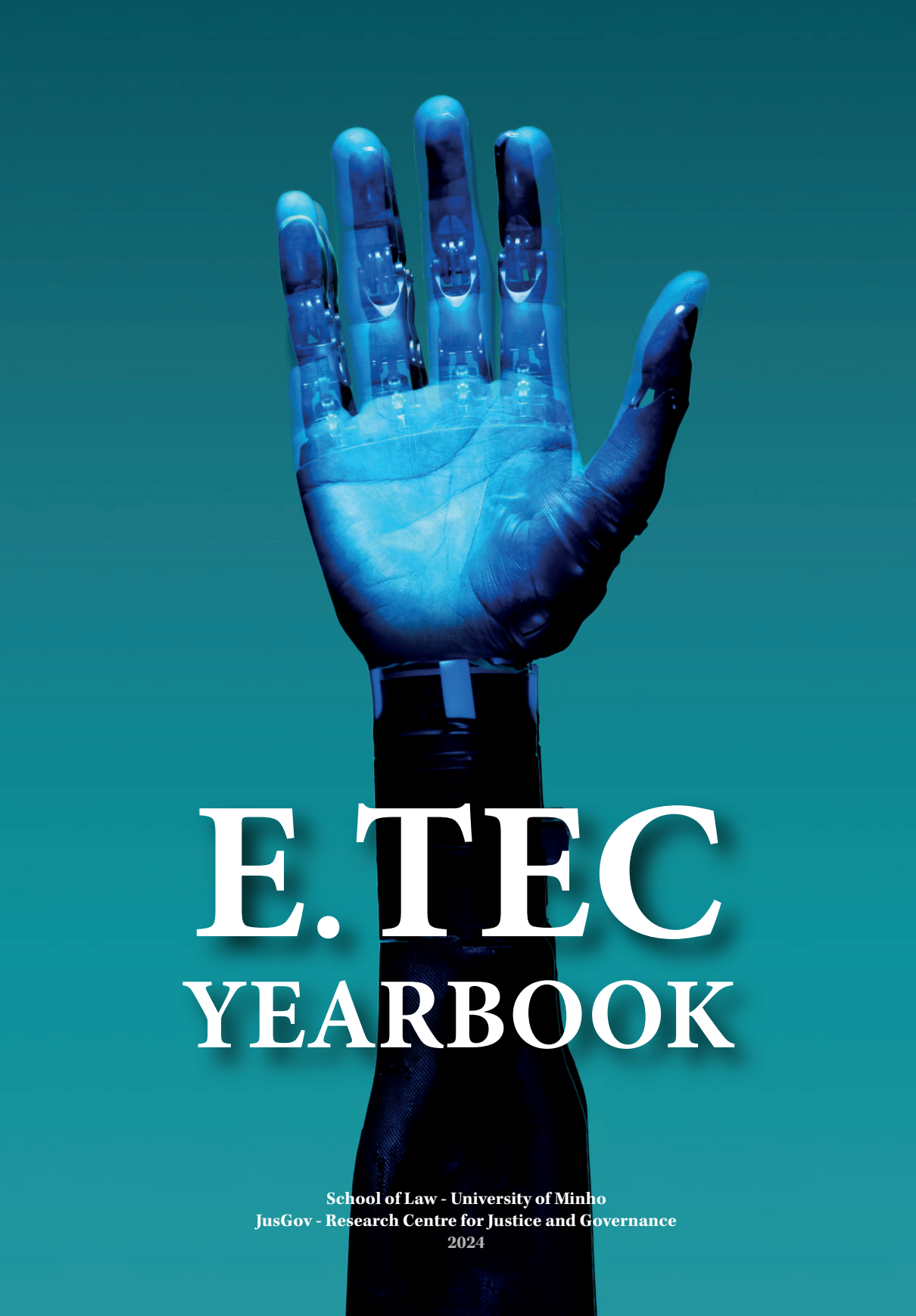


E.TEC YEARBOOK

School of Law - University of Minho
JusGov - Research Centre for Justice and Governance
2024

E.TEC
YEARBOOK

JUSGOV Centro de Investigação em Justiça e Governação

EDUM Escola de Direito da Universidade do Minho

Dezembro 2024

Esta publicação é financiada por fundos nacionais através da FCT — Fundação para a Ciência e a Tecnologia, I.P., no âmbito do Financiamento UID/05749/2020





FICHA TÉCNICA

TÍTULO
Yearbook E-TEC 2024

ORGANIZAÇÃO E EDIÇÃO
Centro de Investigação em Justiça e Governação

Universidade do Minho
Campus de Gualtar
4710-057 Braga

(+351) 253 601 841 / (+351) 253 601 810 | jusgov@direito.uminho.pt

EDITORA
Eva Sónia Moreira da Silva (Sónia Moreira)

INTERVENIENTES
Ana Cristina Gouveia | Luís Manuel Pica | Maria Victória Rocha | Sérgio Manuel da Costa Machado | Sérgio Silva | Yuri R. Ladeia

LOCAL E DATA
Braga, dezembro de 2024

PAGINAÇÃO
Carlos Sousa | Talento & Tradição, Lda.

FOTO DE CAPA
Photo by ThisisEngineering on Unsplash

ISSN
2184-707X

ÍNDICE

PREFACE / PREFÁCIO

ix/xi

ARTIGOS

A introdução da Inteligência Artificial no tratamento de dados: as dificuldades de um efetivo direito à informação
Ana Cristina Gouveia

1

A atividade administrativa da Segurança Social e a Inteligência Artificial: (re)pensar o regime de responsabilidade civil dos atos praticados pela Segurança Social
Luís Manuel Pica

25

The treatment of works of applied art under Portuguese law in the post-*Cofemel* era
Maria Victória Rocha

45

Direitos Digitais dos Consumidores: a portabilidade transfronteiriça de conteúdos e a proibição do *geoblocking*
Sérgio Manuel da Costa Machado

75

Desafios jurídicos na era da Indústria 4.0 e Inteligência Artificial: uma análise das implicações legais e regulatórias
Sérgio Silva

97

Side effects of the (dis)articulation between the Data Governance Act and the General Data Protection Regulation in clinical research: consent is (not) the only applicable legal basis
Yuri R. Ladeia

123

PREFACE

It is with great satisfaction that the E-Tec research group launches its seventh Yearbook.

From 2024 onwards, the editorial option of not establishing a special theme each year will be followed, with the call being open to all topics that relate to E-Tec's thematic axes (Industry 4.0; Space Law and Policy; Artificial Intelligence and Robotics; New Disruptive Technological Areas for Law; and Public and Corporate Governance), with the aim of exploring the legal problems arising from technological innovations in these areas.

In this sense, the texts that are now being published continue to demonstrate the multidisciplinary nature that research into these areas entails: we find reflections on the use of Artificial Intelligence in data treatment, in Industry 4.0 and in administrative activity; on consumers' digital rights, etc.

Once again, our sincere thanks go to the authors, the University of Minho School of Law, in the person of its President, Professor Cristina Dias, and the JusGov Board, in the person of Professor Maria Miguel Carvalho. Without everyone's participation and support, it would not be possible to publicise the results of our research and share legal science with the community.

Braga, December of 2024.

Sónia Moreira
Editora

PREFÁCIO

É com enorme satisfação que o grupo de investigação E-Tec lança o seu sétimo *Yearbook*.

A partir deste ano de 2024, segue-se a opção editorial de não estabelecer um tema especial em cada ano, estando a *call* aberta relativamente a todos os temas que contendam com os eixos temáticos do E-Tec (Indústria 4.0; Direito e Política Espacial; Inteligência Artificial e Robótica; Novas Áreas Tecnológicas Disruptivas para o Direito; e Governação Pública e Empresarial), visando explorar os problemas jurídicos decorrentes das inovações tecnológicas nestas áreas.

Nesse sentido, os textos que ora vêm a lume continuam a demonstrar o carácter multidisciplinar que a investigação sobre estas áreas implica: encontramos reflexões sobre a utilização de Inteligência Artificial no tratamento de dados, na Indústria 4.0 e na atividade administrativa; sobre os direitos digitais dos consumidores, etc.

Mais uma vez, o nosso agradecimento sincero aos autores, à Escola de Direito da Universidade do Minho, na pessoa da sua Presidente, a Professora Cristina Dias, e à Direção do JusGov – Centro de Investigação em Justiça e Governação, na pessoa da Prof.ª Doutora Maria Miguel Carvalho. Sem a participação e o apoio de todos, não seria possível divulgar o resultado da nossa investigação e a partilha da ciência jurídica com a comunidade.

Braga, dezembro de 2024

Sónia Moreira
Coordenadora

A INTRODUÇÃO DA INTELIGÊNCIA ARTIFICIAL NO TRATAMENTO DE DADOS: AS DIFICULDADES DE UM EFETIVO DIREITO À INFORMAÇÃO

Ana Cristina Gouveia *

Resumo: A evolução tecnológica em que vivemos é evidente, galopante e omnipresente. Como tal, o tratamento e processamento de dados por meio da utilização de algoritmos inteligentes, dotados de *machine learning*, sai verdadeiramente potenciado. A sua atuação permite a tomada de decisões automatizadas, sem qualquer tipo de intervenção humana, donde, o impacto na vida do cidadão não só se evidencia variadas vezes significativo, como, até, lesivo, sendo fonte de restrição de bens e serviços aos mais diversos níveis da saúde, do emprego, do crédito, entre tantos outros.

Perante estas situações, partindo do basilar princípio da transparência, e como forma de assegurar a posição do titular dos dados, o Regulamento Geral sobre a Proteção de Dados atribui àquele um conjunto particular de direitos, nomeadamente, o direito à informação. A grande questão que aqui se coloca é de saber qual o particular conteúdo deste direito perante decisões que se evidenciam com um baixo grau de explicabilidade, dada a particular e controversa opacidade de que esta tecnologia é dotada. Desta feita, o presente trabalho visa indagar sobre se se tratará de um mero e simples direito a uma explicação genérica, ou, pelo

* Advogada. Licenciada em Direito pela Escola de Direito da Universidade do Minho e Mestre em Direito Transnacional da Empresa e das Tecnologias Digitais, pela mesma Instituição, em parceria com a Universidade de Santiago de Compostela no âmbito do projeto UNISF (Universidade sem Fronteiras). E-mail: *pg49596@alunos.uminho.pt*

contrário, um verdadeiro direito a uma explicação específica sobre os motivos subjacentes à concreta decisão tomada pela Inteligência Artificial.

Palavras-chave: Decisões individuais automatizadas; Direito à explicação; Inteligência Artificial.

Abstract: The technological evolution we are living in is evident, fast, and omnipresent. As such, the treatment and processing of data through the use of intelligent algorithms, endowed with machine learning, is truly enhanced. Their operation allows for automated decision-making, without any human intervention, which impacts significantly the citizens' lives and may be harmful, by restricting access to goods and services at the most different levels of healthcare, employment, credit, among many others.
In response to these situations, based on the fundamental principle of transparency, and as a way of ensuring the position of the data subject, the General Regulation on Data Protection grants a specific set of rights, namely the right to information. The key question that arises here is to determine the exact content of this right when facing decisions with a low degree of explainability, given the particular and controversial opacity of this technology. In this context, the present work aims to inquire if it is a simple right to a general explanation or, on the contrary, a true right to a specific explanation about the underlying reasons for the specific Artificial Intelligence decision.

Keywords: Automated individual decision-making; Right to explanation; Artificial Intelligence.

1. Introdução

O célere e constante desenvolvimento da sociedade, conjugado com a ininterrupta e crescente introdução das novas tecnologias digitais, levou-nos à denominada sociedade de informação. Nesta, reina a expressão *informação é poder*, tendo-se verificado, pois, uma drástica transmutação dos valores que a caracterizam. Os dados assumem, agora, uma posição de topo, dizem-se o petróleo do século XXI[1], contudo, para que o devido valor lhes seja atribuído, é imprescindível o seu tratamento. Ora, é precisamente aqui que surgem as novas formas de tratamento automatizado de dados, enquanto manifestação da introdução da Inteligência Artificial (IA), também, neste âmbito. Num mundo em que telemóveis, computadores e *tablets* se interconectam, e onde o acesso à *internet* é generalizado, os dados são constante e instantaneamente fornecidos, pelo que a utilização daquela tecnologia se traduz em ganhos de eficiência, tempo e superação de limites humanos.

[1] Esta ideia reporta-se à expressão "data is the new oil", utilizada por CLIVE HUMBY, em 2006.

Não obstante, a introdução exorbitada desta tecnologia suscita riscos desmesurados para a esfera pessoal dos titulares dos dados, quando sujeitos a decisões tomadas de forma completamente autónoma por aquela. No cerne das preocupações que aqui serão tratadas encontra-se a opacidade por que a atuação da IA se pauta. Característica que impede o acesso e compreensão do porquê do sentido da decisão tomada e, consequentemente, a sua eventual alteração, em caso de erro ou injustiça.

Destarte, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD), já desde 2018 que atribui a estes sujeitos um conjunto vasto de direitos, designadamente, no âmbito daquelas decisões ditas tecnológicas e como forma de assegurar o exercício de outros direitos, o direito à informação. Tal é confirmado por via do princípio da transparência, porém, este é um elemento amplamente ausente dos sistemas de IA. A caracterização dos mesmos como *black boxes* é indicativa dessa opacidade que os descreve. Nestes termos, no presente artigo procurar-se-á determinar o conteúdo concreto que aquele direito assume no âmbito das decisões automatizadas e discutir-se-á a sua aplicabilidade perante um algoritmo inteligente e marcadamente opaco.

2. A aplicação da Inteligência Artificial no tratamento de dados

Desde muito cedo que se encetam esforços cujo objetivo se traduz na atribuição à máquina de características tão típicas do ser humano como o é a sua inteligência. Contudo, se, no início, tal realidade tão-somente se traduzia num sonho meramente alcançável pela criatividade escrita e cinematográfica da ficção científica, e após os primeiros avanços datados da década de 50 se tenha verificado um percurso marcadamente invernoso[2], a verdade é que, ao dia de hoje, a IA diz-se omnipresente. Deixando de ser a exceção e passando a ser a regra, esta nova e disruptiva tecnologia invade cada recanto do quotidiano humano, assumindo de tal modo carácter familiar e vital que, não raras vezes, chega mesmo a ser ausente da consciência humana. Certamente já nos deparamos com um assistente virtual como a *Siri* ou a *OK Google*, um sistema de informação geográfica como o *Google Maps*, ou mesmo um aspirador inteligente e um *robot* de cozinha.

Esta realidade encontra razão de ser por conta da afirmação da tecnologia, e em particular da IA, como sinónimo de simplificação, eficiência, produtividade,

[2] ARLINDO OLIVEIRA, *Inteligência Artificial*, Lisboa, Fundação Francisco Manuel dos Santos, 2019, páginas (pp.) 42-56.

facilitismo e redução de custos[3]. O homem foi substituído pela máquina, cujas capacidades – em determinadas circunstâncias concretas – se demonstram superiores às do primeiro. Afastando-se as tarefas perigosas, entediantes e repetitivas, abriu-se, pois, margem à motivação e à criatividade.

Ora, sendo verdadeiramente difícil o aponte de uma área da sociedade na qual se possa afirmar a ausência desta nova realidade, nem tampouco os algoritmos empregues no âmbito do tratamento de dados escaparam aos "tentáculos da IA"[4] e à sua inerente evolução. Hoje, distanciando-se já a dita IA simbólica – uma IA que partia de lógicas de *se isto, então aquilo*, previamente introduzidas pelo programador –, abraça-se uma IA dotada de *machine learning* ou, dito de outro modo, de aprendizagem automática. Acrescentando-se as características da autonomia e da autoaprendizagem às típicas capacidades de recolha, análise e interpretação de dados dos tradicionais algoritmos, aquela última modalidade ou subgrupo de IA veio-lhes permitir a tomada de decisão da totalidade ou de partes de um conjunto de ações *per se*. Os algoritmos passaram a aprender e a modificar o seu comportamento com base nos dados que recolhem e na experiência que acumulam, conseguindo, assim, alcançar soluções muitas das vezes não antes previstas pelos responsáveis pela sua criação.

Nestes termos, passando a intervenção humana a verificar-se, não no plano de ação – o programador deixou de dizer à máquina como se comportar, através de comandos e regras específicas e bem definidas –, mas apenas e tão-somente num plano inicial, com a introdução do maior número de dados possíveis, a partir dos quais o algoritmo, identificando relações, padrões e semelhanças, define as suas próprias regras, desenvolve-se e melhora o seu desempenho, torna-se inevitável a afirmação de que a IA veio indubitavelmente contribuir para este que é o mundo dos dados como o encontramos hodiernamente: um mercado regido pela celeridade, personalização e precisão[5].

---

[3] LEANDRA DIAS, «A Inteligência Artificial como facilitador da conformidade demonstrada à luz do RGPD – oportunidades e desafios», in JOANA COVELO DE ABREU, LARRISSA COELHO, TIAGO SÉRGIO CABRAL (coordenação) (coord.), *O Contencioso da União Europeia e a cobrança transfronteiriça de créditos: compreendendo as soluções digitais à luz do paradigma da Justiça eletrónica europeia (e-Justice)*, Volume (Vol.) III, Braga, Pensamento Sábio – Associação para o conhecimento e inovação, Universidade do Minho, 2022, p. 74 (pp. 73-86), disponível em https://repositorium.sdum.uminho.pt/handle/1822/77932 [consultado em 15/07/2024].

[4] INÊS CAMARINHA LOPES, «Inteligência Artificial e proteção de dados pessoais: a "ditadura" do algoritmo», in MARIA RAQUEL GUIMARÃES, RUTE TEIXEIRA PEDRO (coord.), *Direito e Inteligência Artificial*, Coimbra, Almedina, 2023, p. 558 (pp. 556-572).

[5] FINALE DOSHI-VELEZ e outros (*et al.*), «Accountability of AI under the law: the role of explanation», *Berkman Klein Center Working Group on Explanation and the Law*, 2017, p. 1 (pp. 1-21), disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064761 [consultado em 08/07/2024].

3. As decisões individuais automatizadas

O atual quadro regulatório no âmbito da temática da proteção de dados e da sua concretização enquanto direto fundamental, tal como consagrado no artigo 8.º da Carta dos Direitos Fundamentais, é marcado pelo RGPD. Substituto da anterior Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995, e estando vigente desde 25 de maio de 2018, este surgiu com um propósito duplo. Por um lado, garantir um maior controlo dos dados por parte das pessoas singulares, assim tutelando o direito à proteção de dados e à autodeterminação informativa – objetivo jusfundamental –, por outro lado, caucionar a livre circulação daqueles – objetivo económico[6].

Sendo certo que "[é] comum a acusação de que o Direito não consegue acompanhar a realidade, em particular o ritmo da evolução tecnológica"[7], mas que na origem do regime geral da proteção de dados se encontra, desde logo, o objetivo de prevenir os riscos caucionados pelo tratamento de dados pessoais resultante dos avanços tecnológicos[8], o nosso objeto de estudo impõe, como primeira questão a de saber se, e em que circunstâncias, as particulares atividades da IA estarão abrangidas e reguladas por aquele diploma.

Ora, bem sabendo que o tratamento automatizado de dados e as inerentes decisões individuais automatizadas[9] – decisões tomadas por meios tecnológicos e em cuja intervenção humana se vê apartada – são um dos principais resultados da introdução da IA no âmbito do tratamento de dados, resposta a esta questão encontramos, desde logo, e num primeiro momento, no número (n.º) 1 do artigo 2.º Aqui pode ler-se que "[o] presente regulamento [se] aplica [...] ao tratamento de dados pessoais por meios total ou parcialmente automatizados". Por outro lado, importa igualmente chamar à colação o artigo 22.º do mesmo diploma. Se aquele primeiro nos responde afirmativamente à questão *supra* colocada, este segundo consagra, especificamente, um regime a atender e aplicar àqueles particulares casos. Esta resposta não podia deixar de ser. Como nos ensina GRAÇA CANTO MONIZ, o RGPD, enquanto regime geral e transversal,

---

[6] Cfr. artigo 1.º e considerandos 7 e 10 do RGPD, bem como GRAÇA CANTO MONIZ, *Manual de Introdução à Protecção de Dados Pessoais*, Coimbra, Almedina, 2023, pp. 13-17.

[7] FILIPA URBANO CALVÃO, *Direito da Proteção de Dados Pessoais: Relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina*, Porto, Universidade Católica Editora, 2018, p. 23.

[8] GLORIA GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht, Springer, 2014, p. 75.

[9] A. BARRETO MENEZES CORDEIRO, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021, p. 221.

"regula os tratamentos de dados pessoais independentemente [...] da tecnologia em causa"[10].

Debruçando-nos sobre aquele último preceito, dispõe o mesmo que "[o] titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis"[11]. Encontramos, pois, conforme veio clarificar o Tribunal de Justiça da União Europeia (TJUE), e pese embora a discussão que sobre a norma se colocava acerca da presença de um princípio geral ou, pelo invés, um direito cujo exercício dependesse da vontade e invocação pelo seu titular, uma geral proibição de tais decisões[12]. E isto por conta dos malefícios que das mesmas podem derivar. Estando em causa a atuação de máquinas, parte-se do princípio de que as mesmas, uma vez desprovidas de emoções, ao contrário do ser humano, serão isentas de juízos discriminatórios e parciais. Todavia, longe de ser neutros e objetivos, os algoritmos são concebidos e construídos pelo ser humano, pelo que, tal como este, e enquanto sua extensão e reflexão, não isentos de imperfeição. Se os dados fornecidos, ainda que de forma não intencional, forem insuficientes a uma atuação exemplar – dados imprecisos ou com grupos sub- ou sobre-representados –, ou se contiverem algum tipo de estereótipo – origem étnica ou racial, opinião política, orientação sexual, religiosa, situação económica, género, entre outros[13] –, o algoritmo certamente o irá identificar, extrair e replicar nos seus resultados[14].

---

[10] GRAÇA CANTO MONIZ, *Manual de Introdução à Protecção de Dados Pessoais*, obra citada (*op. cit.*), p. 44 e, no mesmo sentido, DANIEL J. SOLOVE, PAUL M. SCHWARTZ, *Information Privacy Law*, Austin, Wolters Kluwer, 2009, p. 1.

[11] Importa ter em conta que decisões automatizadas e definição de perfis não são conceitos sinónimos. Pese embora as decisões automatizadas sejam algo recorrente na definição de perfis e, por esse motivo, estejam sujeitas ao mesmo regime, têm um âmbito de aplicação distinto, podendo sobrepor-se às segundas ou delas resultar. Conforme (cfr.) MARIA RAQUEL GUIMARÃES, «Inteligência Artificial, Profiling e Direitos de Personalidade», in EVA SÓNIA MOREIRA DA SILVA, PEDRO MIGUEL FREITAS (coord.), *Inteligência Artificial e Robótica: Desafios para o Direito do Século XXI,* Coimbra, Gestlegal, 2022, p. 208 (pp. 187-211).

[12] Esta posição vinha a ser a adotada pela doutrina maioritária, contudo, a 7 de dezembro de 2023, o TJUE veio sufragá-la, assim terminando com um dos maiores debates que em torno de uma redação ambígua se colocavam. Cfr. Proc. C-643/21, Land Hessen contra Schufa Holding AG, §52-53, disponível em https://curia.europa.eu [consultado em 13/08/2024].

[13] Cfr. considerando 71 *in fine*.

[14] ANA FRAZÃO, CARLOS GOETTENAUER, «Black Box e o Direito face à opacidade algorítmica», in MAFALDA MIRANDA BARBOSA *et al.* (coord.), *Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa*, São Paulo, Editora Foco, 2021, p. 29 (pp. 27-42).

De facto, vivemos um período dito de "ditadura do algoritmo"[15], "[o]s sistemas automatizados permitem hoje criar perfis e categorizar os indivíduos em níveis de alto ou baixo risco em matéria de saúde, crédito, emprego, classificá-los como potenciais infratores ou mesmo como potenciais criminosos ou terroristas"[16]. Tendo tais atividades impacto significativo na "passagem de fronteiras, no acesso à segurança social, na assistência médica, na entrada em estabelecimentos de ensino, etc."[17], facilmente redundam na restrição e negação de bens e serviços, ou mesmo discriminações infundadas e ilegítimas[18].

Por conta deste cenário, a regra é, portanto, a da proibição de todas aquelas decisões que hajam sido tomadas com base exclusiva no tratamento automatizado, quando tal se traduza na produção de "efeitos na esfera jurídica" do titular dos dados "ou que o afete significativamente de forma similar"[19]. De notar que, pese embora a utilização do termo "exclusivamente" induza numa intenção clara por parte do legislador de restrição do campo de aplicação da norma, sempre se deverá exigir que o seu afastamento não se baste com uma mera, nominal e

---

[15] INÊS CAMARINHA LOPES, «Inteligência Artificial e proteção de dados pessoais: a "ditadura" do algoritmo», *op. cit.*, p. 571.

[16] GABRIELA CALDAS, «O direito à explicação no Regulamento Geral sobre a Proteção de Dados», in FRANCISCO PEREIRA COUTINHO, GRAÇA CANTO MONIZ (coord.), *Anuário da Proteção de Dados*, Lisboa, CEDIS – Centro de I&D sobre Direito e Sociedade, 2019, p. 46 (pp. 37-54), disponível em https://cedis.novalaw.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf [consultado em 23/07/2024].

[17] *Ibidem.*

[18] No mesmo sentido ALESSANDRA SILVEIRA, «Pistas de reflexão sobre dados inferidos à luz da jurisprudência do TJUE», in JOANA COVELO DE ABREU, LARRISSA COELHO, TIAGO SÉRGIO CABRAL (coord.), *O Contencioso da União Europeia e a cobrança transfronteiriça de créditos…*, *op. cit.*, p. 11 (pp. 10-20), disponível em https://repositorium.sdum.uminho.pt/handle/1822/77932 [consultado em 15/07/2024].

[19] Sendo, em ambos os casos, basilar a presença de um impacto grave no titular dos dados, o primeiro ocorrerá quando houver lugar à constituição, modificação ou extinção de relações jurídicas; quando resultar na afetação dos pressupostos para o exercício de um direito; ou quando se verificar a lesão de um direito alheio ou de uma faculdade jurídica primária. Já o segundo caso, concedendo ao preceito um âmbito amplo, verificar-se-á quando não haja lugar à afetação de direitos ou obrigações do titular dos dados, mas a decisão, ainda assim, detenha um impacto de tal modo suficiente na esfera deste que justifique a aplicação do regime em questão, porque lesado um interesse digno de proteção no âmbito da tutela da proteção de dados. Isto acontecerá quando a decisão afete o comportamento ou as escolhas do cidadão titular dos dados; origine a exclusão ou discriminação de pessoas; ou tenha impacto prolongado ou permanente naquele. Cfr. SANDRA BARBOSA, SARA FÉLIX, «Algorithms and the GDPR: An analysis of article 22», in FRANCISCO PEREIRA COUTINHO, GRAÇA CANTO MONIZ (coord.), *Anuário da Proteção de Dados*, Lisboa, CEDIS – Centro de I&D sobre Direito e Sociedade, 2021, p. 75 (pp. 67-93), disponível em https://protecaodedadosue.cedis.fd.unl.pt/anuario-edicao-2021/ [consultado em 23/07/2024], e Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (GT29), *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*, de 3 de outubro de 2017, p. 23, disponível em https://www.ua.pt/file/53846 [consultado em 09/08/2024].

simbólica intervenção humana, mas sempre uma intervenção humana relevante e significativa, sob pena de desvirtuamento do preceito[20]. De facto, a intervenção humana, frequentemente, se verifica, mais não seja na aplicação dos resultados à situação concreta, basta pensar num mecanismo de pontuação de solvabilidade utilizado por um banco. Neste caso, o algoritmo, com base nos dados recolhidos e na sua análise, atribui ao cliente uma pontuação específica, após o que, e com base nesta, o banco toma a sua decisão de atribuir ou não o crédito respetivo. Dúvidas não existem de que, aqui, a decisão é formalmente tomada por um ser humano, contudo, originada a partir de uma operação automatizada cujo resultado não foi avaliado antes de ser formalizado e traduzido enquanto decisão final.

O que está em causa deverá ser, sempre, um critério material e não meramente formal[21], assim obstando a situações de abuso da letra da lei pelo fabrico de uma intervenção humana que, meramente confirmadora e acrítica da decisão sugerida pela máquina, sustaria como único intuito o afastamento da proibição consagrada[22].

Não obstante este cenário, bem sabendo não existirem regras absolutas, nem mesmo o artigo 22.º se desvanece deste dogma, apresentando o n.º 2 um conjunto de três casos para os quais, excecional e taxativamente, as decisões individuais automatizadas são permitidas.

A primeira exceção verifica-se quando a tomada de decisão exclusivamente automatizada seja necessária para a celebração – aqui se incluindo a formação[23] –, ou execução de um contrato, em que sejam partes o titular dos dados e o responsável pelo tratamento. Aquilo que se exige é uma conexão direta entre o tratamento e os fins concretos do contrato, ou porque do próprio resulta a obrigação de tratamento, ou porque este se evidencia necessário para a sua preparação ou conclusão. Para que a exceção possa operar, caberá ao responsável fazer prova do critério da necessidade pela demonstração, por um lado, de que o meio automatizado é adequado ao alcance dos fins e objetivos do contrato[24] e, por outro lado, de que inexiste um outro meio que, igualmente eficaz, seja menos intrusivo

[20] O GT29, *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*, *op. cit*., p. 23, estabelece um exemplo onde facilmente compreendemos quando é que a intervenção humana é relevante: "Um processo automatizado gera, na prática, uma recomendação relativa a um titular de dados. Se um ser humano examinar e ponderar outros fatores ao tomar a decisão final, esta não será «tomada exclusivamente com base» no tratamento automatizado".

[21] Cfr. A. BARRETO MENEZES CORDEIRO, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, *op. cit.*, p. 224.

[22] *Ibidem.*

[23] *Ibidem*, p. 226.

[24] GRAÇA CANTO MONIZ, *Manual de Introdução à Protecção de Dados Pessoais, op. cit.*, p. 84.

para a privacidade, sendo certo que, conveniência ou vantajosidade, devido a uma maior eficiência ou menores custos não deverão ser considerados[25].

A segunda exceção, por seu turno, operará sempre que a decisão automatizada esteja autorizada pelo direito da União Europeia (UE) ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, nomeadamente, para fins de "controlo e prevenção de fraudes e da evasão fiscal [...] e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento"[26]. Exige-se, portanto, que exista uma prévia, expressa e permissiva disposição legal. Não obstante, e para que aquela normativa, a existir, opere, na mesma igualmente têm de estar previstas medidas adequadas à salvaguarda dos direitos, liberdades e legítimos interesses do titular dos dados, sobre as quais o n.º 3 dá pistas quanto ao seu âmbito: além da prestação de informações, o direito a obter intervenção humana, manifestar a sua opinião e contestar a decisão.

Por último, a decisão exclusivamente automatizada será permitida quando seja baseada no consentimento do titular dos dados, se este se verificar explícito. Exige-se, pois, um consentimento mais exigente que o previsto no artigo 6.º, n.º 1, alínea a), pois que não se basta com uma "manifestação de vontade livre, especificada [e] informada"[27], mas, igualmente, explícita, ou seja, expressa, por oposição àquelas manifestações que, implícitas ou inferidas de certos comportamentos, especificamente aqui, e ao contrário da regra geral, não serão suficientes[28].

As alíneas a) e c) do n.º 2 do artigo 22.º compõem, portanto, duas situações de licitude do tratamento referenciadas nas alíneas a) e b) do n.º 1 do artigo 6.º, ao passo que a alínea b) estipula uma "cláusula aberta"[29] que permite reprimir o princípio geral, quando se verifique uma norma permissiva nesse sentido. Neste último caso, e para que a exceção opere, exige-se, como se disse,

---

[25] INÊS DA SILVA COSTA, «A proteção da pessoa na era dos *big data*: a opacidade do algoritmo e as decisões automatizadas», *Revista Eletrónica de Direito*, Vol. 24, n.º 1, 2021, p. 62 (pp. 33-82), disponível em https://cij.up. pt/pt/red/edicoes-anteriores/2021-nordm-1/a-protecao-da-pessoa-na-era-dos-big-data-a-opacidade-do-algoritmo-e-as-decisoes-automatizadas/ [consultado em 08/07/2024].

[26] Considerando 71 do RGPD.

[27] *Ibidem*, artigo 4.º, n.º 1.

[28] Note-se que a versão portuguesa do artigo 4.º, n.º 1, contém a expressão "explícita", contudo, atendendo às longas discussões que na fase de aprovação legislativa do diploma se verificaram e que culminaram na decisão do afastamento daquela referência e, por outro lado, à referência única nesta versão, a doutrina tem vindo a afirmá-la como erro de tradução que, enquanto tal, não deve ser considerado. Cfr. A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019*, *op. cit.*, pp. 184 e 240, e GRAÇA CANTO MONIZ, *Manual de Introdução à Protecção de Dados Pessoais*, *op. cit*., pp. 80-30.

[29] A. BARRETO MENEZES CORDEIRO, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, *op. cit.*, pp. 223 e 226.

que tal norma permissiva tenha sido estabelecida ao lado das devidas salvaguardadas. Da mesma forma, e com igual intuito, no caso das duas primeiras, é o próprio RGPD que estipula e replica estas salvaguardas. Particularmente nestes casos, e como meio de salvaguardar o objetivo de proteção e preservação dos direitos e liberdades dos cidadãos – objetivo que, como explanamos *supra*, assenta no princípio geral de proibição –, ao titular dos dados é conferida uma tríade de distintos direitos: direito de obter intervenção humana; manifestar o seu ponto de vista; e contestar a decisão.

Para que haja lugar ao exercício efetivo de um qualquer destes direitos, é condição indispensável, todavia, que o titular dos dados se encontre na posse de um conjunto de informações mínimas, quer sobre a presença de tais decisões, quer sobre o seu conteúdo e fundamentos, aditando-se, deste modo, a estes diversos direitos, e como condição indispensável ao seu exercício, o intitulado direito à informação[30].

4. O direito à informação

O direito à informação, desiderato aclamado pela doutrina como um dos mais importantes direitos consagrados pelo RGPD[31], surge, no âmbito deste diploma, como manifestação e corolário de um dos princípios fundamentais que o iluminam e suportam: o princípio da transparência[32].

A sua consagração vê-se, contudo, ausente de previsão expressa e clara. Não encontramos, no diploma, um artigo especificamente dedicado à temática, mas, pelo contrário, um acervo vasto de disposições, o que lhe confere um conteúdo amplo e diversificado. Presente nos artigos 13.º, 14.º e 15.º, bem como nos considerandos 60, 63 e 71, o direito à informação engloba, entre outras informações, a informação acerca da identidade e contactos do responsável pelo

---

[30] JOEL A. ALVES, *O Novo Modelo de Proteção de Dados Pessoais Europeu*, Coimbra, Almedina, 2021, p. 58.

[31] Neste sentido, entre tantos, ALESSANDRA SILVEIRA, JOANA COVELO ABREU, TIAGO SÉRGIO CABRAL, «Breves apontamentos quanto aos direitos dos titulares de dados no RGPD», in *Direito à Informação Administrativa e Proteção de Dados Pessoais*, E-book do Centro de Estudos Judiciários, Coleção Formação Contínua – Jurisdição Administrativa e Fiscal, Lisboa, 2021, p. 94 (pp. 93-111), disponível em file:///Users/cristinagouveia/Downloads/ssrn-3962947.pdf [consultado em 20/08/2024].

[32] Plasmado no artigo 5.º do RGPD, bem como nos artigos 11.º, n.º 2, e 15.º do Tratado da União Europeia e do Tratado sobre o Funcionamento da União Europeia, o princípio da transparência impõe-se como vetor orientador em matéria de proteção de dados e garante, no seio da própria União, da confiança dos cidadãos que se pretende construir. No seio da Ordem Jurídica Interna manifesta-se e encontra presença no n.º 1 do artigo 9.º da Carta Portuguesa de Direitos Humanos na Era Digital.

tratamento dos dados, as finalidades e fundamento jurídico deste, o prazo de conservação, categoria e destinatários dos dados em questão.

Pese embora tal amplitude, perante técnicas de tratamento de dados por meio da IA, o direito à informação vê-se particularmente exigente. Passando a intervenção do ser humano a restringir-se a um momento inicial, com a introdução de dados e definição de objetivos, são cognoscíveis os dados pessoais iniciais – *inputs* – e os resultados obtidos – *outputs.* Porém, explicar a forma como a tecnologia, a partir dos primeiros, chegou aos segundos, o raciocínio a este curso subjacente, bem como a combinação de fatores de entrada preponderante, constitui uma questão deveras distinta e cuja dificuldade se atribui ao denominado efeito *black box*[33], próprio dos algoritmos.

A máquina passa a atuar com base em deduções de axiomas e regras de inferência[34] muitas das vezes invisíveis *a priori* de forma direta, mas tão-somente de forma indireta por meio da experimentação e análise posterior de um número imenso de dados, processados por um sistema imerso num número imenso de passos.

Destarte, quanto mais avançada é a tecnologia, mais difícil é a sua compreensão[35], porquanto, se, por um lado, a regressão absoluta se evidencia praticamente impossível[36], por outro lado, se alcançada, demonstra-se difícil a tradução

---

[33] A doutrina tem vindo a afirmar que a opacidade surge a três níveis distintos: opacidade cognitiva; opacidade corporativa; e opacidade técnica. A primeira impõe-se para a sociedade em geral, por conta do contraste entre a complexidade da tecnologia inerente à IA e aos algoritmos inteligentes e a ausência de conhecimentos técnicos e científicos necessários à compreensão do seu funcionamento. A segunda nasce da intensão do seu próprio criador, programador, proprietário ou responsável pelo tratamento, como forma de garantir a sua propriedade intelectual e industrial. A terceira revela as dificuldades enfrentadas por estes agentes, tal é a discrepância entre aquilo que são os modelos matemáticos gerados pela IA e as capacidades de raciocínio humano. Cfr. MIQUEL MARTÍN-CASALS, «An approach to some EU initiatives on the regulation of liability for damage caused by AI-Systems», *Revista Ius et Praxis*, Ano 28, n.º 2, 2022, p. 7 (pp. 3-24), disponível em https://www.scielo.cl/scielo.php?pid=S0718-00122022000200003&script=sci_abstract&tlng=en [consultado em 10/07/2024], e JENNA BURRELL, «How the machine 'thinks': Understanding opacity in machine learning algorithms», *Big data & Society,* 2016, pp. 3-5 (pp. 1-12), disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2660674 [consultado em 16/08/2024].

[34] STEVEN S GOUVEIA, «O Problema da Lacuna da Responsabilidade na Inteligência Artificial», in MANUEL CURADO, ANA ELISABETE FERREIRA, ANDRÉ DIAS PEREIRA (coord.), *Vanguardas da Responsabilidade: Direito, Neurociências e Inteligência Artificial*, sem local (s.l.), Petroni, 2019, p. 176 (pp. 171-184).

[35] BEATRIZ SANTIAGO TRINDADE, «Two years in: does the GDPR already need updates? A question brought by algorithmic decision-making», in FRANCISCO PEREIRA COUTINHO, GRAÇA CANTO MONIZ (coord.), *Anuário da Proteção de Dados*, Lisboa, CEDIS – Centro de I&D sobre Direito e Sociedade, 2020, p. 91 (pp. 79-104), disponível em https://protecaodedadosue.cedis.fd.unl.pt/edicao-2020/ [consultado em 12/08/2024].

[36] ANA FRAZÃO, CARLOS GOETTENAUER, «Black Box e o Direito face à opacidade algorítmica», *op. cit.*, p. 31.

de uma linguagem matemática para uma linguagem percetível e inteligível pelos sujeitos[37].

Nestes termos, manifestando-se os tradicionais remédios à data consagrados notoriamente insuficientes, como forma de acautelar a concretização, não só dos riscos inerentes à desigualdade de informação, como de outros que, nesta particular área se assomam – pense-se na perda de controlo dos próprios dados pessoais, na limitação de direitos, nos riscos de discriminação, de roubo ou usurpação de identidade, ou mesmo a perda de confidencialidade[38] –, o legislador europeu acabou por atribuir a este direito um conteúdo específico quando perante um tratamento automatizado. Ao titular dos dados acrescerá o direito ao conhecimento da verificação da decisão automatizada; de obtenção de informações úteis relativas à lógica subjacente a esta; a sua respetiva importância; e consequências previstas[39].

Ora, o cumprimento prático, em geral, de todas estas concretizações demonstra dificuldades perante os desafios convocados pela IA. Todavia, a segunda delas destaca-se manifestamente frente às restantes, porquanto impõe, dada a técnica legislativa adotada, exigências prévias e acrescidas quanto à sua interpretação. O legislador europeu, recorrendo a conceitos indeterminados – lógica subjacente e informações úteis –, não estipulou as suas definições no artigo 4.º, fazendo recair, assim, sobre a própria doutrina e jurisprudência o árduo papel da sua concretização, perante uma realidade complexa.

4.1. O conceito de lógica subjacente

No que concerne à concretização do conceito de lógica subjacente, diante de um tratamento de dados levado a cabo por um algoritmo dotado de IA, a doutrina tem vindo a afirmar tratar-se de um conceito matemático, traduzido em termos puramente informáticos[40]. Como tal, é lugar comum o equacionar da facilitação ao titular dos dados, das árvores de decisão, dos critérios de classificação, bem como das predefinições do algoritmo.

---

[37] FRANCISCA CARDOSO RESENDE GOMES, «O conteúdo do direito fundamental à proteção de dados à luz do novo Regulamento Geral de Proteção de Dados: em especial, a problemática do controlo das decisões automatizadas», *op. cit.*, p. 117.

[38] Cfr. considerando 85 do RGPD.

[39] No mesmo sentido dispõe o n.º 2 do artigo 9.º da Carta Portuguesa de Direitos Humanos na Era Digital.

[40] GIOANCLAUDIO MALGIERI, GIOVANNI COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», *International Data Privacy Law*, Vol. 7, n.º 4, 2017, p. 24 (pp. 1-36), disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3088976 [consultado em 29/07/2024].

Não obstante, igual consenso não se verifica quanto à disponibilização, neste âmbito, do seu código-fonte, desde logo e por conta do disposto no considerando 63 do RGPD. Menciona este que o cumprimento do direito à informação sempre deve ter em conta e ser efetuado de forma compatibilizada e equilibrada com os direitos e liberdades de terceiros, tais como segredos comerciais, propriedade intelectual e direitos de autor.

Pois bem, sendo certo que, por um lado, e em abstrato, a disponibilização do código-fonte de um algoritmo é causa direta e adequada à lesão efetiva daqueles direitos e, assim, perentoriamente, fonte de restrição do direito à informação – trata-se, nas palavras de JENNA BURREL, de uma opacidade legal[41], imposta pela própria letra da lei – e que, por outro lado, esta é uma ideia sufragada única e exclusivamente num considerando do diploma, será razoável a aplicação prática de tal restrição?

Ora, ainda que existam autores que prontamente respondem em sentido negativo[42], não nos conseguimos rever na mesma posição. É verdade que os considerandos de um diploma não se encontram no mesmo patamar de vinculatividade dos artigos que o próprio compõem. Todavia, acompanham-no e auxiliam na sua aplicação e interpretação, permitem a retirada da intenção do legislador e dos objetivos do diploma[43]. Donde, parecendo-nos clara a ponderação que ambos, aos direitos de terceiro, pretenderam atribuir, não nos

[41] JENNA BURRELL, «How the machine 'thinks': Understanding opacity in machine learning algorithms», *op. cit.*, pp. 4-5.

[42] É o caso de ALESSANDRA SILVEIRA, JOANA COVELO ABREU, TIAGO SÉRGIO CABRAL, «Breves apontamentos quanto aos direitos dos titulares de dados no RGPD», *op. cit.*, p. 100, e GIOANCLAUDIO MALGIERI, GIOVANNI COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», *op. cit.*, p. 31.

[43] Neste sentido vem indicando o TJUE em variados acórdãos. A título exemplificativo, *vide* o acórdão de 13 julho de 1989, Processo 215/88, Casa Fleischhandels-GmbH, §31; o acórdão de 7 de fevereiro de 2018, Proc. C-643/16, American Express Company, contra The Lords Commissioners of Her Majesty's Treasury, § 51; e o acórdão de 11 de junho de 2009, Proc. C-429/07, Inspecteur van de Belastingdienst contra X BV, §31. Todos disponíveis em https://curia.europa.eu [consultados em 29/07/2024].

apraz outra conclusão se não a de que os mesmos não deverão ser, sem mais, totalmente desconsiderados[44].

