REVISTA DE DIREITO COMERCIAL

# Proteção de dados e inteligência artificial (também a propósito do ChatGPT)

Mafalda Miranda Barbosa[1]

## 1. Introdução

A proteção de dados está na ordem do dia, contaminando o discurso jurídico e levando o jurista a debruçar-se sobre os problemas que faz emergir. Vários são os fatores determinantes deste fenómeno. Entre eles, destaca-se o desenvolvimento das novas tecnologias de informação, de utilização generalizada, que tornam mais fácil o acesso a dados pessoais e o cruzamento das informações recolhidas[2].

O mundo atual vive, de facto, um período de transformação informacional, caracterizado por uma produção e armazenamento

[1] Univ Coimbra, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra/University of Coimbra Institute for Legal Research, Faculdade de Direito da Universidade de Coimbra. Orcid: 0000-0003-0578-4249. Professora Associada com Agregação.

[2] Cf. Jorge MIRANDA/Rui de MEDEIROS, *Constituição Portuguesa Anotada*, tomo I, Coimbra Editora, Coimbra, 2005, artigo 35º, 379-380; Alexandre de Sousa PINHEIRO, "A proteção de dados na proposta de regulamento comunitário apresentado pela Comissão Europeia: primeiras reflexões", *Direito e Política*, nº1, 2012, 9 s.; Alexandre de Sousa PINHEIRO, *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*, AAFDL, Lisboa, 2015, 427.

em massa de dados gerados continuamente. À medida que os diversos *smartphones*, *tablets*, computadores e múltiplos outros aparelhos se conectam, são recolhidos e transmitidos dados através de redes de alta velocidade, que depois são armazenados em bases de dados distribuídas e analisados com as mais variadas finalidades por *softwares* cada vez mais poderosos e sofisticados[3]. Os três *«Vês»* – volume, velocidade e variedade – que caracterizam a explosão informacional dos nossos dias garantem uma análise mais fidedigna, permitindo novas formas de inferência e predição, num movimento acelerado que se incrementará ainda mais com o advento do 5G e o surgimento da computação quântica[4]. Os dados pessoais, ao mesmo tempo que permitem o desenvolvimento de sistemas de inteligência artificial, são por estes gerados e trabalhados, aumentando-se o potencial risco para os seus titulares[5].

O risco a que se alude refrate-se a diversos níveis: ao *nível da privacidade*, pelo potencial intrusivo que o processamento de certos dados comporta, permitindo, em alguns casos, a sequenciação dos movimentos do titular daqueles ao longo de toda a sua vida; *ao nível da igualdade*, pelo perigo de discriminação que pode resultar da análise dos dado pessoais (falamos a este nível de

[3] Mikel NIÑO/Arantza ILLARRAMENDI, "Understanding Big Data: antecedents, origin and later development", *Dyna New Technologies*, 2, 2018, 1 s.
[4] Cf. Laney, *3D Data Management: Controlling Data Volume, Velocity, and Variety*, META group Inc., 2001. http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf
[5] Cf. Mafalda Miranda BARBOSA, "*Dos expert systems* aos *data systems AI*: impacto ao nível da proteção de dados", *Julgar*, 45, 2021

diversos tipos de discriminação[6]: discriminações *stricto sensu* – v.g. no caso de uma instituição financeira que, sabendo que um seu potencial cliente faz recorrentemente pesquisas acerca de mecanismos de proteção em situações de incumprimento contratual, recusa conceder crédito ou, concedendo-o, fixa um *spread* muito elevado; ou nas hipóteses de discriminação laboral, social, étnica, política; e situações de *adaptative pricing*, ou seja, a prática de variação dos preços em função do perfil do consumidor, de tal modo que a proposta negocial apresentaria um preço mais elevado aos consumidores que se mostrassem aptos a aceitar aquela oferta mais valiosa); *ao nível da liberdade*, pelo fomento de fenómenos como o *boxing*, que tem expressão em termos comerciais e em termos políticos e ideológicos, abrindo-se as portas a formas de manipulação informativa, agravada pelas hipóteses de difusão de falsidades geradas pelos algoritmos generativos. Mais recentemente, assiste-se inclusivamente a casos de manipulação emocional, como veremos.

