UNIVERSIDADE CATÓLICA PORTUGUESA

Decisões automatizadas com recurso a algoritmos opacos: uma perspetiva legal

Miguel Ângelo Oliveira Nunes da Silva

Mestrado em Direito

Faculdade de Direito | Escola do Porto

Março de 2022

UNIVERSIDADE CATÓLICA PORTUGUESA

Decisões automatizadas com recurso a algoritmos opacos: uma perspetiva legal

Miguel Ângelo Oliveira Nunes da Silva

Orientação do Professor Doutor Nuno Sousa e Silva

Mestrado em Direito

Faculdade de Direito | Escola do Porto

Março de 2022

AGRADECIMENTOS

Endereço as minhas primeiras palavras de agradecimento ao Professor Doutor Nuno Sousa e Silva, pelos sábios ensinamentos que me transmitiu na unidade curricular de Direito da Propriedade Industrial no Mestrado, bem como pela atenção, disponibilidade e apoio na elaboração da presente dissertação.

Agradeço à minha família, de forma muito especial, aos meus pais. Sem eles, nada disto seria possível. Obrigado por me permitirem concretizar todos os objetivos e por estarem sempre presentes no meu percurso. Estarei eternamente grato.

Aos meus amigos, pelo apoio e pela amizade incondicional.

RESUMO

A presente dissertação tem como objetivo a análise legal das decisões automatizadas por algoritmos opacos, no sentido de expor os meios de tutela que o Direito da União confere aos cidadãos em matéria de proteção de dados pessoais e de que forma se podem defender e contestar estas decisões.

Em primeiro lugar, será feito um breve enquadramento do tema e clarificar-se-á conceitos relacionados com Big Data e decisões automatizadas, importantes à compreensão dos pontos que serão desenvolvidos.

Em segundo lugar, será estudado o Regime Geral da Proteção de Dados, em especial as bases legais para o tratamento de dados pessoais e as categorias especiais de dados.

Os dados assumem-se cada vez mais como um recurso poderoso para as empresas, em determinadas situações são até comercializados, o que se traduz em insegurança e desconfiança relativamente ao tratamento dos dados. Assim, importa perceber de que forma é que estes são tutelados e salvaguardados.

Posteriormente, será aprofundado o regime estipulado no artigo 22º do Regime Geral da Proteção de Dados que compõe o regime jurídico das decisões automatizadas.

Em seguida será abordada a problemática da opacidade dos algoritmos utilizados na tomada de uma decisão automatizada e o estudo da possibilidade de existir um direito a obter uma explicação. No contexto da opacidade dos algoritmos, será abordado também o papel dos direitos de propriedade industrial e a forma como o legislador europeu contorna possíveis problemas que estes podem trazer para a tutela dos direitos dos cidadãos.

Por último, será efetuada a análise da proposta de regulamento da inteligência artificial, com o intuito de perceber qual é a direção do legislador europeu neste contexto.

Palavras-chave: Algoritmos, Decisões Automatizadas, Inteligência Artificial, Inteligência Artificial Blackbox, Proteção de Dados, Direito da União Europeia,

ABSTRACT

This dissertation aims at the legal analysis of automated decision-making by opaque algorithms, in order to know the means of protection that European Union Law confers on citizens on the protection of personal data and how they can defend and challenge these decisions.

Firstly, a brief framework will be made of the theme. Concepts related to Big Data and automated decisions will be clarified, important to understanding the points that will be developed.

Secondly, the General Data Protection Regulation will be studied, the legal basis for the processing of personal data and the special categories of data. Data is increasingly becoming a powerful resource for companies, in certain situations they are even marketed, which translates into insecurity and mistrust regarding the processing of data. It is important to understand how they are protected and safeguarded.

Subsequently, the regime stipulated in article 22 of the General Data Protection Regulation will be deepened. It makes up the legal regime of automated decisions, which consists of decisions taken through technological means and without human intervention.

Next, the problem of the opacity of the algorithms used in automated decisions and the study of the possibility of there being a right to obtain an explanation will be addressed. In the context of the opacity of algorithms will also be attended the role of industrial property rights and how the European legislator circumvents possible problems that they can arise to the protection of citizens' rights.

Finally, the proposal for an artificial intelligence regulation will be carried out, to understand the direction of the European legislator in this context.

Keywords: Algorithms, Automated Decision-making, Artificial Intelligence, Blackbox Artificial Intelligence, Data Protection, European Union Law

ÍNDICE

INTRODUÇÃO

Atualmente, vivemos numa sociedade fundada na partilha de dados a grande velocidade. A cada segundo é partilhada uma quantidade astronómica de dados entre biliões de pessoas quer através da utilização direta da internet, por via de sites, de aplicações e redes sociais, quer na captação de informação através de outras vias como satélites, câmaras de videovigilância, etc. Toda esta informação é armazenada num arquivo com memória infinita.

Dos dados que são objeto de partilha destacam-se os dados pessoais. Estes são, atualmente, o bem mais valioso que possuímos. Nos tempos que correm todas as empresas tratam e processam estes dados para proveito próprio, com vista a obter lucro e vantagens concorrenciais no mercado. O tratamento destes dados é realizado recorrendo a algoritmos, alguns deles inteligentes que não pressupõe qualquer tipo de intervenção humana. Assim, podemos estar na presença de uma economia movida artificialmente, da qual não há qualquer tipo de conhecimento acerca do seu funcionamento. A este respeito referiu Alan Greenspan que os mercados operam, atualmente, por uma versão irremediavelmente opaca da "mão invisível" de Adam Smith e que ninguém, nem mesmo as entidades reguladoras, é capaz de ter mais que um mero vislumbre do funcionamento interno destes[1].

Os sistemas de inteligência artificial assumem um elevado grau de utilização na determinação de decisões, que podem ter efeitos jurídicos significativos na esfera dos destinatários. Por isso, urge a necessidade de haver uma tutela forte dos direitos dos titulares de dados assente na transparência e explicabilidade destas decisões[2].

O confronto entre as empresas e as autoridades públicas nacionais e internacionais centra-se nas fronteiras legais que regulam o processamento destes dados e das suas implicações. Por um lado, as empresas procuram um processamento de dados automatizado, sem grandes restrições, desburocratizado e pragmático assente nos sistemas de inteligência artificial e algoritmos. Por outro lado, a Comissão Europeia e os legisladores nacionais tendem a regular esta matéria assente na garantia da tutela dos direitos dos titulares de dados e na transparência das decisões automatizadas.

[1] Alan Greenspan, "*Dodd- Frank Fails to Meet Test of Our Times*," Financial Times, março de 2011

[2] Francesca Palmiotto Ettorre, "*Assessing Transparency and Explainability from a Legal Perspective*", fevereiro de 2022, disponível em: https://digi-con.org/the-right-to-contest-automated-decisions/

1. Big Data, definição de perfis e as decisões automatizadas

1.1. Big Data

Existem várias formas de definir e interpretar o conceito de Big Data, mas há uma conceitualização tripartida que tem ganho relevo. Podemos, sucintamente, definir Big Data como a informação (conjunto de dados) que contém muita variedade, que chega em grande volume e a elevada velocidade[3]. Esta definição é conhecida pelos "três V's".

Após descrevermos sumariamente o que é a Big Data, outra questão se coloca. Sendo a Big Data um conjunto de dados, de onde são provenientes estes dados? Qual é a fonte destes dados? A principal fonte destes dados é o lugar onde provavelmente procuraríamos a resposta a esta mesma questão - a Internet. Toda a atividade dos internautas é convertível em informação. Existem, obviamente, outras formas de reter informação quer através da Internet da Coisas (Internet of Things – IOT) quer através de meios mais tradicionais como as câmaras de videovigilância ou os satélites. Relativamente à Internet, os dados podem ser fornecidos pelo seu titular consciente ou inconscientemente[4], podendo, por exemplo, ser retirados através do seu comportamento online, localização geográfica ou IP. A recolha dos dados baseada no comportamento online do titular incide sobre o seu histórico de pesquisas e páginas visitadas, compras efetuadas e publicações, comentários ou reações nas redes sociais.

Os dados recolhidos são posteriormente analisados. A análise de dados pode ser feita diretamente pela entidade com quem o titular de dados está a contactar ou por prestadores de serviços contratados para o efeito. Atualmente, muitas empresas optam por esta última via pelo seu custo manifestamente reduzido e pela promessa de uma eficiência inigualável no tratamento de informação, suscetível de gerar avultados lucros, compondo uma questão complexa e com implicações sérias que será aprofundada mais à frente. A análise da Big Data afigura-se extremamente importante. Esta serve fins como a publicidade comportamental, a previsão e adequação de preços, a previsão da probabilidade de cumprimento de contratos de mútuo, a avaliação de risco, o cálculo da probabilidade de reincidência de criminalidade pelos

[3] Laborde, Rebecca, "*The Three V's of Big Data: Volume, Velocity, and Variety*", janeiro de 2020 disponível em: https://blogs.oracle.com/health-sciences/post/the-three-vx27s-of-big-data-volume-velocity-and-variety

[4] Relativamente à facultação de dados, estes podem ser fornecidos pelo seu titular conscientemente quando o sujeito é informado com tempo e de forma clara que os seus dados serão recolhidos, armazenados e tratados. Os dados são facultados, de forma inconsciente, quando tal não se verifica.

tribunais[5] e da probabilidade de sucesso de uma ação judicial[6], a previsão de locais mais propensos à ocorrência de crimes[7] e a seleção de candidatos a um posto de trabalho[8].

1.2. Definições de Perfis e decisões automatizadas

Com o intuito de clarificar algumas noções importa explicitar alguns conceitos que se revelarão fulcrais para uma melhor compreensão dos pontos seguintes.

No número quatro do seu artigo 4º, o Regulamento Geral sobre a Proteção de Dados (doravante designado RGPD) conceitualiza a definição de 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". De um modo geral, a definição de perfis acarreta três fases distintas: a recolha de dados, a análise dos dados para recolher correlações e aplicação das correlações a uma pessoa no sentido de identificar características comportamentais presentes ou futuras. A grande finalidade de uma definição de perfis é agrupar os titulares de dados em categorias e/ou grupos para análise e previsão dos seus interesses.

A título de exemplo, pensemos num corretor de dados que recolhe dados de várias fontes. Depois de recolher os dados, analisa os mesmos para definir perfis relativos às pessoas e criar categorias. O corretor de dados procede à definição de perfis, inserindo uma pessoa numa determinada categoria de acordo com os seus interesses. Por último, vende essa informação a empresas que desejem melhorar a adequação dos seus bens e serviços ao público-alvo.

Neste processo de definição de perfis podem realizar-se ou não decisões automatizadas. As decisões automatizadas serão analisadas mais adiante, aquando do escrutínio do seu regime

---

[5] Karen Hao, "*AI is sending people to jail—and getting it wrong*", MIT Technology Review, janeiro de 2019, disponível em: https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/

[6] Renato Lovato Neto*, Responsabilidade civil do advogado por perda de chance processual*, Dissertação de Doutoramento, Porto, Faculdade de Direito da Universidade do Porto, 2018 (inédita), p. 717 e ss.

