692266

CABRAL, T. S. (18 de set. de 2020). "Liability and artificial intelligence in the EU: Assessing the adequacy of the current Product Liability Directive". *Maastricht Journal of European and Comparative Law*, p. 615-635. Disponível em: https://journals.sagepub.com/doi/pdf/10.1177/1023263X20948689?casa_token=lJ52ueDH_kMAAAAA:5K80icDqn8t00H5IdFl9I-NIHqzZOsQwLG-gVkejgRp_JT8X_f9i8BzINAAPoKwFT-gU2pxGSQ3-

CHATZIPANAGIOTIS, M., & Leloudas, G. (2020). *Automated Vehicles and Third-Party Liability: A European Perspective.* Illinois: University of Illinois Journal of Law. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3519381

CORDEIRO, M. (1991). *Manual de Direito do Trabalho* - Dogmática básica e princípios gerais: direito colectivo do trabalho. Coimbra: Almedina.

_____. (2010). *Tratado de Direito Civil II, Direito das Obrigações, Tomo III.* Coimbra: Almedina.

CORREIA, D. F. (2019). *O "R" de Robótica no "R" da Responsabilidade Civil: O paradigma da inteligência artificial.* Tese de Mestrado em Direito e Prática Jurídica, Faculdade de Direito da Universidade de Lisboa, Lisboa. Disponível em: https://repositorio.ul.pt/bitstream/10451/49814/1/ulfd0149038_tese.pdf

COSTA, M. d. (1998). O concurso da responsabilidade civil contratual e da extracontratual. Em A. Varela, *Ab uno ad omnes - 75 anos da Coimbra Editora (1920-1995)* (p. 555-565). Coimbra: Coimbra Editora.

_____. (2009). *Direito das Obrigações*. 12ª ed. Coimbra: Almedina.

DHEU, O., De Bruyne, J., & Ducuing, C. (2022). *The European Commission's Approach To Extra-Contractual Liability and AI – A First Analysis and Evaluation of the*

Two Proposals. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4239792

FARIA, J. R. (2023). "A teoria das esferas do risco. A utilização de agentes eletrónicos no cumprimento dos contratos e a proposta de Diretiva de 28.09.2022 relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial". *Revista de Direito Civil* (Ano VIII, Nº 1), p. 77-103. Disponível em: https://www.revistadedireitocivil.pt/artigos/a-teoria-das-esferas-do-risco-a-utilizacao-de-agentes-eletronicos-no-cumprimento-dos-contratos-e-a-

FARIA, Jorge R. (2023). *Direito das Obrigações.* Vol. 2, 2ª ed., Coimbra: Almedina.

FLORIDI, L. (03 de dez. de 2023). "On the Brussels-Washington Consensus About the Legal Definition of Artificial Intelligence". *Philosophy & Technology*. Disponível em: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4652136_code2644503.pdf?abstractid=4652136&mirid=1

GOUVEIA, J. B. (2017). *Manual de Direito Internacional Público, 5ª ed.* Coimbra: Almedina.

HACKER, P. (2023). "The European AI liability directives – Critique of a half-hearted approach and lessons for the future". *Computer Law & Security Review, 51*. Disponível em: https://www.sciencedirect.com/science/article/pii/S026736492300081X#cit_84

Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission. (08 de abr. de 2019). *A Definition of AI: Main Capabilities and Disciplines.* Disponível em: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60651

JANIESCH, C., Zschech, P., & Heinrich, K. (8 de abril de 2021). "Machine learning and deep learning". *Electronic Markets, 31*(3), p. 685–695. Disponível em: https://link.springer.com/content/pdf/10.1007/s12525-021-00475-2.pdf

KERKHOVE, S. V. (04 de jun. de 2019). *Unethical and Illegal Practices in Coding: From Prevention to Action.* Consultado a 18 de jan. de 2024, de Welcome to the jungle: https://www.welcometothejungle.com/en/articles/ethical-illegal-coding

KOCH, B., & et alii. (2023). *European Commission's Public Consultation on Civil Liability - Adapting Liability Rules to the Digital Age and Artificial Intelligence.* Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322623

LEITÃO, L. M. (2016). *Direito das Obrigações*. 10ª ed. Coimbra: Almedina.

