DOS *EXPERT SYSTEMS* AOS *DATA SYSTEMS AI*: IMPACTO AO NÍVEL DA PROTEÇÃO DE DADOS

Mafalda Miranda Barbosa[1]

Sumário: 1. A formulação do problema. *Expert systems* e *data systems AI*; 2. Os níveis de proteção de dados pessoais; 3. A criação de perfis (*profiling*); 4. As decisões automatizadas; 5. Uma decisão discriminatória: *quid iuris*?; 6. Breve conclusão: uma necessária mudança de perspetiva.

Resumo: O desenvolvimento da inteligência artificial, com o recurso às técnicas de *machine learning* e *deep learning*, é tributário do processamento de grandes quantidades de dados. Incluindo-se nestes os dados pessoais, facilmente acessíveis através da navegação em rede, são muitos os riscos que a realidade atual comporta para os seus titulares. Depois de analisarmos alguns desses riscos e de darmos conta dos níveis de proteção que o Regulamento Geral de Proteção de Dados dispensa, centrar-nos-emos num problema concreto, qual seja do potencial discriminatório que as decisões totalmente automatizadas encerram. Estudar-se-ão, assim, as soluções consagradas em matéria de criação de perfis e decisões automatizadas, para, *in fine*, questionarmos qual os mecanismos de reação se, apesar da proteção dispensada ao nível europeu, se chegar, por via algorítmica, a uma decisão discriminatória. A fragilidade de alguns dos remédios leva-nos a concluir pela necessidade de uma mudança de perspetiva a este nível.

Palavras-chave: dados pessoais, inteligência artificial, perfis, decisões automatizadas, responsabilidade civil.

Abstract: The development of artificial intelligence, through the techniques of machine learning and deep learning, depends on the processing of huge amounts of data, including personal data. These data are easily accessible through web browsing; therefore, data subjects are exposed to various risks. In this paper, after analysing some of these risks and after analysing the levels of protection that the General Data Protection Regulations provides, we will focus on a specific problem, namely the discriminatory potential that fully automated decisions entail. Thus, we will study the rules provided by the relevant Community legislation, concerning profiling and automated decisions. In the end, we will have the opportunity to think ahead what would be the right solution if, despite the despite the protection provided at the European level, we reach, by algorithmic means, a discriminatory decision. The weakness of some of the remedies leads us to conclude that there is a need for a change of perspective at this level.

Keywords: personal data, artificial intelligence, profiling, automated decisions, civil liability.

---

[1] Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra/University of Coimbra Institute for Legal Research of the Faculty of Law. Doutorada em Direito pela Faculdade de Direito da Universidade de Coimbra. *Curriculum*: https://www.cienciavitae.pt/C313-72CA-DFB7

1. A FORMULAÇÃO DO PROBLEMA. *EXPERT SYSTEMS* E *DATA SYSTEMS AI*

O mundo atual vive um período de transformação informacional, caracterizado por uma produção e armazenamento em massa de dados gerados continuamente. À medida que os diversos *smartphones*, *tablets*, computadores e múltiplos outros aparelhos se conectam, são recolhidos e transmitidos dados através de redes de alta velocidade, que depois são armazenados em bases de dados distribuídas e analisados com as mais variadas finalidades por *softwares* cada vez mais poderosos e sofisticados[2]. Os três *«Vês»* — volume, velocidade e variedade — que caracterizam a explosão informacional dos nossos dias garantem uma análise mais fidedigna, permitindo novas formas de inferência e predição, num movimento acelerado que se incrementará ainda mais com o advento do 5G e o surgimento da computação quântica[3].

A profusão de dados que os novos *softwares* conseguem computar permitiu, ao nível da inteligência artificial, o alargamento do campo de aplicação de formas mais complexas, mas mais fidedignas de reprodução da capacidade de raciocínio humano nas máquinas, com a *machine learning* e o *deep learning*.

De facto, os primeiros sistemas de computação que reproduziram a capacidade de tomar decisões de um ser humano, conhecidos por *expert systems* e desenhados para resolver problemas mais ou menos complexos, através do conhecimento pré-adquirido, de acordo com a regra *if/then* (*se/então*)[4], baseavam-se em dois subsistemas: um mecanismo inferencial e uma base de conhecimento, representativo de factos e regras, de tal forma que o mecanismo inferencial aplicava as regras aos factos conhecidos para deduzir novos factos. Adotados em inúmeros domínios, conheceriam limitações pela utilização de métodos tradicionais, relativos à teoria probabilística e ao encaixe de padrões estatísticos[5].

Foram exatamente tais limitações que levaram os especialistas na matéria a procurar novos tipos de abordagens que se mostrassem mais eficientes e flexíveis, de modo a simular o processo de decisão humana.

O acesso ao *big data* viria facilitar a aceleração desta evolução[6]. A disponibilidade generalizada de dados fornecidos a partir da internet e da internet das coisas viabilizou o predomínio da investigação centrada em algoritmos que, acedendo a tais informações, aprendem com base em exemplos, gerando o seu próprio conhecimento, que representam através de regras (*inducive learning*).

---

2 Niño, Mikel / Illarramendi, Arantza, «Understanding Big Data: antecedents, origin and later development», *Dyna New Technologies*, n. 2, 2018, p. 1 s.

3 Laney, *3D Data Management: Controlling Data Volume, Velocity, and Variety*, META group Inc., 2001, http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

4 Jackson, Peter, *Introduction to Expert Systems*, Addison Wesley, Portland, 1998, p. 2 s.

5 Coats, Pamela K., «Why expert systems fail», *Financial Management*, 17-3, 1988, pp. 77 s.

6 Shan, Ning / Ziarko, Wojciech, «Data-based acquisition and incremental modification of classification rules», *Computational Intelligence*, 11-2, 1995, pp. 357 s.

A máquina deixa de atuar em termos meramente dedutivos, para garantir a dedução a partir da indução que ela própria protagoniza[7].

Do mesmo modo, desenvolvem-se algoritmos que, acedendo à vastíssima quantidade de informação disponível, acumulam experiência acerca da contribuição das regras para um correto conselho que seja formulado (*problem solving learning*) ou que colecionam casos numa base de dados aberta, e processada em redes de alta velocidade, para resolver problemas com base na procura de um caso similar, inferindo a favor da melhor experiência, numa lógica abdutiva (*case-based learning*)[8].

Machine learning e *deep learning* desenvolvem-se, assim, a partir da disponibilização de grandes quantidades de dados, que se assumem como a matéria-prima fundamental do incremento do uso da inteligência artificial, com todas as vantagens que ela comunica no dia-a-dia das pessoas e das empresas. Educação, saúde, transportes, serviços em geral, comércio em particular podem beneficiar das novas e complexas tecnologias, que apenas sobrevivem em face da disponibilização dos dados a que nos referimos[9].

Contudo, não sem riscos. Desde logo, o acesso aos dados é diretamente proporcional ao incremento do perigo de intrusão na vida privada dos cidadãos, relativamente aos quais pode passar a ser facilmente reconstituído o seu percurso de vida, pelos traços que vão deixando inscritos no mundo digital ou através da internet das coisas[10].

Por outro lado, a utilização de dados recolhidos ou comprados aumenta o risco de eventuais discriminações. Estas podem ser de dois tipos: a) discriminações *stricto sensu*. Pense-se no exemplo de uma instituição financeira que, sabendo que um seu potencial cliente faz recorrentemente pesquisas acerca de mecanismos de proteção em situações de incumprimento contratual, recusa conceder crédito ou, concedendo-o, fixa um *spread* muito elevado. Mas pense-se, também, nas hipóteses de discriminação laboral, social, étnica, política; e b) situações de *adaptative pricing*, ou seja, uma forma de variação dos preços em função do perfil do consumidor, de tal modo que a proposta negocial apresentaria um preço mais elevado aos consumidores que se mostrassem aptos a aceitar aquela oferta mais valiosa.