[7]Claude Castelluccia; Daniel Le Métayer; Parlamento Europeu, *Understanding algorithmic decision making: opportunities and challenges*, 2019, p. 9, disponível em: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)624261

[8]Charles Hymas, *AI used for first time in job interviews in UK to find best applicants*, setembro de 2019, disponível em: https://www.telegraph.co.uk/news/2019/09/27/ai-facial-recognition-used-first-time-jobinterviews-uk-find

legal, o artigo 22º do RGPD. As decisões exclusivamente automatizadas correspondem à capacidade de tomar decisões através de meios tecnológicos e sem intervenção humana.

As decisões automatizadas podem basear-se em qualquer tipo de dados, como, por exemplo, em dados fornecidos diretamente pelas pessoas em causa (por exemplo, respostas a um questionário), dados observados por diferentes meios (internet, satélites, videovigilância, etc) acerca das pessoas (por exemplo, dados sobre a localização recolhidos através de uma aplicação) e/ou dados inferidos através de correlações, tais como um perfil de uma pessoa que já tenha sido criado. Um exemplo[9] de uma decisão automatizada é a aplicação de uma coima por excesso de velocidade com base, exclusivamente, em provas obtidas através de um radar de velocidade. Neste caso, nem sequer implica a definição de perfis. No entanto, passaria a constituir uma decisão tomada com base na definição de perfis se os hábitos de condução da pessoa tivessem sido alvo de um controlo, ao longo do tempo, e o montante da coima aplicada resultasse de uma avaliação que tivesse em conta outros fatores, como a reincidência ou não do excesso de velocidade ou o facto de o condutor ter incorrido recentemente em infrações rodoviárias.

Também poderá haver definição de perfis numa decisão que não seja exclusivamente automatizada. Por exemplo, os bancos antes da concessão de um crédito hipotecário, podem ter em atenção a pontuação de crédito do mutuário através de uma intervenção humana, de modo a tomarem a decisão. Tal também poderia acontecer sem intervenção humana significativa, constituindo uma decisão exclusivamente automatizada, o que levanta uma série de questões a vários níveis, visto que a concessão ou não de um crédito hipotecário é uma decisão com impacto na vida jurídica de uma pessoa.

Importa referir que a definição de perfis tem um papel cada vez mais importante na economia atual. Segundo dados da Eurostat, em 2020, um número significativo de empresas portuguesas e europeias compostas, no mínimo, por 250 trabalhadores, indicaram recorrer à análise de Big Data[10]. Como foi referido num dos exemplos acima, existe uma necessidade crescente das empresas conhecerem melhor os seus utilizadores/consumidores e de adequarem os bens e serviços prestados ao seu público-alvo. Ora, tal necessidade poderá ser atendida através da

[9] Exemplo retirados dos esclarecimentos dados pelo Grupo de Trabalho 29, o Grupo de Trabalho para a proteção das pessoas no que diz respeito ao tratamento de dados pessoais, em "Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679", disponíveis em: https://ec.europa.eu/newsroom/article29/items/612053

[10] Eurostat, https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_eb_bd&lang=en

análise de dados e da compra, por parte das empresas, de dados tratados e geralmente já agrupados em perfis. Para uma melhor compreensão deste fenómeno importa referir um conceito relevante neste contexto - publicidade comportamental. Este tipo de publicidade baseia-se nos interesses dos consumidores. Os interesses são partilhados através de um simples clique num website que determina a divulgação do histórico de pesquisa a terceiras entidades, vulgo, em inglês, third parties. Os interesses partilhados são agrupados num perfil e os consumidores recebem publicidade que corresponde aos seus interesses[11].

Podemos concluir que vivemos numa economia de dados. Os dados assumem-se cada vez mais como um recurso poderoso para as empresas, em determinadas situações são até comercializados. Tudo isto parece gerar uma certa relativização dos dados pessoais o que se traduz em insegurança e desconfiança relativamente ao tratamento dos nossos dados.

Assim, é fundamental perceber de que forma é que estes são tutelados e salvaguardados.

2. Regime Geral de Proteção de Dados

Como tem sido aqui referido, os dados pessoais assumem uma real importância multidisciplinar na atualidade. Os dados constituem um valor fundamental para muitas empresas, tanto que até já foram considerados como o "novo petróleo"[12].

A partilha destes dados a um nível gigantesco entre diferentes entidades, sem regulamentação devida, conduziria a uma total indiferença para com os seus titulares, quase como se os dados deixassem de lhes pertencer. Assim, urge a necessidade preeminente de proteção destes dados.

Neste contexto, a Comissão Europeia criou um regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados – o Regulamento Geral sobre a Proteção de Dados. Conforme está plasmado no seu artigo 1º, este regulamento tem como objetivo "defender os direitos e liberdades fundamentais das pessoas singulares, nomeadamente, o direito à proteção dos dados pessoais".

[11] No entendimento de Susana Navas Navaro em "*La personalidad virtual del usuario de internet*", a definição de perfis pretende criar uma relação pessoal com o consumidor/usuário da Internet, de modo que este se sinta como em sua casa, que sinta experiência e sentimentos.

[12] Frase, originalmente em inglês, "Data is the new oil", foi uma inspiração do matemático londrino, especialista em ciência de dados, Clive Humby.

O RGPD aplica-se ao tratamento de dados pessoais efetuado por responsável, ou por um subcontratante, situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União, de acordo com seu artigo 3º. Este regulamento aplica-se também a uma empresa constituída fora da União Europeia (doravante designada UE), mas que ofereça bens/serviços (pagos ou a título gratuito) ou que controle o comportamento de pessoas na UE.

De modo a exemplificar esta última situação, pensemos numa empresa sediada no Alasca, ativa na área dos serviços de tradução que opera na internet e dirige a sua atividade, principalmente, em Portugal e Espanha em que os utilizadores deste site de modo a inscreverem-se no mesmo, fornecem os seus dados aquando do preenchimento de um formulário de inscrição.

Relativamente ao âmbito de aplicação material do regulamento, ou seja, a matéria a que este regulamento se destina, o artigo 2º do RGPD reitera o seguinte: "aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados." Importa salientar que o regulamento se aplica apenas a dados pessoais. Neste aspeto, o Considerando 13 de tal regulamento informa que o RGPD não diz respeito a dados das empresas ou outras pessoas coletivas, excetuando o caso das informações respeitantes a empresas unipessoais que possam constituir dados pessoais caso permitam a identificação de uma pessoa singular. Ainda, neste contexto, as regras também se aplicam a todos os dados pessoais relacionados com pessoas singulares no âmbito de uma atividade profissional[13].

2.1. As bases legais para o tratamento de dados pessoais

Conforme o artigo 6º do RGPD, o tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

(i) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

[13] Dados como endereços de correio eletrónico profissionais ou os números de telefone profissionais dos trabalhadores. A este respeito importa referir o caso *Manni* (Processo C-398/15), em que se abordou a possibilidade, para as pessoas singulares em causa, de pedir à autoridade encarregada da manutenção do registo, com base numa apreciação casuística e a título excecional, a limitação de acesso aos dados que lhes dizem respeito inscrito no registo da sociedade, a terceiros que demonstrem um interesse específico na consulta desses dados. Consultado em: https://curia.europa.eu/juris/document/document.jsf

(ii) 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;

(iii) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

(iv) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

(v) 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;

(vi) 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.

Relativamente ao conceito de "consentimento", para além do que está disposto no artigo 7º do RGPD, é imperativo fazer algumas ressalvas. O RGPD contém no número onze do seu artigo 4º a definição de consentimento. Segundo este, o consentimento corresponde a uma "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento". O consentimento relaciona-se com o exercício do direito à autodeterminação informacional, que é um direito constitucionalmente consagrado no artigo 35º da Constituição da Républica Portuguesa. O direito à autodeterminação informacional dá "a cada pessoa o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em "simples objeto de informação"[14].

O consentimento é a melhor forma do titular dos dados controlar os seus dados pessoas, mas revela-se de suma importância que o titular tenha uma consciência real do seu consentimento, caso contrário, esta concessão por parte do titular de dados constitui apenas uma mera falsa ideia de controlo. A realidade é que na maioria dos casos (pense-se nos sites, por exemplo) a solicitação do consentimento não é intuitiva, vem acompanhada de um vasto número de solicitações e de quantidades exageradas de informação que levam ao desinteresse do titular de dados que dá o seu consentimento sem que este seja válido, representando uma manifestação de vontade que não corresponde à realidade. Nas palavras de Alessandro Moretti:" a

[14] Gomes Canotilho/Vital Moreira, *Constituição da República Portuguesa Anotada*, vol. 1, Coimbra: Coimbra Editora, 2007 (4.ª ed.), p. 551).

manifestação de vontade traduzir-se-á num exercício meramente aparente da liberdade de autodeterminação informacional"[15].

Outro ponto que importa esclarecer refere-se à necessidade de tratamento para "efeitos dos interesses legítimos". O artigo 6º, nº1, f) do RGPD admite que o tratamento de dados pessoais poderá ser efetivado na prossecução de um interesse legítimo do responsável pelo tratamento ou de terceiro. Um interesse é considerado legítimo quando após uma cautelosa ponderação dos interesses em jogo, podermos concluir que o interesse em questão prevalece sobre os direitos e liberdades fundamentais do titular que demandem a proteção dos dados pessoais. Assim, a necessidade do tratamento para a prossecução do determinado interesse legítimo terá que suplantar os efeitos lesivos nos direitos e liberdades do titular dos dados. Importa salientar que nos casos em que a operação de tratamento tenha como fundamento um interesse legítimo do responsável pelo tratamento, recai sobre este a obrigação legal de comunicar ao titular dos dados quais os interesses prosseguidos, por si ou por terceiro, independentemente de os dados serem ou não recolhidos junto do titular, ao abrigo do artigo 13º/ nº1, d) e artigo 14º/ nº2, b) do RGPD.

2.2. As categorias especiais de dados

No artigo 9º do RGPD, o legislador europeu proíbe o tratamento de determinadas categorias de dados pessoais que constituem conteúdos informativos sensíveis que, por exemplo, numa tomada de decisões automatizadas, o seu tratamento poderia levar à produção de resultados discriminatórios para os titulares dos dados, futuros recetores da decisão. Aquilo que o RGPD denomina de "categorias especiais de dados" são os dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa". Pela sua natureza, estes dados requerem uma proteção mais forte. Desta forma, o RGPD consagra a proibição geral do tratamento deste elenco de dados, com um leque de dez exceções reconhecidas nas alíneas do número dois do seu artigo 9º.

[15] Moretti Alessandro (2018), *Algoritmi e diritti fondamentali della persona*, pp. 809-810

Posto isto, importa compreender a amplitude da proteção conferida pelo artigo 9º ao titular dos dados, ou seja, saber se a proibição é aplicável apenas ao tratamento direto destes dados sensíveis ou se abrange também o tratamento de dados correlacionados.

A este respeito, existem duas visões doutrinais que na opinião de Bryce Goodman e Seth Flaxman possuem deficiências práticas. Na visão minimalista, a proibição só engloba a utilização direta dos dados sensíveis, o que se traduz na ineficácia da mesma porque também permite que os dados sensíveis sejam tratados, embora de forma indireta. Por outro lado, na visão maximalista, a proibição inclui também o tratamento correlacionado e indireto dos dados sensíveis, o que é completamente impraticável, segundo estes autores[16].

Para estudar outras questões que envolvem as decisões automatizadas e o seu impacto na proteção de dados, revela-se importante aprofundar a análise no regime jurídico das decisões automatizadas.

3. O regime jurídico das decisões automatizadas

Como já referido anteriormente, as decisões exclusivamente automatizadas correspondem à capacidade de tomar decisões através de meios tecnológicos e sem intervenção humana.