MACHADO, J. (2013). *Direito internacional: do paradigma clássico ao pós 11 de setembro* (4ª ed.). Coimbra: Coimbra Editora.

MAIA, A. R. (2021). "A Responsabilidade Civil na Era da Inteligência Artificial – Qual o caminho?". *Julgar*. Obtido de https://julgar.pt/a-responsabilidade-civil-na-era-da-inteligencia-artificial-qual-o-caminho/

MARTINEZ, P. R. (1999). *Direito do Trabalho II Volume - 1º Tomo (Contrato de Trabalho)*. 3ª ed., Vol. 3. Lisboa: Pedro Ferreira Editor.

MATOS, F. A. (2020). "Responsabilidade por Danos Causados a Terceiros por Robôs". Em i. j. consumo, *Direito e Robótica* (p. 155-211). Coimbra.

MELLO, A. d. (set. de 1989). "Critérios de apreciação da culpa na responsabilidade civil : breve anotação ao regime do código". *Revista da Ordem dos Advogados, 2* (Ano 49), p. 519-542. Disponível em: https://portal.oa.pt/upl/%7Ba2b9529f-1b59-4cec-94ff-b02dab234224%7D.pdf

MENDES, J. d. (1979). *Direito Civil, Teoria Geral*. Vol. 2. Lisboa: AAFDL.

MIRANDA, J. (2016). *Curso de Direito Internacional Público*. 6ª ed. Lisboa: Principia.

MONTEIRO, J. F. (1983). *Estudos sobre a responsabilidade civil.* Coimbra: Almedina.

MOREIRA, G. A. (1925). *Instituições do direito civil português.* Coimbra: Coimbra Editora.

PEREIRA, I. P. (2023). "O impacto da inteligência artificial no atual regime da responsabilidade do produtor: um regime em revisão pelas instâncias europeias". *Revista Eletrónica de Direito* (Nº2). Disponível em: https://cij.up.pt/pt/red/edicoes-anteriores/2023-nordm-2/o-impacto-da-inteligencia-artificial-no-atual-regime-da-responsabilidade-do-produtor-um-regime-em-revisao-pelas-instancias-europeias/

PINTO, C. A. (1982). *Cessão da posição contratual.* Coimbra: Almedina.

_____. (1999). *Teoria Geral do Direito Civil*. 3ª ed. Coimbra: Almedina.

RAMALHO, M. d. (2023). *Tratado de Direito do Trabalho, Parte II- Situações Laborais Individuais* (9 ed.). Coimbra: Almedina.

ROUHIAINEN, L. (2019). *Artificial Intelligence: 101 Things You Must Know Today About Our Future.* Disponível em: https://books.google.pt/books?id=SQ06swEACAAJ&printsec=copyright&redir_esc=y#v=onepage&q&f=false

RUSSELL, S., & Norvig, P. (2010). *Artificial Intelligence: A modern approach*. 3ª ed. New Jersey: Pearson Education, Inc. Obtido de Artificial Intelligence A Modern Approach 3ª ed. Disponível em: https://people.engr.tamu.edu/guni/csce421/files/AI_Russell_Norvig.pdf

RUSSELL, S., Perset, K., & Grobelnik, M. (29 de nov. de 2023). *Updates to the OECD's definition of an AI system explained*. Obtido em 18 de jan. de 2024, de OECD.AI: https://oecd.ai/en/wonk/ai-system-definition-update

SHAFFER, G. C., & Pollack, M. A. (2010). "Hard Vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance". *Minnesota Law Review, 94*, p. 706-799. Disponível em: https://scholarship.law.umn.edu/mlr/491

SILVA, J. C. (1990). *Responsabilidade Civil do Produtor.* Coimbra: Almedina.

_____. (2008). *Compra e Venda de Coisas Defeituosas, (Conformidade e Segurança)*. 5ª ed. Coimbra: Almedina.

SILVA, N. S. (2019). *Inteligência Artificial, robots e responsabilidade civil: o que é diferente?*

SURDEN, H. (2019). *ARTIFICIAL INTELLIGENCE AND LAW: AN OVERVIEW.* Colorado: University of Colorado Law School. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3411869

TELLES, I. G. (1997). *Direito das Obrigações.* 7ª ed. Coimbra: Coimbra Editora.