Em todo o caso, também não se demonstra razoável uma interpretação que considere que todo e qualquer direito de terceiro é fonte suficiente, *per se*, de uma total exclusão do direito à informação, sob pena de tal mecanismo jurídico funcionar, paradoxalmente, como instrumento que torna a caixa ainda mais negra e fechada. Pelo contrário, sempre se deverá verificar um juízo de ponderação e adequação casuístico que permita aferir, no caso em concreto, e de forma específica, quais as informações que afetam e quais aquelas que não afetam estes direitos, garantindo-se, invariavelmente, a disponibilização das segundas. O próprio considerando sufraga esta posição, onerando o responsável pelo tratamento com a necessidade de encontro de uma forma de fornecer a informação a que o titular dos dados tem direito, sem colocar os restantes bens jurídicos relevantes em cheque.

Ultrapassada esta questão, importa atender ao disposto nos considerandos 39 e 58, bem como ao artigo 12.º. Todos estes impõem que a informação seja prestada de forma transparente, inteligível, de fácil acesso e compreensão e em linguagem simples e clara. Para o efeito, dever-se-á utilizar como referência o critério do homem médio, a sua instrução e capacidades de entendimento.

Ora, a população, em geral, caracteriza-se pela iliteracia digital. Uma pessoa média, em regra, não detém o tempo, os recursos e os conhecimentos técnicos e científicos necessários à compreensão do código de um algoritmo, o qual, pautado pela complexidade, não se basta com um mero e geral conhecimento

[44] Com semelhante opinião LUCIANO FLORIDI, SANDRA WACHTER, BRENT MITTELSTADT, «Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation», *International Data Privacy Law*, Vol. 7, n.º 2, 2017, p. 90 (pp. 76-99), disponível em https://academic.oup. com/idpl/article/7/2/76/3860948 [consultado em 05/07/2024]; ANDREW D. SELBST, JULIA POWLES, «Meaningful Information and the Right to Explanation», *International Data Privacy Law*, Vol. 7, n.º 4, 2017, p. 242 (pp. 233-242), disponível em https://academic.oup. com/idpl/article/7/4/233/4762325 [consultado em 05/07/2024]; e LILIAN EDWARDS, MICHAEL VEALE, «Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for», *Duke Law & Technology Review*, n.º 1, 2017, p. 81 (pp. 18--84), disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855 [consultado em 13/07/2024].

informático para que haja lugar à compreensão do seu funcionamento, do procedimento da tomada de decisão e do seu mérito[45]/[46].

Daqui decorre que, ainda que se opte por considerar que os direitos de terceiro não figuram como obstáculo à disponibilização do código-fonte para efeitos de concretização do direito à informação, sempre figurará a carência de capacidades informáticas do cidadão médio, a menos, claro, que tal disponibilização seja acompanhada de uma descrição do algoritmo em linguagem naturalmente compreensível a qualquer pessoa[47] – circunstâncias que, como demonstramos *supra*, se assume verdadeiramente difícil.

Em poucas palavras, a informação tem de ser prestada e tem de ser prestada de modo que o seu recetor a possa entender, sob pena de, e por mais poderosa que a ferramenta equacionada seja, a sua disponibilização se demonstre inútil. Transparência e compreensibilidade devem demonstrar-se indissociáveis[48].

Por último, quanto a este ponto, importa ainda destacar que, de igual modo, em caso algum será viável a divulgação de todos os fatores tidos em consideração numa decisão individual automatizada, mas antes e apenas aqueles considerados importantes, significativos e relevantes para a tomada de decisão concreta e o funcionamento do sistema que permitiu o culminar naquela[49]. Isto, sempre de forma eficiente e, ainda que simples e não complexa, detalhada, completa e suficiente para a compreensão da decisão. Inundar o titular dos dados com informações desnecessárias ou inúteis pode mesmo figurar, antagonicamente, como veículo de obscuridade que cria uma falácia de transparência.

---

[45] A Comissão Europeia destaca que para a construção de uma IA de confiança se deverá atender a todas as partes interessadas, donde, e para o alcance de tal desiderato, realça que se deve promover uma "literacia básica no domínio da IA em toda a sociedade". Cfr. COMISSÃO EUROPEIA, *Comunicado da Comissão ao Parlamento Europeu e ao Conselho: Segundo relatório sobre a aplicação do Regulamento Geral sobre a Proteção de Dados*, 2018, p. 28, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=COM:2024:357:FIN [consultado em 23/08/2024], e considerando 20 do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024 (Regulamento IA).

[46] LILIAN EDWARDS, MICHAEL VEALE, «Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for», *op. cit.*, p. 67.

[47] LORENZO COTINO HUESO, «Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida», *Revista Española de la Transparencia*, n.º 16, 2023, p. 38 (pp. 17-63), disponível em https://revistatransparencia.com/ojs/index.php/ret/article/view/272 [consultado em 23/08/2024].

[48] GIOANCLAUDIO MALGIERI, GIOVANNI COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», *op. cit.*, p. 4.

[49] ALESSANDRA SILVEIRA, JOANA COVELO ABREU, TIAGO SÉRGIO CABRAL, «Breves apontamentos quanto aos direitos dos titulares de dados no RGPD», *op. cit.*, pp. 94 e 101.

4.2. O conceito de informações úteis

No que respeita ao conceito de informações úteis, importa desde já aditar que o legislador se demonstrou particularmente aquém do figurado enquanto necessário para este campo. Dizemos isto de forma tão assertiva por dois motivos distintos: se, por um lado, o legislador não atribuiu uma definição para aquele termo, por outro lado, tampouco estabeleceu um elenco – ainda que meramente exemplificativo – de informações que, ali enquadráveis, permitissem a retirada da *ratio* efetivamente pretendida. Como resultado, deixando a concretização do conceito nas mãos do responsável pelo tratamento, de acordo com aquilo que são as suas experiências, conhecimentos e, até, interesses e conveniências, acabou, inevitavelmente, por abrir margem à subjetividade e subsequente variação casuística.

Assim, considerar-se-ão aqui enquadráveis informações específicas quanto ao caso em concreto ou, pelo contrário, somente informações gerais e abstratas?

Pois bem, não adotando o RGPD uma posição clara, também a doutrina se viu ausente de homogeneidade quanto ao conteúdo a atribuir ao direito à informação, de acordo com aquela que é a interpretação adotada do conceito de informações úteis.

Num dos polos, e acolhendo a primeira posição, encontramos, desde logo, BRYCE GOODMAN e SETH FLAXMAN. Baseando-se na indispensabilidade de informações específicas sobre a concreta decisão para um exercício pleno e efetivo do direito a contestar previsto no artigo 22.º, n.º 3, estes Autores vêm defender a consagração no RGPD de, mais do que um qualquer direito à informação, um verdadeiro direito à explicação da decisão, por meio de informações concretas, específicas e precisas. Como forma de sustento, pese embora num momento inicial tenham chamado à colação a expressão "obter uma explicação" do considerando 71, atualmente veem na concretização individualizada das salvaguardas do artigo 22.º levada a cabo pelos artigos 13.º, 14.º e 15.º o fundamento jurídico da posição que adotam[50].

No polo oposto da doutrina, e com uma posição particularmente interessante, encontramos SANDRA WACHTER, BRENT MITTELSTADT e LUCIANO FLORIDI. Dizemos isto porque estes Autores começam, efetivamente, por afirmar a relevância da posição que de imediato acabamos de identificar,

[50] BRICE GOODMAN, SETH FLAXMAN, «European Union regulations on algorithmic decision-making and a «right to explanation», *AI Magazine*, Vol. 38, n.º 3, 2017, pp. 1-2 (pp. 1-9), disponível em https://arxiv.org/abs/1606.08813 [consultado em 03/08/2024]. Com o mesmo entendimento, ANDREW D. SELBST, JULIA POWLES, «Meaningful Information and the Right to Explanation», *op. cit*., p. 236, e MARGOT E. KAMINSKI, «The Right to Explanation, Explained», *op. cit.*, pp. 204 e 211.

assim, destacando a efetiva tutela que a instituição de um direito à explicação acarretaria para os titulares dos dados, para, logo de seguida – reconhecendo uma lacuna de urgente supressão –, destacarem a impossibilidade de adoção daquela orientação, face à atual letra do RGPD[51]. Para tal raciocínio, e deste modo afirmando a consagração de um mero direito a informações abstratas, sustentam a posição adotada com base na utilização pelo RGPD, nos artigos 13.º, 14.º e 15.º, da expressão "consequências previstas", afirmando que a mesma impele a uma lógica de futuro e, por isso mesmo, genérica, e nunca presente e concreta[52]. Além do mais, não deixando de considerar os argumentos invocados pela posição contrária, e como meio de refutação da mesma, consignam que a expressão "explicação" se encontra unicamente presente no considerando 71, o qual, nessa condição, carece de vinculatividade, em contraponto com os artigos que compõem o Regulamento.

Ora, relativamente a esta dicotomia doutrinal, não somos indiferentes às dificuldades de concretização que, neste âmbito, um direito à explicação encetaria. Destarte, além de os algoritmos dotados de *machine learning* não serem, em regra, construídos para fornecer explicações – tendo antes como prioridade a eficiência[53] –, o pensamento humano e as capacidades destes demonstram-se de tal forma discrepantes que a exigência aos mesmos de um esclarecimento concreto dos dados inicialmente utilizados e a relação entre estes e o resultado final poderá assumir custos verdadeiramente significativos para a sua produção e, até mesmo, expressiva diminuição daquela eficiência que se pretende[54].

Ademais, em matéria de utilização de algoritmos inteligentes para tratamento de dados opera uma pluralidade de agentes. A pessoa que retira o benefício deste tratamento, frequentemente, não coincide com aquela que o realizou, nem com aquela que programou o sistema utilizado para tal, pelo que, a quem exigir esta explicação? Ao beneficiário? Ao responsável pelo tratamento? Ao programador do algoritmo?

Mais, se a compreensão da forma de operar destes sistemas, necessária à prestação de uma explicação, é por vezes inexequível para os programadores dos

---

[51] LUCIANO FLORIDI, SANDRA WACHTER, BRENT MITTELSTADT, «Why a right to explanation of automated decision- making does not exist in the General Data Protection Regulation», *op. cit*., pp. 96 e ss.

[52] *Ibidem*, pp. 96-99.

[53] LILIAN EDWARDS, MICHAEL VEALE, «Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for», *op. cit.*, p. 26.

[54] Cfr. JENNA BURRELL, «How the machine 'thinks': Understanding opacity in machine learning algorithms», *op. cit.*, p. 5, e COMISSÃO EUROPEIA, *Comunicado da Comissão ao Parlamento Europeu e ao Conselho: Segundo relatório sobre a aplicação do Regulamento Geral sobre a Proteção de Dados*, *op. cit.*, p. 22.

mesmos, como exigir que tal se cumpra por aqueles que apenas recorrem à sua utilização ou aos seus resultados?

Não obstante, e pese embora este reconhecimento, não nos conseguimos rever na segunda posição. Estão em causa direitos fundamentais da pessoa humana, pelo que, ainda que um direito à explicação não resulte de forma clara do texto do RGPD, sempre se deverá completar uma interpretação literal da sua letra, com uma interpretação teleológica e sistemática[55]. Assim o destaca o TJUE quando menciona que "a interpretação de uma disposição do Direito da União exige que se tenham em conta não só os seus termos mas também o contexto em que se insere, bem como os objetivos e a finalidade que prossegue o ato de que faz parte"[56].

Neste caso, o grande objetivo do RGPD é a garantia de que as trocas de dados indispensáveis à criação de um Mercado Único Digital se caracterizam pela segurança e tutela dos direitos e interesses legítimos dos titulares dos dados, circunstância somente passível de concretização se à sua disposição for colocada toda a informação necessária ao gozo pleno dos direitos e prerrogativas pelo mesmo consagrados[57]. Esta ideia é, além de tudo, confirmada pelo artigo 12.º quando menciona que "[o] responsável pelo tratamento facilita o exercício dos direitos do titular dos dados nos termos dos artigos 15.º a 22.º".

Efetivamente, não vemos como o titular dos dados pode contestar a decisão tomada sem, pelo menos, uma explicação, ainda que simples, sobre os motivos que lhe subjazem. Aliás, é justamente isto que se passa quando se trata de uma decisão tomada por um ser humano. Se neste caso é requisito mínimo para uma contestação o conhecimento e a compreensão sobre o raciocínio da decisão, naquela primeira situação, somente porque diante de uma decisão tomada por uma máquina o discurso não poderá ser diverso.

Sem prescindir da resposta às questões "quem?" e "quando?" a que o princípio da transparência obriga, trata-se do escrutínio das questões "o quê?", "porquê?" e "como?". Como menciona MARGOT E. KAMINSKI no título do artigo que escreve, estamos perante um "Right to Explanation, Explained"[58], cabendo ao próprio responsável pelo tratamento a precaução de

[55] Com igual posição, destacando o preponderante papel dos considerados na interpretação a atribuir aos artigos de um diploma e, neste concreto caso, do considerando 71, ANDREW D. SELBST, JULIA POWLES, «Meaningful Information and the Right to Explanation», *op. cit*., p. 235.

[56] Cfr. acórdão de 7 de dezembro de 2023, Proc. C-643/21, Land Hessen contra Schufa Holding AG, §41 e acórdão de 22 de junho de 2023, Proc. C-579/21, Pankki S, §38, ambos disponíveis em https://curia.europa.eu [consultados em 13/08/2024].

[57] MARGOT E. KAMINSKI, «The Right to Explanation, Explained», *op. cit.*, p. 211.

[58] *Ibidem.*

que utiliza, somente, algoritmos que assim o permitam, sob pena de demanda e risco de responsabilização[59].

De outra banda, é de atender que o RGPD recorre a uma diferenciação de regimes quanto ao momento da prestação de informações de acordo com o facto de os dados serem ou não recolhidos junto do seu titular. No primeiro caso, impõe o artigo 13.º que as mesmas sejam concedidas *ex ante*, no próprio momento da recolha e, bem assim, antes do tratamento. No segundo caso, por seu turno, verificamos que o artigo 14.º, no seu n.º 3, estabelece vários prazos para que o mesmo se verifique: um mês após a obtenção dos dados pessoais; no momento da primeira comunicação com o titular dos dados, quando os mesmos se destinem a ser utilizados para fins de comunicação; e aquando da primeira divulgação dos dados quando estiver prevista a sua divulgação a um outro destinatário.

Assim, a concessão de informações gerais e abstratas ou específicas e concretas sempre dependerá do momento em que as mesmas sejam prestadas. Se o tratamento em si mesmo ainda não se verificou, há uma clara impossibilidade de conceção de informações específicas sobre a decisão concreta, porquanto esta tampouco se concretizou, e o artigo 13.º, n.º 2, alínea f), surge, precisamente, em corroboração desta lógica. Este preceito determina que, uma vez perante decisões automatizadas, ao titular dos dados sejam fornecidas informações sobre as possíveis consequências destas, e não as consequências em si mesmas.

Não obstante, surgindo o direito à informação como corolário do princípio da transparência, tal como o segundo, deve apresentar um conceito que, centrado no próprio titular dos dados, assista quer o momento do tratamento, quer o período que o antecede[60], o que impõe que a informação seja o mais completa possível. Deste modo, uma vez prestada de forma geral e abstrata, de acordo com os elementos disponíveis aquando da recolha dos dados, quando novos elementos surjam com o seu tratamento, sobre o responsável por este sempre recairá o dever de completar as informações prestadas com outras, agora, específicas e

[59] INÊS CAMARINHA LOPES, «Inteligência Artificial e proteção de dados pessoais: a "ditadura" do algoritmo», *op. cit.*, p. 568, e GIOANCLAUDIO MALGIERI, GIOVANNI COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», *op. cit.*, p. 2.

[60] GT29, *Orientações relativas à transparência na aceção do Regulamento (UE) 2016/679*, de 29 de novembro de 2018, p. 6, disponível em chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.uc.pt/protecao-de-dados/suporte/20180411_orientacoes_relativas_a_transparencia_wp260_rev01 [consultado em 09/08/2024].

concretas[61], assim se passando de um direito à informação que sempre existirá *ex ante*, para um direito à explicação que reinará *ex post*.

5. As soluções preconizadas pelo Regulamento Inteligência Artificial

Face à análise realizada, e partindo do princípio de que "qualquer explicação adequada deve, no mínimo, descrever como os dados recolhidos se articulam com as previsões"[62], a questão que assola é a de saber como regular os algoritmos de modo a assegurar os direitos dos cidadãos sem retirar o devido espaço à investigação e à eficiência.

Precisamente neste meio, e tendo como objetivo viabilizar o equilíbrio entre estes dois pontos aparentemente antagónicos[63], importantes avanços têm sido traçados pela UE, naquilo que é a construção de uma IA que se denomina de confiança. Desde a Comunicação da Comissão sobre a IA para Europa, de abril de 2018, até ao Livro Branco sobre a IA, de fevereiro de 2020, com especial destaque surgiu o Regulamento IA[64]. Com proposta apresentada pela Comissão Europeia a 21 de abril de 2021, publicação no Jornal Oficial da UE a 12 de julho de 2024 e entrada em vigor a 1 de agosto do mesmo ano, este surge com um objetivo claro: assegurar, reforçar e incentivar um desenvolvimento tecnológico, contudo, integrado e confluente com o respeito pelos direitos e valores estruturantes da União.

Materializado em vastos deveres e obrigações que faz recair sobre prestadores, responsáveis pela implantação, distribuidores e importadores de sistemas de IA, este recente, pioneiro e harmonizado diploma, simultaneamente, promove uma estratificação do risco em quatro níveis distintos, para os quais aqueles deveres e obrigações variam e intensificam conforme a gravidade do risco ao sistema atribuído. Falamos de práticas de IA proibidas (capítulo II), sistemas de

[61] Com orientação semelhante GIOANCLAUDIO MALGIERI, GIOVANNI COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», *op. cit.*, pp. 4 e 11, e ALESSANDRA SILVEIRA, JOANA COVELO ABREU, TIAGO SÉRGIO CABRAL, «Breves apontamentos quanto aos direitos dos titulares de dados no RGPD», *op. cit.*, pp. 99-101.

[62] GABRIELA CALDAS, «O direito à explicação no Regulamento Geral sobre a Proteção de Dados», *op. cit.*, p. 6.

[63] Considerandos 1 e 2 do Regulamento IA.

[64] De destacar que o caminho percorrido pela UE, neste âmbito, se tem revelado longo. Àqueles documentos assomam-se outros como a Comunicação da Comissão denominada Aumentar a Confiança numa IA centrada no ser humano, de abril de 2019; as Orientações Éticas para uma IA de Confiança, de abril de 2019, do Grupo Independente de Peritos de Alto Nível; e as três Resoluções do Parlamento Europeu, de outubro de 2020.

IA de risco elevado (capítulo III), sistemas de IA de risco limitado (capítulo IV) e sistemas de IA de risco mínimo (capítulo IV).

No que toca às práticas proibidas, estas integram todos os sistemas de IA de utilização considerada inaceitável, pela particular lesividade e prejudicialidade que acarretam para os valores da UE, desde logo, a dignidade humana, a liberdade, a igualdade, a democracia e o Estado de Direito, bem como todos os direitos fundamentais ali projetados, entre os quais, e naturalmente, a proteção de dados[65]. Nestes termos, serão de considerar sistemas de IA que distorcem o comportamento das pessoas; sistemas que tem a suscetibilidade de causar danos físicos e psicológicos, tanto para os que os utilizam como para terceiros; sistemas que exploram vulnerabilidades de pessoas de grupos específicos em razão da sua idade ou capacidade física ou mental; sistemas utilizados por intervenientes públicos ou para estes e que visem proceder a classificações sociais; e, ainda, sistemas de identificação biométrica à distância para efeitos de aplicação da lei[66].

No lado oposto da graduação de risco encontramos dois tipos de sistemas de IA: os sistemas de IA de risco mínimo e os sistemas de IA de risco limitado. Os primeiros[67], como o próprio nome o indica, são sistemas de IA que apresentam um nível de risco baixo para os direitos fundamentais e, por esse mesmo motivo, veem-se ausentes de conexão a obrigações ou regras específicas, ainda que, e não obstante, se apele à criação e cumprimento voluntário de códigos de conduta onde a transparência e a informação saiam destacadas[68]. Já os segundos, apresentando um igual nível de risco, mas perspetivando-se, diferentemente, uma maior interação com o cidadão, veem-se associados a requisitos e obrigações mínimas de transparência e informação clara e acessível. Tais obrigações, presentes quer na conceção, quer no desenvolvimento do algoritmo, corroboram o incremento da transparência na comercialização e utilização dos sistemas de IA que o Regulamento almeja[69].

Por último, e como patamar intermédio de risco, despontam os sistemas de IA de risco elevado. Apresentando como marca distintiva, face aos restantes, a vasta escolta de deveres por que se fazem acompanhar, serão aqui enquadráveis

---

[65] JOSÉ RICARDO MARCONDES RAMOS, «Supervisão, classificação e certificação dos sistemas de IA na Proposta de Regulamento sobre Inteligência Artificial », in SUSANA AIRES DE SOUSA (coord.), *Direito em Mudança – A Proposta de Regulamento Europeu sobre Inteligência Artificial – Algumas questões jurídicas*, Coimbra, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, 2023, p. 36, (pp. 31-64), disponível em https://estudogeral.uc.pt/handle/10316/108674 [consultado em 02/09/2024].

[66] Artigo 5.º do Regulamento IA.

[67] Enquadram-se aqui filtros de *spam* e jogos de computador.

[68] Artigo 95.º do Regulamento IA.

[69] *Ibidem*, considerando 132 e artigo 50.º.

sistemas de IA de gestão e operação de infraestruturas relativas ao trânsito rodoviário, abastecimento de água, gás, aquecimento e eletricidade; sistemas que atuam no domínio da educação; sistemas com relevância no âmbito do acesso e usufruto de prestações e serviços de assistência pública; bem como sistemas de seleção e recrutamento de trabalhadores, de promoção da carreira e de cessação do vínculo[70].

Entre o mencionado rol de obrigações encontramos a obrigação de avaliar a conformidade do sistema antes da colocação no mercado[71]; a obrigatoriedade de supervisão humana por pessoas com a formação e autoridade necessárias para interpretar corretamente os resultados do sistema bem como anular ou reverter o seu resultado[72]; a exatidão, solidez e cibersegurança[73]; a implantação de sistemas de gestão de riscos e qualidade, de execução ao longo de todo o ciclo de vida do sistema[74]; o estabelecimento de práticas que garantam a qualidade e quantidade de dados[75]; e, ainda, a comunicação a uma autoridade nacional competente de incidentes nos quais o sistema tenha estado envolto por mau ou defeituoso funcionamento[76].

Dentro daquelas, e não menos despiciendas, assomam-se outras tantas que, de modo resplandecente, destacam a transparência dos sistemas de IA que se pretende abraçar e garantir. Desde logo, a compreensão por parte do responsável pela implantação do sistema de IA, do seu modo de funcionamento, por forma a deter a capacidade de interpretar os resultados obtidos e, assim, garantir a transmissão de informação transparente[77]; a obrigatoriedade de detenção de um sistema de registo automático da atividade que assegure a rastreabilidade dos resultados[78]; a manutenção de documentos e registos do sistema de IA; bem como, e como suporte do afastamento de grande parte das dificuldades que descrevemos *supra* a propósito de um princípio à explicação, a existência de documentação técnica detalhada sobre o sistema e a sua finalidade, sempre redigida e passada de forma concisa, clara, suficiente, adequada, acessível e compreensível[79].

---

[70] *Ibidem*, considerandos 54 a 62.

[71] *Ibidem*, considerando 123.

[72] *Ibidem*, considerando 73 e artigo 14.º

[73] *Ibidem*, considerando 74 e artigo 15.º

[74] *Ibidem*, considerando 65 e artigo 9.º

[75] *Ibidem*, considerando 67 e artigo 10.º

[76] *Ibidem*, considerando 131 e artigo 73.º

[77] *Ibidem*, artigo 13.º

[78] *Ibidem*, considerando 71 e artigo 12.º

[79] *Ibidem*, considerando 71.

Particularmente aqui enquadrar-se-á, de uma banda, uma descrição pormenorizada dos elementos do sistema de IA – circunstância que, permitindo aceder às especificações de conceção do sistema, consequentemente caucionará a existência de uma especificação concreta acerca da sua lógica geral, bem como, mais adentro, da sua lógica subjacente e dos pressupostos por si utilizados –, de outra banda, ainda, uma análise das soluções técnicas necessárias à facilitação da interpretação dos resultados apresentados[80].

Para terminar, não podemos deixar de destacar o artigo 86.º desta nova legislação. Referindo-se de modo expresso às decisões individuais automatizadas – o conceito aqui presente é em tudo similar ao introduzido pelo RGPD –, e apresentando-se com a epígrafe "Direito à Explicação", este vem mencionar que "[q]ualquer pessoa afetada sujeita a uma decisão tomada pelo responsável pela implantação com base nos resultados de um sistema de IA [...] tem o direito de obter do responsável pela implantação explicações claras e pertinentes sobre o papel do sistema de IA no processo de tomada de decisão e sobre os principais elementos da decisão tomada". Pois bem, dúvidas houvesse quanto à materialização do direito à informação como um direito à explicação da decisão no RGPD, com o Regulamento IA, essa existência torna-se, pois, irrefutável.

6. Conclusão

O crescente surgimento de aplicações de IA reporta-se a uma realidade dificilmente reversível. Não obstante, os riscos que esta comporta para os direitos, liberdades e garantias dos cidadãos não podem, de modo e em caso algum, ser desconsiderados. O RGPD reflete, precisamente, esta preocupação, atribuindo aos titulares dos dados uma panóplia diversa de direitos, particularmente, quando perante decisões individuais automatizadas tomadas pela tecnologia.

Entre aqueles, especial relevância e controvérsia tem assumido, como apontamos, o direito à informação e a sua eventual concretização enquanto direito a uma explicação. Quanto ao que nos apraz, parece-nos clara a intensão do legislador de consagração de um direito a informações específicas e concretas. Por um lado, o próprio diploma, ao longo do seu texto, faz alusão à necessidade de adequação das informações disponibilizadas com as circunstâncias particulares e contextos específicos em que surgem, assim assegurando um tratamento equitativo. Por outro lado, ainda que somente encontremos referência a uma explicação no considerando 71 e este careça de carácter vinculativo, não podemos deixar de refletir sobre a relevância que os considerandos de um qualquer diploma assumem, seja na sua aplicação, seja na sua interpretação. O considerando 71 informa os artigos 13.º, 14.º e 15.º do RGPD.

[80] *Ibidem.*

Sem prescindir, o direito a uma explicação é a concretização, no âmbito do tratamento e proteção de dados, do direito a uma fundamentação das decisões adotadas, por forma a viabilizar o exercício de tantos outros, desde logo, a possibilidade de manifestar outro ponto de vista e de contestar qualquer decisão. Trata-se, enfim, de uma dimensão fundamental no âmbito de um Estado de Direito Democrático, pelo que não se deverá, jamais, abrir margem para a sua desconsideração.

Questão por deveras diversa é a da possibilidade de concretização desta explicação perante sistemas de IA que, dotados de *machine learning*, se caracterizam pela opacidade.

Terminando com a ideia de uma área desguarnecida de regulação e resultando de modo evidente do considerando 10 o propósito de facilitar a "aplicação efetiva e permitir o exercício dos direitos dos titulares dos dados [...] incluindo os direitos relacionados com as decisões individuais exclusivamente automatizadas", importantes avanços foram traçados pelo pioneiro Regulamento IA. Atendendo tanto ao momento *ex ante* como ao momento *ex post*, do seu texto resulta reiterada a importância dos deveres de transparência e o foco colocado na mesma. A transparência e a explicabilidade devem estar presentes, por predefinição, desde o momento da conceção dos sistemas de IA, até à sua efetiva utilização. Se isto for cumprido e o algoritmo for transparente e compreensível, os benefícios são mútuos: de uma banda, passa a ser possível a identificação dos preconceitos da máquina, dos erros e deturpações do algoritmo e a sua consequente correção e melhoria; de outra banda, os direitos dos cidadãos saem protegidos. Ainda que o diploma não se dirija ao público em geral, no final, se a transparência se verificar para aqueles que se encontram no topo da pirâmide, consequentemente, poderá ser transmitida aos demais.

Trate-se, enfim, de não mais do que assegurar que o desenvolvimento da tecnologia seja feito ao serviço da pessoa humana e dos seus direitos e nunca em seu detrimento. No alcance de uma IA segura, confiável e ética, acreditamos que é, precisamente, este o caminho que está a ser traçado pela UE.

A ATIVIDADE ADMINISTRATIVA DA SEGURANÇA SOCIAL E A INTELIGÊNCIA ARTIFICIAL: (RE)PENSAR O REGIME DE RESPONSABILIDADE CIVIL DOS ATOS PRATICADOS PELA SEGURANÇA SOCIAL

Luís Manuel Pica[*]

Resumo: A criação de sistemas informáticos cada vez mais inteligentes e sofisticados é um desenvolvimento inegável. A utilização destes sistemas informáticos é transversal aos vários domínios da sociedade, sendo inclusive inegável a sua utilização pela Administração Pública, designadamente pela Segurança Social no domínio legal que lhe está atribuído. Todavia, os desafios e as questões que se suscitam na utilização de sistemas de inteligência artificial crescem exponencialmente, paralelamente à complexidade crescente destes sistemas informáticos. Por isso, mostra-se necessário estabelecer um marco legal atualizado direcionado a mitigar os novos riscos associados a estas realidades.

* Doutor em Ciências Jurídicas Públicas pela Escola de Direito da Universidade do Minho; Professor Adjunto Convidado do Instituto Politécnico de Beja; Professor Auxiliar Convidado do Instituto Superior Manuel Teixeira Gomes; Investigador Doutorado-Integrado do CEAD – Francisco Suárez da ULHT e Investigador do JusGov – Centro de Investigação em Governação e Justiça da EDUM. E-mail: *luispica280@gmail.com*

Palavras-chave: Inteligência Artificial; Segurança social; Administração Pública; Responsabilidade civil; Atos ilícitos.

Abstract: The creation of increasingly intelligent and sophisticated computer systems is an undeniable development. The use of these computer systems cuts across the various domains of society, and their use by the Public Administration is even undeniable, particularly by Social Security in the legal field assigned to it. However, the challenges and issues that arise in the use of artificial intelligence systems are growing exponentially, in parallel with the increasing complexity of these computer systems. It is therefore necessary to establish an up-to-date legal framework aimed at mitigating the new risks associated with these realities.

Keywords: Artificial Intelligence; Social security; Public administration; Civil liability; Unlawful acts.

1. Introdução

A inteligência artificial tem conquistado espaço e atraído atenção diariamente, tornando-se um tema central na sociedade, na imprensa e nas instituições nacionais, europeias e internacionais.

A sua relevância é inegável, tanto pela utilidade prática que oferece quanto pelas preocupações que levanta. Este protagonismo é mais do que justificável, considerando a sua crescente aplicação nos vários domínios da sociedade e do saber, designadamente também no domínio da segurança social. Desde sistemas automatizados para análise e concessão de benefícios até ferramentas inteligentes para deteção de fraudes, a inteligência artificial tem potencial para transformar significativamente a gestão e operacionalização dos sistemas de proteção social. Um exemplo disso são os algoritmos que otimizam a análise de dados para prever situações de risco social, calcular pensões com maior precisão ou propor políticas públicas mais eficazes, permitindo uma melhor alocação de recursos e uma resposta mais célere às necessidades da população.

Contudo, essa crescente integração também traz desafios importantes. As decisões automatizadas podem conter falhas ou gerar resultados injustos, afetando direitos fundamentais dos beneficiários da Segurança Social.

Como lidar com situações em que da utilização dos sistemas de inteligência artificial resultem a indevida negação de um benefício ou a prática de atuações indevidas? Estas questões levantam debates cruciais sobre como o Direito deve intervir para regular esses sistemas e proteger os cidadãos.

Embora já se observe um movimento para regulamentar o uso da inteligência artificial, principalmente em matéria de responsabilidade civil, ainda há espaço para considerar outras soluções jurídicas. Dever-se-á, por exemplo, criar um regime específico para decisões automatizadas no âmbito da segurança

social? Que salvaguardas e mecanismos de recurso deverão ser implementados para garantir a proteção dos beneficiários diante de eventuais abusos ou falhas?

Com estas reflexões, pretendemos abordar o impacto da inteligência artificial no campo do direito da segurança social, explorando as suas potencialidades e benefícios, mas sem descurar os riscos e desafios associados. O objetivo é dotar o leitor de uma visão abrangente sobre as implicações jurídicas já identificadas e possíveis soluções futuras, promovendo uma abordagem equilibrada entre inovação tecnológica e tutela dos direitos sociais.

2. Conceitos operativos – uma (breve) noção sobre inteligência artificial

2.1. Ponto de partida

A delimitação de um conceito adequado que permita satisfazer os propósitos concetuais para o presente trabalho exige-nos uma reflexão sobre o que deve ser entendido por inteligência artificial (ou sistema inteligente ou de inteligência artificial). O conceito de *inteligência artificial* tem alavancado interesses e debates, mostrando-se tema de irremediável curiosidade e debate entre investigadores, docentes, instituições públicas e privadas, organizações, imprensa, sociedade, setor económico, político, etc. Este debate não tem sido despiciendo de sentido, pois pense-se que estamos perante um acontecimento próprio de ficção científica[1].

Mas, a verdade é que a inteligência artificial é hoje uma realidade inegável e um acontecimento que chegou para ficar e com a qual temos de conviver diariamente. Não será difícil identificar que os *smartphones* atuais são hoje capazes de dar resposta a necessidades de forma quase preditiva e intuitiva ou sistemas de criação de perfis que permitem individualizar serviços de diversa natureza. Todas estas situações (entre outras) são um exemplo de como a inteligência artificial está no nosso quotidiano e se integram nas mais variadas relações. Deste modo, exige-se uma delimitação concreta sobre o que deve ser entendido por inteligência artificial? Um estudo que se anseia (minimamente) rigoroso – em termos científicos – não pode deixar de exigir (ainda que de forma breve) uma

[1] NÚBIA FRANCO DE OLIVEIRA, DEILTON RIBEIRO BRASIL, JAMILE BERGAMASCHINE MATA DIZ, «Decisões Automatizadas e Processos Discriminatórios: a Lei Geral de Proteção de Dados brasileira como mecanismo de governança», *Privacy and Data Protection Magazine – Revista Científica na Área Jurídica,* n.º 02-2021, Universidade Europeia, 2021, p. 52, disponível em https://www.europeia. pt/content/files/pdpm_002.pdf [consultado em 25/07/2024].

aproximação ao objeto do nosso estudo (reservando sempre a dificuldade de delimitação concetual)[2].

Para o efeito, socorremo-nos das considerações tecidas pelo Grupo de Peritos em inteligência artificial da OCDE[3]. Para este grupo, uma definição aberta e tecnologicamente neutra de *inteligência artificial* não pode deixar de considerar três caraterísticas próprias: i) sistemas maquinais suscetíveis de criar previsões, recomendações ou padrões estatisticamente normais que sejam suficientemente sólidos para influenciar o seu ambiente real ou virtual no âmbito de objetivos definidos por seres humanos; ii) sistemas que utilizam dados de entrada concetualmente necessários, gerados por seres humanos ou máquinas, para percecionar ambientes reais ou virtuais e transformá-los em modelos estatísticos; iii) quando aplicados a novos dados, são finalmente capazes de formular opções e informações para ações com base nesses modelos, utilizando a dedução de modelos. Ao fazê-lo, estes sistemas têm diferentes graus de autonomia.

Já o Conselho da Europa formula esta questão de forma um pouco mais abstrata no seu estudo sobre a viabilidade e os possíveis elementos de um quadro jurídico para o desenvolvimento, a conceção e a utilização de sistemas de inteligência artificial no que diz respeito à proteção dos direitos humanos, à democracia e à realização do Estado de direito[4]. A inteligência artificial é aqui definida como a descoberta de padrões e tendências em grandes conjuntos de dados, utilizando para o efeito métodos estatísticos. Através dela, algoritmos inteligentes permitiram o reconhecimento de imagens e sons, a racionalização de produtos e serviços e grandes ganhos de eficiência na realização de tarefas complexas. Foi o aparecimento de sistemas de *big data*, constituídos por grandes memórias, grandes quantidades de dados e processadores rápidos, que, na sequência do aparecimento da *world wide web*, acelerou o desenvolvimento de novos métodos de desenvolvimento de algoritmos com base nos quais podem ser criados e treinados modelos probabilísticos.

Com efeito, quando intentamos restringir o conceito de *inteligência artificial* (aplicada ao setor económico, político, administrativo ou na própria agricultura), somos impelidos, desde logo, a afirmar que, mais do que uma inteligência propriamente dita, estamos perante uma inteligência maquinal representada

---

[2] Philip Glass, «Datenschutzrecht für künstliche Intelligenz in der öffentlichen Verwaltung», in *Datenschutz Rechtliche Schnittstellen*, Zurich, Dike, 2023, p. 179, disponível em https://digitalcollection.zhaw.ch/bitstream/11475/26659/2/2023_Widmer_Datenschutz-rechtliche-Schnittstellen_Dike.pdf [consultado em 25/07/2024].

[3] Oecd, *Artificial Intelligence in Society*, Paris, OECD Publishing, 2019, disponível em https://doi.org/10.1787/eedfee77-en [consultado em 25/09/2024].

[4] AD HOC COMMITTEE ON ARTIFICIAL INTELLIGENCE, Feasibility Study, CAHAI (2020)23, n.º 4, 2020, disponível em https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da [consultado em 25/09/2024].

por pré-resultados identificados previamente pelo produtor e cuja aglomerado constitui um algoritmo que é utilizado pelo sistema informático[5]. Ou seja, estamos perante uma verdadeira máquina capaz de reproduzir impulsos humanos, com vista à utilização por estes e para os seus fins e interesses. Com base na representação de conhecimentos específicos e no processamento de conhecimentos, os algoritmos efetuam o reconhecimento de padrões, as instruções de controlo/ação e o processamento de problemas para atingir o resultado previamente determinado[6]/[7].

Insere-se no contexto precedente uma extensão de "inteligência artificial fraca", a qual funciona dentro dos limites da programação, sem desvios para os programas predeterminados pelo criador do algoritmo. Daí que se coloque em crise a verdadeira natureza de "inteligência", pois estamos na presença de uma mera reprodução de conclusões a que se haviam chegado previamente e que foram integradas como conclusão num algoritmo. Mas, é na chamada "*inteligência artificial forte*" que se desenvolve o verdadeiro conceito moderno de inteligência artificial. Perante uma "inteligência" capaz de se desenvolver internamente no seu funcionamento, forma autónoma após uma fase inicial e com base numa programação específica, posteriormente os métodos de aprendizagem automática e clássicos como as redes neuronais artificiais preditivas utilizados como procedimentos complexos de resolução de problemas permitem desenvolver o algoritmo inicial criado.

Por isso, e tendo por base as precedentes considerações, importa concluir com a seguinte ideia: *mais do que uma verdadeira "inteligência", devemos considerar a existência de uma máquina instrumentalizada aos objetivos do ser humano, a qual é destinada à análise sequencial de dados e informações para reprodução*

---

[5] O termo "algoritmo" refere-se a instruções de ação claramente estruturadas que não são inicialmente descritas como artificialmente inteligentes. Em termos metafóricos, são como "receitas culinárias" e outros processos de dedução lógica. Assim, um algoritmo é definido como qualquer instrução de ação não ambígua que é utilizada para resolver certos problemas em passos individuais definidos. O momento da inteligência artificial não está no algoritmo, mas no modelo que é implementado pelo algoritmo. Assim, um sistema algorítmico não tem necessariamente de ter funções artificialmente inteligentes. Cfr. Luís Manuel Pica, *A inteligência artificial no Direito Tributário: Fundamentos e Limites Constitucionais*, Coimbra, Almedina, 2023, p. 32.

[6] Christian Würschinger, «Künstliche Intelligenz – Zwischen Wunsch und Wirklichkeit», *Wirtschaftsinformatik & Management*, 2, 2020, p. 86.

[7] Seguindo esta ideia, o Regulamento Inteligência Artificial, aprovado pelo Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, consagra, no seu artigo 3.º, n.º 1, que um *sistema de inteligência artificial* é "um programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage". Cfr. Regulamento Inteligência Artificial, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:L_202401689 [consultado em 19/11/2024].

dos resultados identificados previamente[8]. Como resultado, não se procurará uma substituição do ser humano, mas sim um instrumento destinado à concretização dos seus objetivos.

Assim, deixam-se de lado questões éticas (cujo sentido e teor não se negligencia nem se menospreza), mas procuraremos conceber um estudo jurídico direcionado à aplicabilidade da inteligência, designadamente no que concerne ao domínio da aplicação do direito à segurança social.

2.2. A digitalização, a inteligência artificial e os meios eletrónicos na atividade administrativa

Falar em digitalização e sistemas de inteligência artificial parece, numa primeira aproximação, abordar as realidades perante um literalismo homogéneo e tendencialmente uniforme, pois parecem realidades análogas, sendo, por vezes, utilizados indistintamente. Por exemplo, se tomarmos como exemplo o disposto no n.º 1 do artigo 14.º do Código do Procedimento Administrativo, o qual dispõe que, "os órgãos e serviços da Administração Pública devem utilizar meios eletrónicos no desempenho da sua atividade, de modo a promover a eficiência e a transparência administrativas e a proximidade com os interessados", parece que o conceito de "meios eletrónicos" abrange qualquer realidade, sendo utilizado como um termo com enorme amplitude semântica. Ou seja, do mencionado normativo não se vislumbra uma cisão entre os mencionados conceitos de digitalização e automatização. A lei refere, apenas, a utilização de meios eletrónicos, o qual parece apontar para qualquer uma das aludidas realidades.

i) Porém, tal ideia não poderá deixar de revestir um certo grau de confusão e, até, tendencial engano, já que os conceitos de digitalização e automatização são realidades distintas, com implicações diferentes e repercussões que são profundamente heterogéneas:

ii) De forma mais precisa, podemos entender a *digitalização* como a transposição do procedimento administrativo e tributário tradicional para um suporte digital, sem alterar a essência do mesmo. Trata-se de um modelo que utiliza plataformas eletrónicas em vez de documentos físicos, mantendo inalteradas as fases, os atores e os atos envolvidos no procedimento. A única diferença reside na substituição do suporte utilizado por um formato digital.

Por outro lado, a *automatização* traz um *plus*, pois existe uma transformação mais profunda, introduzindo sistemas de apoio à decisão, como a inteligência artificial, que podem substituir os agentes humanos na tomada de decisões e na

[8] LUÍS MANUEL PICA, *A inteligência artificial no Direito Tributário*…, *op. cit.*, p. 29.

execução dos atos procedimentais. Aqui, a inteligência artificial vai além da simples digitalização, utilizando algoritmos baseados em critérios pré-estabelecidos para interpretar e aplicar as normas jurídicas, formulando projetos de decisões, ideias ou conclusões que podem ser adotadas no procedimento[9]. A inovação reside não na decisão em si, mas no processo que a antecede: a decisão inteligente é o resultado da análise e processamento de dados pela máquina, enquanto a decisão digital se limita à informatização do procedimento já existente.

Na situação descrita (da *automatização*), colocam-se, contudo, três realidades distintas, mas necessárias entre si: (i) a realidade em que os dados – no nosso caso, os dados públicos – implicam o elemento estruturante de um novo "modelo" de Administração – uma "Administração Datificada" – em que os programas (incluindo os algoritmos) farão o que os burocratas faziam; (ii) a realidade na qual a modernização, a automatização e a integração da sistemas de inteligência artificial redefinem a marca do Direito Administrativo como direito positivo, porque esses processos exigem a tradução da linguagem natural "típica" da norma jurídica para uma linguagem "informatizada"[10]; (iii) a tomada de decisões é conseguida com suporte a um elemento externo que forma um elemento persuasivo na decisão final, podendo, inclusive, colocar-se em crise a vontade da administração.