O número um do artigo 22º do RGPD consagra o seguinte: "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." No número seguinte são enumeradas as exceções ao direito de não sujeição, isto é, o conjunto de situações em que a produção de efeitos por parte deste direito é excluída.

A analise meticulosa do artigo 22º do RGPD deve focar-se, em primeiro lugar, na explicitação do conjunto de conceito indeterminados presentes de modo a uma melhor compreensão do alcance da norma. Em segundo lugar, na explicitação da natureza jurídica do direito e de que forma é que produz os seus efeitos, e por último, na análise das suas exceções.

[16] Bryce Goodman, Seth Flaxman (2016), *European Union regulations on algorithmic decision-making and a "right to explanation*", pp. 53-55, disponível em: https://arxiv.org/pdf/1606.08813.pdf

3.1. A decisão automatizada e os efeitos da decisão

Enuncia-se que o titular de dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado que produza efeitos na sua esfera jurídica ou que afete significativamente de forma similar.

Primeiramente importa perceber o alcance do conceito de "decisão". Será que há um absoluto afastamento da intervenção humana? Se houver intervenção humana mínima e pouco significativa o "direito de não sujeição" não poderá ser exercido? A "decisão" consiste numa decisão final de um processo de tomada de decisão ou também se pode referir a um passo intermédio nesse processo? Qual terá sido a intenção do legislador europeu?

O RGPD só responde explicitamente apenas a uma destas questões. O Considerando 71 esclarece que o direito de não ficar sujeito a uma decisão "poderá incluir uma medida", assim sendo, uma decisão intermédia no procedimento será suscetível de integrar o disposto no seu artigo 22º, assumindo que a mesma resulta de um procedimento exclusivamente automatizado e que cause efeitos significativos na esfera do titular dos dados[17].

Foquemos a nossa atenção agora no alcance do conceito de "decisão". A norma apenas se refere às decisões tomadas exclusivamente com base no tratamento automatizado. No entanto, é fundamental esclarecer se há uma intenção do legislador europeu de afastar do âmbito da norma toda e qualquer decisão em que haja uma intervenção humana, ainda que pouco significativa e sem expressão na decisão final, ou apenas onde a intervenção é significativa. Esta é uma questão que divide a doutrina europeia. Por um lado, a doutrina que defende que uma mínima intervenção humana é suficiente para impedir a aplicação deste preceito, invoca como principal argumento o procedimento legislativo e a força da letra da lei. No processo de redação da disposição, discutiu-se incluir que a proteção se aplicasse também a situações em que os meios utilizados são "predominantemente" automatizados, desde que a intervenção humana não fosse muito significativa[18]. Contudo, tal nunca chegou a ser introduzido na versão adotada, o que

[17] Ronald Leenes, Rosamunde Van Brakel, Serge Gutwirth, Paul De Hert, (2017) *Data protection and privacy: the age of intelligent machines*, Oxford, Hart, p. 98

[18] Artigo 20.º do Relatório do Parlamento Europeu sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, de 21 de novembro de 2013 (A7-0402/2013)

parece indicar que o legislador europeu pretendeu, efetivamente, limitar o âmbito de aplicação da norma as decisões baseadas em meios exclusivamente automatizados.

Contudo, o Grupo de Trabalho do artigo 29º formado para ajudar na interpretação desta norma do regulamento, tem um entendimento diferente na definição concetual de "decisão". Este entendimento enquadra-se na perspetiva maioritária. O Grupo de Trabalho do artigo 29º determina a necessidade de proceder a uma interpretação extensiva do artigo 22º, devendo considerar-se compreendidas no seu âmbito de aplicação as decisões automatizadas nas quais tenha havido intervenção humana irrelevante. Se tal não acontecesse, o responsável pelo tratamento poderia eximir-se do disposto no artigo 22.º fabricando uma intervenção humana. Para que se considere haver uma intervenção humana, o responsável pelo tratamento deve garantir que qualquer supervisão da decisão seja relevante, e não um mero gesto simbólico[19].

Dissipadas as dúvidas relativamente ao conceito de "decisão", torna-se pertinente esclarecer quais são os efeitos (das decisões automatizadas) com relevância jurídica ou que afetem o titular dos dados significativamente de forma similar que fazem operar a proteção conferida pelo artigo 22º do RGPD. Neste sentido, o Grupo de Trabalho do artigo 29º (doravante, GT Art. 29º), relativamente aos efeitos com relevância jurídica, refere que para haver efeitos jurídicos, é necessário que a decisão, tomada exclusivamente com base no tratamento automatizado, afete os direitos de alguém.

É pertinente ainda clarificar que efeitos afetam o titular dos dados significativamente de forma similar aos efeitos jurídicos. Neste âmbito, o GT art. 29º sugere que a decisão é abrangida pelo artigo 22º se for suscetível de "afetar significativamente as circunstâncias, o comportamento ou as escolhas das pessoas em causa", se tiver "um impacto prolongado ou permanente no titular dos dados" ou se originar "uma exclusão ou discriminação das pessoas"[20].

3.2. Natureza jurídica do direito de não sujeição

O que importa perceber agora é a natureza jurídica deste direito, isto é, saber qual era a vontade do legislador europeu ao conferir ao titular de dados um direito de não sujeição a decisões

[19] Grupo De Trabalho Do Artigo 29.º, Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, p. 23
[20] Grupo De Trabalho Do Artigo 29.º, Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, p.24

automatizadas em determinadas circunstâncias. Numa interpretação à letra da lei, ficamos com a ideia que o legislador europeu pretende conferir ao titular dos dados um direito de não sujeição a decisões automatizadas em determinadas circunstâncias. Mas terá sido mesmo esta a vontade do legislador? Uma parte da doutrina acredita que sim. Segundo esta[21], o direito só produz efeitos se for exercido pelo titular de dados. Deste modo, as decisões automatizadas serão lícitas até ao momento em que o titular de dados exerça o seu direito de não sujeição. Neste contexto, para que o direito lhe seja conferido importaria que o titular de dados fosse devidamente informado que foi tomada uma decisão automatizada. O dever de informar o titular dos dados acerca da existência de decisões automatizadas recai sobre o responsável pelo tratamento de dados, como está previsto nos artigos 13.º/2, f) e 14.º/2, g) do RGPD. Assim sendo, estariam reunidas as condições necessárias à invocação desta proteção conferida pelo artigo 22.º RGPD.

No entanto, esta não é a visão da doutrina maioritária que está em consonância com os pareceres do Grupo de Trabalho do artigo 29º. Segundo estes, a proteção conferida pelo artigo 22º deve ser interpretada como "uma proibição geral da tomada de decisões com base exclusivamente no tratamento automatizado"[22] que se aplica independentemente de o titular dos dados adotar uma medida relativa ao tratamento dos seus dados pessoais. Desta forma, as decisões automatizadas serão, a priori, ilícitas, não estando a produção de efeitos subordinada ao exercício do direito por parte do titular de dados.

Importa ressalvar que a proibição não é absoluta e existem exceções consagradas no número dois do artigo 22º RGPD e que quando aplicadas, devem existir medidas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados[23]. Em primeiro lugar, o preceito não se aplicará se a decisão for necessária para a celebração ou para a execução de um contrato, nos termos do artigo 22.º, nº 2, a) RGPD. Neste contexto, argui-se que o responsável pelo tratamento de dados deve provar que não existe uma forma menos intrusiva de dar seguimento à celebração/execução do contrato, sob pena do tratamento não ser considerado

[21] Mendoza, Isak and Bygrave, Lee A., (2017), "*The Right Not to Be Subject to Automated Decisions Based on Profiling*", disponível em: https://ssrn.com/abstract=2964855

[22] Grupo De Trabalho Do Artigo 29.º, Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679

[23] O considerando 71 do RGPD consagra que tal tratamento deverá ser "acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão".

"necessário" para atingir tal finalidade e, consequentemente, ilícito[24]. A este respeito, o parecer do Grupo de Trabalho do artigo 29º arguiu que um tratamento "necessário para a execução de um trabalho" implicará mais que demonstrar uma maior eficiência e menos custos. Em segundo lugar, a proibição geral não ocorrerá quando essa decisão for autorizada pelo direito da União ou do Estado-Membro aplicável ao responsável pelo tratamento, mais propriamente, para o controlo e prevenção dos crimes de fraude e evasão fiscal[25]. Aqui, também estão previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados, de acordo com o artigo 22.º/2, b). Por último, o artigo 22.º/2, c), legitima a tomada de decisões automatizadas se houver consentimento explicito por parte do titular de dados.

3.3. Direito de oposição

O artigo 21.º confere ao titular dos dados o direito de oposição "a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito" nos casos em que o tratamento seja necessário por motivos de interesse público (artigo 6.º/1, al. e)), para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros (artigo 6.º/1, al. f)), ou ainda no caso em que os dados sejam tratados para uma finalidade distinta daquela para a qual foram recolhidos, nos termos do artigo 6.º/nº. 4, "incluindo a definição de perfis com base nessas disposições".

No entanto, este direito não é absoluto. A segunda parte do número um do artigo 21º RGPD refere que responsável pelo tratamento não terá que cessar o tratamento dos dados pessoais se apresentar "razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial". Que razões imperiosas e legitimas serão estas? O RGPD não esclarece, o que nos leva uma vez mais, a consultar o Grupo de Trabalho do artigo 29º. Segundo este, 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

[24] Buttarelli, Giovanni, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Autoridade Europeia para a Proteção de Dados, abril de 2017, disponível em: https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf

[25] O considerando 71 postula o recurso às decisões automatizadas definidas no artigo 22.º, n.º 1, para o controlo e a prevenção de fraudes e da evasão fiscal, ou para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento.

definição de perfis com vista a prever a propagação de doenças contagiosas"[26]. Acrescentando ainda, que deve haver um exercício de ponderação por parte do responsável pelo tratamento de dados de comparar os seus interesses com os direitos e liberdades do titular dos dados. No fundo, deverá sempre haver uma ponderação entre os interesses concorrentes do responsável pelo tratamento com o fundamento e a objeção do titular dos dados, assente em motivos de ordem pessoal, social ou profissional, por exemplo.

Importa salientar ainda que o artigo 21.º, n.º 2 RGPD, confere ao titular dos dados um direito de se opor ao tratamento dos seus dados pessoais para efeitos de comercialização direta, incluindo a definição de perfis, na medida em que esteja relacionada com a comercialização direta.[27] O responsável pelo tratamento tem de respeitar a vontade da pessoa sem questionar os motivos da objeção, não havendo lugar a ponderação de interesses como vimos anteriormente no referente "às razões imperiosas e legítimas".

4. A opacidade dos algoritmos utilizados na tomada de decisão automatizada e o possível direito a obter uma explicação

O RGPD tem como um dos seus princípios fundamentais, o princípio da transparência. Quer isto dizer que um dos campos de atuação fundamental do RGPD é a defesa da transparência dos procedimentos automatizados de tomadas de decisão, de modo a salvaguardar os dados pessoais dos seus titulares e protegê-los de possíveis danos que surjam como consequência desse processo de decisão.

Ora, como foi explicado previamente, uma decisão exclusivamente automatizada não tem intervenção humana. Quer isto dizer que o processo de tomada desta decisão é através de meios tecnológicos, e na maioria das vezes, com recurso a sistemas de inteligência artificial, como os algoritmos, por exemplo.