Compreende-se, por isso, que o direito não possa ser alheio a este segmento do real, devendo procurar edificar uma tutela efetiva dos dados pessoais. Sendo concebido como um direito de personalidade e como um direito fundamental, a proteção de dados justifica-se em vários planos, que acompanham, *grosso modo*, os níveis de risco a que aludimos.

Em primeiro lugar, afigura-se vital para salvaguarda da identidade do sujeito, já que a divulgação de dados pessoais pode

[6] Cf., para maiores desenvolvimentos, Mafalda Miranda BARBOSA, "Proteção de dados, consentimento e tutela do consumidor", *Estudos de direito do consumidor*, 15, 2019, 37 s.

levar a que outros se apropriem daquela ou que haja dela uma deturpação, fazendo com que a pessoa seja confundida com outra ou que seja desvirtuada a verdade pessoal do sujeito; em segundo lugar, torna-se essencial para garantir que não se divulgam determinados elementos que, dizendo respeito ao sujeito, podem ser motivo de discriminação, sendo por isso determinante para a defesa da igualdade[7]; em terceiro lugar, é fulcral para a defesa da privacidade do sujeito, bem como para a tutela de outros direitos de personalidade como a honra ou a liberdade. Isto significa que a proteção de dados não tem como objeto último um direito de personalidade, mas vários direitos de personalidade do titular dos dados. E, por outro lado, significa que, e fazendo apelo a uma classificação jus-subjetiva muito cara ao constitucionalismo, estamos diante de um direito-garantia, uma guarda-avançada de

---

[7] Cf. Jorge MIRANDA/Rui de MEDEIROS, *Constituição Portuguesa Anotada*, 380. Sobre os dados ditos sensíveis, a que a Constituição se refere no artigo 35º/3, consideram Jorge Miranda e Rui de Medeiros que são "os elementos de informação cujo tratamento informático, além de poder contender com a privacidade do sujeito, pode vir a dar origem a tratamentos desiguais ou discriminatórios" – cf. Jorge MIRANDA/Rui de MEDEIROS, *Constituição Portuguesa Anotada*, 386.
Sobre os dados sensíveis, para uma outra visão do problema, cf. Alexandre de Sousa PINHEIRO, *Privacy e proteção de dados pessoais*, 487 s. e Spiros SIMITIS, "Sensitive datenzur Geschichte und Wirkung einer Fiktion", *Festschrift zum 65. Geburstag von M. Pedrazzini* (E. Bem/J. Nicolas Druey/Ernest A. Kramer/ Ivo Schwander, ed.), Stämpfli & Cie. AG., 1990, 469 s., também citado por Alexandre Sousa Pinheiro., considerando que não há dados pessoais inofensivos e que, por isso, não faz grande sentido a autonomização dos dados sensíveis, já que tudo depende do contexto global do tratamento que deles é feito.
Veja-se, igualmente, Anne Cammmilleri SUBRENAT/Claire Levallois-BARTH, *Sensitive data protection in the European Union*, Bruylant, Bruxelles, 2007

certas posições jurídicas ativas, estabelecendo-se entre o direito à proteção de dados e os direitos que lhe subjazem uma relação de interioridade constitutiva[8].

Simplesmente, se o potencial intrusivo e o caráter arriscado são reconhecidos, não é menos seguro que a solução não pode passar pela proibição *tout court* do tratamento de dados, não só porque ele se afigura imprescindível em muitas situações, como porque é consabido que, por seu intermédio, se potenciam inovações profundas e benéficas para todos. A preocupação do jurista deve, portanto, ser a de encontrar um equilíbrio necessário que garanta a salvaguarda do núcleo essencial dos diversos interesses e valores em jogo.