Embora seja este o nosso entendimento, não podemos deixar de concluir pela ideia de que a *digitalização* do procedimento se traduz num mero ato de integração de sistemas tecnológicos destinados a digitalizar o suporte dos atos praticados no procedimento tributário, sem que exista, conquanto, um suporte

---

[9] Neste sentido, veja-se a definição dada pelo 3.º, n.º 1, do Regulamento Inteligência Artificial, aprovado pelo Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, o qual estabelece que um Sistema de Inteligência Artificial será "um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais".

[10] Uma posição mais restritiva pode ser encontrada em Alexandre Dias Pereira, segundo o qual "[d]o que fica dito poderia encontrar-se o «código-fonte» do sistema jurídico na Constituição. Ao intérprete da lei ordinária estaria reservada a possibilidade de, quando muito, «desvendar» princípios consignados na Constituição, ainda que não explícita ou expressamente consagrados, e mesmo assim sob o controlo do Tribunal Constitucional. Com efeito, princípios consignados serão, por muito fluida que seja a palavra consignar, princípios previstos na Constituição ou que pelo menos (o que já não será assim tão pouco) não ofendam o espírito do sistema constitucional vigente". Para além disso, "[o]s sistemas informáticos de inteligência artificial prometem uma justiça sem arbítrio. Árbitro seria apenas o programador político do sistema que implementaria tecnicamente no software o programa político de domínio e ordenação social contido no código-fonte constitucional e das leis. Juízos só os provenientes da vontade política do legislador. A máquina limitar-se-ia a reproduzi-los mecanicamente nos casos concretos por via de aplicação silogística". Alexandre Dias Pereira, «*Ius Ex Machina*? Da Informática Jurídica ao Computador-Juiz», *RJLB*, ano 3, n.º 1, 2017, p. 81.

na atividade decisória; pelo contrário, a adoção de meios de inteligência artificial, procurando a *automatização* procedimental, implica integrar um sistema capaz de ler dados que a administração tem em sua posse, os quais são tratados massivamente para efeitos de produzir uma decisão que servirá de base à prática do ato decisório final.

3. A inteligência artificial aplicada ao direito à segurança social

3.1. Enquadramento sistémico

A simples referência a um direito à segurança social levanta logo um conjunto de questões que merecem reparo e atenção.

Perante uma dimensão axiológica, o direito da segurança social corresponde a um verdadeiro direito fundamental espelhado como uma verdadeira concretização dos Estados contemporâneos[11]. Neste sentido, facilmente se compreende a sua consagração constitucional e a sua ascensão enquanto valor enformador do Estado. Conforme resulta do artigo 63.º, n.º 1, da Constituição da República Portuguesa, "todos têm direito à segurança social", desenvolvendo o seu n.º 2 um verdadeiro "caderno de encargos" que encarrega o Estado de desenvolver medidas que permitam dar concretização ao conteúdo programático delimitado constitucionalmente. Como refere Ilídio das Neves[12], o direito à segurança social estabelece o "poder, reconhecido pela ordem jurídica, de exigir do Estado prestações, pecuniárias ou em espécie, como resposta a situações ou eventualidades traduzidas na interrupção, redução ou cessação dos rendimentos do trabalho, ocorrência de determinados encargos, como os relativos à educação dos filhos e à satisfação de necessidades em matéria de saúde, verificação de insuficiência de rendimentos por estes serem inferiores a um determinado nível mínimo, considerado pela lei como exigência de dignidade humana e fronteira da pobreza".

Mas, enquanto direito axiologicamente relevante, a sua aplicabilidade rege-se pelo conjunto de normas jurídicas que enformam um verdadeiro corpo normativo de natureza administrativa e tributária. Daí que caibam às normas jurídicas administrativas (consideradas em sentido amplíssimo) a aplicação

[11] ANA VAZ, JOÃO VINHA BARRETO, LUÍS MANUEL PICA, «Breves Notas sobre as Contribuições e Quotizações para a Segurança Social», in JORGE CAMPINO, SUZANA FERNANDES DA COSTA, NUNO MONTEIRO AMARO (coord.), *Segurança Social – Sistema, Proteção, Solidariedade e Sustentabilidade*, Lisboa, AAFDL, 2020, p. 549; ILÍDIO DAS NEVES, *Direito da Segurança Social, Princípios Fundamentais Numa Análise Prospectiva*, Coimbra, Coimbra Editora, 1996, p. 230.

[12] ILÍDIO DAS NEVES, *Direito da Segurança Social, Princípios Fundamentais Numa Análise Prospectiva*, *op. cit.*, p. 230.

das medidas jurídicas destinadas à concretização do direito à segurança social. Seja por via das normas destinadas à cobrança das contribuições devidas para a sustentabilidade da própria segurança social, seja por via das normas jurídicas procedimentais que dão corpo ao procedimento administrativo-tributário destinado à concretização do direito à segurança social.

Por isso, e constituindo a *inteligência artificial* um instrumento destinado à concretização dos interesses do ser humano, a sua conexão surge aqui como fonte para aplicação e gestão das medidas destinadas à concretização do direito à segurança social.

Procura-se, através da utilização dos sistemas de inteligência artificial, a aplicação das normas jurídicas reservadas à concretização daquele direito fundamental, operando numa automatização de procedimentos, mecanizando a prática de atos e a gestão destes, racionalizando meios e procurando dotar os contribuintes e a administração de novas soluções e técnicas capazes a facilitar a relação entre ambos, formulando hipóteses, previsões e medidas administrativas criadas especificamente para casos determinados.

A atividade da Segurança Social, enquanto órgão próprio da Administração Pública, será objeto de uma reformulação, pois o procedimento clássico destinado à arrecadação das contribuições e à atribuição dos benefícios perante um procedimento administrativo próprio será desmaterializado, automatizado e alvo de uma antropomorfização que, em muitos casos, procurará substituir o ser humano. Pense-se, por exemplo, na criação de *chatbots* destinados a auxiliar os contribuintes na resolução de questões. Através de plataformas digitais e segundo sistemas autómatos, a lógica da Administração Pública em geral, e da Segurança Social em particular, é reformulada para uma atividade mais *inteligente* e que se baseia nestes sistemas inteligentes de processamento massivo de dados pessoais, de atuação automatizada e de administração de massas.

Como tivemos ocasião de referir noutra sede, falamos, assim, de uma Administração Pública "artificialmente *inteligente*", em que se reconhece a utilização de uma máquina que acrescenta novas técnicas, introduzindo novas componentes decisórias de formação autónoma de vontade e cuja base de atuação encontra génese nos sistemas inteligentes. Falamos de sistemas de inteligência artificial que procuram a recolha de dados pessoais e a sua leitura massiva, através de máquinas pensantes (*selbst denkende Maschinen*), e pelos quais resultam a atuação em conformidade com a simulação de comportamentos humanos através de condutas programáticas previamente delimitadas (*Simulation menschlichen Verhaltens durch Maschinen*). O caso paradigmático são as ilações retiradas por estas máquinas "pensantes", nas quais os sistemas inteligentes adotam novas técnicas através das quais são disponibilizados um conjunto de resultados prece-

dentes do tratamento massivo de dados pessoais disponibilizados pelos contribuintes, entidades internas e estrangeiras[13].

Entre vários benefícios na utilização de sistemas de inteligência artificial aplicado pela Segurança Social, identificam-se, entre outros, os seguintes:

i) A obtenção de dados relevantes para efeitos de apuramento da situação contributiva, o cruzamento desses mesmos dados e a formulação de ideias, premissas e soluções que demonstrem situação patológicas, situações de atribuição de benefícios, correção de anomalias procedimentais, as quais são conseguidas de forma célere e desmaterializada, permitindo uma majoração da eficiência e procurando-se otimizar os procedimentos existentes, agilizando a sua tramitação e potenciando as suas virtudes e benefícios, eliminando eventuais assimetrias ou dificuldades derivadas da morosidade burocrática clássica[14];

ii) Através de um funcionamento adequado, sustentável e eficiente da Segurança Social, consegue-se uma majoração no aspecto psicológico dos contribuintes, persuadindo-os no cumprimento voluntário das obrigações contributivas e declarativas que sobre estes impendem[15];

iii) Por via do grande recurso aos dados pessoais, consegue-se criar um sistema analítico e estatístico que formula hipóteses sobre factos ocorridos, conseguindo prever com algum grau de probabilidade acontecimentos que poderão vir a ocorrer. Falamos neste caso da criação de perfis de risco sobre pessoas ou atividades, permitindo criar medidas preventivas destinadas a formular decisões direcionadas a uma maior supervisão sobre os atos dos contribuintes[16];

iv) A criação de instrumentos de cooperação e de auxílio entre a Segurança Social e os contribuintes, criando mecanismos de apoio personalizado e direcionado ao contribuinte concreto, formulando opiniões e recomendações adequadas para uma simplificação da relação jurídica existente, procurando o cumprimento atempado e correto das obrigações.

---

[13] LUÍS MANUEL PICA, *A inteligência artificial no Direito Tributário*…, *op. cit.*, p. 35.

[14] *Ibid.*

[15] LUÍS MANUEL PICA, "El uso de la Inteligencia Artificial por parte de las Administraciones Tributarias: ¿Una Necesidad o una Utopía?", in *Inteligencia Artificial y Administración Tributaria: Eficiencia Administrativa y Defensa de los Derechos de los Contribuyentes*, Navarra, Thomson Reuteurs, 2021, pp. 532-533.

[16] LUÍS MANUEL PICA, «A inteligência artificial no sistema de gestão fiscal: uma dimensão preventiva e as presunções (jurídicas) na identificação e combate aos fenómenos patológicos», *Revista Jurídica Portucalense*, n.º 32, 2022, pp. 171-191.

Como se compreende, algumas das intervenções indicadas permitem formular vantagens que são suficientes para consentir estes instrumentos no plano administrativo-tributário. A concretização do direito fundamental à segurança social bem como a dimensão tributária associada a este direito fundamental são receitas mais do que suficientes para formular uma Segurança Social mais inteligente e apoiada em sistemas de simplificação e de apoio de decisão automatizada. Por isso, a evolução não deixará de seguir o rumo da automatização, da autonomização procedimental e da instrumentalização dos sistemas de inteligência artificial para criar uma Segurança Social mais eficiente, mais capaz e mais preparada para dar resposta aos desafios e às necessidades dos contribuintes.

3.2. A inteligência artificial na aplicabilidade das normas de direito da segurança social

Como vimos *supra*, a inteligência artificial tem potencial para transformar significativamente o direito da segurança social, trazendo benefícios e desafios. No contexto da Segurança Social, a inteligência artificial é aplicada para otimizar processos administrativos, melhorar a gestão de recursos e prever necessidades sociais.

Os sistemas de inteligência artificial podem analisar automaticamente pedidos de benefícios, como pensões, subsídios de desemprego ou rendimento social de inserção, verificando se os requisitos legais estão preenchidos através dos dados inseridos pelo requerente. Em Portugal, o Instituto da Segurança Social, I.P. já utiliza um sistema de base automatizada em que a plataforma digital analisa os rendimentos declarados de um cidadão, cruzando dados fiscais e contributivos, para decidir se ele tem direito à pensão e qual o valor da mesma.

Por outro lado, veja-se que a concessão de benefícios fiscais está suportada por um conjunto de requisitos legais fechados e que devem ser cumpridos. O não preenchimento de algum desses requisitos determina a não concessão ou a perda do benefício social. Por isso, os sistemas de inteligência artificial podem, através do cruzamento de dados, criar sistemas fiscalizadores que visam a identificação de irregularidades nas contribuições ou benefícios atribuídos, cruzando grandes volumes de dados em tempo real. Falamos, por exemplo, da criação de perfis sobre determinados sujeitos e que podem servir para alocar os recursos de fiscalização em matéria de segurança social.

Resultando num conjunto massivo de leitura de dados pessoais, os sistemas baseados em inteligência artificial permitem dar conselhos, previsões ou deduções sobre factos que lhe sejam conhecidos. E, através desta leitura de dados sobre situações concretas, os chamados *chatbots* podem auxiliar os cidadãos na obtenção de informações sobre benefícios e procedimentos administrativos. Assim, um *chatbot* explica como solicitar a reforma ou que documentos são

necessários para pedir um abono de família, ou para criar medidas ou previsões sobre eventuais situações que lhes sejam aproveitadas.

Contudo, veja-se que a utilização da inteligência artificial pode, também, ser utilizada para efeitos de medidas políticas preventivas em matéria de segurança social. Sendo um dos problemas da sustentabilidade da segurança social o envelhecimento da população e a diminuição da população ativa, a inteligência artificial pode ser utilizada para prever tendências demográficas e identificar necessidades futuras em termos de pensões ou subsídios. Um modelo preditivo calcula o impacto do envelhecimento da população na sustentabilidade do sistema de segurança social, auxiliando na criação de novas políticas públicas que poderão ter um impacto a médio e longo prazo.

Em todas estas situações, veja-se que, secundariamente, poderemos ter implicações numa dimensão puramente administrativa. As ferramentas de inteligência artificial podem otimizar a alocação de recursos humanos e financeiros no âmbito da atividade administrativa da Segurança Social. Através da implementação de algoritmos em áreas concretas de atuação do domínio da segurança social, podem os recursos humanos e financeiros ser mais bem alocados para ajudar a distribuir pessoal entre os diferentes serviços da Segurança Social, priorizando locais com maiores necessidades e carências.

4. A responsabilização dos atos praticados pela inteligência artificial aplicada pelas instituições de segurança social

4.1. Enquadramento

À capacidade automatizada de a inteligência artificial atuar em nome da Segurança Social e por conta dos interesses estaduais contrapõem-se um conjunto de questões que não devem ser absolvidas de importância. A par das preocupações éticas que subjazem à substituição do ser humano pelas máquinas pensantes, dir-se-á que problemas de natureza jurídica também se evidenciam na utilização destes sistemas de inteligência artificial. E falamos, essencialmente, na repercussão que os atos praticados têm e a sua imputabilidade enquanto atos dotados de juridicidade. Ou seja, centramo-nos no aspeto negativo que estes atos podem ter na esfera jurídica dos sujeitos envolvidos, designadamente em caso de os mesmos repercutirem negativamente e serem geradores de danos e prejuízos.

Ora, perante um Estado de Direito que espraia garantias de salvaguarda pela posição jurídica dos sujeitos, não pode o Direito deixar de se imiscuir na regulação das relações constituídas entre o Estado e os contribuintes, que sejam intermediadas ou instrumentalizadas por via de sistemas de inteligência artificial. É que diz-se desde já que não se admite uma integração de sistemas inteligentes

e automatizados que repercutam na esfera jurídica dos contribuintes por via do sacrilégio de direitos e interesses legalmente protegidos, de forma anacrónica e disruptiva do sistema jurídico. Ou seja, a admissibilidade destes sistemas de inteligência artificial termina onde o sacrifício pelos direitos e interesses legalmente protegidos dos contribuintes não sejam adequados, necessários e proporcionais. Por isso, impõe-se medidas regulatórias que visem adotar uma tutela digna e robusta que permita aos contribuintes reagir contra os atos praticados pelos sistemas de inteligência artificial adotados pela Segurança Social.

Pense-se, por exemplo, numa má recomendação feita por um *chatbot* criado pela Segurança Social. Quem deve ser responsabilizado por esses danos e, consequentemente, quem deve suportar os prejuízos causados por via de condutas positivas ou negativas dos sistemas de inteligência artificial? Por outro lado, são os institutos de responsabilidade civil clássicos capazes de responder às questões e especificidades próprias da inteligência artificial?

Vejamos então.

4.2. A responsabilização dos atos praticados pela inteligência artificial aplicada pelas instituições de Segurança Social

A responsabilidade pelas ações (ou omissões) praticadas por sistemas de inteligência artificial é uma das questões mais relevantes e desafiadoras no atual contexto social e jurídico. O tema tem despertado intenso debate doutrinário, com contribuições que exploram as diferentes modalidades de responsabilidade civil aplicáveis a danos causados por esses sistemas. Entre as principais abordagens destacam-se a aplicação dos institutos clássicos da responsabilidade civil, como a *objetiva* e a *subjetiva*, a *contratual* e a *extracontratual*, bem como a responsabilidade pelo *risco*, do *comitente* e do *produtor*.

Cada uma dessas teses busca oferecer um modelo adequado para lidar com as especificidades da inteligência artificial, contribuindo para o enriquecimento do debate jurídico e para a formulação de soluções que assegurem a proteção dos direitos das partes afetadas[17].

Porém, em todas as posições assumidas pela doutrina, emerge um consenso: os institutos clássicos de responsabilidade civil, na sua forma atual, são insuficientes para enfrentar os desafios impostos pela inteligência artificial. Essa insuficiência decorre da incapacidade dessas estruturas tradicionais de abarcar as particularidades da inteligência artificial, tais como a sua autonomia decisória, a opacidade dos seus algoritmos e a complexidade em estabelecer nexo causal ou atribuir culpa em contextos onde as decisões são tomadas por sistemas inteligentes.

---

[17] LUÍS MENEZES LEITÃO, *Direito das Obrigações: Volume I – Introdução. Da Constituição das Obrigações*, 15.ª ed., Coimbra, Almedina, 2019, pp. 279 e ss.

Diante disso, torna-se evidente a necessidade de repensar e adaptar os quadros jurídicos para responder de maneira eficaz às novas realidades tecnológicas[18].

No âmbito da atividade das instituições públicas de segurança social, veja-se que a atuação destes órgãos administrativos está vinculada à Constituição e à lei. Tal incumbência decorre do artigo 266.º, n.º 2, da Constituição da República Portuguesa, sendo a responsabilidade pelos atos e condutas dos seus agentes, funcionários ou instrumentos por ela utilizados disciplinada pelo regime da responsabilidade civil extracontratual do Estado, consagrado na Lei n.º 67/2007, de 31 de dezembro.

Este regime jurídico reflete o dever do Estado de ressarcir os danos causados pela administração, alinhando-se ao princípio da reposição da legalidade a que o poder público está sujeito. Tal consagração encontra-se no artigo 100.º da Lei Geral Tributária – o qual é aplicável por se tratar de uma norma de direito subsidiário face ao Direito da Segurança Social (cfr. artigo 3.º, alínea a), do Código dos Regimes Contributivos do Sistema Previdencial de Segurança Social) –, resultando desta norma o dever de reparação por danos causados aos contribuintes em decorrência da procedência total ou parcial de reclamações ou recursos administrativos, bem como de decisões judiciais favoráveis. Nesses casos, o Estado está obrigado a restituir plenamente a situação que existiria se o ato ilícito e danoso não tivesse sido praticado, garantindo, assim, a proteção efetiva dos direitos dos administrados[19].

Dessa forma, o referido instrumento normativo deve ser utilizado como parâmetro orientador na análise em curso, considerando que a atuação da Administração Pública está diretamente em questão. É importante esclarecer, desde já, que esta abordagem não pretende esgotar a complexidade do tema, mas, sim, focar especificamente na vertente da responsabilidade civil aplicável ao Estado e às demais pessoas coletivas de direito público. Essa delimitação é justificada pelo facto de que as condutas do Instituto da Segurança Social, I.P. se enquadram de maneira clara no regime especial de responsabilidade civil extracontratual do Estado, consagrado pela Lei n.º 67/2007, de 31 de dezembro. Tal enquadramento assegura um arquétipo jurídico adequado para tratar das situações em que a

[18] MAFALDA MIRANDA BARBOSA, *Inteligência Artificial. Entre a Utopia e a Distopia, Alguns Problemas Jurídicos*, Coimbra, Gestlegal, 2021; *Idem*, «O futuro da responsabilidade civil desafiada pela inteligência artificial: as dificuldades dos modelos tradicionais e caminhos de solução», *Revista de Direito Civil*, Vol. 2, Coimbra, Almedina, 2020, pp. 263 e ss.

[19] BÁRBARA PIAIRO DE SOUSA, *A Responsabilidade Civil da Administração Tributária – Os Atos Lesivos em Matéria Tributária*, Coimbra, Almedina, 2021, pp. 101 e ss.

administração, por ação ou omissão, venha a causar danos no exercício de suas funções públicas[20]/[21].

O regime jurídico da responsabilidade civil assenta numa verdadeira responsabilidade civil aquiliana. Tal entendimento pressupõe que, para que haja esta responsabilização da administração, importa verificar o preenchimento dos

[20] Foi com a reforma instituída em 1930 ao Código de Seabra que foi implementado, em Portugal, um regime jurídico que obrigava o Estado a reparar os danos causados pelos agentes e funcionários da Administração Pública. Consagrava, assim, o artigo 2399.º do mencionado diploma legal, que "os empregados públicos, de qualquer ordem ou graduações que sejam, não são responsáveis pelas perdas e danos que causem no desempenho das obrigações que lhes são impostas pela lei, excepto se excederem ou não cumprirem, de algum modo, as disposições da mesma lei, sendo neste caso, solidariamente com eles responsáveis as entidades de que forem serventuários".

[21] Historicamente, este instituto jurídico emerge do Estado Liberal, o qual resultou na ideia de que o Estado, obrigando-se ao cumprimento da legalidade, deveria respeitar que a sua atuação se mostrasse pautada pela legalidade vigente e em respeito por esta. Nesta senda axiológica, foram sendo aprovados um conjunto de institutos que procuravam dotar os administrados de meios de reação contra os atos lesivos do Estado e das demais pessoas coletivas públicas. Estas medidas foram constando de legislação avulsa e principalmente através do novo Código Civil de 1966, o qual consagra no seu artigo 501.º que "o Estado e demais pessoas coletivas públicas, quando haja danos causados a terceiro pelos seus órgãos, agentes ou representantes no exercício de actividades de gestão privada, respondem civilmente par esses danos nos termos em que os comitentes respondem pelos danos causados pelos seus comissários". Porém, não foi até 2007 que este instituto jurídico foi verdadeiramente autonomizado, sendo aprovado o regime da "Responsabilidade Civil Extracontratual do Estado e demais Entidades Públicas", pela Lei n.º 67/2007, de 31 de dezembro. O objeto de aplicação do presente instituto jurídico abrange danos resultantes do exercício da função legislativa, jurisdicional e administrativa, compreendendo nesta última, para efeitos deste exercício, ações e omissões adotadas no exercício de prerrogativas de poder público ou reguladas por disposições ou princípios de direito administrativo. Precisamente pelo dever de indemnização materializado obrigacionalmente na responsabilização do Estado, acaba por se consolidar um verdadeiro dever de reposição da situação factual, nomeadamente através das normas constitucionais previstas nos artigos 18.º e 266.º, n.º 1, da Constituição da República Portuguesa. Retira-se de uma leitura conjunta dos mencionados preceitos constitucionais, uma preocupação do legislador constituinte em dar cumprimento ao princípio da reposição da legalidade, designadamente pela proibição dos atos que sejam considerados danosos aos administrados, impedindo-se, assim, na tradução material de danosidade e de lesão na esfera jurídica dos sujeitos e na violação dos direitos e interesses legalmente tutelados destes. José Casalta Nabais, «Considerações sobre a responsabilidade civil da Administração Fiscal», *Scientia Iuridica*, tomo LXI, n.º 329, 2012.

seguintes pressupostos: i) o facto voluntário; ii) a ilicitude; iii) a imputação do facto ao lesante; iv) o dano; v) e o nexo de causalidade entre o facto e o dano[22]/[23].

Todos estes pressupostos podem ser arrumados, para efeitos sistemáticos do presente estudo, segundo um arranjo *objetivo* e *subjetivo*.

Numa dimensão *objetiva*, para que haja responsabilidade civil da administração, é necessário que seja praticado um ato que esteja em desconformidade com as regras e normas a que esta está vinculada, podendo tal ato ser imputado à administração, desde que exista um nexo de causalidade entre o ato e o dano causado. Esses atos ilícitos podem consistir em ações ou omissões de titulares de órgãos, funcionários ou agentes que violem disposições ou princípios constitucionais, legais ou regulamentares, infrinjam normas técnicas ou descumpram deveres objetivos de cuidado, resultando na violação de direitos ou interesses legalmente protegidos. Assim, a violação de normas jurídicas, sejam elas de natureza regulamentar, disciplinar, legal ou constitucional, que cause danos aos contribuintes, constitui fundamento para a responsabilização da administração. No entanto, a complexidade tecnológica e a ausência de uma disciplina jurídica específica sobre o tema desafiam a adaptação dessas condutas às realidades já conhecidas no ordenamento jurídico.

Perante uma dimensão *subjetiva*, é essencial destacar que o regime jurídico da responsabilidade civil extracontratual do Estado incorpora duas vertentes fundamentais no que diz respeito à responsabilização pelos atos praticados pelo Estado e outras entidades públicas. A primeira vertente, de natureza subjetiva, está prevista no artigo 7.º da Lei n.º 67/2007, de 31 de dezembro, segundo o qual "o Estado e as demais pessoas coletivas de direito público são exclusivamente responsáveis pelos danos que resultem de ações ou omissões ilícitas, cometidas com culpa leve, pelos titulares dos seus órgãos, funcionários ou agentes, no exercício da função administrativa e por causa desse exercício". A segunda vertente refere-se à responsabilidade objetiva pelo risco, consagrada no artigo 11.º do mesmo diploma. De acordo com esse dispositivo, "o Estado e as demais pessoas coletivas de direito público respondem pelos danos decorrentes de atividades, coisas ou serviços administrativos especialmente perigosos, salvo

[22] Sobre estes pressupostos do instituto jurídico da responsabilidade civil, LUÍS MENEZES LEITÃO, *Direito das Obrigações – Vol. I*, 8.ª ed., Coimbra, Almedina, 2009, pp. 287 e ss; ANTUNES VARELA, *Direito das Obrigações em Geral – Vol. I*, 10.ª ed., Coimbra, Almedina, 2000, pp. 525 e ss.; MÁRIO JÚLIO ALMEIDA COSTA, *Direito das Obrigações*, 12.ª ed., Coimbra, Almedina, 2011, pp. 557 e ss.

[23] Neste sentido, refere o Supremo Tribunal Administrativo que "são pressupostos da responsabilidade civil extracontratual por fatos lícitos: o ato administrativo legal ou material ilícito, o dano de que advenham prejuízos especiais e anormais, um interesse geral e o nexo causal entre o fato e o dano" – Acórdão do Supremo Tribunal Administrativo de 10/05/2006, processo n.º 0246/04, relatora: Conselheira Fernanda Xavier, disponível em http://www.dgsi.pt [consultado em 19/11/2024].

quando, nos termos gerais, se prove que houve força maior ou concorrência de culpa do lesado, podendo o tribunal, neste último caso, tendo em conta todas as circunstâncias, reduzir ou excluir a indemnização".

Perante a utilização de sistemas de inteligência artificial pelos órgãos da Segurança Social, essa dicotomia de responsabilidade é especialmente relevante. Não se pode conceber os sistemas de inteligência artificial como uma entidade distinta do órgão público que utiliza essas ferramentas. A implementação de inteligência artificial nas operações não exime o Instituto da Segurança Social, I.P. da obrigação de atuar conforme as normas jurídicas que regulam a sua função administrativa. Ademais, considerando a natureza potencialmente perigosa ou sensível das atividades mediadas por sistemas inteligentes, pode-se enquadrá-las como uma atividade de risco, sujeita ao regime de responsabilidade objetiva. Assim, mesmo que a instrumentalização da inteligência artificial vise a eficiência administrativa, a administração permanece vinculada às obrigações legais que norteiam a sua atuação, sendo responsável pelos danos que possam surgir da sua utilização, direta ou indireta[24].

O Instituto da Segurança Social, I.P. que utilize na sua gestão e aplicação das normas jurídicas sistemas de inteligência artificial é um órgão administrativo, pois não deixa de ser a Administração Pública, e, portanto, está sujeito às prerrogativas legais exigidas na sua função administrativa. Por isso integra esta dimensão subjetiva, e responde nos termos da mencionada Lei n.º 67/2007, de 31 de dezembro, sendo o Estado responsável, civilmente, pelos danos e prejuízos causados (cf. artigo 1.º, n.º 1 e n.º 2, da referida lei).

Deste modo, a sua aplicabilidade é inegável e até desejada num contexto garantístico em que se pretende salvaguardar os direitos e liberdades dos contribuintes. O Estado acabará por ser responsável – de forma solidária com o próprio produtor, se se revelar culpa deste – quando o dano ocorrido for resultado de ações ou omissões que sejam praticados de forma ilícita, cometidas com dolo ou culpa grave, por agentes ou funcionários no decorrer da sua atividade pública. Daí que, atendendo à fragilidade dos sujeitos, ressalve o legislador que, sem prejuízo da demonstração de dolo ou culpa grave, presume-se a existência de culpa leve na prática de atos jurídicos ilícitos (cf. artigo 10.º, n.º 2, e artigo 11.º,

[24] JOSÉ GONZÁLEZ, «Responsabilidade por danos e Inteligência Artificial (IA)», *Revista de Direito Comercial*, n.º 1, 2020, pp. 69-112, disponível em https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5e5c279317c29a501a4c55e2/1583097749667/2020-02+-+069-112.pdf [consultado em 19/11/2024].

n.º 2, da Lei n.º 67/2007, de 31 de dezembro)[25]. Assim, é-lhe conferido um potencial aplicativo que obriga a administração a provar que o ato ilícito praticado não lhe pode ser censurado, segundo um juízo de culpabilidade. A identidade deste regime de responsabilidade civil mostra a preocupação do legislador em consagrar um instituto jurídico adequado e assente na preocupação pelos contribuintes[26], já que a distribuição probatória ficaria gravemente comprometida – sendo ainda assim criticável –, caso tal inversão não se verificasse, traduzindo-se numa verdadeira *diabolica probatio*.

Por outro lado, a utilização de sistemas de inteligência artificial deve ser pautada por princípios próprios, designadamente de matriz publicista, quando a relação jurídica em causa seja ou tenha por objeto o interesse público. Os sistemas de inteligência artificial que sejam considerados de risco elevado devem ser concebidos e desenvolvidos segundo critérios de funcionamento simples, suficientemente transparentes e cujas informações essenciais de funcionamento e que envolvam atuações consideradas potencialmente perigosas para os sujeitos sejam conhecidas, de modo a permitir aos utilizadores interpretar o resultado do sistema (cfr. artigo 13.º do Regulamento Inteligência Artificial, aprovado pelo Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho). E, dadas as especificidades da própria inteligência artificial, veja-se que a atuação é objeto de um registo de todos os eventos suscetíveis de gerarem um dano (cfr. artigo 12.º, n.º 1, do Regulamento Inteligência Artificial). Os registos dos atos praticados pelos sistemas de inteligência artificial direcionam-se no sentido de dotar os destinatários e utilizadores de informações completas e precisas sobre toda a tramitação praticada, assegurando assim um nível de rastreabilidade que identifica o *iter* decisório do sistema de apoio informatizado. Por isso, concebe-se um sistema instrumental e não autónomo (pelo menos no sentido pleno), pois, conforme dispõe o artigo 14.º, n.º 1, do Regulamento Inteligência Artificial, "os sistemas de inteligência artificial de risco elevado devem ser concebidos e desenvolvidos de tal modo, incluindo com ferramentas de interface homem-máquina apropriadas, que possam ser eficazmente supervisionados por pessoas singulares durante o período de utilização do sistema de inteligência artificial". Ou seja, suscita-se uma supervisão humana plena e imprescindível que

[25] Como refere VIEIRA DE ANDRADE, esta responsabilidade está ligada à prática de atos com "diligência e zelo manifestamente inferiores àqueles a que se encontravam obrigados em razão do cargo". JOSÉ CARLOS VIEIRA DE ANDRADE, «Responsabilidade por danos decorrentes do exercício da função administrativa na nova Lei sobre responsabilidade civil extracontratual do Estado e demais entes públicos», *Revista de Legislação e de Jurisprudência*, ano 137.º, n.º 3951, julho-agosto de 2008.

[26] "O ónus da prova inverte-se quando exista uma presunção legal ou quando a parte contrária tiver, com culpa, tornado impossível a prova do onerado". Acórdão do Tribunal da Relação de Coimbra de 10/09/2013, processo n.º 171/10.8TBSAT.C1, relator: desembargador Henriques Antunes, disponível em http://www.dgsi.pt [consultado em 19/11/2024].

procura prevenir ou minimizar os riscos para a saúde, a segurança ou os direitos fundamentais que possam surgir quando um sistema de inteligência de risco elevado é usado em conformidade com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsíveis, em especial quando esses riscos persistem apesar da aplicação das condicionantes impostas legalmente.

Assim, conclui-se que todos estes mecanismos garantísticos e de mitigação de riscos adotados no Regulamento Inteligência Artificial permitem convergir na convocação de um instituto de responsabilidade civil. Será através do incumprimento dos deveres a que a máquina e o seu supervisor humano estão adstritos, cognoscíveis através das medidas indicadas, que os sujeitos terão conhecimento dos atos ilícitos praticados, permitindo-lhes, assim, reagir contra as atuações lesivas e que causem um prejuízo ou dano considerável no seu património. Apenas tendo como premissa este dever de informação será possível aferir o momento concreto em que o comportamento desviante operou e gerou a conduta considerada lesiva para o lesado e, consequentemente, a determinação da pessoa responsável por este ato danoso.

5. Conclusão

Ora, após esta breve digressão por alguns considerandos de positividade e de tensões geradas pela utilização da inteligência artificial pela Segurança Social, somos obrigados a tecer algumas considerações finais, sem, contudo, apresentar soluções "mágicas" e perentórias, pois não temos uma "varinha mágica" que nos permita dotar o leitor perante um balanço positivo ou negativo na sua utilização.

Neste sentido, uma ideia principal assume-se como matricial neste trabalho: a utilização de sistemas de inteligência artificial no âmbito da Segurança Social é uma realidade e uma inevitabilidade, mas sem descuidar a posição jurídica dos destinatários envolvidos, designadamente os contribuintes. Tal reconhecimento concentra-se na ideia do Estado de Direito, pelo que uma solução adequada se desenvolve mediante a centralidade que o ser humano assume no sistema jurídico. Não discutimos teses disruptivas (e até utópicas), designadamente a incorporação dos arquétipos societários nos sistemas de inteligência artificial. Consideramos, sim, que a solução passará pela adaptação dos institutos de responsabilidade civil clássicos, ou mesmo a criação de um novo regime que permita dar enquadramento aos problemas e vicissitudes derivadas destas novas realidades.

Mas o caminho passará por ser pacientes e, devido ao facto de não existirem soluções mágicas, é dever da academia e dos órgãos legiferantes competentes encontrar soluções adequadas, com base na sensibilização e na estabilidade das relações jurídicas constituídas para, assim, estabelecer um instituto jurídico suficientemente robusto e forte para tutelar todas as posições e sujeitos envolvidos.

THE TREATMENT OF WORKS OF APPLIED ART UNDER PORTUGUESE LAW IN THE POST-*COFEMEL* ERA

Maria Victória Rocha[*]

Abstract: The preliminary ruling of the Court of Justice of the European Union (CJ) in *Cofemel*, C-683/17 (*Cofemel*) addressed two issues. First, partial cumulation was unequivocally established. Not all designs may be protected by copyright. Only those that qualify as "works" deserve cumulation of protections. Second, the CJ considered that the concept of "work" is already harmonized, being an autonomous and uniform concept of the European Union (EU). Copyright protection requires originality in the sense that the subject matter at issue is an intellectual creation of its author, and the subject matter must be expressed in an identifiable object with sufficient precision and objectivity. Yet, the CJ *Cofemel* ruling was vague and ambiguous. It did not provide guidelines capable of leading to a coherent and predictable case law, expressing a uniform understanding of what an "artistic creation" is regarding designs, works of applied art, and works of design, under Article 2(1)(i) of the Portuguese Copyright and Related Rights Code. The absence of consensus regarding this concept was the main reason for the divergent and unpredictable national case law. The Portuguese provision is not clear, and there were different approaches in national scholarship. This led

* Auxiliar Professor of Universidade Católica Portuguesa, Escola de Direito do Porto. Member and investigator of CEID – Católica Research Centre for the Future of Law. Senior investigator of GEDAI – Grupo de Estudos de Direito Autoral e Industrial da Universidade Federal do Paraná. Member of the Spanish Project of "Moda y Bienes Immateriales". This work is part of the project I + D + i PID2020-112707GB-I00, MODA Y BIENES INMATERIALES, funded by MCIN/AEI/10.13039/501100011033. Email: *virocha@ucp.pt*

to the twofold inquiry made by the Portuguese Supreme Court, but the issue remains unsolved. After the CJ *Cofemel* ruling, the question of what should be understood as "artistic creation" has been deepened by scholarship, which, as before, has influenced the national case law in the post-*Cofemel* era.

Keywords: Copyright; Design; Works of pure art; Works of applied art; Works of design; Originality; Work; Flos; Cofemel; Brompton.

Resumo: A decisão prejudicial do Tribunal de Justiça da União Europeia (TJ) no caso *Cofemel*, C-683/17 (*Cofemel*), abordou duas questões. Em primeiro lugar, a cumulação parcial foi inequivocamente estabelecida. Nem todos os desenhos ou modelos podem estar protegidos por direitos de autor. Apenas aqueles que se qualificam como "obras" merecem cumulação de proteções. Em segundo lugar, o TJ considerou que o conceito de "obra" já está harmonizado, sendo um conceito autónomo e uniforme da União Europeia (UE). A proteção pelo direito de autor exige originalidade no sentido de que o bem em causa seja uma criação intelectual do seu autor, devendo ser expresso num objeto identificável com suficiente precisão e objetividade. No entanto, o Acórdão *Cofemel* do TJ é vago e ambíguo. Não forneceu orientações capazes de conduzir a uma jurisprudência coerente e previsível, expressando um entendimento uniforme do que é uma "criação artística" no que respeita a desenhos ou modelos, obras de arte aplicada e obras de design, nos termos do artigo 2.º, n.º 1, alínea i), do Código do Direito de Autor e dos Direitos Conexos. A ausência de consenso em relação a este conceito foi a principal razão para a divergência e imprevisibilidade da jurisprudência nacional. A norma portuguesa não é clara e foi alvo de abordagens diferentes na doutrina e jurisprudência nacionais. Tal conduziu às questões colocadas pelo Supremo Tribunal de Justiça em sede de reenvio prejudicial. Todavia, o problema continua por resolver. Após a decisão do TJ no caso *Cofemel*, a questão do que deve ser entendido como "criação artística" foi aprofundada pela doutrina, que, como antes, continuou a influenciar a jurisprudência nacional na era pós-*Cofemel*.

Palavras-chave: Direito de autor; Desenhos ou modelos; Obras de arte pura; Obras de arte aplicada; Obras de design; Originalidade; Obra; Flos; Cofemel; Brompton.

Introduction

The protection of designs, works of applied art, and works of design results from two different sets of law in Portugal. The Portuguese Industrial Property Code[1] and Regulation 6/2002[2] address the protection of design. The Portuguese Copyright and Related Rights Code[3] addresses the protection of this subject matter by copyright.

The exterior appearance of a product may be protected as exclusive industrial property right and as copyrighted work. The requirements of both protections are different. In certain situations, there may be a cumulation of protections, as stated under Articles 194 of CPI, 96(2) of CDR, and 2(1)(i) of CDADC. The cumulation of protections is imposed by Article 17 of Directive 98/71[4], but each Member State may seemingly determine the conditions of protection, including the degree of "originality", as stated by the second sentence of this provision.

The Portuguese legislator never defined the concept of "originality," leaving that matter to be solved by scholarship and case law. The legislator transcribed the wording of the first part of Article 17 of the Design Directive[5], ignoring the invitation of the second part of the same provision. Article 194 of the CPI (that repeat Article 200 of the CPI of 2003) titled "Relationship with copyright" states that any registered design shall also be eligible for protection under copyright law as from the date when the design was created, or defined, in any form. The inertia of the national legislature led to doubts on the meaning and scope of Article 194 CPI regarding the requirements for cumulation of protections.

Because of the wording of Article 194 (and before, of Article 200 of CPI 2003), which only refers to "registered design", doubts on whether unregistered design could benefit from cumulation of protections were raised. Nevertheless, if

[1] Código da Propriedade Industrial of 2018 (CPI).

[2] Council Regulation (EC) No. 6/2002 of 12 December 2001 on Community designs, *OJ L 3*, 5.1.2002, pp. 1-24 (CDR).

[3] In portuguese, Código do Direito de Autor e dos Direitos Conexos of 1985 (CDADC).

[4] Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs. *OJ L 289*, 28.10.1998, pp. 28-35 (Design Directive).

[5] Article 17 of Directive 98/7 headed "Relationship to copyright" states, "A design protected by a design right registered in or in respect of a Member State in accordance with this Directive shall also be eligible for protection under the law of copyright of that State as from the date on which the design was created or fixed in any form. The extent to which, and the conditions under which, such a protection is conferred, including the level of originality required, shall be determined by each Member State."

the EU law protects unregistered design, it also applies for copyright protection.[6] For the fashion industry it is crucial to know whether and when design may be protected by copyright, namely because copyright grants a much longer protection and does not require any formality to arise.

1. Portuguese situation before the CJ *Cofemel* preliminary ruling

EU copyright legislation formally harmonized the concept of originality only in relation to specific subject matter, namely software (Article 1(3) of both Software Directives)[7], databases (Article 3(1) of Database Directive)[8] and photographs (Article 6 of Term Directives)[9]. Article 14 of Directive 2019/790 codifies CJ case law, stating that works must be the author's own original creation[10].

---

[6] In the judgment of the Court of Appeal of Guimarães of 27.02.2012, Case *J. M. Carvalho Araújo v Bruma* (Proc. 1607/103TBBRG), when the 2003 CPI was in force, and the provision concerning cumulation of protections of design and copyright was Article 200 of said CPI (repeated in Article 194 of 2018 CPI) the Court of Appeal ruled that cumulation of protections was only possible when the design is registered. That interpretation is wrong. Article 96(2) of CDR allows copyright protection to any design protected by the CDR, regardless of whether it is registered or unregistered (the latter is protected under Article 11 of CDR). In Portugal the cumulative protection of unregistered Community designs is inevitable because of CDR. Article 194 of 2018 CPI cannot be understood considering only the wording of the provision. Recent proposals to amend the CDR and Directive 98/71/CE reflect this idea. Proposed Article 96(2) states that any design protected as EU design benefits also from the protection granted by copyright from the moment when that design was created of defined in any manner, provided that the requirements of EU copyright law are met (see Proposals of amendment of the CDR and of Directive 98/71/CE, COM (2022) 666 final, and COM (2022) 667 final, of 28 November 2022). Regarding unregistered design, see Sara Louredo Casado, *El Diseño Industrial no Registrado*, Madrid, Aranzadi-Thomson Reuters, 2019, pp. 237ff.

[7] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance), *OJ L 111*, 5.5.2009, pp. 16-22 (Software Directive), that replaced Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *OJ L 122*, 17.05.1991, pp. 0042-0046 (first Software Directive), consolidating the various minor amendments the original directive received over the years.

[8] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of database, *OJ L 77*, 27.3.1996, pp. 20-28 (Database Directive).

[9] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version) *OJ L 372*, 27.12.2006, pp. 12-18, that replaced the original Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights, *OJ L 290*, 24.11.1993, pp. 9-13, codifying and harmonizing several changes. Directive 2011/77/EU of the European Parliament and of the Council of 27 September 2011 amending Directive 2006/116/EC on the term of protection of copyright and certain related rights, *OJ L 265*, 11.10.2011, pp. 1-5, did not touch this subject.

[10] E.g., Judgment of 13.11.2018 *Levola Hengelo*, C-310/17, EU:C:2018:899, par. 36, Judgment of 4.10.2011, Football Association Premier League, C-403/08 y C-429/08, EU:C:2011:631, par. 97

Case law before the *Cofemel* preliminary ruling[11] was erratic and unpredictable because Portuguese scholarship had (and still has) divergent approaches regarding the concept of "artistic creation" under Article (2)(1)(i) of the Portuguese CDADC. Article 2 provides a non-exhaustive list of protectable subject matter, including, in section (1), subparagraph (i), "works of applied art, industrial designs and design works that constitute an artistic creation".