[26] Grupo De Trabalho Do Artigo 29.º, Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679

[27] O Considerando 70 do RGPD sustenta que "Sempre que os dados pessoais forem objeto de tratamento para efeitos de comercialização direta, o titular deverá ter o direito de se opor, em qualquer momento e gratuitamente, a tal tratamento, incluindo a definição de perfis na medida em que esteja relacionada com a referida comercialização, quer se trate do tratamento inicial quer do tratamento posterior. Esse direito deverá ser explicitamente levado à atenção do titular e apresentado de modo claro e distinto de quaisquer outras informações".

Um algoritmo pode ser definido, tecnicamente, como uma sequência lógica e finita (ou infinita, no caso dos algoritmos de aprendizagem automática) de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa. Um exemplo bastante utilizado na explicação de um algoritmo é equipará-lo a uma receita de culinária. Esta tem os ingredientes necessários (os dados de entrada ou inputs), tem o conjunto de passos necessários para realização da receita (instruções lógicas) até chegar ao prato final (o resultado ou outputs).

O RGPD regula o apenas tratamento de dados pessoais e não tem qualquer tipo de aplicação prática no desenvolvimento e comercialização de sistemas de inteligência artificial. Portanto, não poderia impor que todos os algoritmos fossem transparentes, nem tal se afigura uma tarefa simples devido às especificidades técnicas dos mesmos. Há algoritmos efetivamente transparentes, no entanto, quanto mais complexos e eficazes, de um modo geral, menos transparentes são. Reparemos, por exemplo, no caso dos algoritmos machine learning ou algoritmos de aprendizagem automática, em português. Estes algoritmos são, na sua generalidade, desenhados por empresas privadas, não "nascendo" transparentes. Os responsáveis pelo desenvolvimento do algoritmo, até podem saber a sequência de comandos iniciais, anteriores ao conjunto de comandos "machine-learning" que serão posteriormente adicionados aos algoritmos por estes mesmos, sem intervenção humana, à medida que a informação vai passando por estes.

Os sistemas de inteligência artificial, devido às suas especificidades técnicas, possuem, por vezes, "blackboxes", ou caixas pretas, em português. Num algoritmo, por exemplo, que possua uma blackbox, os seus inputs (dados de entrada) e o conjunto de instruções lógicas não são visíveis, apenas o resultado final é visível. Uma blackbox é impenetrável e este fenómeno é uma das principais preocupações no que à utilização de sistemas de inteligência artificial diz respeito. Atualmente, há uma grande pressão por parte das empresas para haver uma utilização a uma maior escala dos sistemas de inteligência artificial, no entanto, não há ainda uma regulação em vigor relativamente a estes sistemas. A este respeito, a Comissão Europeia apresentou uma proposta de regulamentação do desenvolvimento e da comercialização destes sistemas que será escrutinada adiante numa tentativa de perceber se há coadunação com a princípio da defesa transparência.

Posto isto, importa relacionar a problemática da opacidade das decisões automatizadas com os processos de tratamento de dados de modo a analisar os possíveis perigos que estas podem constituir e que mecanismos de tutela existem no que concerne aos direitos dos titulares de

dados que se encontram numa posição vulnerável e extremamente desequilibrada na relação que estabelecem com o responsável pelo tratamento dos seus dados. A este respeito, é de conhecimento geral a existência de uma tutela indemnizatória, no artigo 82º RGPD, quando o titular de dados sofre danos consideráveis que surgem das operações de tratamento de dados. No entanto, o contexto de fluxo de dados em constante análise, a natureza dos dados tratados e o impacto dos efeitos práticos e jurídicos que podem advir das operações de tratamento de dados reclamam uma tutela com mais garantias.

Neste sentido, naquele que é um dos mais afamados debates no que diz respeito ao regime legal das decisões automatizadas, tem sido argumentado por uma doutrina maioritária o reconhecimento, ao titular de dados, de um direito a obter uma explicação sobre as decisões automatizadas.

4.1. O direito a obter uma explicação sobre as decisões automatizadas

Primeiramente, importa explicitar que disposições do RGPD alimentam o debate acerca da possível existência deste direito e posteriormente analisar se há efetivamente bases legais suficientemente seguras para suportar tal direito e a sua fundada existência.

As disposições que alimentam o debate acerca da possível existência deste direito são os artigos 13.º/2, f), 14.º/2 g) e 15.º/1, h) do RGPD, que impõem ao responsável pelo tratamento de dados o dever de facultar ao titular dos dados informações sobre a "existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, nos números 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados". A chave para se tomar uma decisão sobre a questão do reconhecimento do direito de obter uma explicação sobre decisões automatizadas estará no estudo do alcance dos conceitos indeterminados presentes nestes preceitos, mais concretamente, "informações úteis relativas á lógica subjacente".

A expressão "lógica subjacente" conduziu à possibilidade de se "divulgar um algoritmo", ou seja, a divulgação da estrutura de comandos em linguagem informatizada que compõe o algoritmo. Ora, esta hipótese pode ser legalmente e tecnicamente complexa, na medida em que, estaremos perante dois tipos diferentes de blackboxes/opacidade: opacidade legal e opacidade

técnica, como defende Jenna Burrell[28]. Desde logo, este conjunto de comandos pode ser protegido por um direito de propriedade industrial, o que torna o algoritmo inacessível. Neste sentido, o Considerando 63 do RGPD informa que o direito conferido ao titular dos dados de conhecer e ser informado acerca do tratamento, nomeadamente sobre a lógica subjacente, não deverá prejudicar os direitos e liberdades de terceiros, "incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software". No entanto, acrescenta que tais considerações "não deverão resultar na recusa de prestação de todas as informações ao titular dos dados". Assim sendo, podemos concluir que a proteção conferida pelos direitos de propriedade industrial não será fundamento para recusa de informações, per si, embora possa trazer alguns entraves à defesa dos direitos dos titulares de dados como será matéria de análise no ponto seguinte. No que concerne há possível existência de um direito de explicação, os direitos de propriedade intelectual não obstam há divulgação de informações relativas aos algoritmos, em específico à divulgação da "lógica subjacente".

Mais se acrescenta que, se a explicação se consubstancia na divulgação do código, exige-se um grau elevado de literacia técnica, de modo a compreender o funcionamento do procedimento da tomada de decisão e avaliar o mérito da decisão. Quer isto dizer que se o titular de dados não tem conhecimentos técnicos a explicação de pouco ou nada lhe vai valer. O problema agrava-se na presença de algoritmos "machine learning" ou de aprendizagem automática devido à presença de "blackboxes". Como vimos, nestes casos nem mesmo o próprio responsável pelo seu desenvolvimento conseguirá explicar o procedimento naquela dada altura, visto que estes algoritmos processam quantidades astronómicas de informação e a sua lógica interna altera-se em função da sua evolução, dificultando ainda mais a compreensão do seu procedimento. Concluindo, nas palavras de Joshua A. Kroll, "ainda que a divulgação do código venha a ter alguma eficácia e não seja totalmente inócua, da interpretação do código não se conseguirá retirar uma análise dinâmica do funcionamento dos algoritmos perante dados reais e desconhecidos"[29]. Acrescente-se ainda que a revelação do algoritmo pode trazer efeitos indesejáveis se tal facilitar a sua manipulação por parte de utilizadores, podendo conduzir a efeitos perversos como a fraude. Assim, parece que a divulgação dos comandos lógicos de um algoritmo não é o instrumento mais adequado a garantir uma explicação ao titular de dados.

[28] Burrell, Jenna, "*How the machine 'thinks': Understanding opacity in machine learning algorithms*", 2016, pp 4-5, disponível em: https://journals.sagepub.com/doi/full/10.1177/2053951715622512

[29] Joshua A. Kroll , Joanna Huey , Solon Barocas , Edward W. Felten , Joel R. Reidenberg , David G. Robinson &Harlan Yu *Accountable Algorithms* p. 647, 2017, Disponível em: https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3

Uma outra abordagem a esta problemática, parte da expressão no seu todo, isto é através "informações úteis relativas à lógica subjacente", depreendendo que isto se poderá referir à divulgação da informação que incide sobre as categorias dos dados que serviram de inputs, a relação que se estabelece entre os inputs e os resultados, a informação sobre a importância relativa das diferentes características tidas em conta e os motivos pelos quais são consideradas relevantes e os inputs específicos que sejam determinantes no resultado final[30].

Ora tudo isto, parece ser demasiado complexo e profundamente técnico para que o titular de dados possa compreender com clareza a informação que lhe é prestado, contudo tal não pode servir como recusa de partilha da informação. Neste contexto, os pareceres do Grupo de Trabalho 29 indicam que "o responsável pelo tratamento deverá encontrar formas simples de comunicar ao titular dos dados a lógica subjacente, ou os critérios aplicados para tomar a decisão", mas "suficientemente completas para permitir ao titular dos dados compreender os motivos da decisão".

Embora não haja consenso sobre que informações deve incidir o direito de explicação, não se deve abandonar a ideia de que o mesmo deve existir e de que devem ser prestadas informações, acima de tudo, úteis. É inegável a necessidade do reconhecimento de um direito a obter uma explicação como meio de efetivação do princípio de transparência e defesa dos direitos do titular de dados.

Posto isto, assume real importância fazer um estudo da base legal que suporta este direito a obter uma explicação. Como foi referido anteriormente, parte da doutrina acredita que este direito é reconhecido através dos artigos nº 13.º/2, f), 14.º/2, g) e 15.º/1, h) do RGPD. Estas normas conferem aos titulares de dados o direito de dispor de informações relativas às decisões exclusivamente automatizadas, incluindo a definição de perfis, nomeadamente:

(i) a existência de decisões automatizadas, incluindo a definição de perfis,
(ii) informações úteis relativas à lógica subjacente, e
(iii) a importância e as consequências previstas de tal tratamento para o titular dos dados.

Primeiramente, importa saber qual é o momento da exigibilidade das informações. Será antes ou depois da tomada da decisão? Se os dados pessoais forem recolhidos junto do seu titular, o responsável pelo tratamento deverá facultar as informações no momento da recolha, de acordo

[30] Bryce Goodman, Seth Flaxman, (2016) *, European Union Regulations on Algorithmic Decision Making and a "Right to Explanation"*, p.55 Disponível em: https://arxiv.org/abs/1606.08813

com o artigo 13º, nº1 do RGPD. Neste caso, as informações são fornecidas em momento prévio ao da tomada de decisão e consequentemente de cariz geral e abstrato, relativas ao funcionamento do sistema, podendo incluir também consequências e informações específicas sobre o sistema[31]. Em contrapartida, nos casos em que os dados são não sejam recolhidos junto do titular, o responsável pelo tratamento de dados deve prestar as informações dentro dos prazos previstos no artigo 14º/3 do RGPD. Se durante este intervalo de tempo já tiver sido tomada uma decisão, o responsável pelo tratamento de dados não está impossibilitado de fornecer informações. Assim, estas informações poderão versar também sobre a funcionamento do sistema e mais especificamente sobre a decisão que foi tomada[32].

Relativamente ao conteúdo das informações, argumenta-se que quando o legislador se refere à exigibilidade da prestação de informações sobre as "consequências previstas" das decisões automatizadas, indica para informações relativas a uma decisão futura[33]. Ou seja, o legislador europeu parece estar a referir-se às consequências provocadas por uma decisão já tomada.