Por último, a definição de perfis pode conduzir à limitação da liberdade de escolha, num fenómeno conhecido por *boxing*, que tem expressão em termos comerciais e em termos políticos e ideológicos. Podem, de facto, abrir-se as portas a formas de manipulação informativa.

---

7 Joshi, Kailash, «Expert Systems and Applied Artificial Intelligence», https://www.umsl.edu/~joshik/msis480/chapt11.htm, acesso em 30-6-2021.

8 Kailash Joshi, «Expert Systems and Applied Artificial Intelligence» (nota 6).

9 Ralambondrainy/Demonchaux/Jomier, «Data analysis, data bases and expert systems: the common interface», *ESO Conference Workshop Proceedings*, n. 28, 1988, pp. 213 s.

10 Para outros desenvolvimentos, cf. Sergio Gutiãrrez, Armando / Branch, John Willian, «A comparison between expert systems and autonomic computing plus mobile agent approaches for fault management», *Dyna New Technologies,*2011, (http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0012-73532011000400021), pp. 78 s., acesso em 23-6-2021.

Os dados pessoais são hoje vistos como uma *commodity*, como bens que podem ser transacionados com valor económico[11]. Para além do valor que assumem para as empresas que os recolhem, no sentido de ordenar a sua oferta em relação aos dados da procura que vão conhecendo, há terceiros que se dedicam à recolha, mineração e análise de dados, para posteriormente os venderem. A partir de grandes volumes de dados recolhidos estabelecem padrões, por meio de associações ou sequências temporais. Posteriormente, tais informações são vendidas aos chamados corretores de informações, que estabelecem, através da mineração, padrões e perfis e depois são transacionados a ulteriores adquirentes que neles tiverem interesse[12].

Estes terceiros que compram perfis de dados pessoais de múltiplos titulares utilizá-los-ão para oferecer os produtos que melhor se coadunem com aquele perfil ou para difundir as ideias (políticas, ideológicas ou outras) que se mostrem em sintonia com o público alvo. O consumidor e/ou o cidadão, consoante o papel que se assuma em cada momento, passa(m) a viver numa caixa. Do ponto de vista comercial, o fenómeno pode implicar que apenas seja veiculada publicidade que se adapte ao perfil do consumidor, o que envolve uma limitação da possibilidade de escolha da pessoa em concreto[13]. Do ponto de vista político, pode configurar uma limitação ao direito ao esclarecimento, impedindo uma tomada de consciência acerca do espetro ideológico na sua completude. Conduz, portanto, a uma menorização dos cidadãos, podendo pôr em causa direitos fundamentais, entre os quais o direito ao livre desenvolvimento da personalidade[14].

Torna-se, portanto, claro que a inteligência artificial comporta riscos acrescidos em relação ao direito à proteção de dados. O problema, nesta ótica, não é tanto a questão da inteligência artificial em si mesma, mas o do impacto que ela possa ter na tutela dos dados pessoais e dos direitos que lhe subjazem.

Em face destes problemas, surge a questão nuclear: como fazer-lhes face? Qual ou quais o/os remédios predispostos para lidar com eles?

---

11 Departamento de Proteção e defesa do consumidor, *Proteção de dados pessoais nas relações de consumo: para além da informação creditícia*, Brasília, 2010, p. 11, considerando que "a informação pessoal, especificamente, desponta como uma verdadeira *commodity* em torno da qual surgem novos modelos de negócio que, de uma forma ou de outra, procuram extrair valor monetário do intenso fluxo de informações pessoais proporcionado pelas modernas tecnologias da informação".

12 Sobre a criação de perfis, cf., igualmente, Zannatta, Rafael, «Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais», https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais, 2009, acesso em 13-6-2021; Departamento de Proteção e defesa do consumidor (nota 10), p. 14.

13 Departamento de Proteção e defesa do consumidor (nota 10), p. 69. Veja-se, igualmente, Erevelles, Sunil / Fukawa, Nobuyuki / Swayne, Linda, «Big Data Consumer Analytics and the Transformation of Marketing», *Journal of Business Research*, n. 69, 2016, pp. 897 s.

14 Ceron, Andrea / Curini, Luigi / Iacus,Stefano Maria, *Politics and Big Data*, Routledge, Londres, 2016, pp. 12 s.

2. OS NÍVEIS DE PROTEÇÃO DE DADOS PESSOAIS

Se adequadamente reconhecermos que subjacentes ao direito à proteção de dados estão outros direitos fundamentais, em relação aos quais aquele funciona como guarda-avançada[15], então torna-se facilmente percetível que o acesso a tais dados pessoais poderá implicar uma lesão do direito à privacidade. Mas não só: o direito à igualdade, o direito à imagem, o direito à identidade pessoal, e o direito à autodeterminação informacional podem também sofrer lesões, colocando-se em causa a incolumidade da pessoa.

Como forma de combate aos riscos a que se alude, haveremos de ter em conta que o tratamento de dados — qualquer que ele seja — há de obedecer a princípios rigorosos, consagrados no RGPD, e tem de basear-se, para ser lícito, num dos fundamentos previstos no artigo 6.º do mesmo diploma. A saber. O tratamento de dados pessoais deve ser feito de forma lícita, *transparente* e de acordo com o *princípio da boa-fé*. Além disso, os *dados apenas podem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades*. O artigo 5.º/1 b) RGPD reproduz o conteúdo do artigo 5.º/1 b) Lei n.º 67/98, esclarecendo, contudo, que o tratamento posterior para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos não é considerado incompatível com as finalidades iniciais. Consagra-se, igualmente, o *princípio da minimização de dados*, isto é, estes devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados; o *princípio da exatidão* (os dados pessoais devem ser exatos e atualizados sempre que necessário, devendo ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora); o *princípio da limitação da conservação* (os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados); e o *princípio da integridade e confidencialidade*. Este último significa que os referidos dados devem der tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.

Para além da necessária obediência aos princípios referidos, o tratamento de dados pessoais só é lícito se existir consentimento do seu titular ou, em alternativa, se se verificar uma das seguintes situações: se o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; se o tratamento

---

15 Falando de uma relação de interioridade constitutiva, cf. Barbosa, Mafalda Miranda, «Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil», *Estudos de Direito do Consumidor*, n.12, 2017, pp. 75-132 (= «Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil», *AB Instantia*, ano V, n. 7, 2017, pp. 13-47).

for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; se o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; se o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

O consentimento assume um papel importantíssimo, devendo obedecer a condições estritas. Entre elas, importa ter em conta que o consentimento tem de ser esclarecido e tem de ser prestado para uma finalidade determinada, colocando-se a questão de saber se não se poderia justificar, a este nível, uma ideia de *ongoing consent*.

Não obstante a centralidade do consentimento e o rigor com que o mesmo é assumido a este nível, a proteção dos dados pessoais baseada no modelo de escolha do titular dos mesmos de acordo com um esquema informação-consentimento apresenta falhas evidentes. Os consumidores ou cidadãos, consoante o papel que cada um assuma em concreto, são confrontados com notificações explicativas da política de privacidade dos diversos sites e aplicações que utilizam, muitas vezes de forma densa e pormenorizada, mas raramente os leem. E se é certo que não é possível (nem desejável) adotar uma postura paternalista em relação aos cidadãos, sobre os quais recai um dever de diligência, e se é certo que, sempre que esteja em causa a adesão a fórmulas assentes em cláusulas contratuais gerais, os deveres de informação envolvem um dever de esclarecimento relativamente a todas as dúvidas que sejam certas ou que possam ser dirigidas ao predisponente, não é menos seguro afirmar que a complexidade dos processos de decisão automática que envolvam a inteligência artificial torna muitas vezes incompreensível o impacto que a recolha e tratamento de dados, aparentemente inócuos, poderá ter no futuro.