## 2. Linhas gerais da tutela do titular dos dados pessoais

Tendo em conta a importância dos dados pessoais e o potencial intrusivo que o mundo moderno apresenta, o Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, – RGPD – vem consagrar uma disciplina jurídica particularmente protetora do titular daqueles. Assim, depois de elencar uma série de princípios a que deve obedecer o tratamento de dados, estabelece diversas obrigações a cargo do responsável pelo

[8] Para outros desenvolvimentos, cf. Mafalda Miranda BARBOSA, "Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil", *Estudos de Direito do Consumidor*, 12, 2017, 75

tratamento (o *controller*) ou a cargo do seu subcontratante (*processor*), delineando esferas de responsabilidade, no sentido da *role responsibility*, o que facilitará a determinação posterior da responsabilidade, no sentido da *liability*, sempre que ocorra uma violação geradora de danos.

Sem ser nossa pretensão ser exaustivo no tratamento desta questão, importa começar por sublinhar que o tratamento de dados deve, em primeiro lugar, ser feito de forma *lícita – princípio da licitude do tratamento*. Tal licitude fica dependente da existência do *consentimento* do titular dos dados ou, em alternativa, da verificação de uma das situações previstas no artigo 6º/1 RGPD.

No que respeita a certas *categorias especiais de dados*, outrora designados dados sensíveis (dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, os dados genéticos, os dados biométricos que permitam identificar uma pessoa de forma inequívoca, os dados relativos à saúde, dados relativos à vida sexual ou à orientação sexual de uma pessoa), parte-se da *proibição do seu tratamento*, nos termos do nº1 do artigo 9º RGPD. Tal regra – da proibição de tratamento de dados especiais – suscita, contudo, dúvidas a parte da doutrina, sustentando alguns, porque nenhum dado pessoal é inofensivo, não fazer sentido a distinção[9]. Seja como

[9] Sobre a identificação de dados sensíveis, cf. Alexandre de Sousa PINHEIRO, *Privacy e proteção de dados pessoais*, 723. Explica o autor que a conjugação entre o artigo 35º CRP e o artigo 7º Lei nº67/98 "não apresenta uma tipificação de toda a informação desta natureza", permitindo-se a ampliação dos dados sensíveis através da "cláusula aberta da vida privada". O autor dá o exemplo do fumo do

for, pelo potencial discriminatório que encerram, o legislador europeu entendeu dever dispensar-lhes um tratamento também especial, proibindo o seu tratamento. Admite-se, não obstante, que o tratamento de tais dados possa ter lugar em condições particulares, previstas no nº2 do mesmo preceito.

Da análise dos dois citados preceitos (artigos 6º e 9º RGPD) podemos extrair duas conclusões preliminares: em primeiro lugar, os fundamentos de ilicitude do tratamento de dados são desenhados sob condições muito rigorosas; em segundo lugar, pelo menos no que respeita ao tratamento de dados em geral, deixa de se partir do princípio do consentimento para colocar em pé de

---

cigarro que tem sido entendido pela CNPD como um dado sensível, por ser "um hábito da vida passível de comportamentos discriminatórios".
Veja-se, igualmente, Pilar Nicolás JIMÉNEZ, *La protección jurídica de los datos genéticos de carácter personal*, Comares, Granada, 2006; Teodoro de ALMEIDA, "O direito à privacidade e a proteção de dados genéticos: uma perspetiva de direito comparado", *Boletim da Faculdade de Direito*, 79, 2003, 355 s.; Spiros SIMITIS, "Sensitive datenzur Geschichte und Wirkung einer Fiktion", *Festschrift zum 65. Geburstag von M. Pedrazzini* (E. Bem/J. Nicolas Druey/Ernest A. Kramer/ Ivo Schwander, ed.), Stämpfli & Cie. AG., 1990, 469 s., também citado por Alexandre Sousa Pinheiro., considerando que não há dados pessoais inofensivos e que, por isso, não faz grande sentido a autonomização dos dados sensíveis, já que tudo depende do contexto global do tratamento que deles é feito; Anne Cammmilleri SUBRENAT/Claire Levallois-BARTH, *Sensitive data protection in the European Union*, Bruylant, Bruxelles, 2007; Jorge MIRANDA/Rui de MEDEIROS, *Constituição Portuguesa Anotada*, 380. Sobre os dados ditos sensíveis, a que a Constituição se refere no artigo 35º/3, consideram Jorge Miranda e Rui de Medeiros que são "os elementos de informação cujo tratamento informático, além de poder contender com a privacidade do sujeito, pode vir a dar origem a tratamentos desiguais ou discriminatórios" – cf. Jorge MIRANDA/Rui de MEDEIROS, *Constituição Portuguesa Anotada*, 386.