Regarding the relation between Article 194 of CPI 2018 (before, Article 200 CPI 2003) and Article (2)(1)(i) of CDADC, though scholars considered that Portugal had a partial cumulative protection, many of them demanded a higher degree of artistic value for cumulation of protections to be possible. Bárbara Ribeiro Quintela considered that the "artistic creation" was an extra obligation imposing an assessment of the merits of the subject matter in question.[12] This approach is still shared by Menezes Leitão, who considers that cumulation of protections shall only be possible if there is a qualified artistic creation, in the sense that the protected design raises, in addition to its functional application, an assessment of merit in aesthetic terms, which is the subject of external recognition.[13] OLIVEIRA ASCENSÃO also considered that works of applied art could only be protected by copyright when their artistic character clearly prevailed over the industrial destination of the object.[14] Though defending partial cumulation of protections, Portuguese scholars have always been against the idea of entering into the artistic value because copyright protection is independent of the merits of the creation (as stated in the general clause of Article 2 of CDADC). Designs, works of applied art, and works of design ought to be protected by copyright if, as it happens with any type of work, the requirements of copyright protection are met. If we are before a work of the artistic domain, recognized as such by the specialized circles, the subject matter at issue ought to be protected by copyright as "work".[15] PEDRO SOUSA E SILVA always considered that not all designs should be protected by copyright, but only those that constitute an "artistic work", which has nothing to do with merits but has to do with the recognition as such by specialized circles. If deemed necessary, there should be expert evidence. To know if

[11] Judgment of 12.09.2019, *Cofemel v. G-Star Raw*, C-683/17, EU:C:2019:721.

[12] BÁRBARA RIBEIRO QUINTELA, «A tutela jurídica da moda pelos regimes dos desenhos ou modelos», in *Direito Industrial*, Vol. V, 2008, pp. 477-1528 (501 ff., 506 ff.).

[13] LUÍS MANUEL TELES DE MENEZES LEITÃO, *Direito de Autor*, 4.ª ed., Coimbra, Almedina, 2021, p. 93.

[14] JOSÉ DE OLIVEIRA ASCENSÃO, *Direito de Autor e Direitos Conexos*, Reimpressão, Coimbra, Coimbra Editora, 2012, pp. 92ff. (94).

[15] MARIA VICTÓRIA ROCHA, «Proteção autoral para modelos de vestuário? [Ac. do Tribunal de Justiça da União Europeia no caso Cofemel/G-Star (C-683/17) de 12.09.2019]», *Revista de Direito Intelectual*, 2021, no. 1, pp. 221-239 (228-231).

we are before an "artistic work" is a fact that must be proved.[16] JOSÉ ALBERTO VIEIRA, criticizing the way design, works of applied art, and works of design appear in the CDADC, considers that the reason why subparagraph (i) uses the expression "artistic creation" instead of the usual expression "intellectual creation", which appears in the body of Article 2(1) and in Article 1 of CDADC, is just because creativity in this type of works has to do with its aesthetical aspect. The expression does not mean that an extra requirement is needed. Subparagraph (i) is just a different way of saying that the general requirement of "intellectual creation" must exist for the subject matter to be protected by copyright.[17]

Due to the lack of clarity of Article 2 (1)(i) of CDADC and the lack of consensus among Portuguese scholarship, together with the lack of a general definition of the concept of "work" and of "originality on the part of the EU legislator, it was impossible to predict how Portuguese courts would decide the issue of cumulation between design protection and copyright protection.

Here are the most important examples of Portuguese case law before the CJ *Cofemel* preliminary ruling:[18]

a) Court of Appeal of Porto, in 2006, granted copyrights to a furniture designer of a model of armchair and ordered the defendant to pay the author a compensation for the infringement of those rights.[19]

b) Court of Appeal of Guimarães, in 2012, refused the protection by copyright to a range of designer taps for the kitchen and bathroom, conceived by architect Carvalho de Araújo, because they were not considered an artistic creation.[20]

---

[16] PEDRO SOUSA E SILVA, «Desenhos ou modelos no novo CPI. O que muda e o que não muda com o Ac. Cofemel», *Revista de Direito Intelectual*, 2019, no. 2, pp. 189-204 (196-197).

[17] JOSÉ ALBERTO VIEIRA, *Direito de Autor*, Coimbra, Almedina, 2020, pp. 93-98 (95).

[18] For a deeper analysis of this case law and for the relation between protected design and copyright, see PEDRO SOUSA E SILVA, *A Proteção Jurídica do Design*, Coimbra, Almedina, 2017, pp. 243ff.; *Direito Industrial. Noções Fundamentais*, Coimbra, Almedina, 2019, pp. 164-206, «Desenhos ou modelos no novo CPI…», *op. cit.*, pp. 189ff., *Código da Propriedade Industrial Anotado*, annotation to Article 194 (Coord. LUÍS MANUEL COUTO GONÇALVES), Coimbra, Almedina, 2021, pp. 783ff., and «Tutela Jusautoral de Obras de Design na esteira do Acórdão Cofemel: Nada de Novo Debaixo do Céu», *Revista de Direito Intelectual*, 2023, no. 1, pp. 171-196; LUÍS MANUEL COUTO GONÇALVES, *Manual de Direito Industrial*, 9.ª ed., Coimbra, Almedina, 2022, pp. 163--168; MANUEL OEHEN MENDES, «A obra enquanto objecto do direito de autor», *Revista de Direito Intelectual*, 2021, no. 1, pp. 41-73; MARIA VICTÓRIA ROCHA, «Proteção autoral para modelos de vestuário?...», *op. cit.*, pp. 221-239.

[19] Decision of 23.11.2006 (Proc. 0633334, dgsi.pt).

[20] Decision of 27.02.2012 (Proc.1607/103TBBRG, dgsi.pt).

c) Court of Appeal of Lisbon, in 2017, considered that design of jeans, sweatshirts, and t-shirts should be protected by copyright.[21]

d) Court of Appeal of Porto, in 2018, considered that it would be inappropriate to qualify as an artistic creation a line of garden furniture.[22]

e) Court of Appeal of Lisbon, in 2018, refused to protect paper bins, garden benches, and concrete planters as copyrighted works. They were considered objects of urban furniture, of an industrial nature, with a merely functional design. Thus, they could not be considered artistic creations.[23]

f) Court of Appeal of Lisbon, in 2018, considered that design of light fittings by architect Souto de Moura deserved protection by copyright.[24]

[21] Decision of 21.02.2017 (Proc.268/13.2YHLSB, dgsi.pt). This decision was object of appeal to the Portuguese Supreme Court (herein after STJ) that decided to stay the proceedings and requested for a preliminary ruling by the CJ, which originated the decision of the STJ of 15.01.2020, *Cofemel v. G-Star* (Proc. 268/13.2YHLSB.L1. S1, Rel.: Maria do Rosário Morgado).

[22] Decision of 25.10.2018 (Proc. 364/12.3TVPRT, dgsi.pt).

[23] Decision of 9.01.2018 (Proc. 76/14.3YHLSB, dgsi.pt), confirmed by the STJ decision, in 27.09.2018 (dgsi.pt).

[24] Decision of 10.04.2018 (Proc.225/13/13.9YHLSB.L1-7, dgsi.pt). With the same grounds, the STJ confirmed this decision without waiting for the results of the preliminary ruling of the CJ concerning the *Cofemel* case.

In conclusion, it was not really possible to discover a coherent course in Portuguese case law. This led to the request for a preliminary ruling by the CJ.[25]

[25] The dispute in the main proceeding related to the alleged infringement of G-Star's copyrights by Cofemel. Cofemel and G-Star are two clothing companies. G-Star is a Dutch clothing company established in 1989, specialized in manufacturing raw denim. Cofemel is a Portuguese Company established in 1982 that designs, produces, and sells jeans, t-shirts, and sweatshirts under the trademark "Tiffosi". Since the 1990s, G-Star is owner or has exclusive licenses of the trademarks G-STAR, G-STAR RAW, G-STAR DENIM RAW, GS-RAW and RAW. The clothing designed, produced, and placed on the market under these trademarks includes jeans with the design known as "ARC" and t-shirts and sweatshirts with the design known as "ROWDY". In 2013, G-Star company brought an action before a Portuguese Court of first instance requesting that Cofemel be ordered to cease any acts constituting an infringement of its copyright (and unfair competition). In support of its action, G-Star argued that some designs of jeans, t-shirts, and sweatshirts produced and sold by Cofemel were comparable to its "ARC" and "ROWDY" designs. The clothing at issue were intellectual original creations and ought to be considered works, protected by copyright. In its defense, Cofemel argued that the elements that it had allegedly copied represented mere industry trends. The court of first instance partially upheld G-Star's action and considered there was an infringement of its copyrights. In its defence, Cofemel argued that the elements that it had allegedly copied represented mere industry trends. Cofemel maintained that under Article 2(1)(i) of CDADC that designs must be considered as "artistic creations" by the relevant institutional and cultural sector to be eligible for copyright protection, which was not the case. The court of first instance decided in favor of G-Star, considering that the CJ case law on originality entailed that Article 2(1)(i) of CDADC could not demand a reinforced artistic creativity to protect G-Star design. Cofemel brought an appeal against that action before the Court of Appeal of Lisbon, which upheld the judgment of the court of first instance. The Court of Appeal considered that Article 2(1)(i) of the CDADC ought to be seen considering Directive 2001/29, as interpreted by the CJ in the judgments of 16.07.2009, *Infopaq International* (C-5/08, EU:C:2009:465), and of 01.12.2011, *Painer* (C-145/10, EU:C:2011:798). This meant that copyright protection enclosed works of applied art, industrial designs, and works of design, provided that such subject matter was "original," that is, was the result of the author's own creation and no further requirements ought to be added, as a particular degree of aesthetic or artistic value. "ARC" and "ROWDY" clothing designs of G-Star were copyright protected works. Some of the clothing produced and sold by Cofemel infringed G-Star's copyrights.

2. Conclusions taken from the CJ *Cofemel* preliminary ruling

The Portuguese Supreme Court decided to stay the proceedings and refer two questions to the CJ for a preliminary ruling.[26] The first one asked if the CJ's interpretation of Article 2(a) of Directive 2001/29[27] precluded national legislation [Article 2(1)(i) of CDADC], which confers copyright protection upon works of applied art, industrial designs, and works of design that, over and above the utilitarian purpose they serve, create their own visual and distinctive effect from an aesthetic point of view, their originality being the fundamental criterion for the attribution of copyright protection. The second question was if the interpretation by the Court of Article 2(a) of InfoSoc Directive precluded national legislation [Article 2(1) (i) of CDADC] that confers copyright protection on works of applied art, industrial designs, and works of design only if they qualify as "artistic creations" or "works of art", in light of a particularly demanding

[26] The *Cofemel* case has been the subject of extensive analysis by national and international scholarship. Beyond the Portuguese scholars, already mentioned, see FERNANDO CARBAJO CASCÓN, «Objetos Industriales, Derecho de Autor y Libre Competencia, Consideraciones a partir de las SSTJEU de 12 de Septiembre de 2019 ("Cofemel") y 11 de Junio de 2020 (Brompton)», *Cuadernos de Derecho Transnacional*, Vol. 12, No. 2, Octubre 2020, pp. 913-942, and «La protección de los diseños de moda en la Unión Europea (entre el diseño industrial y el derecho de autor)», *Cuadernos del Centro de Estudios de Diseño y Comunicación*, No. 106, Febrero 2020, pp. 139-162; Tobias Endrich-Laimböck, «Litle Guidance for the Application of Copyright Law to designs in *Cofemel*», *GRUR-International*, 69 (3), 2020, pp. 264-269; Koray Güven, «Eliminating "Aesthetics" from Copyright Law: The Aftermath of *Cofemel*», *GRUR International*, 71 (3), 2022, pp. 213--225; Annette Kur, «Unité de l'art is here to stay – Cofemel and its Consequences», *Max Planck Institute for Innovation and Competition Research Paper Series,* 12 Dec. 2019, No. 19-16, pp. 1-22; Matthias Leistner, «Einheitlicher europäischer Werkbegriff auch im Bereich der angewandten Kunst – Warum sich für die deutsche Praxis dennoch nicht viel ändern sollte», *GRUR*, no. 11, 2019, pp. 1114-1120; Eleonora Rosati, «CJEU rules that copyright protection for designs only requires sufficient originality», *JIPLP – Journal of Intellectual Property Law & Practice*, Vol. 14, No. 12, 2019, pp. 931-932; Tito Rendas, «Copyright protection of designs in the EU: how many originality standards is too many?», *JIPLP – Journal of Intellectual Law & Practice*, Vol. 13, No. 6, 2018, pp. 439-441.

[27] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, *OJ L 167*, 22.6.2001, p. 9 (InfoSoc Directive).

appreciation that takes into account the prevailing conceptions within institutional and cultural circles.[28]

The decision of the CJ was not clear in many aspects, but it established the unequivocal solution of partial cumulation of protections. This is the first conclusion we can take from this ruling. The CJ clarified that not all designs can benefit from copyright protection: only those that can be qualified as "works" in the sense of InfoSoc Directive can. A protected design is not, as a rule, a "work" protected by InfoSoc Directive (paragraphs 39 to 42 of the CJ ruling[29]).

The CJ stressed that Article 17 of Directive 98/71 states that registered designs are also eligible for copyright protection, but the second sentence of Article 17 of this Directive leaves total freedom for Member States to determine the requirements for copyright protection. Regarding designs protected at the EU level, rules comparable to those of Article 17 of Directive 98/71 are laid down in Article 96(2) of CDR (for more detail, see paragraphs 41 to 47). According to the CJ, designs can be classified as "works" within the meaning of InfoSoc Directive if they meet the requirements set in paragraph 29 of the CJ ruling (see paragraph 48), but the protection of designs and copyright protection have different objectives and are subject to distinct rules. The protection of designs aims to protect subject matter that, being new and distinctive, is functional and liable to be mass-produced. That protection is to apply for a limited time (up to 25 years regarding registered design and up to three years regarding Community unregistered design), but is sufficient to ensure a return on the investment necessary

[28] The way the Portuguese STJ paraphrased its questions was not the best, and it is rather unclear. What the STJ wanted to know, given the divergent positions in Portuguese scholarship and in Portuguese case law, was whether the reference to "artistic creation" in Article 2(1)(i) of CDADC, means that the works of applied art, designs, and works of design listed in this subparagraph must satisfy a different, higher threshold to achieve copyright protection, or whether all categories of works are subject to the common standard of "originality". But instead of asking whether the standards for protection of works of applied art are the same as for other categories of works, the STJ referred two questions with two different types of qualifiers: one requiring an aesthetically significant visual effect, going beyond the subject matter's utilitarian function; the other referring to a markedly strict assessment of artistic character according to the opinion prevailing in cultural and institutional circles. The way the STJ put the first question created a dilemma for the CJ. The Court wanted to use the criteria enunciated in *Infopaq* and subsequent case law, but the CJ and even more, the Advocate General, did not want to grant protection to the subject matter at issue. Therefore, both declared that while cumulation of design and copyright cannot be excluded, this is not the general rule, but it is an exception in certain cases, with a clear subtext meaning, excluding cases like this (see C-683/17, *Cofemel*, paragraph 52; see also the reasoning of the Advocate General Spuznar, regarding the harmful consequences of overprotection of works of applied art or designs by copyright (Case C-683/17, *Cofemel*, EU:C:2019:363, opinion of Advocate General Spuznar, paragraphs 50 to 66). Criticizing the way the STJ questioned the CJ, see Annette Kur, «Unité de l'art is here to stay – Cofemel and its Consequences», *op. cit.* (pp. 5-6); Maria Victória Rocha, «Proteção autoral para modelos de vestuário?...», *op. cit.* (p. 234).

[29] Paragraph 42 mentions *Levola Hengelo*, C-310/17, EU:C:2018:899, paragraph 38.

for the creation and production of the subject matter at issue without excessively restricting competition. The protection by copyright, the duration of which is significantly greater (as a rule, regarding patrimonial rights, up to 70 years after the death of the author, though other subsidiary rules apply in special cases), is limited to subject matter that may be classified as "work" (see paragraphs 50, 51, and 52). The type of protection granted by each set of rules is different. Copyright protection allows the author to prohibit unauthorized copying and other uses, but the author cannot prevent third parties from creating and exploiting works resulting from an independent creation, though equal or similar. The protection of a registered design covers any design that does not cause in the informed user a different overall impression by providing objective protection that can be relied on even against third parties acting in good faith (though unregistered designs have a "copyright approach" protection).

For some scholars, the indication that cumulation can only occur in "certain cases" seems too vague. A total overlap of protections between design and copyright of a certain subject matter is precluded by the structural diversities between those fields. The author-centered concept of originality in copyright law entails the concept of subjective novelty and the possibility of protecting parallel creations. Copyright protects a design against acts of copying, while design law grants absolute protection against any design producing the same overall impression (except for non-registered EU design that have copyright approach protection). Differences between design law and copyright law are conceptual, not gradual. Partial cumulation exists independently of the "level" of originality required for the protection of designs. Partial cumulation is a description, not a goal that must be achieved by applying the criterion of originality. Paragraphs 50 to 52 of the CJ ruling regarding copyright/design interface are merely descriptive statements.[30]

Other scholars consider that paragraphs 51 and 52 of the CJ decision formulate rules or guiding principles for interpreting copyright law. Since copyright lasts longer, copyright protection is broader and must be limited to certain designs that are particularly worthy of protection. Total cumulation, by granting longer copyright protection to designs, would undermine the still nuanced legislative decisions regarding design law with its narrower scope of protection (namely, defined by its length, the need to register, and stricter exceptions or limitations). From this could follow a rule-exception ratio that seeks to limit

[30] In this sense, see Tobias Endrich-Laimböck, «Litle Guidance for the Application of Copyright Law to designs in *Cofemel*», *op. cit.* (p. 267); Annette Kur, «Unité de l'art is here to stay – Cofemel and its Consequences», *op. cit.* (p. 1011).

the cumulative protection.[31] Though we think that total cumulative protection is never possible, we agree with the authors that consider that the CJ was clear in requiring a restricted partial cumulation of protections.

The concerns expressed by AG that by granting copyright protection too generously, the design regime will run void (see paragraph 52), do not convince us. There is little reason to fear that who makes use of design registration under current conditions will abandon design law in large numbers if it was generally accepted that this area is also covered to a fair extent by copyright. This is for two reasons: first, because EU law grants cumulative protection; second, because design protection carries the advantage of providing the holder with a demonstrable exclusive, absolute right, and the burden of proof is placed on those that challenge the design's validity. The effectiveness of design law is not menaced because such protection is superior to copyright protection under, namely, commercial strategy and procedural convenience.[32]

Partial cumulation of protections implies a restrictive interpretation of Article 194 of CPI in the sense that not any registered design deserves protection by copyright. Cumulative protection only exists for a design that can be qualified as "work". Moreover, despite the wording of Article 194, it includes registered design, community unregistered design, and design that was once registered but whose protection term has already expired.

Article 17 of Design Directive and Article 96(2) CDR were not mentioned in the questions posed by the STJ, but the potential conflict between these provisions and the CJ case law was brought to the Court's attention during the proceedings, namely through the interventions by the United Kingdom and the Czech Republic. The CJ paid little attention to those arguments, considering that those provisions were left unaffected and explicitly stated that InfoSoc Directive was without prejudice to the provisions of design law (CJ paragraphs 8, 11, 44, 46, and 47). An explication for this somehow surprising position of the CJ can be found in Advocate General Szpunar's Opinion (see C-683/17, *Cofemel v G-Star*, Opinion of the AG Szpunar, EU:C:2019:363). The AG submitted that the purpose of both provisions is to ensure, among other aspects, that no interference was drawn from design law as to the conditions under which national copyright

[31] In this sense, see MATTHIAS LEISTNER, «Einheitlicher europäischer Werkbegriff auch im Bereich der angewandten Kunst…», *op. cit.* (pp. 1116-1117); PEDRO SOUSA E SILVA, «Tutela Jusautoral de Obras de Design na esteira do Acórdão Cofemel…», *op. cit.* (pp. 179-182); FERNANDO CARBAJO CASCÓN, «Objetos Industriales, Derecho de Autor y Libre Competencia…», *op. cit.* (pp. 925-933); for a deeper study, see Fernando Carbajo Cascón, «La protección de los diseños de moda en la Unión Europea…», *op. cit.* (pp. 148-156).

[32] In this sense, see TOBIAS ENDRICH-LAIMBÖCK, «Litle Guidance for the Application of Copyright Law to designs in *Cofemel*», *op. cit.* (pp. 267-268); ANNETTE KUR, «Unité de l'art is here to stay – Cofemel and its Consequences», *op. cit.* (p. 1112).

is granted. Also, the provisions do not exclude that, once copyright is harmonized, the conditions applying in the Member States are the same (paragraphs 37 and 38). The standard developed under InfoSoc Directive defines the conditions of copyright protection granted under national laws. This reasoning is not fully convincing because InfoSoc Directive went into force several months before than CDR, and Article 96(2) of the latter re-confirmed the legal prerogative of Member States given in the second sentence of Article 17 of Design Directive. The AG considered but discarded these arguments because the respective legislative processes ran in parallel. Countering that the CDR was younger than InfoSoc Directive, the AG (paragraph 39) noted that the deadline for transposition of InfoSoc Directive (December 2002) was after the date of entry into force of the CDR (March 2002). Therefore, the harmonization of copyright by InfoSoc was not yet achieved when CDR entered into force. There was a time when Article 96(2) CDR actually referred to the not yet harmonized copyright law of Member States, but afterwards their freedom became restricted by InfoSoc Directive. The AG dismissed arguments based on preparatory works of EU design legislation (paragraph 40). While Article 9 of InfoSoc Directive leaves intact provisions of design law, Article 17 of Design Directive and Article 96(2) of CDR are provisions concerning the copyright protection of designs, which means they are part of copyright law and fall under the scope of InfoSoc (paragraph 41). If the legislature intended to leave the area of works of applied art unharmonized, the InfoSoc Directive would have expressly excluded them (paragraph 42). While InfoSoc Directive only harmonizes certain aspects of copyright in the information society, this does not mean that designs, which are incorporated in physical objects, are outside its scope (paragraph 44). Public international law is to be intended without prejudice of EU law and cannot affect the functioning of the internal market (paragraph 46). The AG also turned to *Flos* (Case C-168/09, EU:C:2010:371), where the CJ stated that the Member States' freedom to regulate copyright protection for designs does not include the duration of protection because the term of protection of patrimonial rights is harmonized by the Copyright Term Directive. The same can be said about the InfoSoc Directive, which harmonizes the concept of work and thus removes the issue related to protection requirements from the freedom provided by Articles 17 Design Directive and 96(2) of CDR (paragraph 47). One might reply that to do so, "the legislature would first have to be aware that the CJEU would boldly seize the opportunity to claim that by harmonizing the copyright tort of reproduction in Article 2(a), the notion of a work and the threshold for protection were harmonized as well".

But at that point in time, "that effect was hardly anticipated by anyone"[33] the CJ application of Article 2(a) of InfoSoc Directive might well have been inside the rules, as the AG argued. The Court accepted the opinion of the AG without discussing it.[34]

The second conclusion we can ascertain from the CJ ruling has to do with the concept of "work" under InfoSoc Directive (paragraphs 26, 27, and 28).

The CJ held that it is clear from the Court's settled case law that in all the provisions of InfoSoc Directive, the concept of "work" is an autonomous concept of EU law that must be interpreted and applied uniformly, requiring two cumulative conditions to be satisfied. First, the concept entails that there exists an original subject matter in the sense of being the author's own intellectual creation. Second, classification as "work" is reserved to the elements that are the expression of such creation (paragraph 29).[35] To be protected by copyright, the subject matter must be original, being both necessary and sufficient, in that it reflects the personality of its author in the sense that it is an expression of the author's free and creative choices (paragraph 30).[36] When there is no freedom of choice because the realization of the subject matter was dictated by technical considerations, rules, or other constraints, there cannot exist "originality" (paragraph 31).[37]

The CJ further determined that the concept of "work", according to InfoSoc Directive, implies "the existence of a subject matter that is identifiable with

---

[33] [ANNETTE KUR, «Unité de l'art is here to stay – Cofemel and its Consequences», *op. cit.* (pp. 45)]. As a result of what has been considered a "small foul" in a football match [Matthias Leistner, «Einheitlicher europäischer Werkbegriff auch im Bereich der angewandten Kunst…», *op. cit.* (p. 1117)].

[34] On this subject, with detail, see also TOBIAS ENDRICH-LAIMBÖCK, «Litle Guidance for the Application of Copyright Law to designs in *Cofemel*», *op. cit.* (pp. 264-266); TITO RENDAS, anticipated this problem in «Copyright protection of designs in the EU...», *op. cit.* (pp. 440-441); for the different approaches of EU Member-States before Cofemel, like Italian theory of *scindibilità*, German *Stufentheorie*, French *Unité de l'art*, and Flos ruling (Case C-168/09, EU:C:2010:371), see ELEONORA ROSATI, «CJEU rules that copyright protection for designs only requires sufficient originality», *op. cit.* (p. 931); FERNANDO CARBAJO CASCÓN, «La protección de los diseños de moda en la Unión Europea…», *op. cit.* (pp. 143-151); ANNETTE KUR, «Unité de l'art is here to stay – Cofemel and its Consequences», *op. cit.* (pp. 12-14).

[35] In this paragraph, the CJ mentions *Infopaq International*, C-5/08, EU:C:2009:465, paragraphs 37 and 39, and *Levola Hengelo*, C-310/17, EU:C:2018:899, paragraphs 33 and 35 to 37.

[36] In this paragraph, the CJ mentions *Painer*, C-145/10, EU:C:2011:798, paragraphs 88, 89 and 94, and *Renckhoff*, C-161/17, EU:C:2018:634, paragraph 14.

[37] In this paragraph, the CJ mentions *Football Dataco and Others*, C-604/10, EU:C:2012:115, paragraph 39.

sufficient precision and objectivity" (paragraphs 32 and 33).[38] The work is the expression of the author's individual creation. Precision and objectivity do not exist when the identification of the subject matter is essentially based on the sensations of individuals that perceive it, which are necessarily subjective (paragraph 34).[39] If the subject matter satisfies these two requirements, it constitutes a work entitled to copyright protection under the InfoSoc Directive (paragraph 35).

We can conclude that, for the first time, the CJ stated unequivocally that the concept of "work" is harmonized in the EU (going beyond *Levola Hengelo*, C-310/17, paragraph 33, which was not so assertive). Since *Infopaq* (C-5/08), the CJ has been deciding that if a work falls within the application of InfoSoc Directive, the protection only exists when the work is its "author's own intellectual creation", the work is the result of "free and creative choices" [*Football Association Premier League* (C-403/08,), and *Karen Murphy* (C-429/08)], and the subject matter displays the personal touch of the author (*Painer*, C-145/10).[40]

But in the *Cofemel* ruling, the CJ did not deepen the concept. Though the Court stressed that the conditions for granting copyright protection to works of applied art, works of design, and designs are a matter for uniform interpretation throughout the EU, the Court only stated general principles and did not give clear and sensible guidelines. The CJ sent an ambiguous message, repeating standard formulas already known in previous case law, instead of clarifying the concept of "work" and of "originality" in what concerns designs, works of applied art, and works of design. The approach that the CJ did not follow would have been especially important to elucidate those concepts, giving substantive notions that would replace the ones exiting in national laws.[41] Besides giving no guidelines, the CJ's decision is confusing and somewhat contradictory. It can be said that, rather than clarifying the issue, it complicates the solution to a problem that is becoming more and more acute in the market due to the tendency of design creators and industry to invoke copyright to protect designs for a longer period. The CJ does not provide an objective and coherent hermeneutical basis for solving the scope of the protection that should be granted to hybrid intangible goods such as design creations. The Court does not solve the industrial design/copyright interface and its application to design creations, creating uncertainty for competition in an increasingly important market sector. The Court

---

[38] In this paragraph, the CJ mentions *Levola Hengelo*, C-310/17, EU:C:2018:899, paragraphs 40 and 41.

[39] In this paragraph, the CJ mentions *Levola Hengelo*, C-310/17, EU:C:2018:899, paragraph 42.

[40] See ELEONORA ROSATI, «CJEU rules that copyright protection for designs only requires sufficient originality», *op. cit.*, pp. 931-932.

[41] In this sense, PEDRO SOUSA E SILVA, «Tutela Jusautoral de Obras de Design na esteira do Acórdão Cofemel…», *op. cit.*, pp.183-184.

was before a dilemma. Regarding the concept of "originality", the CJ applied the criteria enunciated in *Infopaq* and subsequent case law. There is originality when the work is the author's own creation, resulting from the author's free and creative choices. But the CJ, and specially Advocate General (AG) Spuznar, knowing that this concept could lead to a too broad cumulation of copyright and design protection, felt the need to clear that such cumulation is not a general rule, but rather an exception, applicable only in "certain cases", with a clear subtext reading "but not in a case like this".[42]

The AG claimed that this could be inferred from the idea/expression dichotomy that governs copyright. The AG held that characteristics such as the "specific composition based on shapes, colours, words and numbers", the "combination of colours", the "placement of the pocket on the stomach", or "the way the jeans are made by assembling the three pieces", which Cofemel was alleged to have copied, should be considered as ideas capable of being expressed differently, or even as practical solutions, and should not be protected by copyright (paragraph 60). By relying on the innovative and unique (at that time) character of its G-Star Elwood design, which was introduced in 1996, the AG considered that it seemed that G-star was seeking copyright protection for its reputation and distinctive character of its goods, which are normally protected as trademarks (paragraph 61). Though the infringement of copyright exists even if only parts of the work are reproduced, they must contain elements that are the expression of the intellectual creation of the author's work.[43] That is not the case when the copied elements are merely inspired by the ideas expressed by the work. Though the assessment to know if we are before ideas or before parts drawn from the work must be carried out by the national court on a case-by-case basis, in the context of that assessment, that court must grant that the subject matter in respect of which protection is sought is sufficiently identifiable (paragraph 61).[44] Copyright differs from designs protection. An exclusive design right is being infringed, in line with the wording of Article 10(1) of CDR, if a design does not produce on the informed user a different overall (visual) impression. The concept of the overall (visual) impression is completely alien to copyright (paragraph 63). Copyright protects a specific work, not a work which has a visual aspect that causes a different overall (visual) impression. Copyright does not require objective novelty. Parallel creations, provided they are original, are lawful and enjoy full

[42] Wording of ANNETTE KUR, «Unité de l'art is here to stay – Cofemel and its Consequences», *op. cit.* (p. 6); see also FERNANDO CARBAJO CASCÓN, «La protección de los diseños de moda en la Unión Europea…», *op. cit.* (p. 153).

[43] In this paragraph, the AG refers to judgment of 16 July 2009, *Infopaq International*, C-5/08, EU:C:2009:465, paragraph 39.

[44] In this paragraph, the AG refers to judgment of 13 November 2018, *Levola Hengelo*, C-310/17, EU:C:2018:899, paragraph 40.

protection as separate works. The same is true if a creation is inspired by earlier works. If that creation does not constitute an unauthorized reproduction of original elements of another's work, there is no copyright infringement, irrespective of whether the overall (visual) impression is different (see paragraphs 64 and 65). In the opinion of the AG, the Court must distinguish what may fall within design protection and what may fall within copyright protection because the protections have different requirements and different purposes, thus avoiding confusion between the two protection regimes (paragraph 66).

The CJ emphasized that the subject matter of copyright must be expressed in a way that makes it identifiable with "sufficient precision and objectivity" (paragraphs 33 and 34, with reference to C-310/17, *Levola Hengelo,* paragraph 40). The Court held that the "aesthetic" appearance of an object is necessarily subjective. Moreover, the presence of an "aesthetically significant visual effect" of a design cannot, in itself, justify the protection of such design as work, under copyright (paragraph 50).[45]

In *Cofemel*, both the CJ and the AG send signals of discrepancy between the words used and the standards that the Court wants to apply.[46] The AG, quoting the description of the special features of the clothing of G-Star, includes them in the field of unprotectable ideas. It is submitted that the AG confuses such description, which may convey an idea with several options for its expression, with the actual clothing of G-Star, which presents a specific and identifiable manifestation of those ideas.[47]

The reference made by the AG to functionality could be understood as establishing a rule that the closer an item corresponds in its appearance to the gender (jeans, t-shirts, sweatshirts), the less it appears to rely on creative choices.

---

[45] Leistner stresses that the CJ emphasis on the requirement that subject matter of copyright "be expressed in a manner which makes it sufficient precision and objectivity" seems to conflate the criteria for concretizing the object of protection with sufficient certainty and the criteria for assessing originality of a work. This author assumes that the CJ was concerned that if the aesthetic appearance ought to be considered relevant, practically every design would qualify for copyright protection. See MATTHIAS LEISTNER, «Einheitlicher europäischer Werkbegriff auch im Bereich der angewandten Kunst…», *op. cit.* (p. 1117). TOBIAS ENDRICH-LAIMBÖCK, «Litle Guidance for the Application of Copyright Law to designs in *Cofemel*», *op. cit.* (p. 266), contends that the CJ rejection of the "aesthetical significant visual effect" is motivated by the consideration that the assessment ought to be focused on the creative process itself and not on its result. According to the CJ, requirements that relate to the characteristics of the subject matter that do not necessarily reflect the required characteristics of the process of creation cannot be part of the originality criterion or be an alternative to such criterion.

[46] In this sense, ANNETTE KUR, «Unité de l'art is here to stay – Cofemel and its Consequences», *op. cit.* (p. 7).

[47] In the same sense, ANNETTE KUR, «Unité de l'art is here to stay – Cofemel and its Consequences», *op. cit.* (p. 7).

But if one follows this reasoning regarding works of applied art or designs, one will have to be more demanding to demonstrate that there is a personal creation, re-establishing different standards in relation to other categories of works.[48] The creative choices do not concern the motive, which may be "prototypical" (like in the *Renckhoff* case) but find their expression in the details. In *Cofemel*, the designs at issue were the result of the free choices of the designers of G-Star regarding details of the clothing. Also, no clear guidance results from the CJ's contention that the assessment whether a subject matter qualifies as a work must be based on objective criteria rather than on a subjective appreciation of aesthetic quality. Aesthetics, in the sense of "beauty", "eye-pleasing character", of an object, is a matter of personal taste, and is totally inappropriate and obsolete in the context of copyright. But the CJ does not address the subject matter in this sense. In the ruling, the sense of "aesthetic" seems to represent the opposite of "functional". The term is very close in its meaning to what the CJ regards as the result of free creative choices made by the authors of the works.[49]

The CJ made it clear that the only valid concept of originality in EU copyright law is the subjective criterion, according to which "originality" is the author's own intellectual creation that reflects their personality and is the result of free creative decisions in the sense that it is not affected by technical considerations. Therefore, the criterion of creative originality or creative height applied by several national courts of the Member States was ruled out. Thus, the access of design to the protection offered by copyright can no longer be justified by the appreciation of a greater creativity expressed in more recognizable aesthetic-artistic visual elements. At the same time, however, the court states that the cumulation of protections can only exist in certain situations. Not every design can be considered a work. But if all intellectual creations of the author that reflect their personality may qualify for copyright protection, including works of design and works of applied art, how can one differentiate those creations that only deserve protection as design from those that deserve cumulative protection under copyright?

The CJ suggests that that the differentiating element does not reside in the concept of "originality", but in the previous concept of "work". But, at the same time, the Court states that the existence of a work cannot be characterized solely by the presence of a visual aesthetic effect in a creative object. How is it possible to know when a work is protected by copyright? There is a subtext in the CJ ruling. A "plus" is required to distinguish between design and an artistic work. But

[48] See, for photographs, *Land Nordhein-Westfalen v Dirk Renckhoff,* C-161/17, EU:C:2018:634.

[49] In this sense, ANNETTE KUR, «Unité de l'art is here to stay – Cofemel and its Consequences», *op. cit.* (pp. 79).

is this not a confirmation that the difference lies in the identification in the object of a "plus" of creativity?

The CJ refuses to resort to the aesthetic element to identify the presence of an original work, but in the field of designs, the aesthetic element is always present because what is protected is the form or ornament of a product when it is novel and singular. The "plus" of creativity that allows affirmation that a design is also a work lies in the identification of aesthetic-artistic elements in the object, especially when the type of work (work of applied art) constitutes a subtype of an artistic work (that has an intrinsic artistic character).[50]

In my opinion, after *Cofemel*, national provisions expressly differentiating between the relevant work categories must be considered as infringing the EU law as interpreted by the CJ. Nevertheless, the standards applied are a matter of court practice, and national courts may simply adapt to the CJ language regime while heeding the subtext implied in *Cofemel* that protection for works of applied art should not be granted too easily. While there are no legislative changes in the proposed EU design reform,[51] this means, in practice, that national courts may continue to interpret the cumulation of protections in different ways. In turn, the *Cofemel* ruling led to no harmonization in this area. The restrictive interpretation the CJ offers of what should be considered an original work seems to lead to a dead end.

The third conclusion one can reach and criticize is that the CJ, at paragraphs 49 and 53 to 55, gave indications of how the Portuguese STJ ought to decide in the main proceedings. The CJ stated that it must be examined whether classification as 'works' is possible for designs such as the clothing designs at issue in the main proceedings, which, going beyond the utilitarian purpose they serve, generate, according to the referring court, a specific and aesthetically significant visual effect. It may be said that the doubts of the Portuguese STJ concerned the issue of whether such a factor of aesthetic originality constitutes the central criterion for the protection to be provided (paragraph 49). At paragraphs 53 and 54, the CJ held that the aesthetic effect that may be produced by a design is the result of an intrinsically subjective sensation of beauty experienced by each

[50] With more detail, FERNANDO CARBAJO CASCÓN, «La protección de los diseños de moda en la Unión Europea…», *op. cit.* (pp. 153-156)". Basically, it seems that the CJ advocates a solution like that established by US case law: a design can only access copyright protection if the object in which it is applied presents aesthetic elements that allow it to identify a work of art separable from the practical use of the industrial object. But the huge difference is that, in the US, the industrial object and its elements are protected separately, while in the EU, the protection can be cumulative. If the object presents artistic elements, it will be able to enjoy both the protection granted by design law and that offered by copyright (which will remain once the design protection has expired).

[51] See https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/industrial-design-protection_en

person who may look at it. That subjective effect does not allow the subject matter to be considered existing and identifiable with sufficient precision and objectivity, that is, to be considered a copyrighted work. Aesthetic considerations are part of creative activity. Nonetheless, the fact remains that the circumstance that a design may generate an aesthetic effect does not make it possible to determine whether that design is an intellectual creation reflecting the freedom of choice and personality of its author, thereby meeting the requirement of originality. As held at paragraphs 55 and 56, the circumstance that designs such as the clothing designs at issue in the main proceedings generate, over and above their practical purpose, a specific and aesthetically significant visual effect is not enough to qualify them as "works" within the meaning of InfoSoc Directive. The CJ considered that the answer given to the first question was sufficient, so there was no need to answer the second one (paragraph 57).

The ruling of the CJ was that Article 2(a) of InfoSoc Directive must be interpreted as precluding national legislation from conferring protection, under copyright, to designs such as the clothing designs at issue in the main proceedings, on the ground that, over and above their practical purpose, they generate a specific, aesthetically significant visual effect. Nevertheless, reading the ruling and looking to what was proved in the main proceedings, it is not clear why the designs of G-Star could not be protected as individual creations of its authors, reflecting their personality and freedom of choices, and why the creations were not recognized as being identifiable with sufficient precision and objectivity. The reasons for the ambiguous decision are in the subtext conveyed by the CJ, which, in a certain way, defies the standard promoted.

3. Portuguese case law after the CJ *Cofemel* preliminary ruling

After the CJ Cofemel ruling, many cases occurred before the courts of EU Member States with different rulings, and in the CJ, there was the Brompton judgement of 11 June 2020.[52] In Portugal there is already case law after the CJ Cofemel ruling, starting with the judgement of the Portuguese Supreme Court in the case that originated the request for the preliminary ruling.

[52] Judgement of 11.06.2020, *SI and Brompton Bicycle Ltd. v. Chedech/Get2Get*, C-833/18, EU:C:2020:461. Regarding this case and national case law in countries of the EU, see FERNANDO CARBAJO CASCÓN, «Objetos Industriales, Derecho de Autor y Libre Competencia…», *op. cit.* (pp. 933-935); DANIEL INGUANEZ, «A Refined Approach to Originality in EU Copyright Law in Light of the ECJ's Recent Copyright/Design Cumulation Case Law», *IIC* 51, 2020, pp. 797-822, pp. 797-821 (pp. 813-819); KORAY GÜVEN, «Eliminating "Aesthetics" from Copyright Law…», *op. cit.*, pp. 213-225 (221-225); PEDRO SOUSA E SILVA, «Tutela Jusautoral de Obras de Design na esteira do Acórdão Cofemel…», *op. cit.* (pp. 184-186).

3.1. Ruling of the Portuguese Supreme Court in the Cofemel Case





Figure 1: *Left:* G-Star's ARC jeans **Figure 2:** *Left:* G-Star's ROWDY sweatshirt *right:* Cofemel copies and t-shirt; *right:* Cofemel copies

Reproduced from case law 15.01.2020, Supremo Tribunal de Justiça, Revista Proc. 268/13.2YHLSB.L1.S1, p. 46 and p. 50.

In the main proceedings[53] (Figure 1; Figure 2), the essential question was whether the "ARC" jeans design and the graphic design incorporated into the "ROWDY" sweatshirts and t-shirts, both belonging to G-Star and imitated by Cofemel, under the trademark "Tiffosi", which were not protected by industrial property, could be protected as "works" according to Portuguese copyright. To address that question, the STJ had to determine the exact meaning of the wording of Article 2(1)(i) of CDADC. This provision headed "Original works" states that intellectual creations of the literary, scientific, and artistic domain, whatever their gender, form of expression, merit, mode of communication, and purpose, include, namely, subparagraph (i) works of applied art, industrial designs, and works of design that constitute artistic creation, regardless of the protection

[53] Judgment of 15.01.2020, *G-Star Raw C.V. v Cofemel – Sociedade de vestuário* – STJ Proc. 268/13.2YHLSB.L1.S1.

relating to industrial property".[54] The provision does not determine the "originality" required to protect utilitarian works, and there are divergent positions in case law and in the scholarship. For some, works of applied art, designs, and works of design, can be protected by copyright if they reflect the sensibility of its creator and result from his freedom of choice, regardless of the functionality of the works. For others, to achieve protection under copyright, the assessment must be particularly demanding and, considering the dominant conceptions in cultural and institutional circles, these works must have an increased artistic character, which goes beyond what is normally required of other categories of works (no. 11 of the STJ decision, pp. 5961). To ascertain whether the subject matter at issue could be considered copyright protected "work", the Supreme Court followed entirely the ruling of the CJ (no. 11 of the STJ decision, pp. 62–67).

It was proved that the G-Star "ARC" design is characterized by the way each of the three denim modules of different lengths and shapes is cut and assembled. Using such modules of different lengths and shapes, a leg with a 3D effect is created, folding in and back, and thus twisting around the user's leg (twisted leg effect); further contributing to this effect are the darts included in the model for the place of the knee, one on each leg. The "ARC" design is characterized by the alluded design with 3D effect and its leg cut with twisted leg effect, resulting from the position of the assembled three modules, the vertical position of the seams, and the seams on the back of the knees in the form of darts. Nevertheless, the G-Star design of the "ARC" jeans, created by designers Rixt van der Trol and Pierre Morriset, working for G-Star Company, according to the STJ, could not be protected by copyright because they were not appropriable. Article 1(2) of CDADC determines that ideas, processes, systems, operational methods, concepts, principles, or discoveries cannot be protected by copyright, expressing the fundamental principle that copyright does not protect the subject or the idea, but the expression given to the theme or idea by the author. Regarding the fashion industry, clothes, ideas, and concepts are many times expressed in fashion trends, or in a common fashion fund, part of the public domain, and thus they cannot be protected by copyright. The STJ considered the "ARC" design elements as trends, thus not protectable by copyright. The same applied for the G-Star design of the t-shirts and hooded sweatshirts "ROWDY", created by designer Ruud de Bruin, who also works in the design department of the company.

[54] The CDADC dates from 1985. Though being eighteen times amended, the reference to industrial design, strangely, was never modified, though industrial application is not anymore a requirement for protection of design under the Industrial Property Code. Article 2(1)(i) of CDADC is in line with Article 2(1) and 7 of the Bern Convention (Act of Paris of 24.07.1971, as amended in 28.09,1979), which allows these type of works to be protected by copyright, and in line with the WIPO Copyright Treaty of 1996, which is part of EU law (Decision 2000/278/CE of the Council, of 16 March 2000), which determines, under Article 1(4), that the Contracting Parties must comply with the provisions of Articles 1 to 21 of the Bern Convention and its attachments.