Não está, de facto, em causa um simples tratamento de dados para o qual o consentimento se mostre garantia suficiente, conjuntamente com os princípios que norteiam a atuação do chamado *controller*, mas um tratamento de dados que, envolvendo conexões, ligações e interconexões, poderá determinar a criação de um perfil e conduzir a formas de decisão automatizada, sem qualquer intervenção humana. Repare-se, neste contexto, que os perfis integram aspetos que, sendo obtidos a partir de dados pessoais transmitidos pelos seus titulares, são novos, porque inferidos a partir desses primeiros dados.

As instâncias europeias, conscientes desta realidade, não hesitaram, por isso, em consagrar medidas que visam combater formas de discriminação especial ou geral. Neste contexto, o considerandum 45 da Diretiva (UE) 2019/2161 do Parlamento Europeu e do Conselho de 27 de novembro de 2019, que altera a Diretiva 93/13/CEE do Conselho e as Diretivas 98/6/CE, 2005/29/CE e 2011/83/UE do Parlamento Europeu e do Conselho, a fim de assegurar uma melhor aplicação e a modernização das regras da União em matéria de

defesa dos consumidores, estabelece que os profissionais podem personalizar o preço das ofertas para consumidores específicos ou categorias específicas de consumidores, baseando-se em *automated decision-making and profiling of consumer behaviour*. Mas, nesse caso, devem informar claramente que os preços apresentados são personalizados com base nas decisões automatizadas, de modo a que o consumidor possa ter em conta o potencial risco da sua decisão de aquisição do produto. Estabelece-se, por isso, uma específica obrigação de informação nesta matéria, sem prejuízo da aplicação do RGPD[16]. Alterada que foi a Diretiva das Práticas Comerciais Desleais, pergunta-se se podemos recorrer ao regime para fazer face a muitos dos problemas relacionados com o marketing personalizado com base em *profiling*.

A solução, sem dúvida meritória, não dá, porém, respostas para além das relações de consumo e das situações de *adaptative pricing*. De fora ficam todas as hipóteses de discriminação, com relevância consumerística ou não, e ainda as hipóteses de manipulação informativa política, publicitária, científica, entre outras.

O perigo haveria, por isso, de ser combatido na sua génese: ao nível da criação de perfis, por um lado, e ao nível da regulamentação das decisões automatizadas.

3. A CRIAÇÃO DE PERFIS (*PROFILING*)

O artigo 4.º/4 RGPD define perfis como «qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações».

São, portanto, três os elementos integradores da noção de perfil[17]: 1) uma forma de tratamento automatizada; 2) relativa a dados pessoais; 3) que tem como finalidade avaliar os aspetos pessoais de uma pessoa singular.

Consoante explicita o Grupo de Trabalho (GT) do Artigo 29.º[18], não se exige que o tratamento seja exclusivamente automatizado, mas que envolva uma qualquer forma de automatização. Por outro lado, a definição de perfis implica ou pode implicar um conjunto de deduções estatísticas, estabelecendo previsões sobre pessoas, com base em dados provenientes de múltiplas fontes[19].

---

16 Cf. Diretiva 2011/83/EU.

17 GT Artigo 29.º, *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679,* 2017 (com revisão em 2018), p. 7 s.
Veja-se, ainda, sobre o ponto, Cordeiro, A. Barreto Menezes, *Direito da Proteção de Dados*, Almedina, Coimbra, 2020, 127 s.; Cordeiro, A. Barreto Menezes (coord.), *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº58/2019*, 2021, pp. 77 s.

18 GT Artigo 29.º (nota 16), p. 7.

19 GT Artigo 29.º (nota 16), p. 7.

Fundamental é que o perfil integre uma apreciação ou juízo acerca da pessoa ou grupo de pessoas[20]. De facto, continuando a acompanhar o GT do artigo 29º, "a simples classificação de pessoas com base em características conhecidas, como a idade, o sexo e a altura, não acarreta necessariamente uma definição de perfis. Tal dependerá da finalidade da classificação"[21].

Assim, e de acordo com o exemplo avançado pelo citado grupo de trabalho, se "uma empresa [...] classificar os seus clientes em função da idade ou do género para fins estatísticos e com vista a obter uma visão de conjunto dos seus clientes, sem realizar quaisquer previsões nem tirar ilações sobre as pessoas", não estamos diante de uma definição de perfil.

A compreensão da natureza de uma definição de perfil permite-nos perceber os remédios que o RGPD dispensa para tentar fazer face aos problemas que aquela comporta. Desde logo, os critérios de legitimação do tratamento de dados devem ser compreendidos de forma adaptada à realidade com que lidamos. Inequívoco é que se terá de verificar uma das condições de licitude previstas no artigo 6.º RGPD ou, tratando-se de dados especiais, também uma das condições previstas no artigo 9.º RGPD.

Contudo, o mecanismo de definição de perfis comporta especificidades. Sabemos já que a definição de um perfil pode determinar a criação de dados novos por inferência de dados já existentes. Ora, pode suceder que a partir de dados pessoais se criem novos dados que se integrem na categoria de dados especiais. Como alerta o GT Artigo 29.º, "existe a possibilidade de [se] inferir o estado de saúde de uma pessoa a partir de registos das suas compras de produtos alimentares, em combinação com dados relativos à qualidade e ao valor energético dos alimentos. Podem ser reveladas correlações que indiquem algo sobre a saúde, as convicções políticas, as crenças religiosas ou a orientação sexual das pessoas [...]"[22].

Nessa medida, haverá que indagar em que medida o fundamento de legitimação do tratamento de dados — referente aos dados iniciais — é ou não extensível aos dados especiais gerados ou se se pode, quanto a estes, autonomizar um novo fundamento de licitude. Concomitantemente, há que garantir que o tratamento não é incompatível com a finalidade previamente delineada e informar o titular dos dados acerca do novo tratamento que seja levado a cabo.

Em segundo lugar, o RGPD estabelece a este nível mecanismos de transparência. Impõe-se, na verdade, um reforço do direito à informação do titular de dados, nos termos dos artigos 14.º e 15.º/1 h) RGPD, não podendo os responsáveis pelo tratamento invocar a proteção do seu segredo comercial como pretexto para negar o acesso ou recusar a prestação de informações ao titular dos dados. Ainda que tais informações não sejam determinantes, podem ser um instrumento importante para o regulador ter acesso à política de tratamento de dados do *controller*.

---

20 GT Artigo 29.º (nota 16), p. 7.
21 GT Artigo 29.º (nota 16), p. 7.
22 GT Artigo 29.º (nota 16), p. 16 s.

O titular dos dados tem, ainda, direito à retificação e ao apagamento deles. Estes direitos, previstos nos artigos 16.º e 17.º RGPD, aplicam-se quer aos dados fornecidos diretamente pelo titular, quer aos dados de segunda geração criados — a partir daqueles — pelo algoritmo.

Finalmente, de acordo com o artigo 21.º RGPD, o titular dos dados pode, por motivos relacionados com a sua situação particular, opor-se à definição de perfis. Neste caso, o responsável pelo tratamento tem de pôr fim à definição de perfis, a não ser que haja razões imperiosas e legítimas que prevaleçam sobre os interesses, os direitos e as liberdades do titular dos dados.