igualdade as situações em que o tratamento é feito com base nele ou com base nas outras circunstâncias especificadas no artigo 6º/1.

Este consentimento a que aludimos tem de ser livre. Mas, para o ser, tem de ser *esclarecido*. De outro modo, o sujeito titular dos dados não compreenderia o verdadeiro alcance da autorização por si prestada, que, assim, não corresponderia a um ato de vontade. O dado prende-se, também, diretamente com a necessidade de dar cumprimento a um segundo princípio relativo ao tratamento de dados: o *princípio da transparência*. De facto, exige-se que o responsável pelo tratamento dos dados forneça ao titular dos dados informações e comunicações relativas ao tratamento, de forma concisa, transparente, inteligível e de fácil acesso, mediante a utilização de uma linguagem clara e simples, nos termos do artigo 12º RGPD[10].

Embora não confinado à necessidade de garantir a plena liberdade, o esclarecimento prévio ao consentimento para o tratamento de dados é condição imprescindível para que o mesmo possa ser considerado livre, e, como tal, válido. De outro modo, o titular dos dados não acederia à compreensão do âmbito e da dimensão do consentimento que estaria a prestar.

A informação a que se alude deve ser simples, clara, compreensível por um titular de dados pessoais mediamente esclarecido[11]. Deve, além disso, ser completa e prestada antes de o

[10] Sobre o ponto, cf. Ana Francisca Pinto DIAS, "Responsabilidade civil pelo tratamento de dados pessoais: a responsabilidade do *controller* por factos próprios e por factos de outrem", *Revista de Direito da Responsabilidade*, I, 2019, 1265 s.

[11] Parecer do grupo de trabalho do artigo 29º 15/2011, 22

consentimento ser dado, não bastando que esteja disponível num qualquer local[12]. Sublinhe-se que, quando o consentimento é prestado através de um formulário elaborado de forma prévia, unilateral e rígida por uma das partes, se devem aplicar as regras contidas no DL nº446/85, relativas aos contratos de adesão, donde os requisitos da comunicação e da informação contidos nos artigos 5º e 6º do citado diploma se devem aplicar.

Tais informações, por parte do responsável, servem para que o titular dos dados possa *compreender a natureza e o alcance do ato*, bem como para que possa *acompanhar o tratamento que deles seja feito*. O direito à informação de que se cura tem, na verdade, um âmbito e uma intencionalidade mais vastos do que de mero instrumento de esclarecimento conducente à licitude do consentimento. Por um lado, ele continua a existir, quando o tratamento dos dados se baseie noutros fundamentos que não essa autorização do titular; por outro lado, revela-se essencial para que o titular dos dados pessoais possa acompanhar o tratamento que deles seja feito. Parece, aliás, ser esta a *ratio* do direito à informação a que se refere o artigo 15º RGPD e que surge associado ao direito de acesso do titular dos dados. Tal direito de acesso é subsequente à recolha dos dados.