These designs include several elements in their composition, namely the image stamped on the front of the t-shirts and hooded sweatshirts, the colour scheme, the numbers, and the placement of the pockets. Though G-Star Company invests in unique and innovative design, with new materials, cuts, and styles, that does not mean that the designs conceived by the company's designers qualify for protection as "works" by copyright. Even if they are new and have a singularity, that is not enough for copyright protection; nor is the visual striking effect from an aesthetic point of view, namely achieved by the "ARC" jeans or by "ROWDY" t-shirts and hooded sweatshirts (no.11 of the STJ decision, pp. 67-72).

The STJ considered that the case law of the CJ harmonized the concept of "originality". Designs protected by industrial property rights may be protected as copyrighted work only if they possess "originality." As a conclusion, although the G-Star design pieces of clothing have a visual and aesthetic effect, due to its shape, colours, words and numbers, and placement of pockets, the proven facts were considered insufficient to conclude that the design of that clothing was "original" in the sense of being an intellectual creation of its author, reflecting the author's freedom of choice, personality, and particular perception of the world, and things expressed in a clear and objective way through the creative act, going beyond the utilitarian and functional vision which they imply (no. 11 of the STJ decision, pp. 75-76).

The STJ annulled the decision of the Court of Appeal of Lisbon, ruling that the designs at issue could not be classified as "works" according to Article 2(1)(i) of CDADC in an interpretation consistent with EU law, *maxime* with InfoSoc Directive (no. 12 of the STJ decision, pp. 76-77). Thus, Cofemel won the case in the Portuguese Supreme Court of Justice. As stated above (section 2), the CJ ruling went too far, giving this guidance to the STJ in relation to facts. The STJ was in some way bound by the indications wrongly given in the specific case by the CJ in its preliminary ruling, clearly pointing to the effect that the design of the clothing at issue could not be classified as "work". But the CJ used vague and imprecise formulas. The qualification of the work as being the author's own intellectual creation, the expression of the author's personality, and the result of the author's free and creative choices, can apply almost to anything. If these were the criteria, there is no reason to maintain that designs of clothing, like the ones in this case, do not reflect the author's personality. Why did the STJ consider unworthy of protection the clothing models at issue though it was proven that they were created by stylists working for G-Star and went beyond the utilitarian purpose they serve, generating a striking visual aspect from the aesthetic point of view? Why were the clothing models at issue not considered identifiable with sufficient precision and objectivity? Why were they all considered mere trends?

The STJ followed the instructions given by the CJ ruling. One does not know where the bar should be set. What separates individual creations of the

author endowed with originality from simple individual creations of the author with his own aesthetically striking visual effect? The answer to these questions cannot be found in vague concepts and empty formulas. These prolong legal uncertainty, allowing a wide variety of interpretations by national courts, which may lead to serious distortions of competition within the EU single market, as has happened in the wake of the *Cofemel* ruling.[55]

The STJ, nevertheless, did not decide that design clothing cannot be protected by copyright. The possibility of protection by copyright was left open. The Court left clear that in future cases the decision might be different. The STJ only stated that the proven facts were clearly insufficient to conclude that the design clothing of G-Star were "original" (no. 11 of the Supreme Court ruling, p. 76).

3.2. Stabilo Case



Figure 3: Stabilo PEN 68

Reproduced from case law 21.04.2020, Tribunal da Relação de Lisboa, Apelação Proc. 279/18.1YHLSB.L1-PICRS, https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/2e5cfd03c403bb7980258553002c75a0

[55] In this sense, see the deep analysist of FERNANDO CARBAJO CASCÓN, «La protección de los diseños de moda en la Unión Europea…», *op. cit.* (pp. 151-156); PEDRO SOUSA E SILVA, «Tutela Jusautoral de Obras de Design na esteira do Acórdão Cofemel…», *op. cit.* (p. 184).

The Court of Appeal of Lisbon, in a judgment of 21 April 2020 (Figure 3)[56] in which an alleged imitation of markers of the well-known trademark "STABILO BOSS" was at issue, decided that the protection of the design of "Stabilo PEN 68" by copyright is only possible if we are before a "work". Only an intellectual creation, in this case, of the artistic domain, namely a work of applied art or of design, that at the same time is an artistic work, regardless the protection that industrial property rights grant, can receive copyright protection. This was not the case. Quoting the *Cofemel* decision, amongst others, and stressing that Portugal has a partial cumulation, but going beyond *Cofemel*, the Court of Appeal gave concrete expression to its understanding of what a copyrighted work is. To protect an "artistic work," it is not enough to know that it is a creation of someone's intellect, a result of their mind. Besides being "original", it must involve intellectual work, going beyond the commonplace, and enriching the available cultural framework and must be recognized by art experts as such.[57]

3.3. Larus Case

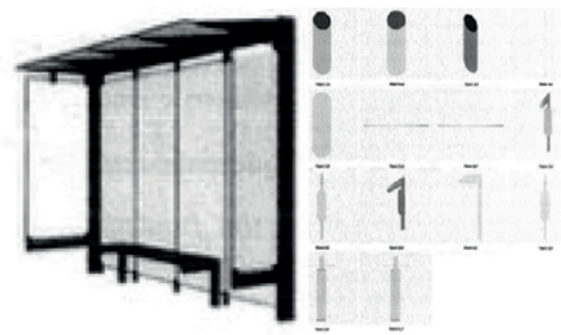


Figure 4: Larus passenger shelter

Reproduced from case law 18.05.2021, Tribunal da Relação de Lisboa, Apelação Proc. 146/20.9YHLSB.L1, p. 43 and p. 44.

[56] Proc. 279/18.1YHLSB.L1-PICRS (Rel. Ana Pessoa), dgsi.pt. In this case, Shwan-Stabilo Schwanhausser Gmbh & Co KG brought an action against Branco e Negro, Lda. and Clave Denia, S.A., amongst other reasons because the latter companies produce, distribute, and commercialize in Portugal in physical stores, named Ale-Hop, and on the internet, pens that copy the design of Stabilo Pen 68, allegedly protected by copyright (amongst other intellectual property rights).

[57] See pp. 30-34 of the decision. The Court quotes PEDRO SOUSA E SILVA, «Desenhos ou modelos no novo CPI. O que muda e o que não muda com o Ac. Cofemel», *op. cit.* (pp. 198 and 202).

The Court of Appeal of Lisbon, on 18 May 2021,[58] in which the alleged copy of a design of a passenger shelter of the Larus company was at issue (Figure 4), decided in a similar way. Without denying the possibility of street furniture equipment benefitting from copyright, the court considered the proven facts insufficient to conclude that the design was "original" enough to be a copyrighted protected work. To protect by copyright the design passenger shelter, it would have been necessary to prove that the same was included in a creative project of expression and was personal interpretation of the object at issue transcending its functional vision. The aesthetic effect that the court recognized in the passenger shelter was not sufficient to support this understanding. Beyond the requirements for protection of design by industrial property, that is, novelty and singularity, copyright protection demands that the object be the result of an individual creation of the author where they reflect their personality, making free and creative choices. The Court of Appeal, in this judgment, quoted both *Cofemel* and *Stabilo* and denied copyright protection.[59]

3.4. Cavalinho Case



Figure 5: Cavalinho trademarks, logotypes, and designs (for more information: www.cavalinho.com)

Reproduced from case law 18.05.2022, Tribunal da Relação de Lisboa, Apelação Proc. 286/21.7YHLSB.L1-PICRS, https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/65367436ed31fd4f80258875002cfd18?OpenDocument

[58] Proc. 146/20.9YHLSB.L1 (Rel. Isoleta de Almeida Costa), Larus – Artigos para Construção e Equipamento, Lda, v Bricantel – Comércio de material elétrico de Bragança, S.A. e outros (dgsi.pt).

[59] See II-B of the decision. The Court also stated that there was no evidence in the process to determine who could be the author (the designer or the company) for the purpose of Article 14 of CDADC, related to works made for hire (see II-A of the decision).

The Court of Appeal of Lisbon, on 18 May 2022,[60] delivered a judgment involving the trademark "CAVALINHO" (Figure 5), where the plaintiff sought to protect the drawing of a horse through copyright. The court denied protection. Referencing *Cofemel*, the court held that partial cumulation is possible if we are before copyright protected "work", which implies that the subject matter at issue reflects the personality of its author, their free, arbitrary, and creative choices, and that it is identifiable with sufficient precision and objectivity. In this case, there was no evidence in relation to the authorship of the subject matter at issue. The court could not establish if the author was an artist, a designer, a craftsman, a worker of the company, a team, or an anonymous artist. Not knowing who the author might be, the court could not conclude whether the design reflected its personality. The first requirement of "originality" was not fulfilled.[61] As for the second requirement, the aesthetic effect of a design or of a distinctive sign of commerce is subjective, experienced by everyone who looks at it. We are not before a subject matter identifiable with sufficient precision and objectivity, to be qualified as "work" under InfoSoc Directive.[62] For these reasons, the court decided that the design of a horse, used in the distinctive signs of the appellant could not qualify for copyright protection under the CDADC.[63]

That said, the Appeal Court ruled that even if both requirements referred were met, the design of the horse used in the distinctive signs of the Appellant did not fulfil the degree of originality demanded by Article 2 of the CDADC. This question was not addressed in neither the *Cofemel* CJ ruling nor in the *Cofemel* STJ decision. The Court of Appeal deepened the concept of "artistic creation" and held that, to determine the degree of originality demanded by CDADC, the work of art must be created by an artist and is only artistic if society recognizes it as such.[64] In assessing whether a work is artistic from the perspective of its surroundings, the court should not consider its conception of art because such a criterion would be controversial and arbitrary. Factors such as the opinion of experts, artists in the same field, or art dealers, as well as publications in art books, the presence in museum collections, or expertise, are decisive.[65] In this case, in the absence of allegation and proof of these elements, the court could not conclude if the degree of originality required by Article 2(1)(i) of CDADC existed.

---

[60] Proc. 286/21.7YHLSB.L1-PICRS (Rel.: Paula Pott) in: dgsi.pt.

[61] See paragraph 103 of the decision.

[62] See paragraphs 101 to 104 of the decision.

[63] See paragraphs 103 to 105 of the decision.

[64] See paragraph 106 of the decision, quoting Pedro Sousa e Silva, *Direito Industrial. Noções Fundamentais*, *op. cit.* (p. 191).

[65] See paragraphs 107 to 110 of the decision.

Conclusion

After the CJ *Cofemel* ruling, Portuguese courts have refused copyright protection to design of clothing, markers, a passenger shelter, and to the design of a horse used in distinctive signs. The fashion sector must be aware that the Portuguese courts have been particularly demanding in their criteria for granting copyright protection to designs. In the post-*Cofemel* era, except for the decision of the STJ, the Court of Appeal of Lisbon has decided that only artistic works may qualify for copyright protection, deepening the concept of "originality", not in the sense of artistic merit, but in the sense that the works in question must be recognized as artistic works or works of art. Besides expressing the personal choices of the author and requiring the existence of an object identifiable with sufficient precision and objectivity, to be considered an artistic work, under Article 2(1)(i) of CDADC, the subject matter at issue must be created by an artist, and the society must recognize it as art. To be protected by copyright, utilitarian creations must be artistic. The improvement of the case law and the mitigation of the unpredictability of decisions must involve the opinion of the concerned circles. The courts are not able to assess the "originality" or "artistic character" of works of design, of designs, or of works of applied art and should refrain from doing so because of the sensitivity and culture of the judges. More reliable and predictable methods should be used. Institutional criteria consider the circumstances in which the work was created and the way the interested parties see it. The artistic character of the work must be assessed, not so much in function of the characteristics of that work or through a previous and controversial subsumption in a certain concept of art, but above all considering the position it occupies in the social and cultural context, according to the perspective both of the author and of the surrounding environment. Only the work that society recognizes as such is artistic. The institutional orientation implies a broad approach, which weighs a multiplicity of factors, *inter alia*, opinions of specialists, artists of the same area, and art dealers; results of expert examinations; and inclusion of the work in specialized publications, art books, or museum collections. Art is a matter of fact, which must be subject to proof. There is no useful normative criterion in the law for this purpose. For the design to be cumulatively protected by copyright, it must have an artistic character, and this is a fact that must be subject to proof.[66]

The *Cofemel* CJ ruling, though clarifying that the unitary concept of work also applies to works of applied art, regarding the application of the originality criterion, left it to national courts to deal with sector-specific difficulties of

[66] In this sense, PEDRO SOUSA E SILVA, «Tutela Jusautoral de Obras de Design na esteira do Acórdão Cofemel…», *op. cit.* (pp. 192-194); MANUEL OEHEN MENDES, «A obra enquanto objecto do direito de autor», *op. cit.*, pp. 41-73 (45).

works of applied art. The Court's remarks on the interface between copyright and design law did not mitigate the lack of specification. They do not help grant a coherent system regarding the relation between design law and copyright by means of interpretation. The CJ's decision is ambiguous and seems somehow contradictory, having a rather clear subtext that demands a "plus" for the cumulative protection of works of applied art by copyright. This explains why the CJ held that the clothing design in the main proceedings did not deserve qualification as works. Without the CJ recognizing it outright, that is something more demanding, something similar, in the context of visual works, to the notion of an artistic character, used by various legal systems to protect design works.[67] If the CJ had clearly assumed its choice, adopting a more specific criterion of eligibility, it could be interpreted in an autonomous and uniform way by the national courts. The CJ left the question unsolved and subject to the interpretation of national courts. Uniformization remains a potential task for the legislature or for other rulings of the CJ (namely, the ruling in Case C-580/23, *Mio and Others*).

[67] On this "plus", as described in this conclusions, see FERNANDO CARBAJO CASCÓN, «La protección de los diseños de moda en la Unión Europea…», *op. cit.* (pp. 151-156); PEDRO SOUSA E SILVA, «Tutela Jusautoral de Obras de Design na esteira do Acórdão Cofemel…», *op. cit.* (p. 183 and 191-195).

DIREITOS DIGITAIS DOS CONSUMIDORES: A PORTABILIDADE TRANSFRONTEIRIÇA DE CONTEÚDOS E A PROIBIÇÃO DO *GEOBLOCKING*

Sérgio Manuel da Costa Machado*

Resumo: O Direito do Consumo visa estabelecer equilíbrios nas relações jurídicas de consumo, designadamente na proteção da parte mais débil, ou seja, proteger o consumidor.

Um dos aspetos caracterizadores do Direito do Consumo é a sua relevância preponderante na sociedade contemporânea, não só na proteção do consumidor, mas também no acompanhamento da evolução de novos mecanismos tecnológicos, nomeadamente na contratação à distância. Ora, o Direito do Consumo é um dos ramos em que se sente um maior impacto da evolução das tecnologias disruptivas.

Como tal, o Direito do Consumo enfrenta desafios de constante mutação no sentido de saber em cada momento temporal qual o seu alcance e papel. Isto porque o avanço tecnológico gerou novos modelos de negócios, de serviços e bens de caráter tecnológico colocados no mercado antes da própria regulamentação.

* Professor Auxiliar da Faculdade de Direito da Universidade Lusíada do Porto e Professor Adjunto Convidado da Escola Superior de Ciências Empresariais do Instituto Politécnico de Viana do Castelo; Investigador Integrado do CEJEIA (Centro de Estudos Jurídicos Económicos, Internacionais e Ambientais). E-mail: *sergiomachado@por.ulusiada.pt*

Este incessante progresso tecnológico, daí que vivemos na "era digital", ou numa rede aberta, na qual a Internet desempenha um papel fulcral nas telecomunicações e nas transações comerciais, acaba por revolucionar de forma significativa o *modus vivendi* social.
Consequentemente, o legislador europeu tem procurado acompanhar este progresso. A exemplo, o Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, relativo à portabilidade transfronteiriça de conteúdos em linha no mercado interno ou o Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018, que visa prevenir o bloqueio geográfico injustificado e outras formas de discriminação baseadas na nacionalidade.

Palavras-chave: Consumidor; Portabilidade transfronteiriça de conteúdos; *Geoblocking*.

Abstract: Consumer law aims to establish balance in consumer legal relations, particularly in the protection of the weaker party, that is the consumer. One of the defining aspects of consumer law is its predominant relevance in contemporary society, not only in the protection of the consumer but also in keeping pace with the evolution of new technological mechanisms, particularly in remote contracting. Indeed, consumer law is one of the branches most impacted by the evolution of disruptive technologies.
As such, consumer law faces challenges of constant change in determining its scope and role at any given time. This is because technological advancement has generated new business models, services, and technological goods that have been placed on the market before regulation itself.
This incessant technological progress, hence we live in the "digital age" or in an open network in which the Internet plays a crucial role in telecommunications and commercial transactions, is ultimately revolutionizing the social modus vivendi. Consequently, the European legislator has sought to keep pace with this progress. For example, Regulation (EU) 2017/1128 of the European Parliament and the Council of June 14, 2017, concerning cross-border portability of online content in the internal market, or Regulation (EU) 2018/302 of the European Parliament and the Council of February 28, 2018, aimed at preventing unjustified geographical blocking and other forms of discrimination based on nationality.

Keywords: Consumer; Cross-border content portability; Geoblocking.

1. Introdução

As transformações ocorridas no mundo, designadamente a partir dos finais dos anos 60 do século XX, levaram a certas mudanças de hábitos e geraram, *per se*, novos comportamentos. A verdade é que as mudanças que sentimos na

sociedade contemporânea são resultado de uma evolução social, que se fez sentir em toda a Europa, principalmente após a Segunda Guerra Mundial, com afirmação de Estados Democráticos a par do desenvolvimento tecnológico e económico. Tudo isto provocou uma rutura de comportamentos e novas filosofias de vida e de consumo[1].

A nível da União Europeia, a partir da década citada até aos tempos atuais, foram produzidas normas de defesa do consumidor em matérias diversas tais como a regulamentação da comercialização de alimentos, da indicação de preços, da comercialização de materiais perigosos, da publicidade enganosa, da responsabilidade por produtos defeituosos, das vendas fora de estabelecimento comercial e à distância, às matérias inerentes ao crédito ao consumo, às práticas comerciais desleais e às garantias nas vendas de consumo[2].

Nesta medida, o Direito do Consumo tem uma função de evitar desequilíbrios, pois adjacente a ele está o princípio da justiça comutativa, de forma a conduzir a um equilíbrio contratual[3].

Concretizando, o Direito do Consumo tem em vista proteger a parte mais desfavorecida numa relação contratual[4]. Daí que, ao longo das últimas décadas, preocupou-se em, primeiro lugar, com a proteção dos consumidores na aquisição de bens, como por exemplo um frigorífico, um rádio, um televisor; em segundo, com a prestação de serviços, a exemplo, água, energia elétrica, gás e telefone fixo; em terceiro, com a proliferação de informações, ou seja, com a sociedade digital e a expansão da Internet; e, por fim, no presente, com incidência nas preocupações de cariz ambiental, mormente a interligação do consumo com a tecnologia (consumo tecnológico) e a sustentabilidade ambiental[5].

---

[1] Cfr. SANDRA PASSINHAS, *Propriedade e Personalidade no Direito Civil Português*, Coimbra, Almedina, 2017, pp. 36-42.

[2] Cfr. TERESA HUALDE MANSO, *Del Consumidor Informado al Consumidor Real – El Futuro del Derecho de Consumo Europeo*, Madrid, Dykinson, 2016, pp. 11 e ss.; DIONISIO FERNÁNDEZ DE GATTA SÁNCHEZ, «Sistema Normativo, Competencias y Organización Administrativa en Materia de Consumo: Unión Europea, Estado y Comunidad de Castilla y León», in *Estudios Sobre Consumo*, Valencia, Tirant lo Blanch, 2012, pp. 134 e ss.

[3] Cfr. ANTÓNIO AGOSTINHO GUEDES, *Estudos sobre a Decisão Judicial – Coordenadas da Decisão Judicial em Direito Privad*o, Lisboa, UCP Editora, 2024, pp. 53-55. Para uma compreensão em torno do equilíbrio negocial nos contratos de consumo, nomeadamente nas relações B2C, *vide* ANA FILIPA MORAIS ANTUNES, «Equilíbrio negocial e fair dealing no Direito dos contratos», in *Encontros de Direito Civil – Limites à Autonomia Privada*, Lisboa, UCP Editora, 2023, pp. 141 e ss. (pp. 125-156).

[4] Cfr. PEDRO ROMANO MARTINEZ, *Introdução ao Estudo do Direito*, Lisboa, AAFDL, 2021, p. 433.

[5] Cfr. MÁRIO BEJA SANTOS, *Sociedade de Consumo e Consumidores em Portugal*, Lisboa, Fundação Francisco Manuel dos Santos, 2023, pp. 67-92.

Não podemos esquecer os novos mecanismos que surgem com o apogeu dos meios tecnológicos, nomeadamente com a Internet, que possibilitou novos mecanismos de contratação à distância. O seu aparecimento revolucionou o *modus vivendi* social, facilitando a vida dos consumidores na comparação de preços e na aquisição de bens e serviços[6].

A Internet tornou-se uma ferramenta indispensável no trabalho, na escola e em casa, permitindo-nos aceder de imediato a todo o tipo de informação. Isto faz-nos sentir parte da chamada "Aldeia Global", já que, em poucos minutos, podemos obter notícias de qualquer parte do mundo. Além disso, é um espaço aberto para o setor empresarial, onde surgem novas formas de operar e promover produtos, a tal ponto que este contexto tecnológico tem sido denominado como a "Quarta Revolução Industrial" ou "Transformação Digital"[7].

MANUEL CASTELLS fala-nos do surgimento das novas tecnologias, do seu impacto e do relevo que a Internet teve na sociedade. O mesmo fornece uma visão do novo campo das tecnologias e das alterações que estas provocaram na vida em sociedade, tais como as novas formas de sociabilidade *online*[8].

Neste novo tempo da Internet, gerou-se uma proliferação de informação que nos permitiu estar em contacto permanente com interlocutores diversificados, permitindo o debate de ideias e opiniões, assim como expressar a nossa forma de ver as coisas, de estar em sociedade e de realizar os mais diversificados tipos contratuais.

Com o apogeu desta tecnologia, surgiram as redes sociais, entre elas o *Hi5*, *Twiter*, *Orkut*, *Badoo*, *Facebook*, *Instagram*, *Tik Tok*, *Vsco*, *Flickr* e tantas outras. Muito têm contribuído para uma facilitação da comunicação, criação de novos laços de amizade e de relacionamento, divulgação de produtos e de serviços, com o objetivo de celebrar um determinado contrato[9].

Nesta sociedade de rede, Gustavo Cardoso demonstra que através da Internet comunicamos com os nossos familiares próximos ou distantes; trabalhamos em empresas que compram produtos ao estrangeiro; acedemos às contas bancárias *online*; vemos filmes, novelas e peças de teatro nacionais e estrangeiras.

---

[6] Cfr. ELSA DIAS OLIVEIRA, «Contratos Eletrónicos e Tutela do Consumidor», in *Estudos de Direito do Consumo*, Vol. I, Coimbra, Almedina, 2023, p. 831 (pp. 831-850).

[7] Cfr. ANTÓNIO ANDRADE e JORGE JULIÃO, *Sistemas de Informação e Tecnológicos*, Porto, Universidade Católica Editora, 2019, pp. 27 e ss.

[8] Cfr. MANUEL CASTELLS, *A Era da Informação: Economia, Sociedade e Cultura – A Sociedade em Rede*, Vol. I, 5.ª ed., Lisboa, Fundação Calouste Gulbenkian, 2016, pp. 33 e ss.

[9] *Vide* JOAN RAMOS TOLEDANO, *Propiedad Digital – La Cultura en Internet como Objeto de Cambio*, Madrid, Editorial Trotta, 2018, pp. 67 e ss.

Deste modo, deixamos a relação face a face para utilizar uma ferramenta mais facilitadora de comunicação[10].

MANUEL CASTELLS questiona o papel da sociedade em rede, no plano da economia, assim como os novos hábitos de comunicação pessoal; as novas formas de participação na sociedade, como, por exemplo, os movimentos feministas, ecologistas, sindicais, religiosos, entre outros que vão ganhando espaço na rede; as questões da liberdade e da privacidade na rede; e a relevância do *e-learning* como uma forma de formação contínua na vida profissional e familiar. Porém, o autor não omite as desigualdades e a exclusão da utilização desta ferramenta de classes de menor rendimento perante as classes de maior rendimento, de maiores habilitações académicas e do caráter geográfico que em muito pode restringir a utilização da Internet[11].

Estas preocupações, em torno das desigualdades de acesso à Internet, são observadas, entre nós, por ANTÓNIO FIRMINO DA COSTA, referindo que o acesso a esta ferramenta, que é a Internet, depende muito dos contextos sociais. Ora, a desigualdade está intimamente relacionada com a idade, a escolaridade, a categoria socioprofissional, pelo que o uso da Internet tende a ser mais intenso e diversificado nas classes etárias mais novas, mais escolarizadas e nas categorias profissionais mais qualificadas[12].

De tudo isto podemos concluir que, com a Internet, gerou-se um novo paradigma da forma de estar em sociedade e que, apesar de tudo, estas novas formas de comunicação são salutares, desde que se pretenda, acima de tudo, valorizar a dignidade da pessoa humana e reforçar os valores da democracia.

Com todo este avanço tecnológico, as crianças têm cada vez mais cedo acesso a aparelhos eletrónicos com Internet e, assim, desde cedo começam a familiarizar-se com os meios digitais[13].

---

[10] Cfr. GUSTAVO CARDOSO, *Os Media na Sociedade em Rede*, 2.ª ed., Lisboa, Fundação Calouste Gulbenkian, 2014, pp. 40 e ss.

[11] Cfr. MANUEL CASTELLS, *A Galáxia Internet – Reflexões sobre Internet, Negócios e Sociedade*, 2.ª ed., Lisboa, Fundação Calouste Gulbenkian, 2007, pp. 25 e ss.

[12] Cfr. ANTÓNIO FIRMINO DA COSTA, *Desigualdades Sociais Contemporâneas*, Lisboa, Mundos Sociais, 2012, pp. 77 e ss.

[13] Cfr. JOANA COSTA LOPES, «A tutela do consumidor menor à luz do Regulamento dos Serviços Digitais (Digital Services Act)», in *Novo Liber Amicorum Mário Frota – Sempre a Causa dos Direitos dos Consumidores*, Coimbra, Almedina, 2023, pp. 543-544 (pp. 543-574).

A par destes novos modelos de comunicação têm surgido *sites* especializados, como plataformas digitais[14] para determinadas áreas de comercialização de produtos ou serviços. Por isso, a Internet vai ganhando força nas relações sociais, não sendo de desprezar a sua influência nas relações contratuais[15].

O legislador não esqueceu este novo elo de comunicação que é a Internet. Assim, entre nós, o regime jurídico do comércio eletrónico encontra a regulamentação no Decreto-Lei n.º 7/2004, de 7 de janeiro[16].

No entanto, há outros regimes legais que podem ser chamados à colação a nível da contratação por via eletrónica, como, por exemplo, o Decreto-Lei n.º 24/2014, de 14 de fevereiro, que estabelece o regime dos contratos celebrados à distância e fora do estabelecimento comercial[17], dispondo, no seu artigo 3.º, alínea h), que o contrato celebrado à distância é aquele que se celebra "entre o consumidor e o fornecedor de bens ou o prestador de serviços sem presença física simultânea de ambos, e integrado num sistema de venda ou prestação de serviços organizado para o comércio à distância mediante a utilização exclusiva de uma ou mais técnicas de comunicação à distância até à celebração do contrato, incluindo a própria celebração". Também o Decreto-Lei n.º 12/2021, de 9 de fevereiro, relativo à identificação eletrónica de confiança para as transações

---

[14] Cfr. AINHOA FERNÁNDEZ GARCÍA DE LA YEDRA, «Cambios normativos en torno a la responsabilidad de las plataformas electrónicas de intermediación», in *Plataformas Digitales: Aspectos Jurídicos*, Cizur Menor – Navarra, Thomson-Aranzadi, 2021, pp. 34 e ss. (pp. 31-48); ANTÓNIO PINTO MONTEIRO e MAFALDA MIRANDA BARBOSA, «A Imposição das Obrigações Decorrentes do DL n.º 67/2003, de 8 de abril, ao Intermediário», *Revista de Legislação e Jurisprudência*, n.º 147, 2018, p. 383 (pp. 368-386); MARÍA TERESA ÁLVAREZ MORENO, «La Protección del Consumidor en la Contratación Electrónica de Bienes y Servicios a través de Plataformas», in *Innovación Tecnológica, Mercado y Protección de los Consumidores*, Madrid, Reus, 2018, p. 42 (pp. 39-109).

[15] *Vide* RAFAEL ILLESCAS ORTIZ, *Derecho de la Contratación Electrónica*, Cizur Menor – Navarra, Civitas-Thomson Reuters, 2019, pp. 37 e ss.

[16] *Vide* HEINRICH EWALD HÖRSTER e EVA SÓNIA MOREIRA DA SILVA, *A Parte Geral do Código Civil Português*, 3.ª ed., com a colaboração de António Agostinho Guedes, Coimbra, Almedina, 2024, pp. 536-541; LUÍS DE LIMA PINHEIRO, «Direito Aplicável aos Contratos Celebrados através da Internet», in *Estudos de Direito da Internet*, Lisboa, AAFDL, 2024, pp. 43 e ss. (pp. 43-104); JOANA CAMPOS CARVALHO, *Os Contratos Celebrados Através de Plataformas Digitais*, Coimbra, Almedina, 2023, pp. 227-247; SÓNIA MOREIRA, «A Formação do Contrato por Via Eletrónica», in *Estudos em Homenagem ao Professor Doutor António Cândido de Oliveira*, Coimbra, Almedina, 2017, pp. 993 e ss. (pp. 993-1009).

[17] Este Decreto-Lei transpõe para a ordem jurídica a Diretiva n.º 2011/83/UE do Parlamento Europeu e do Conselho de 25 de outubro de 2011, estabelecendo um conjunto de regras aplicáveis aos contratos celebrados à distância e aos contratos celebrados fora de estabelecimento comercial. Ele revogou o Decreto-Lei n.º 143/2001, de 26 de abril. Sobre o regime do Decreto-Lei n.º 24/2014, de 14 de fevereiro, *vide* JORGE MORAIS CARVALHO e JOÃO PEDRO PINTO FERREIRA, *Contratos Celebrados à Distância e Fora do Estabelecimento Comercial – Anotação ao Decreto Lei n.º 24/2014*, Coimbra, Almedina, 2014, pp. 13 e ss.

eletrónicas, a Lei n.º 16/2022, de 16 de agosto, relativa às comunicações eletrónicas, o Decreto-Lei n.º 80/2019, de 17 de junho, e a Lei n.º 7/2022, de 10 de janeiro, relativos ao bloqueio geográfico e discriminação nas vendas eletrónicas a consumidores.

Ora, perante esta nova realidade que é a Internet, surgem, no seu seio, os mais variados espaços, onde podemos efetuar as mais diversas transações. Desde o seu aparecimento, esta nova forma de contratação à distância conquistou rapidamente os consumidores, que se deixaram cativar pelas várias vantagens oferecidas. Entre essas vantagens, destacam-se a maior rapidez na aquisição de produtos ou serviços, a facilidade em encontrar exatamente o que procuram e a redução de problemas como a concentração excessiva de pessoas.

Com a grande adesão dos consumidores, as empresas, por sua vez, também adotaram rapidamente essa nova abordagem, explorando amplamente essa mecânica no mercado.

Deste modo, com o surgimento da Internet, testemunhámos, num espaço de tempo relativamente curto, uma transformação na forma de estar e de se comportar do ser humano, que passou a depender, cada vez mais, das tecnologias emergentes. Essas tecnologias influenciam todos os setores de atividade e todos os aspetos da vida quotidiana. O uso de computadores portáteis, telemóveis e outros dispositivos digitais tornou-se omnipresente na sociedade hodierna, numa evolução constante que nos empurra, de forma irreversível, para um modo de viver, interagir e sobreviver sustentado pelas vantagens da sociedade digital; consequentemente, o ser humano é hoje "um ser puramente digital"[18] ou um "*homo digitalis*"[19].

Ao negociar com uma empresa virtual, o consumidor nem sempre conhece realmente quem é o empresário, contudo, acaba por ser atraído pela facilidade do processo de compra *online*. Isto pode originar problemas, como o fornecimento de dados pessoais e bancários que poderão ser utilizados indevidamente, além de enfrentar dificuldades em caso de insatisfação, uma vez que a reclamação seria contra um "fantasma na nuvem"[20].

Importa destacar que, na sociedade contemporânea, o comércio eletrónico desempenha um papel fundamental na economia, oferecendo vantagens significativas, como o acesso conveniente a bens e serviços sem a necessidade de deslocações físicas.

---

[18] SIMÃO MENDES DE SOUSA, *Constitucionalismo Digital: Uma Introdução*, Coimbra, Almedina, 2022, p. 40.

[19] ERNESTO CAPOBIANCO, «Il New Deal For Consumers», in *Mercato Digitale e Tutela dei Consumatori Prove di Futuro*, Torino, G. Giappichelli Editore, 2023, p. 116 (pp. 111-124).

[20] JOSÉ ENGRÁCIA ANTUNES, *Direito do Consumo*, 2.ª ed., Coimbra, Almedina, 2024, p. 380.

No entanto, é importante considerar também as desvantagens associadas, em particular aquelas resultantes de práticas discriminatórias, como o *geoblocking*. Estas práticas levantam sérias preocupações quanto à igualdade no acesso a bens, produtos e serviços, além de questões sobre a transparência e a justiça nas transações *online*.

Nesse sentido, é essencial compreender de que forma o *geoblocking* se insere no contexto do comércio eletrónico, analisando as práticas adotadas por algumas empresas que restringem ou limitam o acesso com base na localização geográfica do consumidor.

É nítido que, por todas as mudanças que ocorrem na sociedade e face às circunstâncias das mesmas, surgem naturalmente novos comportamentos e práticas económicas associadas ao consumo. Assim, as mutações sociais têm o seu reflexo no campo jurídico, sendo o Direito do Consumo alvo dessas alterações.

Por conseguinte, temos vindo a assistir a uma constante transformação do Direito do Consumo, com forte impacto na economia, na política e na sociedade em geral. De facto, existe um desafio constante, no Direito do Consumo, de determinar, em cada momento temporal, o seu alcance e o seu papel na sociedade, especialmente numa sociedade cada vez mais digital[21].

2. O consumidor na contratação eletrónica

No início do século XIX, ocorreu na Europa um movimento de codificação que teve como referência a publicação do PRIMEIRO Código Civil em França, em 1804[22]. Este código, amplamente reconhecido como um importante marco legislativo, exerceu uma profunda influência nas codificações que se seguiram ao longo do século XIX no continente europeu[23].

Acontece que a figura jurídica do consumidor era inteiramente desconhecida das codificações oitocentistas. Com isto, importa ter em linha de conta que as codificações oitocentistas influenciaram de sobremaneira as codificações novecentistas, que ainda marcam as ordens jurídicas hodiernas, onde a figura

[21] *Vide* MARTIM FARINHA e JORGE MORAIS CARVALHO, «Direito do Consumo e Tecnologia», in *Estudos de Direito do Consumo*, Vol. I, Almedina, Coimbra, 2023, p. 884 (pp. 883-914).

[22] Sobre as condicionantes da elaboração, redação e promulgação do Código Civil Francês de 1804, *vide* R. C. VAN CAENEGEM, *Introduction Historique au Droit Privé*, Bruxelles, E. Story-Scientia, 1988, pp. 3 e ss., que considera que o Código Civil Francês de 1804 foi um marco importante, para a época, na afirmação do direito da propriedade e do direito da família. Ora, o Código Civil Francês de 1804 procurava uma sociedade nova, para concretizar a liberdade e a igualdade (só jurídica), mas não a própria fraternidade. *Vide*, MARIO ASCHERI, *Introduzione Storica al Diritto Moderno e Contemporaneo – Lezioni e Documenti*, Torino, G. Giappichelli Editore, 2003, p. 278.

[23] Cfr. ANTONIO PADOA SCHIOPPA, *Storia del Diritto in Europa – Dal Medioevo all´età contemporânea*, Bologna, Socità Editrice il Mulino, 2007, p. 465.

jurídica do consumidor é desconhecida; assim, são diversas as dúvidas que ainda hoje persistem em torno do conceito de consumidor e isso é visível a nível legislativo, jurisprudencial e doutrinal[24].

Como nos informa FERNANDO BAPTISTA DE OLIVEIRA, os primeiros movimentos associados à consciencialização do desequilíbrio intrínseco à relação contratual de consumo surgiram nos anos 20 do século XX, nos Estados Unidos da América, dando início às preocupações com os direitos do consumidor, enquanto contraente mais débil numa relação jurídica. Por sua vez, na Europa, esse movimento protecionista do consumidor começa a surgir na década de 1950[25].

Um marco histórico na proteção dos consumidores é o discurso do presidente norte-americano, John F. Kennedy, proferido ao Congresso a 15 de março de 1962, em que refere: "consumidores, por definição, somos todos nós". A partir daqui inicia-se, paulatinamente, um movimento legislativo com vista à proteção das relações de consumo, nomeadamente da parte mais frágil, o consumidor[26].

Na Europa, o primeiro passo de um esboço de noção de consumidor surgiu na Carta de Proteção do Consumidor do Conselho da Europa, de 17 de maio de 1973, definindo-o como "pessoa física ou colectiva, a quem são fornecidos bens e prestados serviços, para uso privado"[27].

Posteriormente, a Comunidade Económica Europeia (atual União Europeia) no Programa Preliminar de 1975, destinado à tutela do consumidor, indica que, "no futuro, o consumidor não será só considerado como um comprador ou utilizador de bens e serviços para uso pessoal, familiar ou colectivo, mas como uma pessoa que participa nos diferentes aspectos da vida social que o podem afectar directa ou indirectamente enquanto consumidor"[28]. A partir daqui a Comunidade Económica Europeia desencadeia um processo legislativo com vista à proteção do consumidor, à promoção dos seus direitos e interesses, designadamente com a emanação de Diretivas.

---

[24] Cfr. JOSÉ ENGRÁCIA ANTUNES, *Direito do Consumo*, *op. cit.*, pp. 77-78.

[25] Cfr. FERNANDO BAPTISTA DE OLIVEIRA, *O Conceito de Consumidor: Perspectivas Nacional e Comunitária*, Coimbra, Almedina, 2009, p. 47.

[26] Cfr. ALBERTO HIDALGO CEREZO, *Nuevas Tendencias de Derecho de Consumo – Aspectos generales, legislación especial y de consumo digital*, Madrid, Dykinson, 2023, pp. 31-34; JORGE MORAIS CARVALHO, *Manual de Direito do Consumo*, 8.ª ed., Coimbra, Almedina, 2022, p. 35; MIGUEL CORCHERO e ANA GRANDE MURILLO, *La Protección de los Consumidores*, Cizur Menor – Navarra, Thomson-Aranzadi, 2007, pp. 15-19.

[27] Cfr. FERNANDO BAPTISTA DE OLIVEIRA, *O Conceito de Consumidor…*, *op. cit.*, p. 47.

[28] Conselho das Comunidades Europeias, Resolução do Conselho de 14 de abril de 1975 relativa a um programa preliminar da Comunidade Económica Europeia para uma política de protecção e informação dos consumidores, *Jornal Oficial das Comunidades Europeias*, 1975, p. 66.

Damos nota de algumas Diretivas, a título meramente exemplificativo, que avançam com uma noção de consumidor: 1) a Diretiva 2005/29/CE do Parlamento Europeu e do Conselho de 11 de maio de 2005, relativa às práticas comerciais das empresas face aos consumidores no mercado interno e que altera a Diretiva 84/450/CEE do Conselho, as Diretivas 97/7/CE, 98/27/CE e 2002/65/CE e o Regulamento (CE) n.º 2006/2004 (diretiva relativa às práticas comerciais desleais), no artigo 2.º, alínea a), prevê: "«Consumidor»: qualquer pessoa singular que, nas práticas comerciais abrangidas pela presente diretiva, atue com fins que não se incluam no âmbito da sua atividade comercial, industrial, artesanal ou profissional"; 2) a Diretiva 2011/83/UE do Parlamento Europeu e do Conselho de 25 de outubro de 2011, relativa aos direitos dos consumidores, no artigo 2.º, n.º 1, dispõe: "«Consumidor»: qualquer pessoa singular que, nos contratos abrangidos pela presente diretiva, atue com fins que não se incluam no âmbito da sua atividade comercial, industrial, artesanal ou profissional"; 3) a Diretiva (UE) 2019/770 do Parlamento Europeu e do Conselho de 20 de maio de 2019, sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais, no artigo 2.º, n.º 6, refere: "«Consumidor»: uma pessoa singular que, no que respeita aos contratos abrangidos pela presente diretiva, atue com fins que não se incluam no âmbito da atividade comercial, empresarial, artesanal ou profissional".

No ordenamento jurídico português, não existe um conceito único de consumidor, mas várias noções de consumidor, sendo a Lei de Defesa do Consumidor (Lei n.º 24/96, de 31 de julho) a mais relevante, uma vez que é o diploma que incorpora os princípios gerais de Direito do Consumo[29]. À luz do artigo 2.º, n.º 1, da Lei de Defesa do Consumidor, entende-se que, consumidor é "todo aquele a quem forem fornecidos bens, prestados serviços ou transmitidos

[29] *Vide* FERNANDO DE GRAVATO MORAIS, *Teoria Geral das Obrigações. A Relação Jurídica Obrigacional – Fontes das Obrigações: Contratos*, Vol. I, Coimbra, Editora d´Ideias, 2024, pp. 18-21.

quaisquer direitos destinados a uso não profissional por pessoa que exerça com caráter profissional uma atividade económica que vise a obtenção de benefícios"[30].

Neste sentido, considera-se consumidor o adquirente de um bem ou serviço para fins que não pertençam ao âmbito da sua atividade profissional, isto é, que são para uso privado, seja a nível pessoal, familiar ou doméstico. Não são consideradas as aquisições de bens para satisfação de necessidades profissionais ou de empresa[31].

Havendo dúvida sobre a qualidade de consumidor, face às regras de repartição do ónus da prova previstas no artigo 342.º, n.º 1 do Código Civil, cabe ao autor alegadamente lesado o ónus dessa prova[32].

Importa notar que, no caso de uso misto, dispõe o artigo 49.º do Decreto-Lei n.º 84/2021, de 18 de outubro (regula os direitos do consumidor na compra e venda de bens, conteúdos e serviços digitais, transpondo as Diretivas (UE) 2019/771 e (UE) 2019/770), o seguinte: "a verificação de um uso profissional dos bens, conteúdos ou serviços digitais pelo consumidor, desde que a finalidade

---

[30] No ordenamento jurídico português, encontramos várias noções de consumidor, veja-se, a exemplo: artigo 4.º, n.º 1, alínea a), do Decreto-Lei n.º 133/2009, de 2 de junho (Contratos de Crédito aos Consumidores): "«Consumidor» a pessoa singular que, nos negócios jurídicos abrangidos pelo presente decreto-lei, atua com objetivos alheios à sua atividade comercial ou profissional"; artigo 3.º, alínea e), do Decreto-Lei n.º 24/2014, de 14 de fevereiro (Contratos Celebrados à Distância e Fora do Estabelecimento Comercial): "«Consumidor», a pessoa singular que atue com fins que não se integrem no âmbito da sua atividade comercial, industrial, artesanal ou profissional"; artigo 2.º, alínea g), do Decreto-Lei n.º 84/2021, de 18 de outubro (Direitos do Consumidor na Compra e Venda de Bens, Conteúdos e Serviços Digitais): "«Consumidor», uma pessoa singular que, no que respeita aos contratos abrangidos pelo presente decreto-lei, atue com fins que não se incluam no âmbito da sua atividade comercial, industrial, artesanal ou profissional". *Vide* NUNO MANUEL PINTO OLIVEIRA, *Contrato de Compra e Venda – Introdução, Formação do Contrato*, Vol. I, Coimbra, Gestlegal, 2021, pp. 121-210, e JOSÉ ENGRÁCIA ANTUNES, «O Conceito de Consumidor», *Revista de Direito Civil*, n.º 4, 2018, pp. 771 e ss. (pp. 771-796). Também, a nível da União Europeia, o conceito de consumidor varia de Diretiva para Diretiva, não havendo uma definição unívoca: *vide* GIOVANNI CRISTOFARO, *Diritto Italiano ed Europeo dei Consumatori – Studi*, Milano, Cedam – Wolters Kluwer, 2024, pp. 23-26; MARIA JESÚS SANDE MAYO, «La evolución del concepto de consumidor en el ordenamento interno y comunitário», *Dereito: Revista Xurídica da Universidade de Santiago de Compostela*, n.º 1, 2018, pp. 119 e ss. (pp. 119-152); BASTIAN SCHÜLLER, «The Definition of Consumers in EU Consumer Law"», *op. cit.*, p. 124, que considera que consumidor é a pessoa que está a agir para fins não comercias ou profissionais.