Para além disto, a doutrina que defende o reconhecimento do direito a obter uma explicação cita a menção expressa a este direito efetuado no Considerando 71 do RGPD. Segundo este: "tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão." Ora, os considerados não são vinculativos, estes têm apenas uma função de auxiliar na interpretação, têm um valor orientador, não consagram direitos ou impõe obrigações[34]. No entanto, não devemos negar a existência de um direito à explicação com base no facto de a única menção constar de um Considerando, tal seria uma posição demasiado rígida e estritamente semântica na ótica dos defensores desta doutrina.

Concluindo, de acordo com esta interpretação, o direito a obter informações úteis sobre uma decisão automatizada nos artigos 13.º/2, f), 14.º/2, g) e 15.º/1, h), deve ser entendido

---

[31] Sandra Watcher, Brent Mittelsdadt, Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 2017, p.78, disponível em: https://papers.ssrn.com/sol3/papers.cfm

[32] Sandra Watcher, Brent Mittelsdadt, Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 2017, p.78, disponível em: https://papers.ssrn.com/sol3/papers.cfm

[33] Sandra Watcher, Brent Mittelsdadt, Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,* 2017*,* p.83-84, disponível em: https://papers.ssrn.com/sol3/papers.cfm

[34] António Barreto Menezes Cordeiro, "*A interpretação dos regulamentos europeus e das correspondentes leis de execução: o caso paradigmático do RGPD e da lei n.º 58/2019*", in Revista de direito e tecnologia, vol. 1, n.º 2, 2019, p. 190 disponível em: https://blook.pt/publications/fulltext/fe04d9de6b48/

verdadeiramente como um direito a obter uma explicação. Esta interpretação vai de encontro ao espírito do diploma que visa segurar um "elevado nível de proteção de dados pessoais". No que às decisões automatizadas diz respeito e principalmente aquelas cuja tomada de decisão é diretamente efetuada por algoritmos inacessíveis, indecifráveis devido à presença de blackboxes, o apelo à transparência para já tem sido insuficiente, no entanto, este direito pode revelar-se importante no combate a problemas como a discriminação, por exemplo.

5. O apelo à transparência dos algoritmos e os direitos de propriedade intelectual

Até agora, a análise desta problemática tem vindo a ser feita de um ponto de vista da proteção do titular de dados e da defesa da transparência das decisões automatizadas com recurso a algoritmos, no entanto, importa também perceber o reverso da medalha. As empresas estão, na maioria das vezes, do outro lado do debate. Não quer isto dizer que estas procurem que as decisões automatizas sejam opacas, até porque as suas motivações em nada se relacionam diretamente com uma menor tutela dos direitos pessoais e maior liberdade de tratamento, mas sim com defesa dos seus investimentos. As preocupações empresariais não deixam de constituir um lobby preponderante no que concerne à legiferação de Direito da União Europeia em determinados aspetos, quer isto dizer que as empresas pretendem que haja uma regulação fundamentalmente mais pragmática e desburocratizada, como tem sido exemplo a pressão relativa à regulação da inteligência artificial.

Desde os primórdios da atividade económica que as empresas têm a necessidade de proteger os seus investimentos, inovações e criações. A proteção das inovações é efetuada através de direitos de propriedade industrial. Atualmente assistimos a uma digitalização económica crescente, implicando que haja uma partilha de dados muito maior, constituindo aquilo que muitos autores consideram uma "economia de dados". Sendo assim, as empresas desenvolveram métodos de analisar quantidades astronómicas de dados (Big Data) sob forma de algoritmos. Estes métodos são ferramentas úteis para as empresas pois possuem valor e devem ser protegidos. Existem formas de proteção destes algoritmos, mas implicam uma certa vontade e impulso por parte do empreendedor/criador, na medida em que terá que provar o secretismo destas ferramentas e do investimento canalizado para a sua criação. As empresas utilizam estes algoritmos para obter uma posição mais vantajosa no mercado através de uma

mais eficiente recolha e partilha de informação que leva a um maior conhecimento do mercado, público-alvo, padrões de consumo, necessidades do consumidor, por exemplo. As empresas mais bem preparadas e eficientes são aquelas que desenvolveram métodos de decisão automatizada e empregam analistas de dados nos seus quadros para o desenvolvimento das suas estratégias comerciais. Dito isto, torna-se mais fácil de perceber a importância dos sistemas de inteligência artificial, como os algoritmos, para o sucesso comercial de uma empresa.

5.1. Algoritmo como objeto de proteção por um direito de propriedade industrial

Numa abordagem inicial poderíamos pensar que a proteção dos algoritmos seria efetuada através de patentes e direitos de autor, talvez por serem os meios de proteção mais utilizados. Contudo, os algoritmos não podem ser protegidos através de nenhum destes direitos.

A Diretiva 2009/24/CE do Parlamento Europeu e do Conselho de 23 de abril de 2009 relativa à proteção jurídica de programas de computador estipula que "as ideias e princípios subjacentes a qualquer elemento de um programa de computador, incluindo os que estão na base das respetivas interfaces, não são protegidos pelos direitos de autor ao abrigo da presente diretiva." Sendo assim, a proteção de algoritmos através de Direitos de Autor encontra-se excluída. No que concerne à proteção através de patentes, a "Convenção da Concessão de Patentes Europeias" estipula no seu artigo 52º que "esquemas, regras e métodos para realizar atos mentais, jogar ou fazer negócios" não correspondem a uma solução para um problema técnico e por conseguinte não constituem objeto de proteção por parte de uma patente. A legislação portuguesa tem um entendimento semelhante. Embora, não possam ser protegidos por patentes ou direitos de autor, os algoritmos possuem valor e podem ser protegidos por outros meios legais igualmente eficientes.

Os algoritmos podem ser definidos como ferramentas "know-how"[35]. Neste sentido, podem ser protegidos ao abrigo da Diretiva (UE) 2016/943 do Parlamento Europeu e do Conselho de 8 de junho de 2016 relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais, transposta para o ordenamento jurídico português, na aprovação do novo Código da Propriedade Industrial

[35] Know-how pode ser definido como o conhecimento técnico, informação sobre como alcançar alguma vantagem técnica ou comercial sobre concorrentes, geralmente através de métodos ou processos de produção.

através da Lei n.º 65/2018 de 30 de novembro. Deste modo, os algoritmos devem ser considerados segredos comerciais e protegidos e de acordo com o artigo 313º do Código de Propriedade Industrial, devem preencher os seguintes requisitos:

(i) "Sejam secretas, no sentido de não serem geralmente conhecidas ou facilmente acessíveis, na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos, para pessoas dos círculos que lidam normalmente com o tipo de informações em questão;"

(ii) "Tenham valor comercial pelo facto de serem secretas;"

(iii) "Tenham sido objeto de diligências razoáveis, atendendo às circunstâncias, por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secretas"

Assim sendo, de modo a proteger estes algoritmos tem de haver um esforço por parte das empresas para adotar comportamentos que não ponham em causa o secretismo do algoritmo, de modo a preservar o seu valor e vantagem comercial[36], em consonância, também com o que é referido nas alíneas do número dois do artigo 39º do Acordo TRIPS[37].

Tal como os algoritmos usados para processar Big Data, também a informação recolhida pode e deve ser protegida. A informação não deixa de ser, em concreto, uma base de dados. As bases de dados podem ser protegidas. A sua estrutura é protegida por direitos de autor[38], mas o seu conteúdo, que aqui assume maior importância relevância, pode ser protegido pelo direito sue generis. A este respeito importa atentar à Diretiva 96/9/CE do Parlamento Europeu e do Conselho de 11 de março de 1996 relativa à proteção jurídica das bases de dados. Para uma base de dados ser objeto de proteção, o autor ou fabricante da base de dados deve ser residente ou nacional de um país da União Europeia. Como já foi referido anteriormente, o interessado em proteger a base de dados deve provar que teve de efetuar um esforço substancial (financeiro, material e/ou humano) para a criação e funcionamento da base de dados. Este direito sui generis fornece ao criador da base de dados o direito de a explorar exclusivamente, conferindo o direito

[36] Este esforço traduz-se por exemplo, numa encriptação, numa mudança regular de passwords, acordos de confidencialidade, cláusulas de não concorrência, etc.

[37] "The Agreement on Trade-Related Aspects of Intellectual Property Rights" ou em português "O Acordo Sobre os Aspetos dos Direitos de Propriedade Intelectual Relacionados ao Comércio"

[38] O número dois do artigo 10º do Acordo TRIPS plasma o seguinte: "As compilações de dados ou de outro material, legíveis por máquina ou em outra forma, que em função da seleção ou da disposição de seu conteúdo constituam criações intelectuais, deverão ser protegidas como tal. Essa proteção, que não se estenderá aos dados ou ao material em si, se dará sem prejuízo de qualquer direito autoral subsistente nesses dados ou material"

de proibir a extração ou reutilização da totalidade ou parte da base de dados. A criação de uma base de dados que preencha as condições para ser protegida com o direito sui generis, beneficia automaticamente de uma proteção de 15 anos, a contar da data de criação da base de dados ou da sua disponibilização ao público, ao abrigo do artigo 10º da referida diretiva europeia. Posto isto, importa analisar a fricção existente entre a defesa da transparência motivada incansavelmente pelo RGPD e os direitos de propriedade industrial, com a foco naquilo que alguns autores denominam de "blackboxes legais".

5.1.1. Direitos de propriedade industrial e as blackboxes legais

Os direitos de propriedade intelectual criam frequentemente aquilo que certos autores apelidam de blackboxes legais[39], isto é, estes podem tornar os algoritmos impossíveis de escrutinar, opacos. Noutros casos, os algoritmos podem não estar protegidos por direitos de propriedade industrial e, mesmo assim, o seu escrutínio ser uma tarefa impossível devido à blackbox inerente às suas especificidades técnicas, como já foi abordado anteriormente.

Como já foi referido, a maioria das empresas utiliza algoritmos para recolher informação e não só. Estes algoritmos possuem valor intrínseco, e muito vezes, são ferramentas que constituem vantagens concorrências no mercado. Deste modo, a empresa que desenvolveu o algoritmo, pretende manter esta "arma secreta" bem longe dos seus concorrentes. Para tal, recorre aos direitos de propriedade intelectual, mais propriamente os segredos de negócios e o direito sui generis, como foi abordado neste capítulo. Tal como uma blackbox de índole técnica ou funcional, um algoritmo protegido por um direito de propriedade intelectual é um algoritmo sem possibilidade de escrutínio – opaco. Assim, quando alguém tenha sido afetado por uma decisão automatizada por recurso um algoritmo protegido por um direito de propriedade industrial poderá terá dificuldades em afirmar os seus direitos. Isto pode ter implicações negativas para uma relação já desequilibrada. Será que existem, no entanto, formas de contornar esta problema?

[39] Guido Noto La Diega, "*Against the Dehumanisation of Decision-Making*", 2018, p 8-9, disponível em: https://papers.ssrn.com/sol3/papers.cfm

5.1.2. Transparência algorítmica e os segredos de negócio

Quando foi abordada a existência de um reconhecimento de um direito de explicação colocou-se a hipótese de "analisar o interior" de um algoritmo com a finalidade de entender o processo de uma tomada de decisão, mesmo que isso implique a subjugação de um direito de propriedade intelectual. A Diretiva (UU) 2016/943 do Parlamento Europeu e do Conselho de 8 de junho de 2016 relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais parece, indiretamente, dar resposta à questão.