Os responsáveis pelo tratamento devem imperativamente explicar às pessoas em causa, de forma clara e simples, o funcionamento do processo de definição de perfis ou de decisão automatizada. Conforme sublinha o GT, artigo 29.º, "o RGPD não explica o que poderia ser considerado razões imperiosas e legítimas. Um exemplo possível seria um caso em que a definição de perfis teria vantagens para a sociedade no seu todo (ou a comunidade de forma mais ampla) e não apenas para os interesses comerciais do responsável pelo tratamento, nomeadamente uma definição de perfis com vista a prevenir a propagação de doenças contagiosas"[23]. Abre-se, portanto, lugar a uma ponderação de interesses, exigindo-se que o interesse "legítimo seja imperioso, o que implica um limiar mais elevado para prevalecer sobre as objeções"[24]. O direito de oposição será, contudo, incondicional sempre que esteja em causa um tratamento para efeitos de comercialização direta.

4. AS DECISÕES AUTOMATIZADAS

Os perfis a que nos temos vindo a referir são importantes instrumentos para a tomada de decisões exclusivamente automatizadas[25]. Deve, porém, esclarecer-se que não há uma relação necessária entre os dois termos. Dito de outro modo, uma decisão exclusivamente automatizada pode ser tomada sem ter na base uma definição de perfil; por outro lado, uma definição de perfil não tem de desembocar inexoravelmente numa decisão automatizada. Estas podem basear-se em dados fornecidos pela pessoa, em dados observados ou em dados inferidos a partir de um perfil que haja sido criado. Só neste último caso, haverá uma correlação necessária entre as duas realidades.

Seja como for, os perigos para que se alertou preteritamente no que respeita à definição de perfis parecem agudizar-se quando nos confrontamos com decisões exclusivamente automatizadas. De facto, porque os algoritmos não

---

23 GT Artigo 29.º (nota 16), p. 21.

24 GT Artigo 29º (nota 16), p. 21.

25 Sobre o ponto, cf. Cordeiro, A. Barreto Menezes, «Decisões individuais automatizadas à luz do RGPD e da LGPD», *Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa* (coord. Mafalda Miranda Barbosa/Filipe Braga Netto/Michael César Silva/José Luiz de Moura Faleiros Júnior), Editora Foco, 2021, p. 263 s.

são neutros, antes sendo estruturados pelos valores do seu programador[26], porque os processos decisórios são complexos, podendo escapar ao controlo do próprio criador do *software*, corre-se o risco de emergirem situações injustas e/ou discriminatórias.

Importa, por isso, perceber quais os remédios que o legislador europeu concebeu para fazer face a tais perigos[27].

De acordo com o artigo 22.º/1 RGPD, «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, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar».

Segundo o entendimento do GT do artigo 29.º, a expressão direito é aqui usada em sentido impróprio. Quer isto dizer que não se atribui uma posição subjetiva de oposição a uma qualquer tentativa de tomada de decisão exclusivamente automatizada, mas se estabelece uma proibição genérica de decisões totalmente automatizadas, incluindo a definição de perfis, quando tais decisões produzam efeitos na esfera jurídica do titular dos dados ou o afetem significativamente de forma similar[28].

A proposta interpretativa parece ser autorizada pela articulação da norma com o teor do *considerandum* 71 e com a solução consagrada no n.º 2 do citado artigo 22.º RGPD. Não cremos, porém, que os argumentos deponham no sentido da inexistência de um direito, sem que, contudo, tal implique uma discordância com a solução prático-normativa proposta pelo GT artigo 29.º. De facto, do que se trata é de reconhecer um direito em termos genéricos, que exclui *a priori* a possibilidade de uma tomada de decisão exclusivamente automatizada, e não um qualquer direito unicamente exercitável por reação ao comportamento do responsável pelo tratamento de dados.

Teleologicamente, a solução impõe-se com meridiana clareza. A utilização de algoritmos (quer na definição de perfis, quer na tomada de decisões automatizadas) caracteriza-se pela sua opacidade[29], analisada pelos autores de forma tripartida: opacidade corporativa, deliberadamente gerada como forma de resguardar os segredos de negócios das empresas que desenvolvem os algoritmos; opacidade cognitiva, resultante da incapacidade que as pessoas em geral (e o titular dos dados em especial) têm de entender o funcionamento do algoritmo e

---

26 Cf. Rielli, Mariana Marques, «Críticas ao ideal de transparência como solução para a opacidade de sistemas algorítmicos», *Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa* (coord. Mafalda Miranda Barbosa/Filipe Braga Netto/Michael César Silva/José Luiz de Moura Faleiros Júnior), Editora Foco, 2021, p. 439 s.; O'Neil, C., *Weapons of Math Destruction: how big data increases inequality and threatens democracy*, Crown, New York, 2016, p. 17 s.

27 Cf. Bygrave, Lee A., «Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling», *Computer Law and Security Review*, n. 17, 2001, p. 17 s.

28 GT Artigo 29.º (nota 16), p. 22.

29 Cf. Burrell, Jenna, «How the machine thinks: understanding opacity in machine learning algorithms», 2015, http://ssrn.com/abstract=2660674, acesso em 24-6-2021; Pasquale, F., *The black box society*, Harvard University Press, 2015, p. 79 s.; Rielli, Mariana Marques (nota 25), p. 440.

de perceber a linguagem que o mesmo utiliza[30]; e opacidade técnica, inerente ao recurso ao *deep learning*, inviabilizador da explicitação do percurso decisório do *software*, mesmo por parte dos seus programadores[31].

Nessa medida, porque a incolumidade dos direitos dos titulares dos dados pessoais não se pode garantir com o mero cumprimento de deveres de informação prestados pelo responsável pelo tratamento[32], há que proibir que certas decisões sejam tomadas por algoritmos, de forma totalmente automatizada[33].

É exatamente essa perspetiva que é assumida pelo artigo 22.º/1 RGPD[34]. Importa, por isso, perceber que decisões são assimiladas pelo âmbito de relevância do preceito.

Desde logo, temos de estar diante de uma decisão. A este propósito, A. Barreto Menezes Cordeiro aduz que, "por decisão entende-se um ato, numa aceção não jurídica, que incida sobre um caso concreto e produza efeitos jurídicos relativamente a um ou mais titulares de dados específicos, quer seja a aceitação ou a recusa de um pedido, a sua caracterização, catalogação, atribuição de uma classificação, definição de perfil ou qualquer outra medida análoga produtora de um efetivo resultado"[35].

Tal decisão tem de ser *exclusivamente automatizada*, isto é, uma decisão que não envolva qualquer intervenção humana. Alerta, neste contexto, o GT artigo 29.º[36] que uma supervisão que não seja relevante, ou seja, que se conforme como um gesto meramente simbólico não é suficiente para afastar a qualificação. Assim, "se alguém aplicar de forma sistemática perfis gerados automaticamente a pessoas sem ter qualquer influência efetiva no resultado, tratar-se-á [...] de uma decisão tomada exclusivamente com base no tratamento automatizado"[37].

No mesmo sentido, *A. Barreto Menezes Cordeiro* sustenta que se "trata [...] de um critério material e não de um critério formal, pelo que previsão [...] tem-se por verificada sempre que a intervenção humana assuma contornos burocráticos, meramente confirmadores ou acríticos"[38].

Por outro lado, a decisão tem de produzir efeitos na esfera jurídica do titular dos dados ou de o afetar significativamente, de forma similar. A produção de efeitos na esfera jurídica refere-se à constituição, modificação ou extinção de relações jurídicas, mas também à afetação dos pressupostos de facto de exercício de um direito potestativo ou à lesão de um direito alheio ou de uma faculdade

---

30 Burrell, Jenna, (nota 28); Rielli, Mariana Marques, (nota 25), p. 443.
31 Burrell, Jenna, (nota 28); Rielli, Mariana Marques, (nota 25), p. 443.
32 Edwards, Lilian / Veale, Kichael, «Slave to the Algorithm? Why a "Right to an Explanation" is Probably not the Remedy You Are Looking For», *Duke Law & Technology Review*, n. 16, 2017, p. 18 s.
33 Nesse sentido, a proposta de Chesterman, «Through a glass darkly: artificial intelligence and the problem of opacity», 2020, http://ssrn.com/abstract=3575534, acesso em 24-6-2021.
34 Cf. Cordeiro, Barreto Menezes (nota 16-2), p. 220 s.
35 Cordeiro, A. Barreto Menezes (nota 24), p. 266.
36 GT Artigo 29.º (nota 16), p. 22.
37 GT Artigo 29.º (nota 16), p. 23.
38 Cordeiro, A. Barreto Menezes (nota 24), p. 267.

jurídica primária[39]. De acordo com o grupo de trabalho do artigo 29.º, a decisão apenas será relevante se os efeitos tiverem um impacto grave[40].