VARELA, A. (2000). *Das obrigações em geral*. Vol. 1, 10ª ed. Coimbra: Almedina.

VASCONCELOS, P. P. (2019). *Teoria Geral do Direito Civil*. 9ª ed. Coimbra: Almedina.

VERHEYEN, T. (fev. de 2018). "Full Harmonization, Consumer Protection and Products Liability: A Fresh Reading of the Case Law of the ECJ". *European Review of Private Law*, p. 119-140. Disponível em: https://www.researchgate.net/profile/Thomas-Verheyen-3/publication/323184813_Full_Harmonization_Consumer_Protection_and_Products_Liability_A_Fresh_Reading_of_the_Case_Law_of_the_ECJ/links/5d714ccf92851cacdb23c829/Full-Harmonization-Consumer-Protection-and

WAGNER, G. (2023). *Liability Rules for the Digital Age - Aiming for the Brussels Effect.* Chicago: University of Chicago Law School. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4320285

WOLFEWICZ, A. (15 de fev. de 2023). *Deep Learning vs. Machine Learning – What's The Difference?* Consultado a 22 de jan. de 2024, de Levity: https://levity.ai/blog/difference-machine-learning-deep-learning

Textos de Organizações Internacionais

- Center for AI and Digital Policy. (2023). *Universal Guidelines for AI*. Disponível em: https://www.caidp.org/events/oct2023-dc-ugai/.
- OECD/LEGAL/0449. (22 de maio de 2019). *Recommendation of the Council on Artificial Intelligence.* Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
- The White House. (30 de out. de 2023). Disponível em: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/?utm_source=link.

Legislação e Textos Europeus

- (2020/2014(INL)). (2020). Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime de responsabilidade civil aplicável à inteligência artificial. Disponível em: https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_PT.html#_section2.

- 2021/0106(COD). (2024). 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. Disponível em: https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf.
- COM(2018) 237 final. (25 de abr. de 2018). Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018DC0237.
- COM(2020) 65 final. (19 de fev. de 2020). Livro Branco sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança. Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1.
- COM(2022) 454 final. (2022). Proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454.
- COM(2022) 495 final. (2022). Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à responsabilidade decorrente dos produtos defeituosos. Disponível em: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52022PC0495.
- COM(2022) 496 final. (2022). Proposta de Diretiva do Parlamento Europeu e do Conselho Relativa à Adaptação das Regras de Responsabilidade Civil Extracontratual à Inteligência Artificial. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52022PC0496.
- Comissão Europeia, Direção-Geral da Justiça e dos Consumidores, (2019). *Liability for artificial intelligence and other emerging digital technologies*, Publications Office. https://data.europa.eu/doi/10.2838/573689.
- Comissão Europeia, Direção-Geral das Redes de Comunicação, Conteúdos e Tecnologias, (2019). *Orientações éticas para uma IA de confiança*, Serviço das Publicações. https://data.europa.eu/doi/10.2759/2686.
- Grupo de Peritos de Alto Nível sobre Inteligência Artificial criado pela Comissão Europeia. (08 de abr. de 2019). *A Definition of AI: Main Capabilities and*

Disciplines. Disponível em: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60651

- Parlamento Europeu. (23 de set. de 2020). *Inteligência artificial: oportunidades e desafios*. https://www.europarl.europa.eu/topics/pt/article/20200918STO87404/inteligencia-artificial-oportunidades-e-desafios.
- Parlamento Europeu. (04 de set. de 2020). *O que é a inteligência artificial e como funciona?* https://www.europarl.europa.eu/topics/pt/article/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona.
- SWD(2022) 317 final. (2022). *Documento de trabalho dos serviços da comissão relatório do resumo da avaliação de impacto* que acompanha o documento Proposta de diretiva do Parlamento Europeu e do Conselho relativa à responsabilidade decorrente dos produtos defeituosos. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0317.