Por outro lado, a concretização do direito à informação, tal como acontecia no âmbito da lei nº67/98, vai ser diverso consoante os dados tenham sido recolhidos diretamente junto do seu titular ou não. É esta a solução que decorre dos artigos 13º e 14º RGPD. Acresce que os deveres de informação se incrementam quando em

[12] Parecer do grupo de trabalho do artigo 29º 15/2011, 22

causa esteja a criação de perfis ou a tomada de decisões automatizadas.

Um terceiro princípio fundamental em matéria de proteção de dados diz respeito à *limitação das finalidades.* De acordo com este princípio, os dados pessoais são recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com as mesmas.

A limitação das finalidades a que se alude está, desde logo, intimamente relacionada com a especificidade do consentimento, igualmente justificável à luz do princípio da transparência. De facto, este só é válido se for específico, excluindo-se formas de consentimento genérico, ou seja, ele há de ser orientado para as finalidades a que o responsável se propõe, nos termos dos artigos 12º s. RGPD. De outro modo, não se poderia falar de um consentimento livre. De facto, a declaração do sujeito não traduziria um ato de vontade amadurecido se a autorização fosse prestada em geral, sem atender ao alcance e aos fins do tratamento que vai ser efetuado. O consentimento que seja prestado para legitimar o tratamento de dados tem, então, de ter em conta as finalidades associadas a esse tratamento.

O princípio da limitação das finalidades a que aludimos é, contudo, mais amplo, não derramando a sua eficácia apenas no que toca à especificidade do consentimento. Na verdade, o referido princípio determina uma ligação incindível entre o fundamento que se invoca para o tratamento de dados e as concretas atividades que posteriormente podem ser legitimadas. Nos termos do artigo 13º/1 c) e do artigo 14º/1 c) RGPD, o responsável pelo tratamento de dados deve informar o titular dos dados acerca do fundamento

desse tratamento, antes de ele iniciar e relativamente a uma finalidade específica.

A necessidade de um consentimento específico em combinação com a ideia de limitação das finalidades funciona, consoante esclarece o EDPB, como um instrumento de proteção contra um eventual alargamento das finalidades para os quais os dados são processados. Na verdade, se depois da invocação do fundamento inicial de legitimação do tratamento fosse possível usar os dados para outros fins, o titular dos dados ficava exposto ao risco de uso imprevisto e não controlado dos mesmos. Procura-se, portanto, fazer face ao fenómeno de alargamento de função[13].

Admitem-se, porém, certos tratamentos de dados posteriores, que não sejam considerados incompatíveis com as finalidades iniciais. Assim, os fins de arquivo de interesse público, os fins de investigação científica ou histórica e os fins estatísticos estão salvaguardados. Devem, contudo, estabelecer-se garantias especiais, que podem passar, inclusivamente pela pseudonimização dos dados, nos termos do artigo 89º RGPD. Note-se, contudo, que, numa hipótese como esta, deixando de ser identificável o titular dos dados, estes perdem a natureza de dados pessoais.

Consagra-se, igualmente, o *princípio da minimização de dados*, isto é, os dados recolhidos devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados. Este princípio comporta, em si, diversas

[13] EDPB, *Guidelines 05/2020 on consent under Regulation* 2016/679, 14, que neste ponto acompanhamos de muito perto.

dimensões.

Em primeiro lugar, qualquer que seja o fundamento invocado, ele não legitima o tratamento de dados para além do que se revele essencial às finalidades invocadas. Há que estabelecer-se, portanto, um juízo ponderativo de exigibilidade no que respeita às diversas categorias de dados recolhidos.

Por outro lado, os dados só devem ser guardados durante o período de tempo necessário ao tratamento que foi legitimado e durante o lapso temporal que durar o fundamento da legitimação. Surge, por isso, intimamente relacionado com o *princípio da limitação da conservação*, de acordo com o qual os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados, embora possam ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos.

Do princípio da limitação da conservação associado ao princípio da licitude do tratamento baseado no consentimento podemos extrair, ainda, outros direitos de capital importância. Falamos, desde logo, do *direito ao esquecimento,* a que já nos referimos, mas que parece ter uma intencionalidade mais vasta do que aquela que resultaria da ideia de livre revogabilidade da autorização concedida para o tratamento pelo titular dos dados.