A afetação significativa e similar dos interesses do titular do direito determina, igualmente, a proibição de decisões automatizadas. O Grupo de Trabalho do artigo 29.º considera que, "mesmo nos casos em que não há alterações nos seus direitos ou obrigações legais, o titular dos dados pode, contudo, sofrer um impacto suficiente para solicitar as proteções garantidas pela disposição em análise"[41].

Mais acrescenta que "o RGPD introduz o termo «de forma similar» [...] junto da expressão «afete significativamente». Por conseguinte, o limiar de importância deve ser similar ao da decisão que produz efeitos jurídicos".

Não cremos, no entanto, que a similitude a que se refere o preceito tenha por referente o grau de importância da afetação. Se esta é pressuposta, também, quando é afetada uma posição jurídica subjetiva, o alargamento potenciado pela parte final do preceito apenas se justifica quando a analogia das situações o determine. Dito de outro modo, a afetação de forma similar implica que se estabeleça uma analogia bastante, de tal modo que, não se pondo em causa um direito ou uma faculdade jurídica, seja lesado um interesse digno de proteção que subjaza à tutela dos dados pessoais. Há de, portanto, convocar-se uma lógica de preenchimento da responsabilidade — ainda que de responsabilidade civil não se trate — procurando saber se o interesse lesado se pode ou não reconduzir ao núcleo fundamental de proteção dispensado pelo direito à proteção de dados.

A ideia de que a afetação tem de ser significativa implica, de acordo com a escalpelização oferecida pelo GT artigo 29.º, que a decisão afete "significativamente as circunstâncias, o comportamento ou as escolhas das pessoas em causa"; tenha "um impacto prolongado ou permanente no titular dos dados", ou dê "origem a uma exclusão ou discriminação das pessoas"[42].

Em rigor, a explicitação das hipóteses apresentadas pelo grupo de trabalho, acompanhada dos exemplos que nos oferecem — "decisões que afetem a situação financeira de uma pessoa, designadamente a sua elegibilidade para obtenção de crédito; decisões que afetem o acesso de uma pessoa aos serviços de saúde; decisões que impeçam o acesso de uma pessoa a uma oportunidade de emprego ou a coloquem em séria desvantagem; decisões que afetem o acesso de uma pessoa à educação, como [...] o ingresso em estabelecimentos de ensino superior"[43] —, pode envolver, em termos técnico-jurídicos, atenta a amplitude do conteúdo de alguns direitos subjetivos, uma efetiva violação de posições jus-subjetivas ativas. Por exemplo, tratando-se de decisões que afetem o acesso de uma pessoa à educação ou o ingresso no ensino superior, são lesa-

---

39 Note-se que a própria lesão de um direito pode conduzir à constituição de uma relação jurídica. Contudo, pela diferente natureza das questões, autonomizamos em texto a hipótese.

40 GT Artigo 29.º (nota 16), p. 23.

41 GT Artigo 29.º (nota 16), p. 23.

42 GT Artigo 29.º (nota 16), p. 23.

43 GT Artigo 29.º (nota 16), p. 23.

das dimensões que se integram no âmbito do direito ao livre desenvolvimento da personalidade, tornando-se, então, complexa a questão de saber se tais direitos se integram ou não no âmbito de tutela da proteção de dados.

A mesma opinião é partilhada por *A. Barreto Menezes Cordeiro.* Nas palavras do autor, "não vemos que decisões possam afetar significativamente de forma similar os titulares dos dados, mas que não produzam efeitos na sua esfera jurídica ou que vedam a sua produção, ou seja, que não acionem a produção de efeitos jurídicos. De resto, os exemplos avançados pelo GT artigo 29.º relativos a esta segunda parte produzem, sem exceção, efeitos na esfera jurídica do titular"[44].

Problemática pode ser, a este nível, a questão da publicidade personalizada com base na definição de perfis, conduzindo ao fenómeno de *boxing* a que já nos referimos. O GT artigo 29.º, embora considere que o procedimento, em regra, não terá um impacto significativo nas pessoas, admite que tal possa ocorrer em função das características específicas de cada caso[45]. Designadamente, haveremos de ter em conta aspetos como "a dimensão intrusiva do processo de definição de perfis, nomeadamente o seguimento de pessoas em diferentes sítios *Web*, dispositivos e serviços; as expectativas e a vontade das pessoas em causa; a forma como o anúncio é apresentado; ou a utilização de vulnerabilidades conhecidas dos titulares de dados visados"[46].

A proibição não se aplica sempre que se verifique uma das hipóteses do artigo 22.º/2 RGPD, ou seja, sempre que a decisão seja a) necessária para a execução ou a celebração de um contrato; b) autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou se c) baseie no consentimento explícito do titular dos dados[47].

Sempre que tal ocorra, o responsável pelo tratamento deve procurar adotar medidas de salvaguarda do titular dos dados pessoais. Fundamental é o cumprimento do dever de informação, nos termos dos artigos 13.º e 14.º RGPD. Contudo, pelas limitações que o mesmo implica e a que já nos referimos, o titular dos dados tem direito a obter a intervenção humana e a contestar a decisão, de acordo com o artigo 22.º/3 RGPD. O responsável pelo tratamento deve garantir não só a possibilidade de o titular dos dados obter a intervenção humana e contestar a decisão, como ainda realizar uma avaliação periódica dos procedimentos.

De acordo com o parecer do GT do artigo 29.º, "devem efetuar avaliações frequentes aos conjuntos de dados que tratam, a fim de verificar que não existem enviesamentos, bem como desenvolver formas de dar resposta a eventu-

---

44 Cordeiro A. Barreto Menezes (nota 24), p. 268.
45 GT Artigo 29.º (nota 16), p. 24.
46 GT Artigo 29.º (nota 16), p. 24.
47 A natureza explícita do consentimento requereria considerações adicionais que não são consentâneas com a índole e a intencionalidade deste trabalho. Para outros desenvolvimentos, cf. Barbosa, Mafalda Miranda (nota 14), p. 125 s.

ais elementos prejudiciais, incluindo uma eventual dependência excessiva das correlações"[48].

A avaliação do impacto sobre a proteção de dados afigura-se fundamental, para cumprir as exigências de lealdade impostas pelo artigo 5.º RGPD, de acordo com o artigo 35.º RGPD.

As decisões automatizadas baseadas no artigo 22.º/2 RGPD apenas podem ter lugar quando estejam em causa dados sensíveis se, para além de se verificar uma das situações aí elencadas, houver consentimento explícito do titular dos dados, nos termos do artigo 9.º/a), ou se o tratamento se mostrar necessário por motivos de relevante interesse público, nos termos do artigo 9.º/g) RGPD.

5. UMA DECISÃO DISCRIMINATÓRIA: *QUID IURIS*?

Não obstante os níveis de proteção que são dispensados ao titular de dados pessoais, nada impede que, em concreto, possa emergir uma decisão automatizada discriminatória. Imaginando que estamos no âmbito das permissões abertas pelo artigo 22.º/2 RGPD, são várias as hipóteses em abstrato a considerar.