Os artigos nº 1º, 3º e 5º da referida diretiva limitam a proteção dos segredos comerciais. Em primeiro lugar, o artigo 1º estabelece o objeto e âmbito da aplicação da mesma e no seu número dois enumera aquilo que esta não cobre, isto é, o conjunto de exercício de direitos e aplicação de regras que a Diretiva não se pode opor. Por sua vez, o artigo 3º, expõe os meios legais de obtenção um segredo comercial. E, por último, o artigo 5º foca-se nas exceções, ou seja, o conjunto de situações que verificadas indeferem um pedido de aplicação de medidas, procedimentos e vias de reparação necessários aquando da aquisição ou divulgação de segredos comerciais.

Da análise destes três artigos, na sua generalidade, não há uma alínea em específico que afirme explicitamente a divulgação de algoritmos, contudo, devemos realçar que as alíneas b) e c) do número dois do artigo 1º, o número dois do artigo 3º e a alínea d) do artigo 5º enfatizam a defesa do interesse público, que pode ser o caminho para a transparência algorítmica. Segundo o artigo 1º, nº 2, alínea b), a diretiva não pode afetar à "a aplicação das regras da União ou nacionais que impõem aos titulares dos segredos comerciais a divulgação, por razões de interesse público, de informações, incluindo segredos comerciais, às autoridades públicas, administrativas ou judiciais para o desempenho das funções dessas autoridades". Isto significa, que os detentores de segredos comerciais são obrigados a divulgar a informação protegida, ao público e autoridades administrativas ou judiciais, por razões de interesse público quando tal esteja plasmado na lei europeia ou nos ordenamentos jurídicos nacionais. Assim, certos autores consideram haver espaço para argumentar uma certa obrigação a divulgar algoritmos por razões de interesse público, levando à subjugação da proteção do segredo comercial, no entanto, apenas quando tal estiver comtemplando no ordenamento jurídico europeu ou

nacional[40]. Deste modo, considerando que um algoritmo foi responsável por um comportamento ilegal, a pessoa cuja esfera jurídica foi afetada poderá processar o detentor do algoritmo (segredo comercial) e as autoridades competentes prontamente escrutinarão o algoritmo. Tal como aconteceu, por exemplo no caso *Google Shopping*, em que a Comissão Europeia "abriu" o algoritmo da Google, tendo, inclusivamente, concluindo que o mesmo era manipulado para favorecer a própria Google[41].

Da mesma forma, à luz da alínea c) do número dois do artigo 1º da referida diretiva, as instituições e os organismos da União ou as autoridades públicas nacionais podem divulgar informações transmitidas pelas empresas que essas instituições, organismos ou autoridades tenham em seu poder, "por força e nos termos das obrigações e das prerrogativas previstas no direito da União ou no direito nacional". Assim, também aqui há margem para incluir os algoritmos no conceito de "informações transmitidas pelas empresas a essas instituições".

Concluindo, existem dois casos em que podemos ter divulgação e escrutínio de algoritmos, onde a única diferença existe no sujeito à obrigação de divulgação. Enquanto no primeiro caso a obrigação é imposta aos detentores dos segredos comerciais, no segundo caso são as autoridades públicas obrigadas a divulgar a informação. Embora a Diretiva não declare explicitamente a existência de uma imposição de transparência algorítmica, defende que a proteção dos segredos comerciais terá que ficar para segundo plano quando estejam em causa interesses públicos relevantes, legalmente reconhecidos pelas autoridades públicas.

6. Proposta de Lei da Comissão Europeia sobre a Inteligência Artificial

Importa agora analisar a Proposta de Lei da Comissão Europeia, constituída por um conjunto de normas com implicações práticas no debate aqui exposto, na medida em que pode configurar a chave para um caminho mais transparente no que diz respeito às decisões automatizadas com recurso a sistemas de inteligência artificial.

No dia 21 de abril de 2021, a Comissão Europeia apresentou uma proposta de regulamento que estabelece regras harmonizadas em matéria de inteligência artificial, também conhecido como

[40] Maggiolino, Mariateresa, *EU Trade Secrets Law and Algorithmic Transparency*, Bocconi Legal Studies Research Paper No. 3363178, março de 2019, disponível em: http://dx.doi.org/10.2139/ssrn.3363178
[41] "Google Search" disponível em: http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf

o regulamento da inteligência artificial. O objetivo é regular o desenvolvimento e a comercialização de sistemas de inteligência artificial, proibindo certas práticas com base no risco e impondo um conjunto de obrigações em matéria de transparência que serão escrutinadas neste capítulo.

No artigo 1º deste regulamento é definido o seu objeto, que compreende o seguinte:

(i) Regras harmonizadas para a colocação no mercado, a colocação em serviço e a utilização de sistemas de inteligência artificial na União;

(ii) Proibições de certas práticas de inteligência artificial;

(iii) Requisitos específicos para sistemas de inteligência artificial de risco elevado e obrigações para os operadores desses sistemas;

(iv) Regras de transparência harmonizadas para sistemas de inteligência artificial concebidos para interagir com pessoas singulares, sistemas de reconhecimento de emoções e sistemas de categorização biométrica, bem como para sistemas de inteligência artificial usados para gerar ou manipular conteúdos de imagem, áudio ou vídeo;

(v) Regras relativas à fiscalização e vigilância do mercado;

No artigo 2º deste regulamento é apresentado o seu âmbito de aplicação, ou seja, a quem se destina este conjunto normativo. As normas aplicam-se a "fornecedores que coloquem no mercado ou coloquem em serviço sistemas de inteligência artificial (doravante sistemas de IA) no território da União, independentemente de estarem estabelecidos na União ou num país terceiro", a "utilizadores de sistemas de IA localizados na União" e ainda a "fornecedores e utilizadores de sistemas de IA localizados num país terceiro, se o resultado produzido pelo sistema for utilizado na União".

A Comissão Europeia distingue com base no risco quatro tipos de práticas de sistemas de inteligência artificial: práticas proibidas, práticas de risco elevado, práticas de risco limitado e práticas de risco mínimo. Apenas as práticas proibidas e as práticas de risco elevado serão alvo de uma análise mais profunda. Nas práticas de risco limitado ou mínimo, a Comissão encoraja que sejam respeitadas, voluntariamente, as regras de conduta.

6.1. Práticas Proibidas

O artigo 5º do regulamento proíbe uma série de práticas que podem ser definidas como as "linhas vermelhas" do regulamento[42]. Neste conjunto de aplicações de sistemas de inteligência artificial, todas as práticas são completamente proibidas, exceto uma (que será analisado em último lugar) que apresenta uma exceção à sua proibição.

A primeira prática proibida é relativa aos sistemas de inteligência artificial manipuladores[43].

O artigo 5º, nas suas alíneas a) e b) plasma que é proibido:

(i) "A colocação no mercado, a colocação em serviço ou a utilização de um sistema de IA que empregue técnicas subliminares que contornem a consciência de uma pessoa para distorcer substancialmente o seu comportamento de uma forma que cause ou seja suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa".

(ii) "A colocação no mercado, a colocação em serviço ou a utilização de um sistema de IA que explore quaisquer vulnerabilidades de um grupo específico de pessoas associadas à sua idade ou deficiência física ou mental, a fim de distorcer substancialmente o comportamento de uma pessoa pertencente a esse grupo de uma forma que cause ou seja suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa".

De forma a explicitar estas duas alíneas e clarificar a sua aplicação, a Comissão Europeia utilizou os seguintes exemplos, uma para cada alínea respetivamente. O primeiro consistiria "num som audível e tocado nas cabines de um camião de modo a incentivar o motorista a conduzir mais tempo do que é saudável e seguro de modo a percorrer distâncias mais longas" em que IA seria utilizada para encontrar a frequência que maximizaria este efeito nos motoristas. O segundo exemplo baseia-se em "uma boneca com uma voz integrada que

[42] Thomas Metzinger, Der Tagesspiegel, "*Ethics Washing Made in Europe*", 8 de março de 2019 disponível em: https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html

[43] A categorização como sistemas manipuladores é feita no Considerando 15 da referida proposta, citando: "Além das inúmeras utilizações benéficas da inteligência artificial, essa tecnologia pode ser utilizada indevidamente e conceder instrumentos novos e poderosos para práticas manipuladoras, exploratórias e de controlo social. Essas práticas são particularmente prejudiciais e devem ser proibidas, pois desrespeitam valores da União, como a dignidade do ser humano, a liberdade, a igualdade, a democracia e o Estado de direito, bem como direitos fundamentais da União, incluindo o direito à não discriminação, à proteção de dados pessoais e à privacidade, e os direitos das crianças."

encorajaria as crianças a terem comportamentos perigosos sob o disfarce de ser um jogo divertido"[44].

A noção de manipulação pode configurar um conceito indeterminado. Segundo Marijn Sax, o entendimento deste conceito está assente quatro requisitos cumulativos: o manipulador pretende intencionalmente e secretamente, usar a tomada de decisão para atingir os seus próprios fins através da exploração de alguma vulnerabilidade[45].

A Comissão Europeia proíbe inequivocamente a utilização e comercialização de sistemas de inteligência artificial que tenham o intuito de manipular pessoas, quer seja uma manipulação subliminar ou uma manipulação com base na exploração de vulnerabilidades de um grupo específico de pessoas.

O segundo grupo de proibições está relacionado com o conceito "social scoring". A alínea c) do artigo 5º do regulamento contempla a proibição da "colocação no mercado, a colocação em serviço ou a utilização de sistemas de IA por autoridades públicas ou em seu nome para efeitos de avaliação ou classificação da credibilidade de pessoas singulares durante um certo período com base no seu comportamento social ou em características de personalidade ou pessoais, conhecidas ou previsíveis, em que a classificação social conduza ao tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas".

A Comissão Europeia decidiu, aqui, distinguir duas situações que podem acontecer individualmente ou cumulativamente:

(i) "Tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas em contextos sociais não relacionados com os contextos nos quais os dados foram originalmente gerados ou recolhidos".

(ii) "Tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas que é injustificado e desproporcionado face ao seu comportamento social ou à gravidade do mesmo".

"Social Scoring" é o conceito que denomina o comportamento de avaliação de alguém com base nos movimentos, comportamentos e atitudes em diferentes contextos sociais. As avaliações positivas influenciam positivamente alguém, enquanto uma avaliação negativa

[44] Gabriele Mazzini, '*A European Strategy for Artificial Intelligence*' (2nd ELLIS Workshop in Human-Centric Machine Learning (YouTube), https://youtu.be/OZtuVKWqhl0 ver a partir de 2:52:26
[45] Marijn Sax, *"Between Empowerment and Manipulation: The Ethics and Regulation of For-Profit Health Apps"* Tese de Doutoramento, Univeristeit Van Amsterdam (UvA), 2021, páginas 110–112

conduz a uma situação em que a pessoa é considerada como "não confiável" e é sancionada. A China utiliza o chamado "sistema de crédito social" com o intuito de categorizar cidadãos através das suas ações em contexto social, punindo aqueles que apresentem condutas reprováveis[46].

Vários estudos revelam que empresas monitorizam o comportamento de candidatos a empregos nas redes sociais para posteriormente incluírem estes dados na avaliação do candidato. O exemplo de clarificação fornecido pela Comissão Europeia consiste no seguinte: "um sistema de IA que identifica crianças em risco ou em situação de perigo com base em alguns comportamentos dos pais, comportamentos esses irresponsáveis como por exemplo faltar a uma consulta médica ou então um simples processo de divórcio"[47].