[31] Neste sentido, *vide* o Acórdão do Supremo do Tribunal de Justiça de 15/05/2003, Processo n.º 03B1015, Relator: Abílio Vasconcelos; assim como o Acórdão do Supremo Tribunal Justiça de 27/05/2008, Processo n.º 08A1104, Relator: Paulo Sá, ambos disponíveis em www.dgsi.pt [consultados em 12/09/2024].

[32] Neste sentido, *vide* Acórdão do Supremo Tribunal de Justiça de 24/03/2015, Processo n.º 7002.11.OTBOER.L1.S1, Relator: Gregório Silva Jesus, in *Coletânea de Jurisprudência*, Tomo I, 2015, pp. 167-173: "face às regras de repartição do ónus da prova contemplados no n.º 1 do art. 342.º do Código Civil, recairá sobre o autor alegadamente lesado, primeira e decisivamente, provar a sua qualidade de «consumidor»".

comercial não seja predominante no contexto global do contrato, não obsta à aplicação do regime previsto no presente decreto-lei"[33].

Deste modo, embora atualmente ainda não haja consenso sobre uma noção de consumidor, é evidente que não podemos esperar uma noção clara e estabelecida de consumidor digital. A verdade é que todos nós acabamos por experienciar este novo mundo digital e, ao adquirir um bem ou serviço nesse contexto, inserimo-nos nesta nova categoria, que acarreta novas formas de vulnerabilidade, muitas das quais acreditamos ainda estarem por ser plenamente compreendidas.

Com o acesso generalizado da população aos meios de comunicação e novas tecnologias, nomeadamente um computador, "tablets" e "smartphones" com acesso à Internet, assistimos a um aumento de campanhas publicitárias acerca de produtos e serviços que, em muitas situações, nem se conhecem a sua utilidade e efeitos[34]. Muitos destes produtos apenas têm visíveis as suas principais características, não havendo referência aos perigos do consumo dos mesmos. Ora, por outro lado, hoje mais do que nunca, a compra eletrónica está cada vez mais ao alcance de cada um, bastando apenas um *click* para tal.

No âmbito da aquisição de bens e serviços por meio de transações eletrónicas, os consumidores encontram-se numa posição de desigualdade e vulnerabilidade, necessitando de proteção adicional e de mais informação. Isto deve-se ao facto de a publicidade e as campanhas de *marketing* exercerem uma forte influência nos seus comportamentos. Por exemplo, JOSÉ ENGRÁCIA ANTUNES considera que o consumidor é o "elo fraco" numa relação de consumo[35].

---

[33] No direito da União Europeia, já se adotava o critério do uso predominante. A exemplo, o considerando 17 da Diretiva 2011/83/UE, relativa aos direitos dos consumidores, determina que, "no caso dos contratos com dupla finalidade, se o contrato for celebrado para fins relacionados em parte com a atividade comercial da pessoa e em parte à margem dessa atividade e se o objetivo da atividade for tão limitado que não seja predominante no contexto global do contrato, essa pessoa deverá ser igualmente considerado consumidor", *vide* JORGE MORAIS CARVALHO e JOANA CAMPOS CARVALHO, "O(s) Contrato(s) de Fornecimento de Conteúdos ou Serviços Digitais", in *Estudos em Homenagem à Professora Doutora Maria Helena Brito*, Coimbra, Gestlegal, 2022, pp. 415-416 (pp. 409-445); ÁNGEL JUÁREZ TORREJÓN, *Garantías y Servicios Postventa a Favor de los Consumidores*, Madrid, Marcial Pons, 2016, pp. 55-58.

[34] *Vide* FRANCISCO JAVIER PÉREZ-SERRABONA GONZÁLEZ, «A propósito del nuevo mercado de redes sociales: entre la privacidad, la interpretación contractual y la responsabilidad de los consumidores (usuários)», in *Derecho de la Publicidad en Internet: Redes Sociales y Plataformas Digitales*, Cizur Menor – Navarra, Thomson-Aranzadi, 2023, p. 52 (pp. 51-93).

[35] JOSÉ ENGRÁCIA ANTUNES, *Direito do Consumo*, *op. cit.*, p. 268.

De acordo com o princípio da boa-fé que deve nortear a celebração do contrato (artigos 227.º e 762.º, n.º 2, do Código Civil)[36], o fornecedor de bens ou prestador de serviços tem o dever de informar o consumidor acerca das características e qualidades do bem ou serviço. Este dever de informação assume, portanto, especial relevância nas relações de consumo.

Dessa forma, o artigo 8.º da Lei de Defesa do Consumidor impõe ao fornecedor de bens ou prestador de serviços o dever de informar o consumidor, tanto durante as negociações como na celebração do contrato, sobre um conjunto amplo de informações relacionadas com o contrato e o seu objeto[37].

O dever de informar na aquisição de bens ou serviços pela Internet implica um reforço da confiança do consumidor, sendo essencial que lhe seja disponibilizada informação precisa e atualizada. Assim, o consumidor pode comparar os produtos que pretende adquirir e tomar uma decisão informada, optando pelo que melhor responde às suas necessidades. Contudo, em alguns casos, a informação disponibilizada é insuficiente, não permitindo ao consumidor conhecer as características reais do bem ou serviço em questão.

Atualmente, vivemos numa sociedade cada vez mais digital e tecnológica, o que se reflete significativamente no Direito do Consumo. Para além do surgimento de novos produtos, como serviços digitais e bens com conteúdos digitais, as formas de contratação nas relações "B2C" = *business to consumer*[38] também tendem a alterar-se profundamente, com o tradicional comércio presencial a ver-se confrontado por formas de contratação digitais, que dispensam a presença física das partes, como é o caso paradigmático do comércio eletrónico.

Este desenvolvimento tecnológico não pode ignorar a proteção do consumidor, especialmente no âmbito da contratação eletrónica ou em ambientes digitais, onde se destaca, atualmente, a Carta Portuguesa dos Direitos Humanos na Era Digital (Lei n.º 27/2021, de 17 de maio). Esta estabelece como incumbência do Estado "promover mecanismos que visem o aumento da segurança e da confiança nas transações comerciais, em especial na ótica da defesa do consumidor" (artigo 12.º, n.º 2, alínea b)). Além disso, "a República Portuguesa participa no processo mundial de transformação da Internet num instrumento de conquista

[36] *Vide* ANA PRATA, *Lições de Direito das Obrigações*, Coimbra, Almedina, 2024, pp. 104-118; ANA TAVEIRA DA FONSECA, *Teoria Geral das Obrigações*, Lisboa, UCP Editora, 2024, pp. 67-69; RUI PAULO COUTINHO DE MASCARENHAS ATAÍDE, *Direito das Obrigações*, Vol. II, Coimbra, Gestlegal, 2024, pp. 59-63; JORGE RIBEIRO DE FARIA, *Direito das Obrigações*, Vol. II, atualizada e ampliada por Miguel Pestana de Vasconcelos e Rute Teixeira Pedro, Coimbra, Almedina, 2023, pp. 230-234.

[37] *Vide* ADELAIDE MENEZES LEITÃO, *Direito do Consumo*, Lisboa, AAFDL, 2023, pp. 131-133.

[38] *Vide* MARCIAL HERRERO JIMÉNEZ, *La Protección del Consumidor en el Comercio Electrónico Transfronterizo*, Madrid, Reus, 2021, pp. 219 e ss.; Zofia Bednarz, *Breach of Infomation Duties in the B2C E-Commerce: A Comparative Perspective*, Madrid, Marcial Pons, 2019, pp. 39 e ss.

de liberdade, igualdade e justiça social e num espaço de promoção, proteção e livre exercício dos direitos humanos, com vista a uma inclusão social em ambiente digital" (artigo 2.º, n.º 1, da Carta Portuguesa dos Direitos Humanos na Era Digital)[39].

O avanço tecnológico e a crescente digitalização da sociedade implicam mudanças profundas no Direito do Consumo, tornando imprescindível a adaptação da legislação para assegurar a proteção dos consumidores no ambiente digital. A Carta Portuguesa dos Direitos Humanos na Era Digital demonstra o compromisso do Estado Português em promover um mercado digital seguro e fiável, com prioridade na defesa do consumidor e no respeito pelos direitos humanos no espaço virtual. Deste modo, a proteção do consumidor deve acompanhar o progresso tecnológico, garantindo que a transição para modelos de contratação eletrónica ocorra de forma inclusiva, justa e transparente, reforçando a confiança nas transações digitais e contribuindo para uma sociedade digital mais equitativa.

3. A portabilidade transfronteiriça de conteúdos

O Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, relativo à portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno e que entrou em vigor em 20 de março de 2018[40], foi criado com o intuito de permitir que os consumidores que adquiram conteúdos digitais num Estado-Membro possam aceder a esses conteúdos de forma contínua e sem restrições quando viajam para outros Estados-Membros da União Europeia. Isto pode ser constatado no considerando 1 do referido Regulamento: "o acesso permanente dos consumidores em toda a União a serviços de conteúdos em linha licitamente fornecidos no seu Estado-Membro de residência é importante para o bom funcionamento do mercado único e para uma aplicação efetiva dos princípios da livre circulação de pessoas e de serviços. Uma vez que o mercado interno compreende um espaço sem fronteiras internas com base, nomeadamente, na livre circulação de pessoas e de serviços, é necessário assegurar que os consumidores possam utilizar os serviços de conteúdos em linha portáteis que oferecem acesso a conteúdos como música, jogos, filmes, programas de entretenimento ou acontecimentos desportivos não

[39] Acerca da Carta Portuguesa dos Direitos Humanos na Era Digital, *vide* JOSÉ GASPAR SCHWALBACH, *Direito Digital*, 2.ª ed., Coimbra, Almedina, 2021, pp. 29-32.

[40] Sobre o Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, *vide* JOSÉ JUAN CASTELLÓ PASTOR, «Portabilidad transfronteriza de contenidos digitales protegidos por derechos de autor en la Unión Europea», *Indret: Revista para el Análisis del Derecho*, n.º 1, 2019, pp. 1 e ss. (pp. 1-25), disponível em https://www.raco.cat/index.php/InDret/article/view/354491/446476, [consultado em 12/09/2024].

só no seu Estado-Membro de residência, como também quando se encontram temporariamente presentes noutro Estado-Membro por motivos tais como lazer, viagens pessoais, viagens de negócio ou mobilidade para a aprendizagem. Por conseguinte, deverão ser eliminados os obstáculos que, nesses casos, entravam o acesso aos referidos serviços de conteúdos em linha e a sua utilização".

No contexto da economia digital e do mercado único europeu, a Internet surge como um espaço de liberdade e acessibilidade global, rompendo fronteiras e facilitando a circulação de bens e serviços. A realidade, contudo, demonstra que, apesar do potencial universal da Internet, ainda persistem barreiras artificiais impostas por restrições geográficas e comerciais. É, assim, contraditório que, num meio naturalmente aberto e inclusivo, tais limitações sejam mantidas ou até reforçadas, especialmente num mercado que se pretende único e livre. Esta contradição revela-se particularmente evidente para os cidadãos digitais, habituados a uma cultura que valoriza a acessibilidade e a ausência de restrições[41].

De acordo com o artigo 1.º do Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, o objeto e âmbito de aplicação visam estabelecer "uma abordagem comum na União relativamente à portabilidade transfronteiriça dos serviços de conteúdos em linha, ao assegurar que os assinantes de serviços de conteúdos em linha portáteis que são licitamente prestados nos respetivos Estados-Membros de residência possam ter acesso a esses serviços e utilizá-los quando se encontrem temporariamente presentes num Estado-Membro que não seja o seu Estado-Membro de residência".

Para beneficiar da proteção do Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, o seu artigo 2.º, n.º 1, estabelece que é necessário que "qualquer consumidor que, com base num contrato de prestação de um serviço de conteúdos em linha assinado com um prestador de serviços, mediante o pagamento de uma prestação pecuniária ou sem esse pagamento, possa ter acesso a esse serviço e utilizá-lo no Estado-Membro de residência".

Por outro lado, o prestador de serviços deverá facilitar o acesso, conforme decorre do considerando 18 do Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, que estabelece que o "regulamento deverá ser aplicável aos serviços de conteúdos em linha prestados mediante pagamento de uma prestação pecuniária. Os prestadores de tais serviços estão em posição de verificar o Estado-Membro de residência dos seus assinantes. O direito de utilização de um serviço de conteúdos em linha deverá ser considerado como adquirido mediante o pagamento de uma prestação pecuniária, quer esse pagamento seja efetuado diretamente ao prestador de serviços de conteúdos

[41] Neste sentido, *vide* ALBERTO HIDALGO CEREZO, *Nuevas Tendencias de Derecho de Consumo*…, *op. cit.*, p. 397.

em linha, quer a outra parte, como um fornecedor que oferece um pacote que combina um serviço de telecomunicações e um serviço de conteúdos em linha operado por outro prestador de serviços. Para efeitos do presente regulamento, o pagamento de uma taxa obrigatória para os serviços públicos de radiodifusão não deverá ser considerado como um pagamento de uma prestação pecuniária por um serviço de conteúdos em linha". Esta verificação deve ser feita em conformidade com os requisitos do artigo 5.º do mesmo Regulamento.

Por tudo, o Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, procura assegurar a portabilidade de serviços de conteúdos *online*, como música, filmes, *e-books*, programas de entretenimento e acontecimentos desportivos, eliminando as barreiras geográficas que limitam o acesso a esses conteúdos. Desta forma, oferece aos cidadãos da União Europeia uma experiência mais integrada e prolixa na utilização de serviços digitais em todo o mercado interno europeu.

Em suma, o Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, representa um passo significativo na promoção da portabilidade dos serviços de conteúdos em linha, permitindo que os consumidores da União Europeia acedam a conteúdos digitais de forma contínua e sem restrições, independentemente do Estado-Membro em que se encontrem. Este regulamento não só reforça os princípios da livre circulação de pessoas e de serviços, como também reconhece a importância da acessibilidade num ambiente digital que se pretende inclusivo e igualitário.

4. O bloqueio geográfico injustificado ou *geoblocking*

Na sociedade moderna, o comércio eletrónico assume um papel fundamental na economia, apresentando vantagens notáveis, como o acesso conveniente a bens e serviços sem a necessidade de deslocação física.

É importante abordar as desvantagens inerentes, nomeadamente aquelas decorrentes de práticas discriminatórias, como o *geoblocking*. O *geoblocking* é uma prática que restringe o acesso a conteúdos, produtos ou serviços com base na localização geográfica do utilizador[42]. Estas práticas suscitam sérias preocupações quanto à igualdade de acesso a bens, produtos e serviços, assim como à necessária transparência e justiça nas transações *online*.

[42] O Conselho Europeu, «Bloqueio geográfico: desbloquear o comércio eletrónico na UE», descreve o *geoblocking* da seguinte forma: "O bloqueio geográfico é uma prática discriminatória que impede os clientes online de aceder a produtos ou serviços de websites estabelecidos noutro Estado-Membro ou de os adquirir", disponível em https://www.consilium.europa.eu/pt/policies/geo-blocking/ [consultado em 25/09/2024].

Imaginemos o seguinte: a sociedade "Odisseia da Moda, S.A.", que vende roupas e acessórios através de um *site* na Internet, opera em Portugal e pretende expandir o seu mercado para outros países da União Europeia. Se um cliente francês tentar aceder ao *site* da "Odisseia da Moda, S.A." para comprar uma peça de roupa, por exemplo, um casaco, que só está disponível em Portugal, mas a sociedade bloqueia o acesso ao *site* ou redireciona o cliente francês para uma versão do *site* que não oferece o produto, isso constituiria uma prática de *geoblocking* injustificada. Neste caso, o cliente francês estaria impedido de adquirir um produto que poderia ser do seu interesse, simplesmente por questões geográficas.

De acordo com o Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018, que visa prevenir o bloqueio geográfico injustificado e outras formas de discriminação baseadas na nacionalidade, a "Odisseia da Moda, S.A." não pode adotar essa prática, uma vez que o cliente francês deve poder aceder livremente ao *site* e comprar o referido produto, desde que esteja disposto a pagá-lo, independentemente da sua localização. O Regulamento visa garantir que todos os consumidores da União Europeia tenham acesso a bens e serviços sem restrições arbitrárias baseadas na sua geografia.

O Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018, estabelece disposições que proíbem certas práticas de *geoblocking* injustificadas e garantem a acessibilidade dos bens e serviços na União Europeia[43]. Este Regulamento faz parte da estratégia da Comissão Europeia para um mercado único digital mais justo e acessível. Como podemos constatar no considerando 1 do referido Regulamento: "a fim de atingir o pleno potencial do mercado interno enquanto espaço sem fronteiras internas em que é assegurada, nomeadamente, a livre circulação de bens e serviços, não é suficiente abolir apenas os obstáculos de natureza estatal entre os Estados-Membros. Essa abolição pode ser contrariada por entidades privadas através da criação de obstáculos incompatíveis com as liberdades do mercado interno. É o que

[43] Para uma análise detalhada acerca do Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018, *vide*, entre todos, FRANCISCO GONZÁLEZ DE AUDICANA ZORRAQUINO, *Derecho de los Consumidores y Comercio Electrónico*, Madrid, Wolters Kluwer, 2021, pp. 60-63, onde o autor informa que, em janeiro de 2021, a Comissão Europeia sancionou seis editoras de videojogos com 7,8 milhões de euros por práticas de *geoblocking* aplicadas aos consumidores. Também, BERTA ESTEVE BELTRAN, «El geobloqueig en el mercat: conseqüències i prediccions», *IDP Revista de Internet, derecho y política = revista d'Internet, dret i política*, n.º 28, 2019, pp. 98 e ss. (pp. 98-108), disponível em https://raco.cat/index.php/IDP/article/view/373492/467082 [consultado em 25/09/2024]; ROBERTO CALLES BALLESTEROS, «Implicaciones en el Derecho Internacional Privado del Reglamento sobre Medidas Contra el Geobloqueo», *Revista Jurídica Universidad Autónoma de Madrid*, n.º 41, 2020, pp. 69 e ss. (pp. 69-92); RAÚL LAFUENTE SÁNCHEZ, «El Reglamento sobre bloqueo geográfico injustificado y la aplicación de las normas de Derecho internacional privado a los contratos de consumo concluidos por vía electrónica», in *El Derecho Privado en el Nuevo Paradigma Digital*, Madrid, Marcial Pons, 2020, pp. 255 e ss. (pp. 255-296).

acontece quando os comerciantes que operam num Estado-Membro bloqueiam ou restringem o acesso às suas interfaces em linha, nomeadamente sítios Web e aplicações móveis, aos clientes de outros Estados-Membros que pretendem realizar transações transfronteiriças (prática conhecida como «bloqueio geográfico»). É também o que acontece quando determinados comerciantes aplicam condições gerais de acesso diferentes aos seus bens e serviços em relação a esses clientes de outros Estados-Membros, tanto em linha como fora de linha. Embora, em certos casos, possa existir uma justificação objetiva para esse tratamento diferenciado, noutros casos, as práticas de alguns comerciantes recusam ou limitam o acesso a bens ou serviços aos clientes que pretendem realizar transações transfronteiriças, ou alguns comerciantes aplicam nesta matéria condições gerais de acesso diferentes, que não são objetivamente justificadas".

O Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018, no artigo 1.º, n.º 1 estabelece que "tem por objetivo contribuir para o correto funcionamento do mercado interno, evitando o bloqueio geográfico injustificado e outras formas de discriminação baseadas, direta ou indiretamente, na nacionalidade, no local de residência ou no local de estabelecimento dos clientes".

No entanto, há algumas situações em que o Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018, não se aplica; é o caso dos conteúdos protegidos por direitos de autor que estão sujeitos a restrições geográficas devido a contratos de licença ou direitos de autor (artigo 1.º, n.º 5)[44]. Isso significa que o acesso a conteúdos cinematográficos e de radiofusão, *e-books*, serviços de *stream* de música e videojogos *online* não se encontram sujeitos às regras deste Regulamento. O considerando 8 do Regulamento refere que "os serviços audiovisuais, incluindo os serviços cuja principal finalidade seja o acesso às transmissões televisivas de eventos desportivos, e que são fornecidos com base em licenças territoriais exclusivas, estão excluídos do âmbito de aplicação do presente regulamento. O acesso aos serviços financeiros de retalho, incluindo os serviços de pagamento, deverão, portanto, ser também excluídos, sem prejuízo das disposições do presente regulamento relativas à não discriminação nos pagamentos". Tenha-se, também, em consideração a exceção da segunda parte do artigo 4.º, n.º 1, alínea b), segundo a qual os comerciantes poderão aplicar condições gerais de acesso distintas aos bens ou serviços, por razões relacionadas com a nacionalidade, com o local de residência ou com o local de estabelecimento do cliente, no caso de se tratarem de "serviços cuja principal característica seja a oferta de acesso e a utilização de obras protegidas por direitos

[44] Para um maior desenvolvimento acerca da propriedade intelectual na Internet, *vide* MARIA EDUARDA GONÇALVES, *Ciberdireito – Liberdades, Direitos e Regulação na Era Digital*, Coimbra, Almedina, 2024, pp. 121-132.

de autor, ou de outros materiais protegidos, incluindo a venda, sob forma imaterial, de obras protegidas por direitos de autor ou de material protegido".

Como observa ALBERTO HIDALGO CEREZO, "o Regulamento foi insuficiente e perdeu-se a oportunidade de enfrentar uma das principais perplexidades do mercado único, precisamente num meio como a Internet, que se distingue pela sua ubiquidade, pela sua globalização e pela sua capacidade de quebrar fronteiras, que é uma das razões de ser da União Europeia: os bens digitais protegidos por direitos de autor"[45].

No ordenamento jurídico português, o Decreto-Lei n.º 80/2019, de 30 de maio, tem como objetivo assegurar a execução na ordem jurídica nacional do Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018, que visa prevenir o bloqueio geográfico injustificado e a discriminação nas vendas eletrónicas, promovendo o acesso equitativo a bens e serviços no mercado único da União Europeia.

Por sua vez, a Lei n.º 7/2022, de 10 de janeiro, visa proibir que os comerciantes que disponibilizam bens ou prestam serviços em território nacional, através da Internet, adotem práticas de *geoblocking* ou outras formas de discriminação nas transações *online*, baseadas, direta ou indiretamente, no local de residência ou de estabelecimento do consumidor (pessoa singular ou coletiva), quando este se situe nas Regiões Autónomas dos Açores e da Madeira[46]. Nos termos do artigo 4.º, n.º 1 e n.º 2, da Lei n.º 7/2022, de 10 de janeiro, "o comerciante não pode bloquear nem restringir, por meio de medidas de caráter tecnológico ou qualquer outro, o acesso do consumidor às suas interfaces online por razões relacionadas com o seu local de residência ou com o local de estabelecimento em território nacional". Além disso, "o comerciante não pode redirecionar o consumidor, por razões relacionadas com o seu local de residência ou com o local de estabelecimento em território nacional, para uma versão diferente da interface online a que o consumidor tentou aceder inicialmente".

O comércio eletrónico é fundamental na sociedade atual, ao permitir o acesso a produtos e serviços *online*. No entanto, práticas como o *geoblocking*, que limitam o acesso com base na localização geográfica, levantam questões sobre equidade e transparência nas transações *online*.

---

[45] ALBERTO HIDALGO CEREZO, *Nuevas Tendencias de Derecho de Consumo…*, *op. cit.*, p. 399.

[46] Para maiores desenvolvimentos sobre a Lei n.º 7/2022, de 10 de janeiro, *vide* CARLOS FILIPE COSTA, «Proibição de bloqueio geográfico injustificado e de outras formas de discriminação nas transações eletrónicas para os consumidores das Regiões autónomas dos Açores e da Madeira», in *Consumer Lab*, fevereiro de 2022, disponível em https://novaconsumerlab.novalaw.unl.pt/proibicao-de-bloqueio-geografico-injustificado-e-de-outras-formas-de-discriminacao-nas-transacoes--eletronicas-para-os-consumidores-das-regioes-autonomas-dos-acores-e-da-madeira/ [consultado em 25/09/2024].

O Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018, combate o bloqueio geográfico injustificado e a discriminação na União Europeia, garantindo que todos os consumidores europeus possam adquirir bens e serviços sem restrições arbitrárias. Contudo, o regulamento exclui conteúdos protegidos por direitos de autor, como filmes, música e serviços financeiros. Neste aspeto, ainda há muito caminho a percorrer para eliminar fronteiras.

5. Considerações finais

As transformações sociais e tecnológicas das últimas décadas provocaram mudanças profundas nos hábitos de consumo e nas relações contratuais, amplamente difundidas pelas tecnologias emergentes e pela Internet. Esta evolução, especialmente acentuada a partir da segunda metade do século XX, impulsionou o desenvolvimento de um quadro legal de proteção do consumidor, que responde aos desafios impostos por um mercado cada vez mais globalizado e digital. No âmbito da União Europeia, a criação de diplomas legais que asseguram maior transparência, segurança e equidade nas transações comerciais, tanto físicas como *online*, reflete uma preocupação crescente com o equilíbrio nas relações de consumo.

A contratação eletrónica, por seu turno, introduziu novas questões e desafios para o Direito do Consumo, como a necessidade de proteção de dados pessoais, a luta contra o *geoblocking* e a promoção de uma sociedade digital inclusiva. O comércio eletrónico e as redes sociais abriram possibilidades inéditas de comunicação e transações comerciais, mas também expuseram o consumidor a novos riscos, o que exige regulamentação contínua e adequada.

Desta forma, o Direito do Consumo está em constante evolução, moldado pela própria dinâmica das práticas de consumo e pela contínua evolução tecnológica. À medida que a sociedade se torna mais digital, o Direito do Consumo reforça o compromisso com a proteção dos direitos do consumidor, equilibrando a inovação tecnológica com a justiça social.

Com o avanço das tecnologias digitais e da globalização, o Direito do Consumo enfrenta agora desafios únicos. A transição para o ambiente digital, marcada pela expansão do comércio eletrónico e pela proliferação de serviços e conteúdos digitais, expõe o consumidor a novas formas de vulnerabilidade, exigindo normas adaptadas às especificidades deste contexto. Regulamentos como o (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, e o (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018, evidenciam os esforços para garantir a portabilidade de conteúdos e combater práticas de *geoblocking*, promovendo relações de consumo mais inclusivas e justas no seio da União Europeia.

Em suma, a adaptação contínua da legislação, que incorpora as transformações digitais e promove a proteção dos consumidores de forma equitativa e eficaz, é crucial para consolidar um mercado digital onde os consumidores possam sentir-se seguros e confiantes. O Direito do Consumo deve, assim, evoluir em sintonia com as mudanças tecnológicas, garantindo que as conquistas no domínio do consumo tradicional sejam adequadamente replicadas e reforçadas no domínio digital, promovendo um ambiente de consumo mais justo e inclusivo para todos os cidadãos da União Europeia.

DESAFIOS JURÍDICOS NA ERA DA INDÚSTRIA 4.0 E INTELIGÊNCIA ARTIFICIAL: UMA ANÁLISE DAS IMPLICAÇÕES LEGAIS E REGULATÓRIAS

Sérgio Silva[*]

Resumo: A Indústria 4.0, impulsionada por tecnologias emergentes como Inteligência Artificial (IA), Internet das Coisas (IoT) e automação avançada, transformou profundamente os setores produtivos e a sociedade, gerando novos desafios jurídicos e regulatórios. Este artigo analisa as principais implicações legais dessas inovações, abordando questões como a responsabilidade civil e penal por danos causados por sistemas autónomos de IA, especialmente em casos de acidentes envolvendo veículos autónomos. Também são discutidos desafios relacionados com a proteção de dados e privacidade, dada a recolha massiva de informações por dispositivos conectados. A propriedade intelectual surge como outra área crítica, considerando a criação de invenções e obras artísticas por IA. Além disso, a automação e respetivo impacto no emprego exigem novas regulamentações do trabalho. Questões éticas, como a transparência e imparcialidade nas decisões automatizadas, também são exploradas, bem como as vulnerabilidades de

* Doutorado em Sistemas de Software Inteligentes e Adaptáveis; Professor Auxiliar no Departamento de Ciências da Comunicação e Tecnologias da Informação da Universidade da Maia; Investigador no Departamento de Engenharia Mecânica da Faculdade de Engenharia do Porto. E-mail: *D012196@umaia.pt*

segurança cibernética em infraestruturas críticas. Por fim, o artigo destaca a importância da harmonização regulatória internacional para evitar desequilíbrios competitivos e garantir o uso seguro dessas tecnologias. A resposta jurídica a esses desafios deve equilibrar inovação e proteção de direitos, com regulamentos flexíveis e adaptáveis ao rápido avanço tecnológico.

Palavras-chave: Indústria 4.0; Inteligência Artificial; Direito.

Abstract: Industry 4.0, driven by emerging technologies such as Artificial Intelligence (AI), the Internet of Things (IoT) and advanced automation, has profoundly transformed production sectors and society, generating new legal and regulatory challenges. This article analyses the main legal implications of these innovations, addressing issues such a civil and criminal liability for damage caused by autonomous AI systems, especially in cases of accidents involving autonomous vehicles. Challenges related to data protection and privacy are also discussed, given the massive collection of information by connected devices. Intellectual property emerges as another critical area, considering the creation of inventions and artistic works by AI. In addition, automation and its impact on employment require new labour regulations. Ethical issues, such as transparency and impartiality in automated decisions, are also explored, as well as cyber security vulnerabilities in critical infrastructures. Finally, the article highlights the importance of international regulatory harmonisation to avoid competitive imbalances and guarantee the safe use of these technologies. The legal response to these challenges must balance innovation and the protection of rights, with regulations that are flexible and adaptable to rapid technological advances.

Keywords: Industry 4.0; Artificial Intelligence; Law.

1. Introdução

A Quarta Revolução Industrial, ou Indústria 4.0, integra tecnologias digitais, físicas e outras em que a IA desempenha um papel central. Como tal, grandes transformações ocorrem com várias oportunidades, mas também com enormes desafios jurídicos. Este capítulo apresenta uma breve descrição dos mesmos, tendo em consideração a evolução ao longo dos tempos.

1.1. A Revolução Tecnológica e a Indústria 4.0

A Indústria 4.0 representa a maior transformação atual no setor industrial, marcada pela convergência entre tecnologias digitais e processos de produção tradicionais. Envolve a integração de sistemas, os quais combinam automação de nível avançado, robótica, IoT, Big Data, computação na nuvem e IA. Estes comunicam entre si, atuam de forma autónoma e independente, criando

"fábricas" inteligentes capazes de monitorar, diagnosticar e otimizar operações em tempo real[1].

A IA, por sua vez, é crucial para a Indústria 4.0 e refere-se à capacidade de os sistemas computacionais realizarem tarefas que normalmente requerem inteligência ou intervenção humana, como sejam o reconhecimento de padrões, a tomada de decisões, a aprendizagem de conceitos e a resolução de problemas. Os sistemas de IA são projetados com o intuito de permitir a aprendizagem a partir de dados que, por sua vez, são processados para se ajustarem a novos dados, cenários ou eventos, mas sem intervenção humana, de forma direta[2].

Na prática, a IA na Indústria 4.0 pode ser aplicada, por exemplo, em previsões de produção. Os algoritmos analisam os dados históricos e, em tempo real, permitem prever falhas de máquinas e assim otimizar a manutenção[3]. Outro exemplo está relacionado com as questões logísticas, em que podemos recorrer à IA para otimizar rotas e fluxos de materiais em fábricas, armazéns ou centros de distribuição[4].

Na história, e até à atualidade, foram quatro as grandes revoluções industriais. Uma primeira que ocorreu entre o final do século XVIII e o início do século XIX, marcada pela mecanização do processo produtivo, em particular, uso de máquinas a vapor e a carvão[5]. Neste período assistiu-se a uma grande transformação da agricultura, da manufatura e do transporte, surgindo um enorme número de fábricas[6].

Entre o final do século XIX e o início do século XX assistimos à segunda revolução industrial. Eletrificação, surgimento e aplicação de novas fontes de energia (como o petróleo) e a invenção da linha de montagem são os seus grandes registos. Começam-se a produzir grandes quantidades de bens, assiste-se a uma globalização da indústria e ao aparecimento de novos setores, nomeadamente, o automobilístico[7].

---

[1] KLAUS SCHWAB, *A Quarta Revolução Industrial*, São Paulo, Edipro, 2016.

[2] ERIC TOPOL, *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*, Nova Iorque, Basic Books, 2019.

[3] DAVID GREEN, «The Impact of AI on Employment: The Case for Re-Skilling the Workforce», *Technology & Society*, vol. 18, n.º 1, 2020, pp. 85-102.

[4] MICHAEL E. PORTER e JAMES E. HEPPELMANN, «How Smart, Connected Products Are Transforming Competition», *Harvard Business Review*, vol. 92, n.º 11, 2014, pp. 64-88.

[5] KLAUS SCHWAB, *A Quarta Revolução Industrial*, *op. cit.*

[6] JEREMY RIFKIN, *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*, Nova Iorque, Palgrave Macmillan, 2014.

[7] ANDREAS ZÜST e HELGA NOWOTNY, *Industry 4.0: The Digital Transformation of Industry*, Berlim, Springer, 2017.

A terceira revolução industrial ocorre também no século XX, entre as décadas de 60 e 80, sendo conhecida por revolução digital. Introduzem-se os computadores e sistemas de controle automáticos em que os processos produtivos são automatizados com recurso à eletrónica e informática[8].

A quarta revolução industrial, Indústria 4.0, no corrente século XXI, assenta numa fusão entre os mundos físico e digital. Tecnologias como IA, IoT, Big Data e computação na nuvem são o núcleo desta revolução, transformando radicalmente a produção, alcançando níveis inéditos de automação, conectividade e personalização[9].

A Indústria 4.0 difere de todas as anteriores pelo uso massivo de dados para a tomada de decisões em tempo real. São introduzidos sistemas inteligentes e uma automação total (ou quase) pela integração de sensores, software e algoritmos de aprendizagem máquina. Isso possibilita efetuar previsões de necessidades de manutenção, ajustar processos produtivos sem qualquer intervenção humana e, até mesmo, a personalização de produtos de acordo com as preferências e necessidades dos clientes e em tempo real[10].

A combinação de IA, IoT e Big Data na Indústria 4.0 está a transformar o setor produtivo e o quotidiano das pessoas. A automação avançada, com robôs colaborativos (*cobots*) e IA, permite a otimização dos processos produtivos, reduzindo erros e custos. Equipamentos conectados via IoT fornecem dados em tempo real que, analisados por IA, ajudam a prever falhas e planear manutenções, resultando em maior eficiência e redução de custos operacionais[11].

Com grandes volumes de dados é possível estudar o perfil do consumidor em função da procura de um produto e aumentar o número de clientes através da análise das suas preferências. Isto permite que as fábricas inteligentes alterem a produção conforme os dados do mercado em tempo real[12].

A gestão da *supply chain* é outro dos aspetos a considerar. Com a IoT, a cadeia de suprimentos é interligada. Sensores são conectados a sistemas de IA para monitorarem *stocks*, emitirem previsões de procura, fluxos de transporte,

[8] DAVID GREEN, «The Impact of AI on Employment: The Case for Re-Skilling the Workforce», *op. cit.*

[9] LUCIANO FLORIDI, «The Fourth Industrial Revolution and Its Ethical Challenges», *Philosophy & Technology*, vol. 31, n.º 1, 2018, pp. 1-14.

[10] RAJKUMAR BUYYA e AMIR VAHID DASTJERDI, *Internet of Things: Principles and Paradigms*, Amsterdã, Elsevier, 2016.

[11] KLAUS SCHWAB, *A Quarta Revolução Industrial*, *op. cit.*

[12] MICHAEL E. PORTER e JAMES HEPPELMANN, «How Smart, Connected Products Are Transforming Companies», *op. cit.*

entre outros. Assim, em tempo real, podem ser feitos ajustes para evitar gargalos, melhorar a eficiência logística e reduzir o desperdício de recursos[13].

Na vida quotidiana, o impacto da Indústria 4.0 também é visível em aspetos como a mobilidade urbana, comércio e consumo, saúde e bem-estar, entre outros. Na mobilidade urbana está a questão dos veículos autónomos, por exemplo. As cidades vão-se redesenhando e adaptando a esses novos modos de transporte. A IA e a IoT permitem que os veículos se conduzam de forma autónoma, comuniquem entre si e com a infraestrutura urbana, promovendo um fluxo de tráfego mais eficiente e seguro[14].

Na saúde e bem-estar, com a introdução de sensores ligados a dispositivos de saúde, como relógios inteligentes e monitores de glicose, há uma contínua monitoração dos sinais vitais e outros. Os algoritmos de IA processam as informações e fornecem *feedback*, no imediato, aos utentes e profissionais de saúde, contribuindo para diagnósticos mais precisos e tratamentos mais personalizados[15]. Em particular, no comércio e consumo, as plataformas de e-commerce utilizam IA para sugerir produtos com base no histórico de navegação e compras dos consumidores. E com o auxílio de sistemas de logística inteligentes, as entregas são mais rápidas e eficientes, fazendo uso de dados de tráfego em tempo real para otimizar rotas de entrega[16].

1.2. O direito e as novas tecnologias

A integração de IA, IoT e Big Data oferece oportunidades de inovação e crescimento, mas também levanta desafios em termos de regulamentação legal e questões éticas, como sejam a privacidade de dados, o desemprego tecnológico e a responsabilidade civil e penal em sistemas automatizados.

As inovações tecnológicas, especialmente na era da Indústria 4.0 e da IA, têm transformado profundamente a sociedade e a economia, com mudanças no modo como as pessoas interagem, produzem, compram e consomem. Perante tais transformações, o direito exerce um papel crucial ao fornecer o arcabouço normativo necessário e indispensável para regular o avanço tecnológico e proteger interesses sociais, institucionais, empresariais e individuais. A regulamentação legal para as novas tecnologias deve procurar um equilíbrio entre o incentivo

[13] EDUARDO MAGRANI, *Internet das Coisas: A Internet das Coisas e os Desafios Regulatórios*, 1.ª ed., São Paulo, FGV Editora, 2018.

[14] ERIK BRYNJOLFSSON e ANDREW MCAFEE, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, New York, W.W. Norton & Company, 2014.

[15] GARY MARCUS e ERNEST DAVIS, *Rebooting AI: Building Artificial Intelligence We Can Trust*, 1.ª ed., New York, Pantheon Books, 2019.

[16] TOSHIE TAKAHASHI, *AI and Society: A Convergence of New Ideas in Science and Technology*, 1.ª ed., Cambridge, Cambridge University Press, 2019.

à inovação e a garantia da segurança, privacidade, bem como dos direitos fundamentais e o bem-estar individual e coletivo[17].

Tecnologias como IA, IoT e Big Data trazem desafios jurídicos complexos, como a proteção de dados pessoais, a responsabilidade por danos de máquinas autónomas e a propriedade intelectual de algoritmos[18]. Isso exige que os sistemas legais se adaptem continuamente para antecipar riscos éticos e garantir que os avanços tecnológicos respeitem direitos fundamentais[19].

Assim, o direito deve criar mecanismos que promovam a transparência e a responsabilidade no uso destas inovações, protegendo em simultâneo os indivíduos e a sociedade de possíveis abusos ou malefícios que resultem do uso dos meios tecnológicos. Um exemplo é o Regulamento Geral sobre a Proteção de Dados (RGPD) na União Europeia (UE), de 2016, que estabelece diretrizes rigorosas para o tratamento de dados pessoais, refletindo a crescente preocupação com a privacidade na atual era digital.

Ao longo do tempo, o sistema jurídico demonstrou capacidade de se adaptar aos avanços tecnológicos. Desde a primeira revolução industrial, marcada pelo surgimento das máquinas a vapor e das primeiras fábricas, o direito precisou de se moldar às novas realidades económicas e sociais. Isso gerou questões sobre condições de trabalho, segurança industrial e direitos dos trabalhadores, levando à criação de legislações específicas para protegê-los e regular a indústria[20].

À medida que as inovações tecnológicas se tornaram mais sofisticadas, o direito foi-se adaptando para lidar com os novos desafios. A segunda revolução industrial, caracterizada pela eletrificação e massificação da produção, levou à criação de regulamentações sobre propriedade intelectual e patentes, essenciais para proteger as invenções e promover a competitividade. Da mesma forma, com a terceira revolução industrial surgem os computadores e a automação exigiu que fossem criadas normas, especialmente no campo das tecnologias da informação e comunicação, que até hoje enfrenta o desafio de acompanhar a rápida e contínua evolução da era digital[21].

Atualmente, na quarta revolução industrial, o sistema jurídico enfrenta o desafio de se adaptar a inovações rápidas e imprevisíveis, resultando no "*gap* normativo", em que a tecnologia avança mais rapidamente do que as leis.

---

[17] LUCIANO FLORIDI, «The Fourth Industrial Revolution and Its Ethical Challenges», *op. cit.*

[18] ROLF H. WEBER, «Liability in the Internet of Things», *Journal of European Consumer and Market Law*, vol. 8, n.º 2, 2019, pp. 65-76.

[19] DANIEL SUSSER, *Data Privacy and Ethics in the Age of Big Data*, Nova Iorque, Springer, 2020.

[20] ALFRED D. CHANDLER, *The Visible Hand: The Managerial Revolution in American Business*, Cambridge, Belknap Press, 1977.

[21] LAWRENCE LESSIG, *Code and Other Laws of Cyberspace*, Nova Iorque, Basic Books, 1999.

Os legisladores precisam desenvolver regulações flexíveis que se ajustem a esses avanços sem inibir a inovação[22].

Em resposta a este cenário, surgem novas formas de abordagem regulatória, como a regulação responsiva, que envolve a participação ativa de múltiplos atores e agentes (governo, indústria, consumidores) no processo regulatório. Este modelo vai à procura de uma abordagem colaborativa, onde as políticas públicas podem ser ajustadas de forma ágil e proativa em resposta às inovações tecnológicas[23].

1.3. Desafios globais e a necessidade de regulação

A Indústria 4.0 apresenta uma série de desafios para as estruturas jurídicas e regulatórias que pretendem acompanhar o avanço das tecnologias emergentes. Entre os principais desafios estão a responsabilidade civil, a proteção de dados, a segurança cibernética, as questões éticas e as relações laborais num contexto de automação. Estes aspetos exigem soluções inovadoras por parte dos legisladores e desafiam que se adequem os sistemas jurídicos existentes à nova realidade.

Um dos maiores problemas a enfrentar é a responsabilidade civil quando as decisões são tomadas por sistemas de IA. Por exemplo, quando um carro autónomo está envolvido num acidente, torna-se difícil identificar quem é o responsável: o proprietário do veículo, o programador do software ou o fabricante do automóvel? A dificuldade de atribuir responsabilidade num cenário de automação e de aprendizagem máquina é um dos desafios principais que exige uma reavaliação das normas existentes no âmbito da responsabilidade[24].

Outro ponto crítico é a proteção de dados pessoais. A Indústria 4.0 depende amplamente de grandes volumes de dados obtidos por sensores, dispositivos conectados e redes inteligentes. O uso de Big Data em sistemas de produção, marketing e personalização de produtos implica a necessidade de proteger a privacidade dos indivíduos. Neste sentido, as legislações de proteção de dados, como o RGPD da UE, servem como modelo para os que ainda carecem de regulação robusta.

A segurança cibernética é uma preocupação global devido à crescente conectividade entre sistemas industriais e a infraestrutura digital, o que os torna vulneráveis a ataques. Falhas de segurança em sistemas automatizados podem ter consequências devastadoras para setores essenciais como a energia, saúde e

---

[22] ROGER BROWNSWORD, *Law, Technology and Society: Re-imagining the Regulatory Environment*, Londres, Routledge, 2019.

[23] JULIA BLACK, «Critical Reflections on Regulation», *Australian Journal of Legal Philosophy*, vol. 27, 2002, pp. 1-35.

[24] ROLF H. WEBER, «Liability in the Internet of Things», *op. cit.*

transporte. Assim, é fundamental reforçar as estruturas jurídicas para estabelecer diretrizes de segurança digital[25].