Havendo violação de deveres por parte do responsável pelo tratamento, coloca-se o problema de uma eventual responsabilidade subjetiva deste. Repare-se, aliás, que o artigo 82.º RGPD consagra uma presunção de culpa, entendida por muitos como uma presunção de *faute*, a incluir ainda uma presunção de causalidade[49]. Mas ela pode ser afastada se o *controller* vier provar que não é responsável pelo evento que gerou o dano, ou seja, que a lesão não lhe pode ser imputável[50].

---

48 GT Artigo 29.º (nota 16), p. 31.

49 Sobre o ponto, cf. Barbosa, Mafalda Miranda, «Covid-19 e plataformas de *streaming*: breve reflexão», *Revista de Direito Comercial*, ano 4, 2020, p. 989 s.

50 O regulamento europeu prevê, no artigo 82.º, que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do referido regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. Acrescenta o n.º 2 do preceito que qualquer responsável pelo tratamento que nele esteja envolvido é responsável pelos danos causados por um tratamento que viole o presente regulamento, sendo o subcontratante responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações impostas pelo regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento. Esta responsabilidade pode ser afastada se o responsável pelo tratamento ou o subcontratante provar que não é responsável pelo evento que deu origem aos danos. Havendo mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, que sejam responsáveis por danos causados pelo tratamento, cada um é responsável pela totalidade dos danos, prevendo-se no n.º 5 do artigo 82.º a possibilidade de exercício do direito de regresso em relação à parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano em conformidade com a regra estabelecida no n.º 2. Torna-se, assim, inequívoco que o Regulamento 2016/679 consagra uma regra de solidariedade obrigacional entre os corresponsáveis, ao mesmo tempo que parece inverter o ónus da prova, a partir do momento em que se constata a violação das obrigações por ele impostas. As soluções são de aplaudir, não só pelo cunho protetivo do titular dos dados que apresentam, como porque parecem resultar do funcionamento das regras ressarcitórias, quando entendidas numa ótica personalista.

Significa isto que, resultando a lesão do normal funcionamento do algoritmo utilizado para a decisão automatizada e não havendo violação de quaisquer deveres por parte do responsável pelo tratamento, a responsabilidade que se poderia desenhar exclui-se.

Coloca-se, portanto, o problema de saber a quem pode ser imputada a lesão ou, dito de outro modo, quem pode ser responsabilizado pelos prejuízos sofridos pelo titular dos dados pessoais.

Rejeitando-se, *a priori*, uma eventual responsabilização do *software*[51], inexistindo culpa da parte do *controller*, a única alternativa viável é procurar fundar a responsabilidade objetivamente. Ora, também nesse domínio parece haver limitações evidentes.

Mobilizando a responsabilidade do produtor, deparamo-nos necessariamente com dificuldades óbvias. Desde logo, porque o criador do *software* pode não coincidir com o seu programador e com o *controller*, teremos de alterar a perspetiva responsabilizatória. Por outro lado, suscitam-se dúvidas quanto à qualificação do algoritmo como um produto. E se essas podem ser facilmente ultrapassadas, por a doutrina, há largo tempo, admitir a qualificação dos *softwares*

De facto, a partir do momento em que um determinado sujeito lida com dados alheios, assume uma esfera de risco/responsabilidade, devendo adotar as medidas de cuidado — consagradas pelo legislador — no sentido de garantir a sua incolumidade. Não o fazendo, a primitiva esfera de responsabilidade (*responsabilidade pelo outro, ou pelos dados do outro*) convola-se numa outra esfera, mais ampla, de responsabilidade, no sentido da *liability* (*responsabilidade perante o outro*). A esta esfera são reconduzidos todos os danos-lesão que deveriam ser obviados pelo cumprimento do dever legal imposto, pelo que, a priori, cada interveniente no tratamento dos dados responderá pela totalidade do dano verificado em face do sujeito lesado. Posteriormente, pelo confronto entre a esfera de risco/responsabilidade do lesante e outras esferas de risco, aquele primitivo nexo imputacional que se desenha concretiza-se, podendo em concreto excluir-se ou conjugar-se com outros.

Para outros desenvolvimentos, cf. Barbosa, Mafalda Miranda, «Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil», *Revista de Direito Comercial*, ano 2, 2018, p. 416 s. (=«*Data controllers* e *data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil», *Revista da Banca, Bolsa e Seguros*, n. 3, 2018, p. 147 s.)

51 Tal responsabilização — exceto se correspondesse à imposição de uma forma de responsabilidade objetiva a um sujeito determinado ou à comunidade em geral (hipótese securitária que *ad limine* rejeitamos, por empobrecedora do sentido do direito) — pressuporia, necessariamente, a personalização/subjetivação do algoritmo. Contudo, rejeitamos liminarmente a perspetiva. Por um lado, não é possível justificá-la à luz de uma qualquer analogia com a personalidade jurídica das pessoas humanas, que repousa na ineliminável dignidade ética do ser humano, que inexiste por referência aos algoritmos; por outro lado, mesmo sabendo que a personalidade jurídica das pessoas coletivas é funcionalizada, o expediente explica-se pela necessidade de encontrar um mecanismo que melhor prossiga interesses humanos. Ora, o único interesse que se consegue desvelar na responsabilização do algoritmo é a desresponsabilização de algum ou alguns sujeitos, numa clara contradição com o sentido da juridicidade de onde se parte. Para outros desenvolvimentos, cf. Barbosa, Mafalda Miranda, «Inteligência artificial, *e-persons* e direito: desafios e perspetivas», *Estudos de Direito do Consumidor*, n.16 (número especial Direito e Robótica), 2020, p. 57 s.; Barbosa, Mafalda Miranda, «Nas fronteiras de um admirável mundo novo? O problema da personificação de entes dotados de inteligência artificial», *Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa* (coord. Mafalda Miranda Barbosa/Filipe Braga Netto/Michael César Silva/José Luiz de Moura Faleiros Júnior), Editora Foco, 2021, p. 97 s.

como produtos[52], perguntar-se-á se efetivamente existirá um defeito, dado que a decisão discriminatória pode resultar (e resulta) do normal funcionamento do algoritmo.

Além disso, o produtor não responde pelos riscos de desenvolvimento. Ou seja, não haverá responsabilidade se, no momento da entrada em circulação, o estado da ciência e da técnica não permitiam tornar o defeito cognoscível. Do mesmo modo, não haverá responsabilidade se o defeito inexistir no momento da entrada do produto em circulação. Lidando-se com entes dotados de inteligência artificial, isto é, lidando-se com um domínio onde, por um lado, os avanços tecnológicos são constantes e, por outro lado, sabendo-se que os entes dotados de inteligência artificial podem alterar, por força da interação com o meio, os dados da pré-programação, pode não ser possível detetar, de acordo com o dito estado da ciência e da técnica, o defeito, ao mesmo tempo que a falta de segurança pode resultar *a posteriori*, fruto da característica intrínseca ao *software* de autoaprendizagem e autodesenvolvimento.