O terceiro e último grupo de proibições está relacionado com sistemas de identificação biométrica. Na alínea c), do número um do referido artigo, a Comissão Europeia proíbe "a utilização de sistemas de identificação biométrica à distância em «tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública", salvo exceções. Um exemplo de um sistema de identificação biométrica será uma câmara de videovigilância com um software de reconhecimento facial integrado, normalmente utilizados pelas autoridades policiais. Nestes casos, a utilização de sistemas de identificação biométrica é regulada pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Estes sistemas são autorizados mais facilmente neste tipo de questões do que propriamente em questões de interesse empresarial que estão, em geral, fora do escopo do RGPD.

Esta proposta de regulamento de inteligência artificial proíbe então os Estados Membros da Comissão Europeia o uso de sistemas de identificação biométrica, salvo exceções seguintes:

(i) "A investigação seletiva de potenciais vítimas específicas de crimes, nomeadamente crianças desaparecidas;

[46] Katie Canales, Insider, "*China's 'social credit' system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy*", 24 de dezembro de 2021, disponível em: https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4
[47] Gabriele Mazzini, "*A European Strategy for Artificial Intelligence*" (2nd ELLIS Workshop in Human-Centric Machine Learning (YouTube), https://youtu.be/OZtuVKWqhl0 ver a partir de 2:52:26

(ii) A prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de um ataque terrorista;

(iii) A deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal referida no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho 62 e punível no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro".

Importa referir que, ao contrário das restantes proibições, aqui não há uma proibição da comercialização. A este respeito uma das grandes críticas feitas a esta proposta é a possibilidade de comerciantes europeus venderem estes sistemas de identificação biométrica a regimes opressores[48], tal como aconteceu com a venda por parte da firma francesa Idemia/Morpho, destes sistemas de reconhecimento facial ao Departamento de Segurança Pública de Xangai[49].

6.2. Sistemas de Inteligência Artificial de Risco Elevado

A Comissão Europeia também inclui no título III da proposta de regulamento de inteligência artificial um conjunto de obrigações/requisitos a cumprir na utilização, desenvolvimento e colocação no mercado comercial de sistemas de inteligência artificial que contemplam um risco muito elevado para a "saúde, segurança e direitos fundamentais"[50], ao abrigo do seu artigo 8º. Estes requisitos recaem, na sua maioria, sobre a entidade que desenvolveu o sistema de inteligência artificial.

Em primeiro lugar, estes sistemas de inteligência artificial devem criar um sistema de gestão de riscos que deve ser documentado e atualizado ao longo da vida do sistema de risco elevado. As etapas integrantes deste sistema de gestão de riscos estão plasmadas no artigo 9º da referida proposta de regulamento.

---

[48] Michael Veale, Frederik Zuiderveen Borgesius, "*Demystifying the Draft EU Artificial Intelligence Act*", abril de 2021, disponível em: https://arxiv.org/abs/2107.03721

[49] Amnesty International, "*Out of Control: Failing EU Laws for Digital Surveillance Export*", setembro de 2020, disponível em: https://www.amnesty.org/en/documents/eur01/2556/2020/en/

[50] Considerando 43 da Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da união.

O artigo 10º impõe que "os sistemas de inteligência artificial de risco elevado que envolvam o treino de modelos com dados devem ser desenvolvidos com base em conjuntos de dados de treino, validação e teste" que cumpram um conjunto de critérios de qualidade, mais propriamente de precisão, integridade, representatividade e aplicação a uma área específica.

A proposta de regulamento contém, também, um conjunto de obrigações relacionadas com a exatidão, solidez e cibersegurança. Na medida em que "os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que alcancem, tendo em conta a finalidade prevista, um nível apropriado de exatidão, solidez e cibersegurança e apresentem um desempenho coerente em relação a tais aspetos durante o ciclo de vida", ao abrigo do artigo 15º da referida proposta.

Antes da colocação no mercado ou da colocação em serviço desse sistema, estes sistemas devem elaborar a documentação técnica do sistema de IA de risco elevado, que deve ser mantida atualizada (artigo 11º). A referida proposta obriga também que seja realizado "o registo automático de eventos enquanto o sistema de IA de risco elevado estiver em funcionamento". Pretende-se que os sistemas sejam capazes de manter os registos ao longo do seu ciclo de vida (artigo 12º).

Requer-se também a existência de supervisão humana, de acordo com o artigo 14º da proposta. Os modelos devem ser criados e desenvolvidos de uma maneira que possibilita uma supervisão humana eficaz, "por pessoas singulares durante o período de utilização do sistema de IA", procurando a prevenção e minimização de riscos para a saúde, a segurança e direitos fundamentais. Esta proposta valoriza a transparência dos sistemas de inteligência artificial, dedicando não só um artigo no âmbito dos sistemas de inteligência artificial de risco elevado, mas também, como será analisado mais à frente, um capítulo inteiro. Ainda neste contexto, o artigo 13º reitera que "os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que assegure que o seu funcionamento seja suficientemente transparente para permitir aos utilizadores interpretar o resultado do sistema e utilizá-lo corretamente. Deve ser garantido um tipo e um grau adequado de transparência, que permita cumprir as obrigações que incumbem ao utilizador e ao fornecedor por força do capítulo 3 do presente título".

O capítulo três da referida proposta o conjunto de obrigações dos fornecedores e utilizadores dos sistemas de inteligência artificial de risco elevado. Ao abrigo do artigo 16º, os fornecedores

para além de assegurar que os seus sistemas de IA de risco elevado cumprem os requisitos estabelecidos no capítulo dois, estes devem:

(i) "Dispor de um sistema de gestão da qualidade que cumpra o disposto no artigo 17.º;

(ii) Elaborar a documentação técnica do sistema de IA de risco elevado;

(iii) Quando tal esteja sob o seu controlo, manter os registos gerados automaticamente pelos sistemas de IA de risco elevado que fornecem;

(iv) Assegurar que o sistema de IA de risco elevado seja sujeito ao procedimento de avaliação da conformidade aplicável, antes da colocação no mercado ou da colocação em serviço;

(v) Respeitar as obrigações de registo a que se refere o artigo 51.º[51]";

(vi) Adotar as medidas corretivas necessárias, se o sistema de IA de risco elevado não estiver em conformidade com os requisitos estabelecidos no capítulo 2 do presente título;

(vii) Informar as autoridades nacionais competentes dos Estados-Membros nos quais disponibilizaram o sistema de IA ou o colocaram em serviço e, se for caso disso, o organismo notificado sobre a não conformidade e quaisquer medidas corretivas tomadas;

(viii) Apor a marcação CE[52] nos sistemas de IA de risco elevado para indicar a conformidade com o presente regulamento de acordo com o artigo 49.º;

(ix) Mediante pedido de uma autoridade nacional competente, demonstrar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título."

Depois de analisada a incidência da proposta sobre os sistemas de inteligência artificial que comportam um risco elevado, importa analisar agora as obrigações de transparência que são aplicáveis a determinados sistemas de inteligência artificial, estatuição que corrobora a linha mestra desta proposta, na medida em que se procura um incremento da transparência na comercialização e utilização dos sistemas de inteligência artificial.

[51] O artigo respeita à obrigação do registo do sistema de IA na base de dados da União Europeia.
[52] Marcação CE é um indicativo de conformidade obrigatória para diversos produtos comercializados no Espaço Económico Europeu.

6.3. Obrigações de transparência aplicáveis a determinados sistemas de inteligência artificial

O título IV da proposta de regulamento da Inteligência Artificial enuncia três obrigações: duas direcionadas para os utilizadores (artigo 52º, números dois e três) e uma para os fornecedores dos sistemas de inteligência artificial (artigo 52º, número um).

Os fornecedores têm a obrigação de "assegurar que os sistemas de IA destinados a interagir com pessoas singulares sejam concebidos e desenvolvidos de maneira que as pessoas singulares sejam informadas de que estão a interagir com um sistema de IA, salvo se tal se revelar óbvio dadas as circunstâncias e o conceito de utilização". Existe uma única exceção a esta regra. Não haverá aplicação desta obrigação a sistemas de Inteligência Artificial, legalmente autorizados, a "detetar, prevenir, investigar e reprimir infrações penais". Contudo tal obrigação poderá recair na mesma sobre estes se tais forem disponíveis ao público. Esta obrigação é comumente apelidada de "bot" disclosure. A outra parte tem a obrigação de ser informada de que está a interagir com um "bot", com o intuito da atuação do sistema de inteligência artificial não ser confundido com uma interação humana. Este "dever de informação" não é novo, visto que, está presente no Código de Conduta da UE sobre Desinformação[53].

Os utilizadores, por seu turno, são incumbidos de duas obrigações na interação com sistemas de inteligência artificial. Em primeiro lugar, "os utilizadores de um sistema de reconhecimento de emoções ou de um sistema de categorização biométrica devem informar sobre o funcionamento do sistema as pessoas a ele expostas". Esta incumbência não existe se os sistemas de inteligência artificial estiverem "legalmente autorizados para detetar, prevenir, investigar e reprimir infrações penais, salvo se esses sistemas estiverem disponíveis ao público." Em segundo lugar, "Os utilizadores de um sistema de IA que gera ou manipula conteúdos de imagem, áudio ou vídeo que sejam consideravelmente semelhantes a pessoas, objetos, locais ou outras entidades ou acontecimentos reais e que, falsamente, pareçam ser autênticos e verdadeiros a uma pessoa (falsificação profunda) devem divulgar que o conteúdo foi gerado ou manipulado artificialmente". Esta segunda incumbência está relacionada diretamente com os vulgarmente conhecidos "deepfakes". Neste contexto, existem também

[53] Comissão Europeia, "*Tackling Online Disinformation: A European Approach*", março de 2018, disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

exceções. Como tem sido apanágio no que concerne a estas obrigações de transparência dos sistemas de inteligência artificial, a obrigação não se aplicará a sistemas legalmente autorizados para detetar, prevenir, investigar e reprimir infrações penais. A novidade é o facto de haver exoneração desta obrigação quando esteja em causa o direito de liberdade de expressão. Alguns autores consideram que o objetivo desta incumbência esteja relacionado com proteção de direitos de personalidade, visto que, uma construção facial através destes sistemas pode resultar em semelhanças muito convincentes que quando exibidas num determinado contexto, também ele falso, pode prejudicar a imagem da pessoa em causa[54].

Concluindo, importa relembrar que esta proposta é o primeiro esboço de regulação da inteligência artificial.

Como vimos, a proposta impõe proibições com base no risco e impulsiona o escrutínio público por parte das autoridades europeias e nacionais.

A proposta de regulamento da inteligência artificial pende, plenamente, para uma regulação que implique uma maior transparência a vários níveis: não só no processo de criação, desenvolvimento e comercialização dos sistemas de inteligência artificial, mas também, na relação que se estabelece entre estes sistemas e os seus utilizadores.

Embora a proposta apresente fraquezas e ambiguidades, que aqui não foram aprofundadas, parece haver um equilíbrio relativamente à conjugação das necessidades das empresas e da tutela dos utilizadores e/ou destinatários dos sistemas de inteligência artificial. Do ponto de vista empresarial, é pertinente haver uma regulação dos sistemas de inteligência artificial para que a sua utilização possa acontecer a uma maior escala. Nesse sentido, proposta não esquece as empresas, que assim poderão incluir os sistemas de inteligência artificial nas suas atividades sem receio da incerteza de atuarem numa área desguarnecida de qualquer legislação. Por outro lado, aos utilizadores e/ou destinatários é conferido uma maior salvaguarda na garantia e tutela dos seus direitos.