Por fim, o impacto da automação sobre o mercado de trabalho também representa um desafio significativo para as regulamentações. A substituição de trabalhadores por máquinas ou por sistemas automatizados exige que as legislações do trabalho sejam revistas para lidar com questões de desemprego tecnológico, requalificação profissional e novas formas de emprego. É fundamental que os sistemas legais estabeleçam políticas que incentivem a "recapacitação" da mão de obra para enfrentar as mudanças laborais resultantes da automação[26].

O impacto das tecnologias emergentes, como a IA, a IoT e o Big Data, ultrapassa fronteiras nacionais e exige uma abordagem coordenada de forma global para enfrentar os desafios regulatórios. A natureza transfronteiriça da Indústria 4.0, com empresas que operam em diversos países e mercados interconectados, conduz à necessidade de uma discussão de regulamentação internacional sobre governança tecnológica.

Um dos principais obstáculos à regulação global é a divergência de padrões regulatórios entre diferentes países e grupos económicos. Enquanto a UE implementa uma regulamentação robusta com o RGPD para proteger a privacidade dos dados, outros países, como os Estados Unidos, adotam uma abordagem mais fragmentada e permissiva. Esta falta de harmonização pode criar barreiras para a inovação e aumentar os custos de conformidade para empresas que operam e estão sujeitas a múltiplas jurisdições[27].

O uso da IA levanta preocupações éticas e de direitos humanos que precisam ser abordadas globalmente. A falta de normas internacionais claras pode resultar em violações de direitos fundamentais, como a privacidade. Embora organizações como as Nações Unidas e a OCDE (Organização para a Cooperação e Desenvolvimento Económico) tentem estabelecer diretrizes éticas, a aplicação efetiva dessas normas ainda enfrenta desafios[28].

A regulação internacional é vital para garantir a segurança digital, pois as ameaças cibernéticas afetam todos os países. A cooperação em cibersegurança

---

[25] DAVID FERBRACHE, «Cybersecurity in the Age of Industry 4.0», *Journal of Strategic Risk*, vol. 10, n.º 1, 2020, pp. 45-67.

[26] CARL BENEDIKT FREY e MICHAEL OSBORNE, *The Future of Employment: How Susceptible Are Jobs to Computerisation?*, Oxford, Oxford Martin, 2013.

[27] ROGER BROWNSWORD, *Law, Technology and Society…*, *op. cit.*

[28] STUART RUSSELL e PETER NORVIG, *Artificial Intelligence: A Modern Approach*, 4.ª ed., Nova Jersey, Pearson, 2020.

e a criação de tratados com padrões mínimos de segurança são essenciais para construir uma rede global resiliente e segura[29].

A evolução das tecnologias emergentes exige, portanto, não apenas respostas nacionais, mas também um empenho colaborativo global para estabelecer regras claras que promovam a inovação responsável e que protejam os interesses das sociedades e dos indivíduos. A coordenação internacional será vital para enfrentar os desafios éticos, jurídicos e económicos da Indústria 4.0 e suas implicações.

2. Responsabilidade civil e penal em casos envolvendo IA

Com o avanço da IA, surgem novas questões jurídicas, especialmente quanto à responsabilidade civil e penal por danos causados por sistemas autónomos. A crescente automação desafia os princípios tradicionais de responsabilidade, desenvolvidos para um mundo centrado nas ações humanas. Na Indústria 4.0, que envolve IA em setores como transporte, saúde e produção, é necessária a revisão dos conceitos jurídicos. Este capítulo examina as implicações legais da IA em casos de acidentes, falhas e crimes, discutindo a distribuição de responsabilidades entre fabricantes, usuários, programadores e até, eventualmente, terceiros.

2.1. Conceitos de responsabilidade civil e penal na era da IA

A responsabilidade civil e penal são dois pilares fundamentais do sistema jurídico e ambos devem ser adaptados ao novo contexto da IA. No campo da responsabilidade civil, o objetivo é garantir a reparação de danos causados a terceiros, enquanto a responsabilidade penal visa sancionar condutas que configurem infrações à ordem jurídica especialmente censuráveis.

No direito civil, a responsabilidade por danos pode basear-se na culpa, que inclui tanto a negligência (falta de cuidado esperado) quanto o dolo (intenção deliberada de causar dano). No contexto de sistemas de IA, a negligência é particularmente relevante, devido a falhas no *design*, programação ou supervisão de sistemas automatizados, como veículos autónomos ou sistemas médicos[30].

No direito penal, a responsabilidade é normalmente associada à ação ou omissão de um indivíduo que tenha a capacidade de tomar decisões conscientes e intencionais. A introdução de sistemas autónomos que operam de forma independente levanta questões sobre a aplicabilidade do dolo ou negligência. Um sistema de IA, por exemplo, não possui intencionalidade no sentido humano da

[29] JULIA BLACK, «Critical Reflections on Regulation», *op. cit.*

[30] ANDRÉIA GALDINO, «Responsabilidade Civil na Era da IA», *Revista de Direito Privado*, vol. 12, n.º 4, 2019, pp. 124-130.

palavra[31], pelo que é difícil enquadrá-lo nas estruturas legais atuais que procuram punir ações deliberadas[32].

Desta forma, o direito enfrenta limitações significativas para lidar com danos causados por sistemas de IA, tanto no âmbito civil quanto no penal. Há uma lacuna entre o desenvolvimento tecnológico e a capacidade do direito em lidar com as inovações. A definição de responsabilidade, seja por falhas de sistemas ou por decisões automatizadas que causem danos, necessita de ser revista à luz da autonomia crescente das máquinas.

2.2. Casos práticos e discussão sobre veículos autónomos

Uma das áreas em que mais se discute a responsabilidade envolvendo IA é relativa ao uso de veículos autónomos. Estes veículos, que são capazes de dirigir sem intervenção humana, já estiveram envolvidos em acidentes fatais, o que gerou uma discussão sobre como a responsabilidade deve ser atribuída nestes casos[33].

Um caso emblemático ocorreu nos Estados Unidos, em 2018, quando um veículo autónomo da Uber atropelou e matou um peão, enquanto estava em modo autónomo. Neste caso, gerou-se a discussão sobre quem seria responsável, a empresa que fabricou o carro, a empresa que desenvolveu o software, o motorista que estava no banco do passageiro ou a própria empresa Uber. Eis o desafio de determinar se a responsabilidade deveria ser objetiva e/ou subjetiva e se haverá lugar ao sancionamento de condutas por negligência e em que termos[34].

Em alguns países, como a Alemanha, as legislações emergentes sobre veículos autónomos já preveem a responsabilidade objetiva dos fabricantes em caso de falhas nos sistemas autónomos. Nos Estados Unidos, ainda está em discussão, com os estados a adotarem diferentes abordagens[35]. No entanto, a questão mais ampla que surge é se esses acidentes podem ser considerados falhas técnicas inevitáveis ou se refletem algum nível de negligência por parte dos desenvolvedores de software ou dos fabricantes.

---

[31] Ver, no entanto, GIOVANNI SARTOR, «Cognitive automata and the law: electronic contracting and the intentionality of software agents», *Artificial intelligence and law*, vol. 17, n.º 4, 2009, pp. 253-290.

[32] MARK COECKELBERGH, *AI Ethics*, Cambridge, MIT Press, 2020.

[33] BRYANT WALKER SMITH, «Automated Driving & Product Liability», *Michigan Law Review*, vol. 16, n.º 4, 2019, pp. 760-765.

[34] RYAN CALO, «Robotics and the Lessons of Cyberlaw», *California Law Review*, vol. 103, n.º 3, 2015, pp. 515-523.

[35] UWE SEIDEL, «Automated Vehicles in Europe: Legal and Regulatory Framework», *European Transport Law Review*, vol. 12, n.º 1, 2021, pp. 49-55.

A IA em veículos autónomos levanta questões sobre responsabilidade subjetiva. Se um condutor efetua ativação do modo autónomo, sabendo que está em teste, ele assume a culpa? A complexidade aumenta em situações críticas, como acidentes iminentes, onde o veículo deve escolher entre salvar uma pessoa ou proteger os passageiros. Atribuir responsabilidade nessas circunstâncias representa um grande desafio legal[36].

2.3. Atribuição de responsabilidade: fabricantes, utilizadores e programadores

A questão central em casos envolvendo falhas de IA é: quem deve ser responsabilizado? Diferentes partes estão envolvidas no desenvolvimento e uso de sistemas de IA, desde fabricantes e desenvolvedores de *software* até utilizadores finais e, eventualmente até, terceiros[37]. No entanto, a atribuição de responsabilidade nem sempre é obvia[38].

Em muitos casos, os fabricantes de dispositivos ou máquinas autónomas podem ser responsabilizados pelos danos causados, especialmente se houver uma falha de *design* ou se o sistema for inerentemente perigoso. Nos casos de responsabilidade objetiva, os fabricantes podem ser considerados responsáveis, mesmo que não tenham agido com culpa, especialmente se o produto ou sistema apresentar riscos significativos.

Uma questão interessante surge em relação aos desenvolvedores de software que criam os algoritmos de controle dos sistemas de IA. Se o algoritmo falhar ou tomar decisões que provoquem danos, os programadores devem ser considerados responsáveis? A resposta varia, mas, em muitos casos, defende-se que os programadores têm a responsabilidade de garantir que os sistemas sejam projetados para minimizar erros e tomar decisões seguras.

Os utilizadores de sistemas de IA, especialmente quando estão no controle de máquinas como veículos autónomos, também podem ser considerados responsáveis se forem negligentes no uso da tecnologia. Por exemplo, se um

---

[36] PATRICK LIN, «The Ethics of Autonomous Cars», *The Atlantic*, 2020.

[37] Cfr. artigo 3.º, parágrafo 13, do Regulamento de Inteligência Artificial: "Utilização indevida razoavelmente previsível", a utilização de um sistema de IA de uma forma não conforme com a sua finalidade prevista, mas que pode resultar de um comportamento humano razoavelmente previsível ou de uma interação razoavelmente previsível com outros sistemas, incluindo outros sistemas de IA; e artigo 14.º, n.º 2: "A supervisão humana deve procurar prevenir ou minimizar os riscos para a saúde, a segurança ou os direitos fundamentais que possam surgir quando um sistema de IA de risco elevado é usado em conformidade com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsível".

[38] GABRIELA ZANFIR-FORTUNA, «Data Protection in the Era of AI», *Computer Law & Security Review*, vol. 35, n.º 2, 2019, pp. 124-135.

motorista optar por confiar totalmente num sistema autónomo sem supervisão, mesmo sabendo que o sistema ainda está em fase de teste, ele pode ser considerado negligente[39].

Os tribunais enfrentam dificuldades para decidir como atribuir a responsabilidade nesses casos, e as respostas variam de acordo com a jurisdição e as circunstâncias específicas do caso. Em última análise, a atribuição de responsabilidade em sistemas de IA envolve uma análise detalhada das circunstâncias de cada caso, bem como uma consideração das obrigações de cada parte envolvida no desenvolvimento e uso da IA.

2.4. Crimes e responsabilidade penal relacionados com IA

Além de causar danos no contexto civil, a IA também tem o potencial de ser utilizada para a prática de crimes ou até mesmo cometer atos criminosos por si só. Isto levanta questões sobre a responsabilidade penal e como o sistema jurídico pode lidar com crimes cometidos por ou com a ajuda de sistemas de IA.

Em crimes cibernéticos, por exemplo, a IA pode ser utilizada para *hackear* sistemas, manipular dados financeiros ou até mesmo lançar ataques de *pishing* de maneira automatizada. Nestes casos, os sistemas de IA facilitam a prática de crimes, embora a responsabilidade, geralmente, recaia sobre os indivíduos que controlam ou utilizam esses sistemas[40].

A complexidade aumenta quando um sistema de IA atua autonomamente e causa danos ou viola a lei, como no caso de algoritmos de *trading* que realizam transações ilegais sem intervenção dos desenvolvedores. Atribuir responsabilidade penal nesse contexto pode envolver a análise da programação original para determinar se houve negligência por parte dos programadores ou operadores[41].

A responsabilidade penal da IA ainda é um campo emergente e os tribunais apenas começam a considerar como lidar com tal. Alguns propõem que, no futuro, os sistemas de IA possam ser tratados como agentes legais, com as suas próprias responsabilidades e obrigações[42]. No entanto, essa abordagem levanta questões éticas e jurídicas, que ainda precisam ser discutidas e debatidas[43].

---

[39] JOHN FRANK WEAVER, *Robots Are People Too: How Siri, Google Car, and Artificial Intelligence Will Force Us to Change Our Laws*, New York, Praeger, 2014.

[40] DAVID OPPENHEIMER, «AI and Cybercrimes: The Emerging Legal Landscape», *Journal of Internet Law*, vol. 24, n.º 3, 2021, pp. 18-25.

[41] KEVIN WERBACH, «The AI Tradeoff: Accountability vs. Innovation», *Yale Law Journal*, vol. 28, n.º 2, 2020, pp. 245-250.

[42] GABRIEL HALLEVY, «The Criminal Liabilities of Artificial Intelligence Entities – From Science Fiction to Legal Social Control», Akron Intellectual Property Journal, vol. 4, n.º 2, 2010, pp. 171-201.

[43] SANDRA WACHTER, «The Ethical Challenges of Algorithms», *Oxford Internet Institute*, 2018.

A proposta de Regulamento da Inteligência Artificial da União Europeia (AI Act) apresenta um modelo baseado em níveis de risco, categorizando aplicações de IA como de risco mínimo, limitado, alto ou inaceitável. Aplicações de alto risco, como sistemas usados na saúde ou no setor judicial, estão sujeitas a requisitos rigorosos de transparência e auditabilidade. O princípio da transparência exige que sistemas de IA sejam compreensíveis para os seus utilizadores e regulamentadores, promovendo confiança e responsabilidade[44].

A Diretiva da Responsabilidade do Produtor oferece um enquadramento legal para compensação em casos de danos causados por produtos defeituosos, incluindo sistemas de IA. Complementarmente, a Proposta de Diretiva relativa à responsabilidade civil extracontratual por atos praticados por IA (2022) introduz medidas como a inversão do ónus da prova, facilitando o processo para que as vítimas possam demonstrar defeitos em sistemas de IA. Estas iniciativas refletem a necessidade de equilibrar inovação com proteção dos direitos dos consumidores[45].

3. Proteção de dados e privacidade na Indústria 4.0

A Indústria 4.0 e a revolução digital estão a criar um cenário global com tecnologias como IA, IoT e Big Data que aumentam a eficiência e automação. No entanto, isso traz desafios significativos para a proteção de dados e privacidade, exigindo estruturas regulatórias robustas para garantir um uso ético e transparente dos dados pessoais e industriais.

3.1. A era dos dados e a Indústria 4.0

A Indústria 4.0 depende da recolha massiva de dados para automatizar e personalizar processos industriais, com IA, IoT e Big Data no centro desse novo paradigma. Essas tecnologias permitem o processamento de grandes volumes de dados em tempo real, otimizando a produção, prevendo falhas e personalizando produtos, além de melhorar a eficiência logística. No entanto, essa dependência de dados traz riscos significativos à privacidade, gerando preocupações sobre o uso e proteção dessas informações.

O Big Data permite que grandes volumes de informações sejam analisados para descobrir padrões, tendências e associações que podem ser usados para a tomada de decisões. Na Indústria 4.0, essas tecnologias são cruciais para permitir a automação e a personalização, desde a fabricação até ao atendimento

[44] MARTIN EBERS, «Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act», *SSRN Electronic Journal*, 2021.

[45] ANN-KRISTIN MAYRHOFER, «Product liability in the age of AI — Proposal for a "two track" solution», *RED – Revista Electrónica de Direito*, n.º 1, 2024.

ao cliente. No entanto, a recolha e o uso de dados pessoais levantam sérias preocupações sobre invasão de privacidade ou uso indevido de informações[46].

O uso intensivo de IoT conecta dispositivos físicos a redes digitais, permitindo que máquinas e sensores recolham e transmitam dados sem intervenção humana. Embora isso traga grandes benefícios em termos de eficiência, também apresenta vulnerabilidades, como ataques cibernéticos ou o acesso não autorizado a dados pessoais[47]. A IA, por sua vez, depende de grandes volumes de dados para treino de algoritmos e sistemas de aprendizagem máquina, criando riscos relacionados à transparência e à tomada de decisão automatizada, especialmente quando se trata de decisões que afetam diretamente as pessoas[48].

Essas tecnologias criam um ambiente onde os dados são valiosos, mas também altamente vulneráveis. O "rasto digital" deixado pelas pessoas e empresas no contexto da Indústria 4.0 pode ser utilizado de forma imprevista inicialmente, o que acarreta riscos significativos para a privacidade.

3.2. O Regulamento Geral sobre a Proteção de Dados e modelos internacionais

O Regulamento Geral sobre a Proteção de Dados, introduzido pela UE em 2016, é uma das tentativas mais abrangentes de regulamentar o uso de dados pessoais nesta era digital. O RGPD estabelece uma série de princípios e obrigações para as empresas que processam dados pessoais, com o objetivo de garantir que as pessoas tenham controle das suas informações. Entre os principais aspetos do RGPD, destacam-se os princípios de legalidade, transparência, consentimento informado e responsabilização.

No contexto da Indústria 4.0, o RGPD é um marco importante, pois exige que as empresas que operam com grandes volumes de dados, especialmente através de tecnologias como IA e IoT, adotem práticas rigorosas de proteção de dados. O regulamento também introduz o conceito de *Privacy by Design*, que implica que a proteção de dados deve ser incorporada desde o início no desenvolvimento de sistemas e processos industriais[49].

---

[46] DAVID LANEY, «3D Data Management: Controlling Data Volume, Velocity, and Variety», *META Group*, 2001.

[47] MICHAEL CHUI, «The Internet of Things: Mapping the Value Beyond the Hype», *McKinsey Global Institute*, 2015.

[48] NICK BOSTROM, *Superintelligence: Paths, Dangers, Strategies*, Oxford, Oxford University Press, 2014.

[49] ANN CAVOUKIAN, «Privacy by Design: The 7 Foundational Principles», *Information and Privacy Commissioner of Ontario*, Canada, 2011.

O RGPD enfrenta desafios na Indústria 4.0 devido à recolha contínua de dados e decisões automatizadas, dificultando a obtenção de consentimento válido e informado, pois os usuários muitas vezes não entendem como os seus dados serão utilizados em sistemas complexos de IA[50]. Além disso, a natureza transfronteiriça da recolha e processamento de dados cria desafios para a aplicação efetiva do RGPD, especialmente quando empresas fora da UE não seguem padrões similares.

Modelos regulatórios como o California Consumer Privacy Act (CCPA), de 2018, e a Lei Geral de Proteção de Dados brasileira (LGPD), em vigor desde 2020, procuram garantir maior controle sobre os dados pessoais. O CCPA permite que consumidores saibam que dados são recolhidos e solicitem a sua exclusão. A LGPD brasileira assenta nos princípios do RGPD e visa regular o uso de dados pessoais, impondo obrigações rigorosas para as empresas. No entanto, tanto o CCPA como a LGPD enfrentam os mesmos desafios que o RGPD, especialmente no que diz respeito à aplicabilidade na Indústria 4.0.

Essas legislações, embora importantes, ainda necessitam de melhorias para lidar com as novas complexidades introduzidas pela IA e pela IoT, que tornam o controle sobre os dados pessoais mais difícil de ser implementado e monitorado. O desenvolvimento de regulações globais coordenadas será crucial para garantir que a proteção de dados seja eficaz num contexto internacional, onde as empresas operam em múltiplas jurisdições e com diferentes padrões de privacidade.

3.3. Consentimento informado e transparência em sistemas de IA

A Indústria 4.0 e o uso de IA levantam questões fundamentais sobre o consentimento informado e a transparência no processamento de dados. Um dos principais problemas enfrentados pelas regulamentações de proteção de dados é a dificuldade de garantir que os indivíduos estejam plenamente cientes de como os seus dados são utilizados, especialmente em sistemas de IA que operam com grandes volumes de dados automática e continuamente[51].

O consentimento informado exige explicações claras sobre a recolha e uso de dados, mas muitos indivíduos não têm o conhecimento técnico necessário para entender as implicações, levando a consentimentos inconscientes. Além disso, dados anonimizados ou pseudonimizados podem dar uma falsa sensação de segurança, pois podem ser reidentificados com tecnologias avançadas[52].

---

[50] DANIEL J. SOLOVE, «Privacy Self-Management and the Consent Dilemma», *Harvard Law Review*, vol. 126, 2013, pp. 1880-1903.

[51] SANDRA WACHTER, «The Ethical Challenges of Algorithms», *op. cit*.

[52] LATANYA SWEENEY, «K-Anonymity: A Model for Protecting Privacy», *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, n.º 5, 2002, pp. 557-570.

A transparência nos sistemas de IA é problemática, pois muitos algoritmos funcionam como "caixas-negras", ocultando o processo decisório até mesmo dos desenvolvedores. Isso levanta questões sobre justiça e imparcialidade, especialmente em áreas como contratação e crédito, e dificulta que os indivíduos contestem decisões automatizadas[53].

O Regulamento de Inteligência Artificial reforça a necessidade de que os sistemas de IA operem de forma compreensível e garantam a rastreabilidade das operações. O artigo 12.º, n.º 1, estabelece que "os sistemas de IA de risco elevado devem permitir tecnicamente o registo automático de eventos («registos») durante a vida útil do sistema". Além disso, o artigo 50.º, n.º 1, determina que "os prestadores devem assegurar que os sistemas de IA destinados a interagir diretamente com pessoas singulares sejam concebidos e desenvolvidos de maneira que as pessoas singulares em causa sejam informadas de que estão a interagir com um sistema de IA".

A responsabilização é fundamental na proteção de dados na era da IA. As empresas devem garantir a conformidade com as normas e explicar como os algoritmos funcionam, permitindo que os utilizadores controlem os seus dados. Essa responsabilização é vital para reconstruir a confiança entre consumidores e empresas em tecnologias avançadas[54].

O artigo 22.º do RGPD regula decisões totalmente automatizadas que produzam efeitos jurídicos ou impactem significativamente os indivíduos. Este artigo exige supervisão humana em tais decisões, bem como o direito de os indivíduos obterem explicações sobre os critérios utilizados. No entanto, sistemas complexos de IA, como redes neuronais profundas, dificultam a implementação prática deste direito, dada a sua opacidade técnica e falta de explicabilidade[55].

4. Propriedade intelectual e IA

A IA trouxe avanços em diversas áreas, incluindo a criação de obras de arte, músicas e invenções, levantando desafios jurídicos na proteção dessas criações sobre a propriedade intelectual (PI). As estruturas tradicionais de PI, projetadas para proteger criações humanas, enfrentam agora questões com o aumento da autonomia dos sistemas de IA na geração de inovações. Este capítulo explora os desafios jurídicos da PI no contexto da IA, abordando quem

[53] FRANK PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Harvard, Harvard University Press, 2015.

[54] GIANCLAUDIO MALGIERI, «Automated Decision-Making in the GDPR: Interpretation and Comparative Analysis», *Computer Law & Security Review*, vol. 34, n.º 2, 2018, pp. 222-230.

[55] DANIEL J. SOLOVE, «Privacy Self-Management and the Consent Dilemma», *Harvard Law Review*, vol. 126, n.º 7, 2013.

deve deter os direitos sobre essas criações e como a legislação se deve adaptar a essa nova realidade.

4.1. Desafios da propriedade intelectual na era da IA

Um dos principais debates jurídicos na era da IA é sobre quem detém os direitos de propriedade intelectual de criações geradas por sistemas de IA. As leis de PI foram tradicionalmente concebidas para proteger invenções e obras de autores humanos, mas surgem dúvidas sobre se os direitos pertencem ao programador, ao proprietário do sistema ou, em tese, à própria IA como entidade autónoma[56].

Os sistemas de IA podem, por exemplo, criar obras musicais, como foi o caso da denominada AIVA[57] (Artificial Intelligence Virtual Artist), que compôs várias peças musicais[58] reconhecidas pela SACEM, a sociedade de direitos autorais de França. Eis a questão de quem tem direito sobre essas obras, uma vez que a criação não foi feita por um humano, mas por um algoritmo.

O sistema de IA DABUS (Device for the Autonomous Bootstrapping of Unified Sentience), criado por Stephen Thaler, gerou invenções como uma lanterna intermitente e um recipiente de alimentos em geometria fractal. Thaler tentou patentear essas criações em nome da IA, mas os pedidos foram negados por escritórios de patentes, como o USPTO (United States Patent and Trademark Office) e o EPO (European Patent Office), com base na legislação atual que não reconhece a IA como inventora[59].

Estes exemplos mostram que o direito de PI tem de considerar como classificar criações geradas autonomamente por IA, especialmente em termos de autoria e titularidade dos direitos sobre tais inovações.

4.2. Casos concretos e precedentes legais

O caso do sistema DABUS mostra como a questão da propriedade intelectual no contexto de IA está a ser enfrentada nos tribunais e instituições de patentes. Em 2019, Stephen Thaler efetuou pedidos de patentes para duas

[56] RYAN ABBOTT, «Artificial Intelligence, Big Data, and Intellectual Property: Protecting Creativity in the Age of Machine Learning», *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. 29, n.º 3, 2019, pp. 1087-1101.

[57] Ver https://www.aiva.ai/

[58] Os detentores dos direitos de exploração do AIVA reconhecem, contratualmente, aos utilizadores que iniciam a geração do produto de inteligência artificial (definindo parâmetros como compasso, ritmo, tom, estilo, duração) os direitos de exploração comercial da obra.

[59] USPTO, Decisão sobre o caso DABUS, 2020.

invenções criadas pelo DABUS, argumentando que a IA era a legítima inventora, já que o sistema agiu de forma autónoma sem qualquer intervenção humana. Esse argumento foi rejeitado tanto pelo USPTO como pelo EPO, que afirmaram que, de acordo com as legislações de PI, um inventor terá de ser uma pessoa física e não uma entidade artificial[60].

Outro caso relevante é o uso de IA para criar obras de arte. Um exemplo notável é o retrato "Edmond de Belamy", criado por IA treinada pela Obvious Art, uma entidade francesa que utiliza IA para criar arte. A obra foi vendida por cerca de 432 mil dólares num leilão da Christie's. Embora a IA tenha gerado a obra, os criadores do algoritmo foram reconhecidos como autores, levantando a questão do crédito que a IA merece em relação ao trabalho humano envolvido[61].

Estes casos demonstram que, embora a tecnologia tenha avançado rapidamente, a jurisprudência internacional ainda está a tentar acompanhar e estabelecer precedentes legais para lidar com criações resultantes da IA. Muitos sistemas de PI em todo o mundo assumem que a criatividade e inovação são habilidades exclusivas dos seres humanos, o que cria um conflito quando as máquinas possuem capacidades criativas semelhantes.

4.3. Adaptação das leis de propriedade intelectual

Muitos juristas e tecnólogos têm sugerido adaptações nas legislações de PI para lidar com as criações autónomas geradas por IA. Entre as propostas mais discutidas está a ideia de que o desenvolvedor da IA ou o proprietário do sistema seja considerado o titular dos direitos de PI sobre as criações, visto que investiram em recursos e no desenvolvimento do sistema de IA. No entanto, isso pode gerar desequilíbrios no mercado, especialmente quando grandes corporações se apropriarem das criações de IA sem reconhecer o papel dos criadores originais dos algoritmos[62].

Outro modelo sugerido envolve a criação de uma nova categoria de direitos de PI para obras criadas por sistemas autónomos. Tal categoria poderia considerar as características únicas das criações geradas por IA e a falta de envolvimento humano direto. Contudo, esse modelo ainda enfrenta desafios na implementação, especialmente porque a maioria dos sistemas legais de PI está profundamente enraizada no reconhecimento da autoria humana.

---

[60] EPO, Decisão sobre o caso DABUS, 2020.

[61] DANIEL MCCARTHY, «AI and the Copyright Dilemma», *Journal of Law and Technology*, vol. 15, n.º 2, 2019, pp. 53-65.

[62] PEDRO MARTINEZ e MARIA GARCIA, «Intellectual Property Rights and Artificial Intelligence: A Comparative Study», *European Intellectual Property Review*, vol. 42, n.º 1, 2020, pp. 85-95.

No entanto, a ideia de conceder direitos de PI diretamente a máquinas também foi sugerida. Alguns argumentam que, se um sistema de IA é capaz de gerar inovações e criações de forma independente, o mesmo deve ser considerado como uma entidade jurídica, similar às corporações, com direitos e obrigações legais próprios. Essa abordagem, no entanto, levanta questões éticas e jurídicas complexas, como a responsabilidade da IA pelas suas criações e o papel dos humanos que a desenvolveram[63].

Dado o impacto significativo que a IA já está a causar nas indústrias criativas e inovadoras, é claro que as leis de PI terão de evoluir para refletir as mudanças tecnológicas. Juristas e legisladores terão de trabalhar para encontrar soluções que possam proteger as inovações humanas e, ao mesmo tempo, reconhecer as novas capacidades criativas das máquinas.

5. Ética na tomada de decisões por IA

A crescente adoção de IA em setores críticos, como saúde, finanças e direito, apresenta complexas questões éticas. Apesar de potencialmente melhorar eficiência e precisão, a IA pode amplificar viés e falta de transparência nas decisões. Este capítulo explora esses desafios, destacando o viés algorítmico, a necessidade de transparência e explicabilidade e as implicações éticas da tomada de decisões automatizadas.

5.1. Viés algorítmico e preconceito nos dados

Os sistemas de IA tomam decisões baseadas em dados históricos que frequentemente contêm preconceitos sociais, económicos e culturais. Ao utilizar esses dados enviesados, os algoritmos podem perpetuar e amplificar desigualdades, gerando discriminação algorítmica. Um exemplo é o sistema COMPAS, usado em tribunais dos EUA, que mostrou viés racial ao atribuir pontuações de reincidência mais altas a réus negros em comparação com réus brancos com históricos semelhantes[64]. Esse fenómeno levanta preocupações éticas sobre justiça e imparcialidade nas decisões tomadas por IA.

Esses exemplos mostram como a falta de diversidade nos dados pode ter consequências graves para as minorias e outros grupos historicamente marginalizados, exacerbando as desigualdades sociais.

---

[63] MARGARET BODEN, *Artificial Intelligence: A Very Short Introduction*, 2.ª ed., Oxford, Oxford University Press, 2020.

[64] JULIA ANGWIN et al., «Machine Bias», *ProPublica*, 2016, disponível em https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [consultado em 09/09/2024].

5.2. Transparência e explicabilidade em algoritmos

Uma das principais críticas aos sistemas de IA, especialmente aos que utilizam redes neuronais profundas, é a falta de transparência, funcionando como "caixas-negras". Essa opacidade levanta questões éticas, pois decisões de IA podem afetar vidas sem que as pessoas entendam como foram tomadas. A transparência é crucial em áreas como crédito, justiça e saúde. Especialistas defendem que esses sistemas devem ser auditáveis, permitindo que reguladores e interessados compreendam suas lógicas de decisão[65].

Diversas propostas de regulamentação foram discutidas para abordar essas questões. Por exemplo, o RGPD da UE inclui disposições sobre direito à explicação, permitindo que indivíduos afetados por decisões automatizadas questionem os critérios usados pelos algoritmos. No entanto, a aplicação prática desse direito ainda é um desafio, especialmente quando se trata de algoritmos altamente complexos[66].

A explicabilidade é uma área de pesquisa significativa no campo da IA, com o desenvolvimento de técnicas como a Interpretação Localmente Agregada de Modelos Explicáveis (LIME) para explicar as decisões de sistemas de IA de modo compreensível humanamente[67]. No entanto, ainda há muito a ser feito para tornar essas explicações acessíveis e compreensíveis para o público em geral.

5.3. Questões éticas e tomada de decisões automatizadas

A tomada de decisões automatizadas por IA levanta dilemas éticos sobre responsabilidade e autonomia, especialmente na saúde. Embora a IA possa melhorar diagnósticos, surgem questões sobre quem é responsável por erros, como o médico que segue a recomendação da IA ou o desenvolvedor do software. Isso cria desafios jurídicos e éticos complexos[68].

O uso de IA no sistema judicial para prever reincidência ou tomar decisões judiciais levanta questões sobre equidade e imparcialidade. Embora algoritmos possam identificar padrões em decisões passadas, eles não conseguem capturar os aspetos humanos e contextuais que um juiz considera. Isso pode

---

[65] RUTH C. WYLIE, «Opening the Black Box: Transparency in Artificial Intelligence», *AI Ethics Journal*, 2020, pp. 45-52.

[66] Artigo 22.º do RGPD.

[67] MARCO TULIO RIBEIRO et al., «"Why Should I Trust You?": Explaining the Predictions of Any Classifier», *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016, pp. 1135-1144.

[68] ELIZABETH ADAMS, «Artificial Intelligence in Medicine: Ethical Considerations and Patient Safety», *Journal of Medical Ethics*, 2020, pp. 567-570.

desumanizar o processo, resultando em decisões frias e calculistas que ignoram as nuances de cada caso[69].

Por tal, é necessária uma supervisão humana contínua e robusta no uso de IA em áreas críticas. Enquanto a automação pode trazer inúmeros benefícios em termos de eficiência e precisão, também pode comprometer os princípios éticos fundamentais de justiça, autonomia e responsabilidade se não for adequadamente regulamentada e monitorada.

6. Segurança cibernética e infraestruturas críticas

O avanço da Indústria 4.0, a integração de tecnologias digitais como IoT, IA e Big Data têm aumentado significativamente os riscos cibernéticos. Essa interconectividade, embora essencial para a eficiência e inovação, expõe as infraestruturas críticas a ciberataques cada vez mais sofisticados. Este capítulo aborda os desafios de segurança cibernética enfrentados pela Indústria 4.0, a necessidade de regulação e a importância da cooperação internacional para mitigar ameaças cibernéticas.

6.1. A interconectividade da Indústria 4.0 e os riscos cibernéticos

A interconectividade na Indústria 4.0, envolvendo dispositivos IoT e algoritmos de IA, traz grandes benefícios, mas também expõe vulnerabilidades cibernéticas, pois cada dispositivo conectado pode ser um alvo para ataques. Exemplos notáveis incluem o Stuxnet em 2010, que comprometeu o controle de uma usina nuclear no Irã, e o WannaCry em 2017, que afetou hospitais e serviços públicos, evidenciando a fragilidade dos sistemas interconectados[70].

A conectividade constante, combinada com a complexidade crescente dos sistemas da Indústria 4.0, dificulta a deteção de ataques cibernéticos e a contenção de danos. Hackers podem explorar falhas de segurança em dispositivos IoT, que muitas vezes não são suficientemente protegidos, para lançar ataques coordenados contra infraestruturas críticas, como redes elétricas, sistemas de transporte e instalações de produção automatizada. A falta de padrões de segurança consistentes para dispositivos IoT agrava ainda mais este problema.

---

[69] CATHY O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Nova York, Crown Publishing Group, 2016.

[70] ANDY GREENBERG, «The WannaCry Ransomware Attack Has a Link to North Korea», *Wired*, 2017, disponível em https://www.wired.com/story/wannacry-north-korea-ransomware/ [consultado em 03/09/2024].

6.2. Necessidade de regulação para a segurança cibernética

A rápida evolução da tecnologia e da interconectividade não tem sido acompanhada por uma regulamentação adequada em segurança cibernética. A falta de padrões internacionais para proteger sistemas IoT e IA aumenta a vulnerabilidade a ataques, especialmente em infraestruturas críticas. Atualmente, o quadro regulatório é fragmentado; por exemplo, nos EUA, a Lei de Melhoria de Segurança Cibernética foca em setores essenciais, enquanto, na UE, o Regulamento de Segurança Cibernética procura estabelecer certificações, mas ainda enfrenta limitações na sua eficácia e abrangência[71].

Além disso, a implementação de regulamentos específicos para IA ainda está a inicializar. A IA desempenha um papel importante na automação e na gestão de infraestruturas críticas, mas, ao mesmo tempo, pode ser alvo de ciberataques que comprometam a integridade dos dados utilizados no treino e a confiabilidade das decisões automatizadas. A ausência de um quadro regulatório coerente que abarque tanto a IA quanto a IoT requer urgência de novos modelos regulatórios que protejam esses sistemas complexos de ciberameaças[72].

Propostas para novas regulamentações sugerem que dispositivos IoT e sistemas de IA devem ser projetados com segurança incorporada desde a conceção ("security by design"). Tal incluiria a implementação de padrões de criptografia, atualizações automáticas de segurança e avaliações periódicas de vulnerabilidades. Além disso, a introdução de sanções rigorosas para empresas que não cumprem com os padrões mínimos de segurança cibernética poderia incentivar uma melhor proteção das infraestruturas críticas[73].

6.3. Cooperação internacional para combater ciberameaças

A natureza global dos ciberataques exige uma resposta internacional, já que esses crimes frequentemente cruzam fronteiras. Para uma segurança cibernética eficaz, é essencial a cooperação em compartilhamento de informações, resposta a incidentes e harmonização de regulamentações. Organizações como Interpol e Europol coordenam esforços contra crimes cibernéticos, facilitando

[71] Regulamento de Segurança Cibernética da União Europeia (Cybersecurity Act), 2019, disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881 [consultado em 03/09/2024].

[72] AMIR RAHIMI, «AI in Critical Infrastructure: Security Challenges and Policy Implications», *Journal of Cybersecurity and Privacy*, 2020, pp. 33-41.

[73] BRUCE SCHNEIER, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, Nova York, Norton, 2018.

investigações conjuntas. Um exemplo de sucesso foi a Operação Tovar, que desmantelou a botnet Gameover Zeus com a colaboração de mais de 10 países[74].

A Convenção de Budapeste sobre Crimes Cibernéticos é um dos principais tratados internacionais que visa promover a cooperação jurídica entre nações no combate aos crimes cibernéticos. No entanto, muitos especialistas argumentam que a mesma tem de ser atualizada para lidar com as novas ameaças advindas da Indústria 4.0 e tecnologias emergentes, como IoT e IA[75].

Modelos de regulamentação global começam a surgir. A Iniciativa Global para a Estabilidade Cibernética, liderada pelo Fórum Económico Mundial, visa criar um nível de colaboração entre governos, empresas e organizações para desenvolver um conjunto de normas globais de segurança cibernética. A introdução de padrões internacionais comuns pode ajudar a garantir que infraestruturas críticas em diferentes países sejam protegidas contra as ameaças mais recentes[76].

7. Conclusão

A Indústria 4.0 e a crescente utilização da IA têm transformado radicalmente setores como a manufatura, logística, saúde e transportes, enquanto introduzem uma série de desafios jurídicos e regulatórios. A adoção de tecnologias disruptivas, como Big Data, IoT e automação avançada, obriga a um esforço contínuo por parte dos governos, organizações internacionais e entidades privadas para garantir que o desenvolvimento tecnológico não comprometa direitos fundamentais e a segurança.

Os principais desafios incluem a necessidade urgente de regulamentação em proteção de dados e privacidade. O RGPD da UE, a LGPD do Brasil e o CCPA representam tentativas significativas, mas enfrentam limitações na Indústria 4.0, onde a recolha de dados é contínua e muitas vezes invisível. Questões como consentimento informado, transparência nos algoritmos e responsabilização dos processadores de dados continuam a desafiar o sistema jurídico.

Outro ponto crítico é a responsabilidade civil e penal em casos que envolvem a IA. A dificuldade em atribuir responsabilidade por acidentes causados por sistemas autónomos, como veículos autónomos, levanta preocupações sobre a responsabilidade objetiva e subjetiva. Modelos de responsabilidade para IA,

---

[74] DAVID GLENNY, «How the Global Effort to Stop Gameover Zeus Malware Worked», *BBC News*, 2014, disponível em https://www.bbc.com/news/technology-27617090 [consultado em 06/09/2024].

[75] Convenção de Budapeste sobre Crimes Cibernéticos, 2001, disponível em https://www.coe.int/en/web/cybercrime/the-budapest-convention [consultado em 06/09/2024].

[76] World Economic Forum, «Global Initiative on Cybersecurity Stability», 2020, disponível em https://www.weforum.org/reports/global-cybersecurity-initiative [consultado em 06/09/2024].

incluindo os papéis de fabricantes, programadores e utilizadores, ainda estão em fase de estudo em muitas jurisdições. Este campo exigirá uma atenção especial, à medida que as tecnologias autónomas prevalecem, gerando a necessidade de novas interpretações jurídicas.

A IA levanta desafios na propriedade intelectual, especialmente sobre quem detém os direitos de obras criadas por sistemas autónomos, como o programador, o proprietário ou a própria IA. O caso do DABUS destaca a inadequação das legislações atuais para tratar invenções geradas por IA. Portanto, é essencial criar legislações adaptativas que assegurem a proteção dos direitos de propriedade intelectual e a integridade dessas criações.

A automação gera desafios económicos e sociais, destacando o desemprego tecnológico, que afeta setores como manufatura e serviços. É crucial desenvolver políticas públicas para requalificar trabalhadores e promover a colaboração entre governos e empresas, visando preparar a força de trabalho para as novas demandas digitais e implementar políticas de transição justa para minimizar os impactos negativos da automação.

A segurança cibernética é vital na Indústria 4.0 devido à interconectividade entre sistemas e dispositivos, que aumenta as vulnerabilidades. Ataques a infraestruturas críticas, como redes elétricas e de transporte, podem causar graves consequências. Portanto, é essencial criar um quadro regulatório internacional e cooperativo para garantir a segurança, promovendo a colaboração entre países e organizações na resposta a ameaças cibernéticas que, frequentemente, transcendem fronteiras.

Perante tais desafios, os sistemas jurídicos devem evoluir para se adaptar ao rápido avanço das tecnologias. É fundamental um marco regulatório adaptável, capaz de acompanhar as inovações tecnológicas sem sufocar o desenvolvimento. Isso significa criar leis flexíveis e dinâmicas para se ajustar rapidamente a novas descobertas e aplicações. Ao mesmo tempo, essas leis devem garantir a proteção de direitos individuais e sociais, como o direito à privacidade e segurança.

Um dos maiores desafios enfrentados pelos legisladores é encontrar o equilíbrio entre permitir a inovação tecnológica e garantir a proteção dos direitos fundamentais. A transparência e a explicabilidade nos sistemas de IA são questões centrais nesse equilíbrio. Modelos de IA que tomam decisões em áreas como saúde e justiça devem ser auditáveis e passíveis de revisão, para que as pessoas afetadas por essas decisões possam entender as mesmas. Propostas de regulamentação que visam tornar os algoritmos mais transparentes são essenciais para garantir a confiança nas tecnologias emergentes.

O futuro do direito na era da Indústria 4.0 e da IA exige uma necessidade de uma harmonização internacional de normas e regulações. À medida que

as tecnologias ultrapassam fronteiras, os marcos regulatórios nacionais podem ser insuficientes. Por isso, organismos internacionais, como as Nações Unidas e a Organização Mundial do Comércio (OMC), terão um papel fundamental na coordenação de esforços para criar normas globais que regulem a IA, a segurança cibernética e a proteção de dados.

Além disso, o direito terá de se adaptar às inovações tecnológicas de maneira cada vez mais rápida. Em vez de reagir aos avanços tecnológicos, os legisladores devem antecipar tendências e desenvolver políticas preditivas que assegurem que os benefícios da Indústria 4.0 sejam maximizados e os riscos minimizados.

Em última análise, o sucesso de qualquer sistema regulatório dependerá da sua capacidade de equilibrar a proteção dos direitos fundamentais com a promoção da inovação. A Indústria 4.0 tem o potencial de transformar sociedades inteiras, mas tal transformação só será positiva se acompanhada por marcos regulatórios sólidos, éticos e inclusivos.

SIDE EFFECTS OF THE (DIS)ARTICULATION BETWEEN THE DATA GOVERNANCE ACT AND THE GENERAL DATA PROTECTION REGULATION IN CLINICAL RESEARCH: CONSENT IS (NOT) THE ONLY APPLICABLE LEGAL BASIS

Yuri R. Ladeia[*]

Abstract: The re-use of representative health data endlessly generated in the European Union (EU) constitutes an opportunity and a need for clinical research. This is part of the European Data Strategy, which aims to foster the altruistic co-sharing of data, and which is regulated by the Data Governance Act (DGA). Due to DGA conflicts with the legal framework on the protection of personal data, particularly the General Data Protection Regulation (GDPR), according to the present perspective, it is pointed out that the wording of the DGA has led to disarticulation. It has resulted in a lack of predictability for the altruism mechanism and data reuse ecosystem, contrary to the trust environment it was designed to promote. It is demonstrated how the European legislator has led to a pseudo-overlap between the DGA and the GDPR due to a veiled prioritisation

* Law Researcher, Centre of Justice and Governance (JusGov), School of Law, University of Minho. Braga, Portugal. Lawyer. E-mail: *rodrigueslaw@outlook.pt*

of consent as a legal basis, shaped by an unhealthy intersection. Approaching this situation as a sick legal framework, this paper offers a guiding thread inspired by the clinical journey of a patient. First of all, providing a diagnosis, followed by therapeutic proposals for acute and chronic legal symptoms, and outlining. Lastly, it provides a follow-up, important to all the direct and indirect stakeholders in the biomedical innovation ecosystem, working towards the promotion of legal certainty.