De notar que isto não significa — neste domínio, como noutros — que o produtor esteja dispensado de um dever de vigilância sobre a coisa, depois da sua introdução no mercado (depois da sua colocação em circulação). Nos termos do DL n.º 69/2005, o produtor fica não só obrigado a apenas colocar produtos seguros no mercado, como, de acordo com o artigo 6.º/1/b) DL n.º 69/2005, deve adotar todas as medidas necessárias para, em função das características do produto, se informar sobre os riscos que o produto possa apresentar e para desencadear as ações que se revelarem adequadas, incluindo a retirada do produto do mercado, o aviso aos consumidores em termos adequados e eficazes ou a recolha do produto junto destes. O produtor tem, no quadro de uma obrigação geral de segurança a que está vinculado, o dever de cumprir uma obrigação de acompanhamento do produto. Simplesmente, a violação desta obrigação desencadeia responsabilidade civil de acordo com o regime geral e não de acordo com a disciplina da responsabilidade do produtor que temos vindo

---

[52] Alguma doutrina estrangeira questionou a possibilidade de se ver no *software* uma coisa corpórea, numa posição que acabaria por ser rejeitada. Cf., sobre o ponto, Voit, Wolfgang / Geweke, Götz, «Der praktische Fall — Bürgerliches Recht: Der tükische Computervirus», *Juristische Schulung*, 2001, p. 362; Bydlinski, P., «Der Sachbegriff im elektronischen Zeitalter: zeitlos oder anoassungsbedürftig?», *Archiv für die civilistische Praxis*, 1998, p. 305. Entre nós, dando conta do problema, Cordeiro, A. Menezes, *Tratado de Direito Civil*, III, 4.ª edição (com a colaboração de A. Barreto Menezes Cordeiro), Almedina, Coimbra, 2019, p. 174. Veja-se, ainda, Silva, J. Calvão da, *Responsabilidade civil do produtor*, Almedina, Coimbra, 1999, p. 613, nota 3. Para outros desenvolvimentos do nosso pensamento, cf. Barbosa, Mafalda Miranda, «Responsabilidade civil por danos causados por entes dotados de inteligência artificial», Direito *Digital e Inteligência Artificial: Diálogos entre Brasil e Europa* (coord. Mafalda Miranda Barbosa/Filipe Braga Netto/Michael César Silva/José Luiz de Moura Faleiros Júnior), Editora Foco, 2021, p. 157 s.; Barbosa, Mafalda Miranda, «O futuro da responsabilidade civil desafiada pela inteligência artificial: as dificuldades dos modelos tradicionais e caminhos de solução», *Revista de Direito da Responsabilidade*, ano 2, 2020, p. 280 s. (= «O futuro da responsabilidade civil desafiada pela inteligência artificial: as dificuldades dos modelos tradicionais e caminhos de solução», *Revista de Direito Civil*, ano V, tomo 2, 2020, p. 261 s.).

a acompanhar[53], e sabemos já que, no tocante à culpa, a inteligência artificial coloca inúmeros desafios.

A Resolução do Parlamento Europeu adotada em 23-1-2020, no que respeita aos processos de decisão automatizados, garantindo a proteção do consumidor e a livre circulação de produtos e serviços, reconhece que a emergência de produtos com capacidade de tomar decisões automatizadas coloca novos desafios, na medida em que tais produtos podem atuar de um modo que não estava previsto quando foram colocados no mercado, e solicita à Comissão Europeia, entre outras coisas, que adote propostas para adaptar as regras atinentes à obrigação geral de segurança a esses mesmos desafios[54].

Do mesmo modo, o Livro Branco sobre a inteligência artificial[55] reconhece que "a legislação da UE em matéria de segurança dos produtos centra-se essencialmente na colocação dos produtos no mercado. Embora na legislação da UE em matéria de segurança dos produtos o software, quando faz parte do produto final, deva cumprir as regras pertinentes em matéria de segurança dos produtos, é uma questão em aberto se o software autónomo é abrangido pela legislação da UE em matéria de segurança dos produtos, fora de alguns setores com regras explícitas. A legislação geral da UE em matéria de segurança atualmente em vigor aplica-se aos produtos e não aos serviços e, por conseguinte, não se aplica aos serviços baseados em tecnologia com IA (por exemplo, serviços de saúde, serviços financeiros, serviços de transporte)". Impor-se-ia, por isso, alterações à obrigação geral de segurança, que já foram anunciadas pelas instâncias europeias[56].

Acresce que a responsabilidade do produtor é limitada no tipo de danos que permite indemnizar. Nos termos do artigo 8.º DL n.º 383/89, de 6 de novembro, só são ressarcíveis os danos resultantes de morte ou lesão pessoal e os danos em coisa diversa do produto defeituoso, desde que seja normalmente destinada ao uso ou consumo privado e desde que o lesado lhe tenha dado principalmente este destino. De fora ficam os danos puramente patrimoniais, o que significa que, no tocante a variadíssimas decisões discriminatórias, se perde a possibilidade de tutela do lesado por esta via.

Da mesma forma, os esquemas de responsabilidade independente de culpa consagrados no nosso ordenamento jurídico não permitem encontrar um ponto de apoio seguro para a resolução do problema, o que torna urgente — a este nível, como a muitos outros — a ponderação de uma específica hipótese de responsabilidade objetiva, a recair sobre o programador ou sobre o operador, consoante os casos, quando estejam envolvidos danos causados por algoritmos[57].

---

53 Este dado pode, contudo, ser extremamente importante na configuração da solução para estes problemas.

54 PE, *Draft motion for a resolution on automated decision-making processes: ensuring consumer protection and free movement of goods and services*, 2019/2915 (RSP).

55 COM (2020) 65 final (19-2-2020).

56 COM (2021) 205 final, *Coordinated plan on artificial intelligence 2021 review* (21-4-2021).

57 Nesse sentido, Barbosa, Mafalda Miranda (nota 50-1), p. 301 s.; e Barbosa, Mafalda Miranda (nota 50-1), p. 168 s.

A este propósito, a Resolução do Parlamento Europeu 2020/2014 (INL) oferece-nos importantes pistas, pese embora possa ser vista, em determinados aspetos, como uma oportunidade perdida.

Nos termos do artigo 2.º/1, a disciplina proposta cobre as hipóteses de dano à vida, à saúde, à integridade física de uma pessoa singular, à propriedade de uma pessoa singular ou coletiva ou de ocorrência de uma lesão imaterial significativa que cause um dano económico.

Sem embargo de o artigo 2.º/3 ressalvar a possibilidade de se fundar uma pretensão indemnizatória na responsabilidade do produtor, a responsabilidade, nos termos das recomendações do Parlamento Europeu, deve ser assacada ao operador, de acordo com um esquema dúplice. Inclui-se, aqui, quer o *frontend* quer o *backend operator*. O primeiro surge definido como a pessoa singular ou coletiva que exerça um qualquer nível de controlo sobre um risco ligado ao funcionamento de um sistema de inteligência artificial e beneficie com tal operação; o *backend operator*, por seu turno, é a pessoa singular ou coletiva que, de forma contínua, define os recursos tecnológicos e providencia o acesso aos dados e um serviço de suporte necessário, de tal modo que também exerce um nível de controlo sobre o risco ligado ao funcionamento do sistema de inteligência artificial.

De acordo com o artigo 4.º/1, o operador é objetivamente responsável por qualquer dano que seja causado por uma atividade física ou virtual ou por qualquer processo que envolva inteligência artificial, desde que esteja em causa um sistema de alto risco (*high-risk AI system*), não podendo exonerar-se pela invocação de que atuou diligentemente ou que o dano ou lesão teriam sido causados por uma atividade autónoma ou processo conduzido por um sistema de inteligência artificial. A exclusão da responsabilidade ocorre unicamente por via da invocação da força maior.

Os sistemas de alto risco a que se aludem são definidos, nos termos do artigo 3º/c) como a potencialidade de um sistema de inteligência artificial causar danos a uma ou mais pessoas de maneira aleatória e de forma que ultrapasse o que é razoavelmente espectável, devendo constar obrigatoriamente do anexo de regulamento que é recomendado. A potencialidade a que se alude depende da gravidade do possível dano ou lesão, do grau de autonomia do sistema de decisão, da probabilidade de materialização do risco e do contexto de utilização do sistema de inteligência artificial.

Estando em causa uma hipótese de responsabilidade objetiva, a mesma surge associada à contratação de seguros, previstos no diploma, sendo limitada nos montantes indemnizatórios que, com base nela, podem ser arbitrados.