[54] Jacquelyn Burkell and Chandell Gosse (2019), "*Nothing New Here: Emphasizing the Social and Cultural Context of Deepfakes*", disponível em: https://doi.org/10.5210/fm.v24i12.10287

CONCLUSÃO

A era da Big Data avista-se como desafiante a vários níveis, em especial, ao nível da regulamentação da inteligência artificial e da proteção dos dados pessoais.

O estudo que aqui que se conduziu, procurou fazer uma análise e reflexão sobre as decisões automatizadas por algoritmos opacos, os seus propósitos, objetivos e a funcionalidade destas decisões e a sua compatibilidade com ordenamento jurídico europeu e os princípios fundamentais que regem a nossa sociedade, tendo-se verificado que ainda há um longo caminho a percorrer.

O Regime Geral de Proteção de Dados e os seus corolários, no qual se destaca o princípio da transparência, concede aos titulares de dados vários direitos e, simultaneamente, impõe aos responsáveis pelo tratamento de dados um conjunto de proibições de forma a garantir esses direitos. O Direito da União consagra o direito de não sujeição a uma decisão tomada exclusivamente com base no tratamento automatizado, o direito de oposição ao tratamento de dados e o direito de obter uma explicação sobre as decisões automatizadas. Acrescenta-se ainda, que os titulares de dados gozam de uma tutela indemnizatória quando sofram danos recorrentes do tratamento de dados. Para além disto, em matéria de proteção de algoritmos por parte de direitos de propriedade industrial, o legislador impõe uma limitação do direito de propriedade industrial, na medida em reconhece que a proteção dos segredos comerciais terá que ficar para segundo plano quando estejam em causa interesses públicos relevantes e legalmente reconhecidos.

No entanto, ainda há constrangimentos ao pleno exercício dos direitos dos titulares de dados, mormente devido à quantidade e complexidade de informação sobre a utilização e tratamento dos dados que dificulta uma consciente manifestação de vontade.

Também a inteligência artificial e opacidade dos seus sistemas configuram um ponto de importante estudo e desenvolvimento legislativo por parte dos organismos europeus. A Proposta de Regulamento da Inteligência Artificial, reitera a transparência através da imposição de obrigações e da proibição de certas práticas que possam pôr em causa direitos e garantias dos cidadãos.

Apesar da presença de alguma ambiguidade, poderemos afirmar que a regulamentação das decisões automatizadas e dos sistemas de inteligência artificial prioriza a defesa da transparência, com assento na defesa e na tutela dos direitos e dos dados pessoais.

Embora, os algoritmos e outros sistemas de inteligência artificial sejam funcionalmente úteis para desempenhar várias tarefas no quotidiano de várias empresas e entidades administrativas, é importante não ignorar o seu impacto na vida e na esfera jurídica dos recetores da decisão automatizada. A evolução legislativa deve sempre acompanhar e, se possível, antecipar a evolução tecnológica a fim de evitar o vazio legal, garantir a segurança e salvaguardar os direitos e interesses de pessoas individuais e pessoas coletivas.

BIBLIOGRAFIA

A. Kroll, Joshua, Huey, Joanna, Barocas, Solon,W. Felten, Edward,R. Reidenberg, Joel, G. Robinson, David & Harlan Yu , "*Accountable Algorithms"*, disponível em: https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3

Amnesty International, (2020), "*Out of Control: Failing EU Laws for Digital Surveillance Export*",disponível em: https://www.amnesty.org/en/documents/eur01/2556/2020/en/

António Barreto Menezes Cordeiro, (2019), "*A interpretação dos regulamentos europeus e das correspondentes leis de execução: o caso paradigmático do RGPD e da lei n.º 58/2019*", in Revista de direito e tecnologia, vol. 1, n.º 2, disponível em: https://blook.pt/publications/fulltext/fe04d9de6b48/

Borgesiuis, Zuiderveen Frederik, Veale, Michael, (2021) "*Demystifying the Draft EU Artificial Intelligence Act*" disponível em: https://arxiv.org/abs/2107.03721

Burkell, Jacquelyn, Gosse, Chandell (2019), "*Nothing New Here: Emphasizing the Social and Cultural Context of Deepfakes*", disponível em: https://doi.org/10.5210/fm.v24i12.10287

Burrell, Jenna, (2016), "*How the machine 'thinks': Understanding opacity in machine learning algorithms*", disponível em: https://journals.sagepub.com/doi/full/10.1177/2053951715622512

Buttarelli, Giovanni, (2017), "*Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit"*, Autoridade Europeia para a Proteção de Dados, disponível em: https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf

Canales Katie, Insider, "*China's 'social credit' system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy*", 24 de dezembro de 2021, disponível em: https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4

Carabantes, M. (2020) "*Black-box artificial intelligence: an epistemological and critical analysis"*. AI & Soc disponível em: https://doi.org/10.1007/s00146-019-00888-w

Castelluccia, Claude, Le Métayer, Danie, (2019), "*Understanding algorithmic decision making: opportunities and challenges"*, Parlamento Europeu disponível em:

https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)624261

Comissão Europeia, (2018) "*Tackling Online Disinformation: A European Approach*" disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

Diakopoulos, Nicholas (2014), "*Algorithmic Accountability Reporting: On the Investigation of Black Boxes"*, disponível em: https://academiccommons.columbia.edu/doi/10.7916/D8ZK5TW2

Domingos, Pedro M. (2012) "*A few useful things to know about machine learning*", disponível em: https://homes.cs.washington.edu/~pedrod/papers/cacm12.pdf

Funego, Jaime (2020) "*How to protect algorithms and big data in the digital economy*", Garrigues Digital, disponível em: https://www.garrigues.com/en_GB/garrigues-digital/how-protect-algorithms-and-big-data-digital-economy

Gabriele Mazzini, '*A European Strategy for Artificial Intelligence*' (2nd ELLIS Workshop in Human-Centric Machine Learning (YouTube), https://youtu.be/OZtuVKWqhl0 ver a partir de 2:52:26

Gomes Canotilho/Vital Moreira (2007), "*Constituição da República Portuguesa Anotada*", vol. 1, Coimbra: Coimbra Editora, (4.ª ed.)

Goodman, Bryce, Flaxman, Seth (2016), ***"****European Union regulations on algorithmic decision-making and a 'right to explanation'",* Oxford Internet Institute disponível em: https://arxiv.org/pdf/1606.08813.pdf

Greenspan, Alan, (2011), "*Dodd- Frank Fails to Meet Test of Our Times*," Financial Times, disponível em: https://www.ft.com/content/14662fd8-5a28-11e0-86d3-00144feab49a

Gryz, Jarek, and Marcin Rojszczak. (2021). "*Black box algorithms and the rights of individuals: no easy solution to the 'explainability' problem*". Internet Policy Review, disponível em: https://policyreview.info/articles/analysis/black-box-algorithms-and-rights-individuals-no-easy-solution-explainability

Hamon, R., Junklewitz, H. and Sanchez Martin, J., (2020) "*Robustness and Explainability of Artificial Intelligence*" Publications Office of the European Union, Luxembourg, disponível em: https://publications.jrc.ec.europa.eu/repository/handle/JRC119336

Hao, Karen, (2019) "*AI is sending people to jail—and getting it wrong*", MIT Technology Review, disponível em: https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/

Hymas, Charles, (2019) "*AI used for first time in job interviews in UK to find best applicants"*, disponível em: https://www.telegraph.co.uk/news/2019/09/27/ai-facial-recognition-used-first-time-jobinterviews-uk-find

Laborde, Rebecca, (2020), "*The Three V's of Big Data: Volume, Velocity, and Variety*", disponível em: https://blogs.oracle.com/health-sciences/post/the-three-vx27s-of-big-data-volume-velocity-and-variety

Leenes, Ronald, Van Brakel, Rosamunde, Gutwirth, Serge,De Hert, Paul, (2017) "*Data protection and privacy: the age of intelligent machines"*, Oxford

Leese, Matthias (2014), "*The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union*", disponível em: https://journals.sagepub.com/doi/abs/10.1177/0967010614544204

Lovato Neto, Renato, (2018), *"Responsabilidade civil do advogado por perda de chance processual"*, Dissertação de Doutoramento, Porto, Faculdade de Direito da Universidade do Porto

Maggiolino, Mariateresa, (2019), "*EU Trade Secrets Law and Algorithmic Transparency"*, Bocconi Legal Studies Research Paper No. 3363178disponível em: http://dx.doi.org/10.2139/ssrn.3363178

Malgieri, Gianclaudio and Comandé, Giovanni, (2017) "*Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*" International Data Privacy Law, vol. 7, disponível em: https://ssrn.com/abstract=3088976

Mendoza, Isak and Bygrave, Lee A., (2017),*"The Right Not to Be Subject to Automated Decisions Based on Profiling"*, disponível em: https://ssrn.com/abstract=2964855

Metzinger, Thomas, Der Tagesspiegel, "*Ethics Washing Made in Europe*", 8 de março de 2019 disponível em: https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html

Moretti, Alessandro (2018), *Algoritmi e diritti fondamentali della persona*

Navas Navarro, Susana "*La personalidad virtual del usuario de internet*", Centro de Estudios de Consumo, disponível em: https://blog.uclm.es/cesco/files/2015/03/La-personalidad-virtual-del-usuario-de-internet-.pdf

Noto La Diega, Guido (2018), "*Against the Dehumanisation of Decision-Making*", disponível em: https://papers.ssrn.com/sol3/papers.cfm

Palmiotto Ettorre, Francesca,(2022) "*Assessing Transparency and Explainability from a Legal Perspective*", disponível em: https://digi-con.org/the-right-to-contest-automated-decisions/

Pasquale, Frank (2015), "*The Blackbox Society*", Harvard University Press disponível em: https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf

Sappa, Cristiana, (2019) "*How data protection fits with the algorithmic society via two intellectual property rights – a comparative analysis*", Journal of Intellectual Property Law & Practice, Volume 14, disponível em: https://doi.org/10.1093/jiplp/jpz022

Sax, Marijn, (2021) *"Between Empowerment and Manipulation: The Ethics and Regulation of For-Profit Health Apps"* Tese de Doutoramento, Univeristeit Van Amsterdam (UvA)

Tsai, CW., Lai, CF., Chao, HC. (2015) "*Big data analytics: a survey*". Journal of Big Data, disponível em: https://doi.org/10.1186/s40537-015-0030-3

Veale, Michael, Zuiderveen Borgesius, Frederik (2021), "*Demystifying the Draft EU Artificial Intelligence Act*", disponível em: https://arxiv.org/abs/2107.03721

von Eschenbach, W.J.(2021), "*Transparency and the Black Box Problem: Why We Do Not Trust AI.* " Philos. Technol., disponível em https://doi.org/10.1007/s13347-021-00477-0

Watcher, Sandra Brent Mittelsdadt, Floridi, Luciano (2017) "*Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*," International Data Privacy Law, Volume 7 disponível em: https://papers.ssrn.com/sol3/papers.cfm

Zech, Herbert, (2016) "*A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data*", Journal of Intellectual Property Law & Practice, Vol. 11, disponível em: https://ssrn.com/abstract=2873135