Keywords: General Data Protection Regulation (GDPR); Data Governance Act (DGA); Clinical research.

Resumo: A reutilização de dados de saúde representativos, gerados incessantemente na União Europeia (UE), constitui uma oportunidade e uma necessidade para o ecossistema da investigação clínica. Isto faz parte da Estratégia Europeia para os Dados, que visa promover a partilha altruísta de dados, que é regulada pelo Regulamento Europeu sobre a Governação de Dados (RGD). Devido aos conflitos do RGD com o regime jurídico relativo à proteção de dados pessoais, sobretudo o Regulamento Geral sobre a Proteção de Dados (RGPD), perspetiva-se que a redação do DGA induziu à desarticulação. Tem resultado em incertezas para o mecanismo de altruísmo e para o próprio ecossistema de reutilização de dados, contrariamente ao ambiente de confiança para o qual foi concebido. Aponta-se como o legislador Europeu provocou uma situação de pseudosobreposição entre o DGA e o RGPD, decorrente de uma hierarquização velada, priorizando o consentimento como fundamento legítimo para o tratamento de dados, enformado por uma intersecção malsã. Analisando-se esta situação jurídica enferma, propõe-se um fio condutor inspirado no percurso clínico de um paciente. Em primeiro lugar, apresenta-se um diagnóstico, seguido de propostas terapêuticas para os sintomas jurídicos agudos e crónicos. Por fim, apresenta-se um prognóstico, importante para todos os intervenientes diretos e indiretos no ecossistema da inovação biomédica, no intuito de promover a segurança jurídica face ao diagnóstico de incertezas.

Palavras-chave: Regulamento Geral sobre a Proteção de Dados (RGPD); Regulamento Europeu sobre a Governação de Dados (RGD); Investigação clínica.

1. Diagnostics

Biomedical innovation, particularly clinical research, depends on the use and (re)use of personal data relating to the health of data subjects.[1] An increasing amount of data is required, which must be high-quality and accessible.[2]

With the emergence of artificial intelligence (AI) applied to healthcare, the urgent need for high availability of data to compose databases that support the training of algorithms for, for example, AI software as a medical device, has become even more critical. The quality and availability of the training data means that the device will be more or less reliable.

An exemplary case highlights this situation, regarding the use of AI to support diagnosis and clinical decision-making through medical images. The AI trained with an insufficient database (inputs) – poor diversification of medical images in terms of ethnicity and skin shades – led to outlying inaccuracies and biases when applying it to non-representative use cases in the database.[3] This reflects the fact that the high availability of data is the backbone that supports the evolution of clinical activity and innovation in healthcare.[4]

In fact, the representative availability of data is the solution to fostering biomedical innovation.[5] However, the challenge is to collect such data on a large scale and with high quality – accuracy and integrity. Part of this is the difficulty of reconciling obtaining this data with the strict requirements of the European Union's (EU) highly regulated data recycling and protection ecosystem. At the heart of this challenge is the lawfulness of the collection and the surrounding legal controversies.

The paper focuses on this part of the puzzle, in order to address some remedies for acute legal symptoms and propose approaches for chronic legal symptoms in this domain, which is limited to the health sector. This is also a

[1] TEODORA LALOVA-SPINKS, JANOS MESZAROS and ISABELLE HUYS, «The Application of Data Altruism in Clinical Research through Empirical and Legal Analysis Lenses», *Frontiers in Medicine*, Vol. 10, 2023, pp. 1-2 (pp. 1-14).

[2] LUDOVICA PASERI, «The Ethical and Legal Challenges of Data Altruism for the Scientific Research Sector», in Jorge Pelegrín Borondo (coord.), *The Leading Role of Smart Ethics in the Digital World*, Universidad de La Rioja, ETHICOMP Book Series, 2024, p. 189 (pp. 189-200).

[3] LOUIS KAMULEGEYA and others, «Using Artificial Intelligence on Dermatology Conditions in Uganda: A Case for Diversity in Training Data Sets for Machine Learning», *African Health Sciences*, Vol. 23, 2023, p. 753 (pp. 753-763).

[4] RUI GUIMARÃES and others, «Medical Student Secrecy, Its Link to the Duty of Confidentiality and the Right to Access and Reuse Health Information», *Acta Médica Portuguesa*, Vol. 32, 2019, p. 11 (pp. 11-13).

[5] LOUIS KAMULEGEYA and others, «Using Artificial Intelligence on Dermatology Conditions in Uganda…», *op. cit*.

necessity concerning the development of clinical studies – such as trials – for the safe development of new devices and medicines, as well as for epidemiological research.

Once the availability of representative data is an indispensable pre-condition for the empirical improvement of healthcare processes, services and technology, the approach suggested in this paper may be useful to all stakeholders in the ecosystem – promoters such as the pharmaceutical industry, trials sites such as university hospitals, clinical research organisations such as funding agencies, clinical research centres, software manufacturers (software as medical devices, artificial intelligence as medical devices) – and other direct and indirect stakeholders.

Medical data for secondary use in research is not only produced in hospitals and medical practices. Rather, health services are also provided to a large extent by non-medical professions: from psychologists and pharmacists to nursing services. In addition, health insurance organisations and private insurance companies store health-related data. Last but not least, people are increasingly generating representative data for the health ecosystem through self-collection by wearable devices. The accelerated dissemination of health-related structured data in digital formats represents both a challenge and an opportunity for clinical research. It undoubtedly constitutes the opportunity to extract a significant depth and breadth of knowledge from the data, increasingly towards new diagnostic and therapeutic possibilities, i.e. biomedical innovation.[6]

Recognising that the processing of health-related information is an unavoidable necessity, a strict balance is required with the individual's fundamental right to privacy and the protection of their personal data, highlighting the need for harmonisation with Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR).

In light of this atmosphere of opportunities at scale fostered by data – due to its unlimited nature, notably in terms of re-use – in addition to the European data governance legal landscape – Regulation (EU) 2022/868 of the European Parliament and the Council of 30 May 2022, on European data governance and amending Regulation (EU) 2018/1724 – commonly referred as the Data Governance Act (DGA) came into force on 23 September 2023.

The DGA introduced the so-called data altruism mechanism. Data altruism is a data governance concept. According to the French Data Protection

[6] PHIL DANIEL STRECH and others, «„Datenspende" – Bedarf Für Die Forschung, Ethische Bewertung, Rechtliche,Informationstechnologische Und Organisatorische Rahmenbedingungen», 2020, p. 9 (pp. 1–141). Available at https://www.bundesgesundheitsministerium.de/service/publikationen/details/datenspende-bedarf-fuer-die-forschung-ethische-bewertung-rechtliche-informationstechnologische-und-organisatorische-rahmenbedingungen.html

Authority (CNIL)[7], the concept consists of encouraging relevant parties (organisations, individuals, etc.) to share data which they consider to be useful for the general interest.[8] In the present paper, the discussion is limited to the scientific interest.

This mechanism takes the form of reinforcing the trust of the ecosystem – mainly data holders and data subjects – and the possibility for the data subject to voluntarily donate – to share – their personal data (including non-personal data, which is not explored in this paper) across EU borders. It includes health related data, providing it for non-commercial purposes[9] – such as scientific research – through organisations appointed for this end – such as healthcare organisations that hold the data, under Article 1, recitals 3 and 5 of the DGA.

As part of the European Data Strategy's regulatory package, this mechanism is intended to fulfil the need for high data availability, as defined in the DGA Article 2(16). This Regulation is in conjunction with the proposed regulatory framework for the European Health Data Space (EHDS)[10] which calls for altruism at the European level[11], as one more piece of the – increasingly granular and complex – puzzle of the EU data regulatory framework, by harmonising – not always smoothly – with the already in place legislation, notably the GDPR.

It is important to keep in mind that this paper is only concerned with the voluntary – altruistic – sharing of health-related personal data for the purposes of clinical research. Given this, it should be noted that the DGA mentions consent recurrently – 48 times – hinting – on some of these occasions – as the basis on which data collection for personal data altruism should be based, by data altruism organisations.

This is the case with Article 25 of the DGA, which provides for the standardisation of a European consent form for this purpose. This legal basis is embedded in the DGA, bordering on imposition, which would be the case if it weren't

[7] National Commission on Informatics and Liberty (CNIL).

[8] National Commission on Informatics and Liberty (CNIL), «European Strategy for Data: The CNIL and Its Counterparts Comment on the Data Governance Act and the Data Act», available at https://www.cnil.fr/en/european-strategy-data-cnil-and-its-counterparts-comment-data-governance-act-and-data-act [accessed 30 September 2024].

[9] CORINA KRUESZ and FELIX ZOPF, «European Union – The Concept of Data Altruism of the Draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU», *European Data Protection Law Review*, Vol. 7, 2021, p. 569 (pp. 569-579).

[10] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space.

[11] ELISABETE CASTELA and TIAGO BRANCO DA COSTA, «A Investigação Clínica na Era do Altruísmo dos Dados: Algumas Considerações em Torno da Proteção de Dados Pessoais», *Anuário da Proteção de Dados*, Ano 5, 2023, pp. 282, 251 (pp. 249-282), available at https://protecaodedadosue.cedis.fd.unl.pt/edicao-edition-2023/.

for certain elements that detract from this rationale, like a kind of exemption. A kind of exception to the rule.

Assuming consent is the general rule, it seems that the legislator of the DGA intends to ensure that data subjects can give and withdraw their consent to specific data processing operations, per the GDPR's requirements for lawful consent. In other words, according to the conjunction of Article 6(1) and (2)(a) and Article 9, respectively, as well as Articles 7 and 8 of the GDPR. Notwithstanding compliance with the conditions for the legitimacy of consent as a legal basis, it seems that the – potential – conflict lies in the harmonisation between the DGA and the GDPR, in terms of privileging one legal basis over others.

From this interpretation, it could be assumed that consent was the legislator's pseudo-choice of legal basis – despite the absence of any precedence or priority of legal bases in the GDPR. Since there is no such priority and there is this imposition – by applying the *Lex Specialis Principle*[12]/[13]/[14]. The reason for this would be due to the GDPR being the most specific regulation, ranking first in speciality concerning the DGA, with regard to the protection of personal data.

This assumption would be true if it weren't for the provision in recital 50 of the DGA, which states consent is the default rule for data altruism purposes, implying that exceptions to the default rule exist. The hypothesis is reinforced when the same recital mentions that consent can – in a suggestive sense – be used for clinical research purposes. It is worth pointing out that the word must or similar was not used – implying a quasi-imposition – a highly strong insinuation – which does not constitute a manifest imposition.

Furthermore, according to Recital 4 of the DGA, it applies without prejudice to the GDPR. It should not be interpreted as creating a new legal basis within the framework of any regulated activity.

For example, this paper refers to clinical research as the use case. Although no new grounds are created in the DGA and the same recital refers to the prevalence of EU law in matters of data protection – apparently following the *Lex*

[12] This paper refers to *lex specialis* based on two reasons why the *lex specialis* rule is so widely accepted. A special rule is more to the point ("approaches more nearly to the subject in hand") than a general one and it regulates the matter more effectively ("are ordinarily more effective") than general rules do. This could also be expressed by saying that special rules can better account for particular circumstances.

[13] When norms of Union law overlap – meaning more than one could apply – what principles determine the relationship between them? This paper argues the use of the *lex specialis* principle. This paper proposes GDPR in prejudice of DGA, based on a speciality rank approach.

[14] EMILY HANCOX, «Judicial Approaches to Norm Overlaps in EU Law: A Case Study on the Free Movement of Workers», *Common Market Law Review*, Vol. 58, 2021, p. 1057 (pp. 1057-1096).

Specialis Principle (*lex specialis derogat legi generali*)[15] – the binding wording of the text – articles – does not reflect the omnipresence of this principle throughout the legislation. Therefore, in the event of a conflict, it seems that there is still legal uncertainty as to whether or not consent is imposed over other legal bases.[16]

This paper unfolds against this backdrop, considering this particular practical premise. Although consent is widely used by default as a legal basis for processing data, because it provides greater control to data subjects, its application in practice can be limited by both logistical and procedural issues.[17] This is especially true when data is collected on a large scale and from multiple sources in clinical research, due to the complexity of collecting it both retroactively and individually, while still ensuring compliance with the validity criteria set out in Article 7 of the GDPR. Among the criteria is the withdrawal of consent, which can jeopardise the redundancy of a database and the research itself in a logic of continuous and prospective collection, after withdrawal of consent, despite not jeopardising the lawfulness of the processing carried out based on the consent previously given, according to paragraph 3 of Article 7 of the GDPR.

There is also some controversy regarding the limitation of the right to the erasure of data by the data subject who withdraws consent in the context of altruism for scientific research. This is due to the provision in Article 17(3)(d) of the GDPR, which suggests that the legal basis for research could not be consent solely, by stating that the right to erasure of data is suppressed – if it is impossible or seriously jeopardises the achievement of the research objectives. Actually, the legal basis is indirectly framed as that provided for in Article 9(2)(h) of the GDPR – scientific research.

In the light of these controversies, due to space constraints and the scope of the paper, from the perspective of the principle of lawfulness laid down in Article 5(1)(a) of the GDPR, the aim has been to examine and address the following fundamental questions:

1) Should be specific or could it be broad enough to meet the aims of re-use for purposes undetermined at the time of collection? Would dy-

[15] *Ibid.*

[16] PATRÍCIA CARNEIRO, «Regulamento Geral sobre a Proteção de Dados e o Mercado de Dados – Mercado de Dados 1.0 e a Licitude da Partilha de Dados (Pessoais) através de Serviços de Intermediação de Dados no Âmbito do Regulamento de Governação de Dados, por via do Consentimento do Titular dos Dados – Uma Imposição de Base Legal?», *Anuário da Proteção de Dados*, Vol. 6, 2023, pp. 145, 171 (pp. 145-178).

[17] BART W. SCHERMER, BART CUSTERS, and SIMONE VAN DER HOF, «The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection», *Ethics and Information Technology*, Vol. 16, 2014, p. 171 (pp. 171-182).

namic consent be the balance between the paternalism of supervisory authorities and informational self-determination?

2) Is the data subject's consent, provided for in Article 9(2)(a) of the GDPR, the only valid legal basis for donating data for data altruism in clinical research? Can other legal bases be combined? If so, is it possible to collect the data based on consent and deny the right to erasure based on clinical research purposes?
3) Is the DGA legislator establishing a priority of legal bases that do not co-exist with the GDPR?

Finally, a diagnosis was made as to whether or not there is an interception or overlap between the DGA and the GDPR in terms of legal bases. It also considered whether the level of protection of the rights and freedoms of data subjects and the legal certainty of altruistic organisations in the field of clinical research is being jeopardised, in contrast to the aims of the European Data Strategy, which gave rise to the DGA.

Strategies were suggested for addressing acute legal symptoms in the immediate term – important for the biomedical innovation ecosystem to apply on a day-to-day basis, precisely because innovation does not wait for the law. Strategies for treating chronic legal symptoms were also outlined for the future – relevant for the EU regulator and the wider regulatory and political spectrum at the EU and member state level.

Interpreting the situation addressed in this paper as a legal-regulatory health problem[18], the thread that runs through it is inspired by the clinical path of a patient[19], in terms of the organisation of the section structure. The same is reflected in the strategies suggested – which were the result of reflection mainly from an EU and EU law perspective. Is not considered the specificities of the related national legislation of the member states. The focus is on the (in)existing (dis)articulation between the DGA and the GDPR, and the (un)virtuous wording of part of the DGA, as follows.

2. Analyses and treatment

Enshrined in international treaties, the right to privacy is set out in Article 8 of the European Convention on Human Rights (ECHR), which has been in force since 1953. It is also embodied in the European Union's (EU) Data Protection framework, mainly through the GDPR, which concretises this right under

[18] Semantic analogy that affects the author's writing style, with no official conceptual relationship.

[19] In this paper, the patient is the DGA in terms of legal basis for data altruism.

Article 8 of the Charter of Fundamental Rights of the European Union (CFR), promulgated on 7 December 2000.

In addition to being provided for in the main specific cornerstones of the discipline, data protection is referred to cross-cuttingly in other regulations relating to clinical research at the EU level. A non-exhaustive example is Article 56 in conjunction with Article 3(b) of Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, commonly referred to as the Clinical Trials Regulation (CTR).[20] The DGA is also an example, in recital 50, among other provisions.

In fact, the cross-cutting nature of the GDPR, as a fundamental rights regulation of an agnostic and technically neutral nature, requires its material application in conjunction with other specific regulations and laws at the intersectoral level, as can be seen from the reading of Article 2 of the GDPR, regarding the material scope.

Given the almost omnipresence of the GDPR in terms of data protection, all lawful data processing depends on the correct and adequate application of a legal basis. The legal bases are set out in Articles 6 – for non-sensitive data of special categories – and 9 of the GDPR – for sensitive data of a special category. Since the subject of this paper concerns genetic data and other health-related data, i.e. data falling into the group of 'special categories of personal data', it must be combined with the catalogue of legal bases in Article 9(2) of the GDPR.

A) Acute symptom treatment: operationalising consent

As mentioned above, the general rule of the legal basis chosen by the DGA for the altruism mechanism is consent, provided for in Article 9(2)(a) of the GDPR, as suggested in recital 50 of the DGA. The GDPR determines that consent must refer to a specific purpose, according to Article 4(11), in conjunction with Articles 6(1)(a), 5(1)(b) of the GDPR. Reinforcing this component element of consent, Article 8(2) of the EU Charter of Fundamental Rights also mentions specific purposes for data processing.

Part of the doctrine interprets the principle of purpose limitation as a way of materialising the expression 'prevention is better than cure' and avoiding the indiscriminate collection of data under the pretext that 'you never know when it will be useful'.[21] Under this perspective, purpose limitation is the opposite of

[20] European Commission Directorate-General for Health and Food Safety, «Question and Answers on the Interplay between the Clinical Trials Regulation and the General Data Protection Regulation», available at https://health.ec.europa.eu/document/download/c3042973-b36d-4094-a1fb-a6fc980f065e_en [accessed 27 September 2024], pp. 1–2.

[21] MEREL ELIZE KONING, *The Purpose and Limitations of Purpose Limitation*, Utrech, Radboud University Nijmegen, 2020, p. 58 (pp. 1–280).

processing data for undetermined purposes at the time of collection. In the context of clinical research and a logic of re-use for the European data strategy, this perspective would not be the most favourable.

The purpose limitation principle imposes two conditions on the data controller. First, the principle demands prior transparency of intentions, stating the objectives. Secondly, it binds the data controller to self-predetermined conditions, restricting the use of personal data for the specified purpose. Consequently, it is possible to deduce two requirements: the specification of the purpose and the non-compatibility requirement.[22]

So, are the specific purpose and non-compatibility the cornerstones for interpreting the boundaries governing the purpose limitation principle laid down in Article 5(1)(b) of the GDPR for data altruism?

If so, this is a prerequisite for the validity of the establishment of the data subject's expression of will, respecting their informational self-determination. This will must be specific, informed and unambiguous, according to recital 32 of the GDPR.[23] According to the same recital, 'silence, pre-validated options or omission should therefore not constitute consent'. This mention puts aside the idea of transposing the opt-out – presumed consent – logic to the data altruism mechanism, in analogy with organ donation.[24] This will be briefly discussed below, assuming it is convenient – once it would substantially increase the number of data available – but it is legally impossible.

Considering the multiple requirements for the legitimacy of consent, there are arguments against its use. It is argued that the use of other legal bases that do not require the data subject to express their will in fact constitutes 'silence' on the part of the data subject, which would no longer be a problem since consent would not be applied.

Considering that the GDPR does not prioritize the use of one legal basis over another, not applying consent would not be a concern, as long as there are alternatives to confer lawfulness on data processing. The viability of the legal bases is determined according to their applicability, advantages and disadvantages in the practical context. Consent therefore carries the same weight as other legal bases. If another basis can be used, all the requirements of consent are rendered void. If it is necessary to use consent at one stage – collection – and another legal

[22] *Ibid.*, pp. 57–58.

[23] PHIL DANIEL STRECH and others, «„Datenspende"…», *op. cit.*, p. 95.

[24] SHEILA M. BIRD and JOHN HARRIS, «Time to Move to Presumed Consent for Organ Donation», *BMJ*, Vol. 340, 2010 (pp. 1010-1012).

basis at a subsequent stage – reuse, these requirements apply within the limits of the stage to which it refers.[25]

Exploring alternative or complementary legal bases for consent will follow the demonstration of its (in)viability for altruistic purposes in clinical research, answering the first question. In cases where consent is applied, it will be argued whether it must be specific or could be broad, to meet the aims of reuse for undetermined purposes at the time of collection.

Assuming that it is often not possible to fully identify the purposes of processing personal data for scientific research at the time of data collection, Recital 33 of the GDPR moves towards broader consent. This direction can be recognised in the recital, when it states that 'consent can be given for certain areas – considering the broad concept of areas – of scientific research', making the concept of 'specific' broader.

Considering that several related studies can converge in one area – as all types of cancer care studies – the wording of the aforementioned recital maintains a certain limitation, because it presupposes a link to the general area, while at the same time presenting some openness, to the extent that several related – cancer care data recycling e.g. – studies may converge in one area. From this provision, it is believed that the GDPR legislator has left room for an interpretation that, for scientific research, the requirements for consent to be specific are met only by referring to the categories of purposes, without precisely specifying the species. The controversial possibility of the legitimacy of broad – semi-open – consent is therefore speculated.

Previously to analysing the – potential and not so subtle – preference of the DGA legislator in terms of legal bases and the – possible and dubious – conflict of EU regulations, there is an urgent need to explore the operational and legal viability of consent as a legal basis in the context of data altruism for clinical research.

Three directions are addressed, starting with the already mentioned traditional specific consent, followed by broad consent and finally dynamic consent, as a middle ground that balances the paternalism of the supervisory authorities and the principle of informational self-determination of the subjects, implied by the reading of Article 8 of the Charter of Fundamental Rights of the European Union.

[25] PAUL QUINN, «Research under the GDPR – a Level Playing Field for Public and Private Sector Research?», *Life Sciences, Society and Policy*, Vol. 17, 2021, p. 2 (pp. 2-33).

B) Acute legal symptom treatment: broad consent

In contrast to the strict conservative approach, broad consent is nothing new in the health innovation sector and is common practice in the field of biobanks[26], despite remarks by part of the German doctrine, which considers it a legally dubious practice. Against broad consent, it is considered that Recital 33 is not reflected in the operational part of the GDPR – articles – and would therefore be of little relevance.[27]

Recital 33 of the GDPR proposes a kind of area-based consent, which would apply to several studies in the same scientific area. If the conservative interpretation is applied in this case, then other studies in the same scientific area, but relating to different diseases – e.g. two cancer studies – Each one on a different type of cancer – which takes advantage of the same information, would be excluded from the lawfulness. In this case, the European Data Strategy's claim for altruism in scientific research would once again be jeopardised.

In favour of broad consent in medical research – importing the logic of sampling donors to biobanks – recital 33 of the GDPR is interpreted as meaning that the right to decide autonomously on the broadest use of data is a prerogative of informational self-determination, as a right and freedom.[28] In this direction, legislative paternalism is criticised, to fulfil the principle of the individual's informational self-determination.[29] It is advocated that informational self-determination is one of the fundamental pillars of European Union law, since it is linked to the logic underlying the fundamental right to the protection of personal data, as enshrined in Article 8 of the Charter of Fundamental Rights of the European Union, and can even be qualified as a fundamental right *per se*.[30]

---

[26] DARA HALLINAN and MICHAEL FRIEDEWALD, «Open Consent, Biobanking and Data Protection Law: Can Open Consent Be "Informed" under the Forthcoming Data Protection Regulation? », *Life Sciences, Society and Policy*, Vol. 11, 2015, pp. 1-6 (pp. 1-36).

[27] KONRAD LACHMAYER and EVA SOUHRADA-KIRCHMAYER, «Datenschutzrecht in Der Wissenschaftlichen Forschung», *Zeitschrift für Hochschulrecht Hochschulmanagement und Hochschulpolitik (zfhr)*, Vol. 17, 2018, p. 153 (pp. 153-158).

[28] JOCHEN TAUPITZ and MARIE SCHREIBER, «Biobanken – Zwischen Forschungs- Und Spenderinteressen», *Bundesgesundheitsblatt – Gesundheitsforschung – Gesundheitsschutz*, Vol. 59, 2016, (pp. 304-310).

[29] KRISTIN SOLUM STEINSBEKK, BJØRN KÅRE MYSKJA, and BERGE SOLBERG, «Broad Consent versus Dynamic Consent in Biobank Research: Is Passive Participation an Ethical Problem?», *European Journal of Human Genetics*, Vol. 21, 2013, pp. 897-898 (pp. 897-902).

[30] FLORENT THOUVENIN, «Informational Self-Determination: A Convincing Rationale for Data Protection Law? », *JIPITEC: Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2021, p. 246 (pp. 246-256).

Despite this less paternalistic positioning, it is worth noting that data protection authorities look at the broad consent model with scepticism from a legal and legal policy perspective. In particular, the former Article 29 Data Protection Working Party (WP29) – which has given place to the current European Data Protection Board (EDPB) – has emphasised the need for a specific purpose for consent, not interpreting Recital 33 of the GDPR as an exemption from the requirement of a specific purpose for processing.[31]

Assuming that the purpose of data altruism in clinical research is to reuse data at scale, the application of consent from the strict perspective of purposes as a prerequisite for effectiveness, the ultimate goal of the European strategy for data would be jeopardised. This is because, since it is not possible to identify all the purposes of secondary use at the time of collection, it would only be possible to determine the specific and unique research for which consent is obtained. In this case, re-use would be jeopardised.

Therefore, this paper tends to encourage the logic of non-compatibility, which considers a broader consent to be valid, restricted to the category of data processing – research, e.g. cancer care – and not to the type-specific research on one cancer type. The requirement demands a compatibility assessment between the initial purposes – the processing purposes at the moment of data collection or re-use of personal data – and the new purposes, which are any secondary processing purposes which are different – but related – from the initial purpose.[32]

C) Alternative treatment: dynamic consent

In favour of informational self-determination and as an intermediate alternative that preserves the granular character of consent as a legal basis for biomedical research, the logic of dynamic consent, originally developed in response to the challenges of the informed consent process in the digital age, is urgently needed.[33]

Dynamic consent is an approach to consent that allows study participants, through an interactive digital interface, to make granular decisions about their ongoing participation. This approach has been explored in biomedical

[31] Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679', (2018) WP259 rev.01 28-29.

[32] MEREL ELIZE KONING, *The Purpose and Limitations of Purpose Limitation*, *op. cit.*, p. 204.

[33] Although informed consent is not to be confused with a legal basis for the GDPR, this example is presented as a perspective for interpretation.

research, in fields such as biobanking and genomics, where ongoing contact with participants is required.[34]

It is hypothesised that dynamic consent can increase decision-making autonomy and improve researcher-user communication. Applying the idea to data altruism could be a solution in cases where consent remains the rule, as suggested in Recital 50 of the DGA.

WP29 mainly refers to the path of dynamic consent in favourable of this approach if a complete specification of the purpose is not possible from the very beginning. The decision of the 97th Conference of German Data Protection Authorities of 3 April 2019 on the interpretation of the term 'certain areas of scientific research' in recital 33 is also based on the same approach. This ruling is more permissive and ambivalent than the one in WP29. On the one hand, it rejects a generalised expansion to certain areas of research. On the other hand, it only requires that the respective research project be communicated 'with the greatest possible precision' and recognises that, in individual cases, working with 'broad consent' may be necessary, under conditions which, due to space limitations, will not be further developed in this paper.[35]

In acknowledging that the position of the supervisory authorities is not uniform, this paper points out that there is no general legal priority for dynamic consent over broad consent or traditional consent.[36]

Unless broad consent is deemed absolutely inadmissible by the legislator – which the legislator has not made clear – in cases where consent as a legal basis is maintained as a general rule, it is argued that dynamic consent is the best approach to maintain granularity and specificity. However, for mass re-use, there are doubts about the effectiveness of this solution for multiple unconnected studies, for the European Data Strategy, especially the Europe-wide intentions with the EHDS.

To address this challenge, a brief and limited one-paragraph note – due to space and scope limitations. It simply states that both explicit patient consent (opt-in) and the possibility of objecting to a generally permitted use of data (opt-out) would be possible to legitimise a data donation. Unfortunately, what both options have in common is that their comprehensive, practical and legally

[34] MEGAN PRICTOR and others, «Dynamic Consent: An Evaluation and Reporting Framework», *Journal of Empirical Research on Human Research Ethics*, Vol. 15, 2020, p. 175 (pp. 175-186).

[35] Datenschutzkonferenz (DSK), «Entschließung Der 97. Konferenz Der Unabhängigen Datenschutzaufsichtsbehörden Des Bundes Und Der Länder Am 3. April 2019», available at https://www.datenschutzkonferenz-online.de/media/en/20190405_Entschliessung_Unternehmenshaftung.pdf [accessed 3 April 2019].

[36] For more background details that have not been developed here, please see PHIL DANIEL STRECH and others, «„Datenspende"…», *op. cit.*, p. 95.

compatible implementation is difficult, if not impossible, within the current legal framework. Despite this, it is argued that the opt-out would be more advantageous for scientific purposes. Naturally it would significantly increase the scientific value of medical data donated for secondary use in research, if such donations were made by as many patients as possible – ideally all patients, in analogy to the case of organ donation. This is because it can be assumed that the donation of data in the form of adherence would have little prospect of high adherence and participation. The best approach would be data donation via opt-out, with the option to object, which can be exercised as easily as possible. In this case, the concept of dynamic consent would be compatible, in favourable to the right to object.[37] Furthermore, it is suggested that the donation of data for medical research be designed in such a way that the data donation process is dissociated in time and space from any specific medical treatment or diagnosis.

Once the acute symptom has been addressed, it's necessary to proceed with the analysis of the chronic symptoms, which remain in a grey area. The chronic questions will be answered below. The second question is whether the data subject's consent, as provided for in Article 9(2)(a) of the GDPR, is the only valid legal basis for donating data for altruistic purposes in clinical research, on the part of the data subjects and altruistic organisations as holders of this data.

D) Treatment for chronic symptoms: pseudo-overlapping, intersections and priority of legal bases

The definition of scientific research purposes has substantial ramifications for the range of data processing activities that a controller can carry out. The term scientific research is not defined in the GDPR. Recital 159 is the closest to a definition, which merely states that the processing of personal data for scientific research purposes should be interpreted broadly.

However, the WP29 considers that the notion of this concept cannot be extended beyond its common meaning and takes the view that scientific research means a research project created in accordance with relevant sector-specific standardised methods and ethics, in line with good practice.[38] The attempted definition is equally vague.

For the sake of harmonising the concept for the discussions in this paper, the definitions of clinical study in Article 2(1) of Regulation 536/2014, the Regulation on Clinical Trials of Medicinal Products for Human Use, will be adopted. Therefore, a clinical study is any investigation related to human beings aimed at discovering or verifying clinical effects, identifying any adverse reactions, to

[37] *Ibid*., p. 131.

[38] Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679', *op. cit.*, pp. 27-28.

ascertaining the safety and efficacy of a therapeutic, medicinal product or medical device.

Furthermore, the interpretation of biomedical literature will also be considered, which states that clinical research is an alternative terminology used to describe medical research. Clinical research involves people – including their personal data – and is usually carried out to assess the effectiveness of a drug or therapy, a medical or surgical procedure or a device as part of patient treatment and management. In addition, any research that assesses aspects of health such as symptoms, risk factors and pathophysiology, among others, can be categorised as clinical research.[39]

With the concept of clinical research settled, concerning the chronic symptom under the prioritisation of legal bases, is the consent of the data subject, provided for in Article 9(2)(a) of the GDPR, the only valid legal basis – preferred by the agnostic legislator of the DGA – for donating data for altruistic purposes for clinical studies?

When consent is the legal basis for carrying out research under the GDPR, consent for the use of personal data must be distinguished from other consents that serve as an ethical standard or procedural obligation – like informed consent from the Declaration of Helsinki (DoH), adopted by the 18th WMA General Assembly, Helsinki, Finland, June 1964. An example of such a procedural obligation, where processing is not based on consent but on another legal basis, can be found in the Clinical Trials Regulation. In the context of data protection legislation, this latter form of consent can be considered an additional safeguard, according to recital 161 of the GDPR.

At the same time, the GDPR does not restrict the application of Article 9 to consent only, as far as the processing of data for clinical research purposes is concerned. As long as there are adequate safeguards, such as the derogations provided for in Article 89(1), and the processing is fair, lawful, transparent and complies with the principle of data minimisation and individual rights, other legal bases may be compatible with the processing of special category data, such as biometric, genetic and health-related – sensitive – data, under the terms of the derogation in Article 9(2)(j) of the GDPR. Furthermore, specific trials can be carried out for medical devices, based on EU or national law, under the terms of Article 9(2)(i) of the GDPR. This is the position advocated by the WP29.[40]

Fuelling the controversy, for example, in a decision by the *Garante per la Protezione dei dati personali* (Italy), it was recognised that certain categories of

[39] VENKATARAMANA KANDI and SABITHA VADAKEDATH, «Clinical Trials and Clinical Research: A Comprehensive Review», *Cureus*, Vol. 15(2), 2023, p. 1 (pp. 1–15).

[40] Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679', *op. cit.*, pp. 28, 31.

sensitive data, such as health data, can be used for scientific research purposes according to Article 9(2)(j) of the GDPR. By contrast, in a ruling in Hamburg VG – 21 K 1802/21, the court considered that the transfer and processing of highly sensitive health data by the HKA posed a significant risk to the fundamental rights of the data subject. Despite serving specific and – supposedly – lawful purposes, the court found the processing to be disproportionate and therefore unlawful under Article 9(2)(h), (i) and (j) of the GDPR. The ruling emphasises the need for clear legislative provisions guaranteeing effective protection of sensitive data against abusive use.[41]/[42]

Returning to the fundamental question, if the answer is yes to the homogeneity of consent as the only eligible legal basis for data altruism purposes – which includes clinical research – as the legislator of the DGA seems to imply – as referred to mainly in recital 50 and Article 25 of the DGA – there would be a clear overlap between the GDPR and the DGA. This is because the GDPR does not prioritise legal bases. Evidence of this is the limitation of the right to the erasure of data by the data subject who withdraws consent, in the case of scientific research, on the basis of Article 17(3)(d) of the GDPR, another legal basis in conjunction.

The GDPR's wording suggests that the legal basis for research could not be consent solely, as it states that the right to the erasure of data – or right 'to be forgotten' – may be suppressed if it is impossible or severely jeopardises the achievement of the research objectives. This paper hypothesises that the GDPR legislator is indirectly suggesting a conjunction of legal bases or just the use of the one laid down in Article 9(2)(h) of the GDPR – namely scientific research. This may not be the case in other sectors, as the DGA is agnostic in terms of sectoral application, as is the GDPR.

On the one hand, the DGA legislator over-emphasised consent for altruistic purposes. On the other hand, the GDPR legislator seems to have suggested scientific research purposes as the main legal basis for research, to the extent that it serves as a basis for limiting the exercise of the right to erasure.

Limiting erasure is certainly in the interest of the research ecosystem, in order to maintain the redundancy of the database and safeguard the aims and objectives of the research. Would it be legitimate to collect data for altruistic research purposes on the basis of consent and deny the exercise of a right on another legal basis? Wouldn't the data controller be misleading the data subject, breaching the principles of lawfulness, and fairness, and casting doubt on the

[41] VG Hamburg – 21 K 1802/21, ECLI:DE: VGHH:2022:0728.21K1802.21.00.

[42] ANA KOIAVA, *Challenges of GDPR Compliance with the Data Altruism Concept under DGA: Lessons from the Estonian X-Road*, Master's thesis, Tallinn University of Technology, School of Business and Governance, 2024, pp. 37-38 (pp. 1-67).

lawfulness of the processing, as provided for in Article 5(1)(a) of the GDPR, respectively?

Actually, no. Because the withdrawal of consent does not compromise the lawfulness of the processing carried out based on the consent previously given, according to Article 7(3) of the GDPR, regarding the conditions applicable to consent. Therefore, an analysis of the situation suggests that there is a convergence of different legal bases, applicable at different stages of the data processing.

For the collection of personal data for altruistic scientific research purposes, the consent provided in Article 9(2)(a) of the GDPR, in conjugation with Recital 50 and Article 25 of the DGA, would be used. Once consent has been withdrawn, the data processed before the withdrawal is retained. Lawfulness is maintained on the basis of the convergence of Article 9(2)(h) and Article 7(3) of the GDPR, restricting erasure if the retention of data already collected is indispensable for the pursuit of the research objectives. No further data will be collected after the withdrawal. The old data will be conserved until the purpose of the study – or studies linked to the same area – has been achieved, respecting the principle of purpose limitation and storage limitation, provided for in Article 5(1)(e) and (b) of the GDPR.

Answering the underlying question, therefore, there is (yes) a convergence of legal bases in the sectoral context of clinical research – despite the agnostic way in which the legislator of the DGA has written it. Therefore, it is argued that it is possible to collect data under consent and deny the right to erasure based on clinical research purposes, as long as this basis has been communicated since collection, according to Articles 12 to 14, following the principle of transparency, provided for in Article 5(1)(a) of the GDPR. Based on the conclusions of the previous chapter, dynamic consent is the most appropriate approach also in this relationship with another legal basis.

It should be stressed that the strategy for defining the applicable legal bases does not dispense with the duty to inform the data subject about it, mitigating the break in the data subject's expectations, per Articles 12 to 14 of the GDPR. This is therefore an intersection – confluence – and not an overlap of legal bases.

However, it is advocated that, for the application of data altruism to health research, the wording of the DGA was not very fortunate, leading to confusion about a potential preference of the legislator for consent as a legal basis – almost the only alternative – which leads to wrongly belief that there would be a conflict of Regulations.

The WP29 emphasizes that it is not possible to shift between one legal basis and another. This paper agrees with the impossibility of switching legal bases after informing the data subject directly or indirectly at the time of collection, under the terms of Articles 12 to 14 of the GDPR, otherwise, the data

subject will be mistaken and the principles of lawfulness and transparency will be breached. However, the position is that the conjugation between other legal bases and consent is not an exchange, as it must be done before the processing begins. In this way, the conjugation of legal bases is lawful for altruistic purposes. However, their choice must be carefully defined, without harming the rights and freedoms of data subjects.

It is understood in this article that the legislator of the DGA intended to give preference to consent by default, assuming it in recital 50 as a general rule, to the detriment of other legal bases, dealt with as residual. This choice by the legislator may lead to legal uncertainty and have an anti-efforts effect on what seems to be the aim of the European data strategy.[43]

As a treatment proposal for these chronic symptoms, it is suggested that the text of the DGA be reviewed, given that it seems to have neglected the centrepiece of the data governance framework on ensuring the fundamental right to privacy through data subject protection, the GDPR.

3. Follow-up

In conclusion, there is no outright conflict of norms – overlapping. There is an intersection.

Responding to question 1) of the diagnosis, it is argued that consent is an applicable legal basis and the broad dynamic modality is the one that best responds to the designation of the GDPR and the DGA in terms of data governance.[44] Responding to question 2), it is also argued that consent can be combined with other legal bases for data altruism mechanisms, such as scientific research, per Article 9(2)(a), (i) and (j) GDPR.

Still responding to question 2), it takes the view that consent could apply to the direct data collection phase. It suggests that the other legal bases, also to be informed to the data subject at the time of collection, could also be applied, in conjunction, at the stage of re-use for research purposes. When exercising certain rights, such as the right to erasure, as long as the technical and organizational safeguards have been adopted to protect the individual right to privacy of the data subjects in question, the legal basis relating to scientific research can support the limitation of this right, in the terms set out above.

---

[43] PATRÍCIA CARNEIRO, «Regulamento Geral sobre a Proteção de Dados e o Mercado de Dados…», *op. cit.*, pp. 28-34.

[44] Although an opt-out system, similar to the logic of organ donation, could be the approach that offers the greatest added value to the data. Against this strategy is the difficulty of making it compatible with the data protection regime, as mentioned above.

Responding to question 3) of the diagnosis, is argued that the DGA legislator did not explicitly impose consent as the only valid legal basis for altruism, but strongly reinforced it – disproportionately prioritising it, at odds with the GDPR which did not establish a priority ranking for legal bases. The DGA creates an unfortunate situation concerning its articulation with the GDPR.

It is understood that the wording of the DGA is not favourable to the design of fostering the reuse of data on a scale for new products and services through the altruistic mechanism, undermining the legal security of the ecosystem.

To illustrate this in practical terms, take, for example, a start-up with few human and economic resources – to which part of the European Data Strategy is dedicated – which has a lawyer in-house. As a general rule, these are general practitioners because they have to deal with all legal-related matters of the company. Imagine that this lawyer is confronted with the complex controversy surrounding the legal basis that should be applied to the scope explored in this article. Likely, he or she does not have the specific knowledge or the time to reach the conclusion reached in this text – noting that, despite the rigour of this paper, the arguments presented can be volatile, as they are an interpretation, without binding effect. The binding effect should come from the legislator. The result of this is an illogical cost or disincentive and insecurity for small and medium-sized enterprises (SMEs), as well as for the more dominant and consolidated players, who need to be compliant with an increasingly complex regulatory data governance framework.

The speciality of the subject does not make it easy to find solutions. The minimum that should be achieved is simplification and coherence between the growing regulatory framework. Proportionately to ensure the rights and freedoms of the data subjects and not to suffocate the ecosystem to which it is intended to foster.

Criticism has been levelled at the DGA legislator's distortion of the legal bases, which reflected a secondary account of the GDPR – the main pillar of the structure on which the processing of personal data is laid. Such secondary accounting seems to offer (in)voluntary opposition to the *lex specialis* principle. Is the legislator subverting the corollary of the *lex specialis* – recognized by the EDPB in other similar cases, such as the relationship between

the e-Privacy Directive[45] and the GDPR[46] – and which has a long pedigree in European jurisprudence?[47]

Following these reflections, this paper takes the position that without the harmonization that was supposed, about the laying down of legal bases, the wording of the DGA – contemporary to the date of this paper – has contributed to the undermining of trust in the structures of data altruism in the general context and especially for research purposes, particularly for clinical research, jeopardising the rights and freedoms of data subjects and data holders legal certainty due to regulatory inconsistency.

Surmounting these barriers will not only indirectly support the success of the EHDS, but also the development of healthy European data spaces in general, providing technological opportunities and a competitive advantage for EU citizens – data subjects – and entities, notably start-ups and SMEs, per the EU's strategic goals.[48]

To this end, it is suggested that the text of the DGA be carefully revised in this regard. This topic deserves further development, including other aspects of the intersection between the DGA and the GDPR, which this paper will not be able to address for reasons of scope.

[45] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[46] European Data Protection Board (EDPB), «Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities», 2019, p. 14, available at https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf [accessed 9 august 2024].

[47] Please see: Judgement of the CJEU in Joined Cases T-60/06 RENV II and T-62/06 RENV II, 22 April 2016, ECLI:EU: T:2016:233, at paragraph 81.

[48] MADALENA GOMES CRUZ and IAKOVINA KINDYLUD, «The European Health Data Space and the GDPR – A Problem of Compatibility for the "Donation" of Health Data», *Yearbook of Data Protection*, 2023, pp. 225, 247, 248 (pp. 225-248).

TITLE
E.TEC YEARBOOK

EDITORS
Prof.ª Doutora Sónia Moreira

AUTHORS

Ana Cristina Gouveia | Luís Manuel Pica | Maria Victória Rocha
Sérgio Manuel da Costa Machado | Sérgio Silva | Yuri R. Ladeia

DATE
December 2024

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

ISSN
2184-707X

University of Minho
School of Law

JusGov
RESEARCH CENTRE FOR JUSTICE AND GOVERNANCE

fct Fundação para a Ciência e a Tecnologia