Em todas as outras situações que envolvem a utilização da inteligência artificial e não se configurem como sistemas de alto risco (*other AI-systems*), a responsabilidade do operador baseia-se na culpa. Pode, assim, nos termos do artigo 8.º/2, excluir-se a sua responsabilidade se provar a ausência de culpa, designadamente se se provar que o sistema de inteligência artificial foi ativado sem o seu conhecimento, apesar de terem sido adotadas todas as medidas razoáveis e necessárias para evitar tal ativação; que foi observada a diligência devida na execução de determinados processos, designadamente na seleção

do adequado sistema de inteligência artificial para o desempenho da função, no momento em que o sistema começou a operar, na monitorização das atividades, e na regular atualização do *software*. Do mesmo modo, excluir-se-á a responsabilidade com base na força maior. Mas não se excluirá a responsabilidade com base na ideia de que a lesão foi causada por uma atividade autónoma ou processo levado a cabo pelo processo de inteligência artificial. A responsabilidade subjetiva a que assim somos conduzidos, surge agravada e implica uma presunção de culpa.

Tal agravamento é notório, também, pelo facto de o operador responder pelos danos causados pela interferência de um terceiro no sistema de inteligência artificial, pela modificação do seu modo de funcionamento ou dos seus feitos, desde que aquele terceiro não seja identificado ou não tenha possibilidade de pagar a indemnização. Trata-se de uma hipótese de responsabilidade objetiva, por facto alheio, dependente de requisitos estritos, que obviamente não afasta a possibilidade de responsabilização, em geral, do operador nas hipóteses de lesão causada imediatamente por um terceiro, quando aquela interferência tenha sido potenciada pela violação de deveres de cuidado por parte do referido operador.

Num quadro normativo como este que as instâncias europeias recomendam, tornar-se-ia extremamente interessante analisar a posição ocupada por cada um dos sujeitos envolvidos no processo de decisão automática. Designadamente, atenta a natureza dinâmica do conceito de *controller* e *processor*, dever-se-ia indagar em concreto se o operador ou um dos operadores poderia assumir simultaneamente uma das qualidades referidas e, posteriormente, resolver os problemas atinentes ao concurso de fundamentos de uma mesma pretensão indemnizatória, por a mesma situação de base poder, numa hipótese como essa, ser assimilada por mais do que um regime de responsabilidade.

Sublinhe-se, ainda, que, na hipótese de responsabilização do agente por violação de deveres impostos pelo RGPD (ou na hipótese futura de possível responsabilização independente de culpa), não obsta à imposição de uma obrigação de indemnizar o facto de o titular dos dados ter dado o seu consentimento para a tomada de decisão exclusivamente automatizada. De facto, o consentimento para o tratamento de dados não implica quer a autorização para a obliteração dos deveres que oneram o *controller* (bem como o *processor*), quer a assunção de medidas discriminatórias e atentatórias de outros direitos para além do direito à proteção de dados. Quer isto dizer que, se se exclui a ilicitude do ponto de vista deste direito fundamental, pode não se afastar o caráter ilícito do ato do ponto de vista, *v.g.*, do direito à igualdade ou à identidade. Neste caso — verificável na ausência de esclarecimentos prévios acerca da possibilidade segura de a automatização redundar numa decisão discriminatória (porquanto, existindo informação acerca do ponto, o consentimento poderá abarcar a lesão dos direitos que subjazem à proteção de dados) —, teremos de relevar o comportamento do lesado no quadro da imputação e de uma eventual autocolocação em risco.

6. BREVE CONCLUSÃO: UMA NECESSÁRIA MUDANÇA DE PERSPETIVA

Os perigos que a inteligência artificial comporta para os dados pessoais — sem os quais aquela não pode sobreviver ou desenvolver-se — não podem ser combatidos unicamente à luz de uma ideia de transparência, como forma de resposta à opacidade que envolve os procedimentos. Outros pilares devem ser tidos em conta, exigindo-se uma especial atenção ao tópico da responsabilidade, não só no sentido da *liability*, mas também no sentido da *accountability*, que daquela difere na intencionalidade e na função. O programador deve mostrar-se apto a prestar contas, ou seja, a explicar retroativamente o uso dos algoritmos e a tomada de uma decisão específica. Um terceiro pilar assenta na avaliação do risco. Mas estes pilares só se tornam atuantes em termos subsidiários, quando esteja em causa uma decisão automatizada, na medida em que o primeiro plano de proteção do sujeito passa pela proibição de decisões automatizadas, sempre que afetem a esfera jurídica do titular dos dados.

A mesma lógica parece presidir à proposta de um Regulamento do Parlamento Europeu e do Conselho tendo em conta a necessidade de adoção de regras uniformes em matéria de inteligência artificial[58], que nos oferece uma *abordagem baseada no risco*, definindo três grandes níveis.

Nos termos do artigo 5.º, proíbem-se determinadas atividades que, implicando a utilização da inteligência artificial, envolvem um *risco considerado inaceitável*: sistemas de inteligência artificial que devolvem técnicas subliminares que afetem a consciência de uma pessoa, de modo a que, condicionando o seu comportamento, lhe possam causar um dano físico ou psicológico; que explorem alguma das vulnerabilidades de um específico grupo de pessoas devido à sua idade, fragilidade física ou mental, de modo a que, condicionando o seu comportamento, lhe possam causar um dano físico ou psicológico; que sejam colocados ao serviço das autoridades públicas para avaliar ou classificar as pessoas singulares, durante um determinado período de tempo, tendo em conta as suas características ou o seu comportamento social; que envolvem sistemas de identificação biométrica, em espaços acessíveis ao público, para efeitos de cumprimento da lei, exceto se tal for absolutamente imprescindível para prosseguir uma das finalidades prevista na al. d), do n.º 1, do artigo 5.º.

Paralelamente, configuram-se os chamados *sistemas de alto risco*, relativamente aos quais é imposto o cumprimento rigoroso de diversos deveres, antes de poderem ser colocados no mercado. Tais deveres orientam-se no sentido da supervisão humana e à disponibilização de informação. Os sistemas são qualificados como de alto risco, se cumprirem cumulativamente dois requisitos: o sistema de inteligência artificial destinar-se a ser utilizado como componente de segurança de um produtor ou se for ele próprio um produto, abrangido pela legislação de harmonização enumerada no Anexo II; e o produto ser subme-

58 COM (2021) 206 final, de 21-4-2021.

tido a uma avaliação de conformidade de terceiros, com vista à colocação no mercado do produto nos termos da legislação contida no Anexo II. Os sistemas de inteligência artificial identificados no Anexo III são igualmente considerados sistemas de alto-risco. Este elenco pode ser atualizado pela Comissão. Trata-se, nesse caso, de sistemas que envolvem um risco para a saúde ou a segurança ou um risco de um impacto adverso em direitos fundamentais, se esse risco é, tendo em conta a sua severidade e a probabilidade de ocorrência, equivalente ou superior ao risco de lesão colocado pelos sistemas de inteligência artificial já referenciados no dito anexo III.

Por referência a estes sistemas deve ser criado um sistema de gestão de risco, nos termos do artigo 9.º; devem ser adotadas regras específicas no que respeita à utilização de dados que sejam essenciais para o funcionamento do sistema; devem ser cumpridos especiais deveres de informação. São ainda definidas longas listas de deveres que impedem sobre os produtores, os distribuidores, os importadores, e os próprios utilizadores.

Num terceiro nível, encontramos os *sistemas de risco limitado*, aos quais são impostas obrigações específicas de transparência, e os *sistemas de risco mínimo*, relativamente aos quais não se colocam especiais exigências. Será o caso, por exemplo, dos filtros de spam ou de videojogos.

Parece, portanto, que a par das regras impostas pelo RGPD em matéria de proteção de dados pessoais, os perigos que a inteligência artificial comporta a este nível podem determinar a necessidade de específicas obrigações que reforcem os direitos dos sujeitos na necessária articulação entre os dois domínios.