Se o direito ao esquecimento não se queda num simples direito à livre revogabilidade do consentimento, importa relembrar que, nos termos do artigo 17º RGPD, o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados

pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento; quando o titular retire o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6º/1 a) ou do artigo 9º/2 a) e se não existir outro fundamento jurídico para o referido tratamento; quando o titular se oponha ao tratamento nos termos do artigo 21º/1, e não existam interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular se oponha ao tratamento nos termos do artigo 21º/2; quando os dados pessoais foram tratados ilicitamente; quando os dados pessoais tiverem de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; quando os dados pessoais tiverem sido recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8º/1.

Tal *direito ao esquecimento apresenta determinados limites*. Designadamente, não poderá ser exercido quando o tratamento se revele necessário ao exercício da liberdade de expressão e de informação; ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; quando haja motivos de interesse público no domínio da saúde pública; quando estejam envolvidos motivos de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, e o direito ao esquecimento tornasse impossível ou prejudicasse gravemente a

obtenção dos objetivos desse tratamento; ou quando esteja em causa o exercício de um direito num processo judicial.

Intimamente relacionado com o princípio da limitação da conservação surge, ainda, o chamado *direito de limitação*, previsto e disciplinado no artigo 18º RGPD. De acordo com o preceito, o titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações: a) contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; b) o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; c) o responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

O artigo 18º RGPD permite-nos extrair, ainda, um outro princípio fundamental a este nível: o *princípio da exatidão*. Dito de outro modo, os dados pessoais devem ser exatos e atualizados sempre que necessário, devendo-se adotar todas as medidas adequadas para que, em caso de inexatidão, sejam apagados ou retificados sem demora. Na verdade, nos termos do artigo 16º RGPD, o titular dos dados tem direito a obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito ou que sejam completados os dados incompletos sejam completados. O titular dos dados tem igualmente direito a opor-se ao tratamento de dados nos termos do artigo 21º RGPD.

Consagra-se, igualmente, o *princípio da integridade e*

*confidencialidade.* Ausente do elenco de condições a que devem obedecer os dados pessoais de acordo com a Lei nº67/98, é explicitamente introduzido pelo RGPD, comunicando-nos que os referidos dados devem ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas. Não obstante a referida omissão, importa considerar que ele já se extrairia de uma análise sistemática do regime legal em vigor em Portugal.

Em causa está uma tentativa de reforço da segurança do tratamento de dados[14], impondo-se ao responsável pelo tratamento de dados a adoção das medidas técnicas e organizativas adequadas para face ao risco, entre as quais, de acordo com as circunstâncias, se destacam, nos termos do artigo 32º RGPD, a pseudonimização e a cifragem dos dados pessoais; medidas para assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; medidas para restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; processos para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

A lealdade a que se alude ao nível da proteção de dados – conforme a alínea a), do nº1, do artigo 5º RGPD – implica que se

[14] Cf. Ana Francisco Pinto DIAS, "Responsabilidade civil pelo tratamento de dados pessoais: a responsabilidade do *controller* por factos próprios e por factos de outrem", 1271 s.

tenham em conta as expectativas razoáveis dos titulares dos dados, designadamente as expectativas relativamente à natureza privada de alguns dados, e bem assim as possíveis consequências adversas que podem resultar do seu tratamento. Deve, também, ser ponderada a relação e os potenciais efeitos entre tais consequências e os benefícios que o *controller* possa vir a obter[15].

Consagra-se, finalmente, um *princípio de responsabilidade*, que, de todo o modo, já resultaria da necessária articulação dos princípios normativos que alicerçam o sistema jurídico.

A responsabilidade a que o RGPD alude diretamente, nos termos do artigo 5º e do artigo 24º, deve ser, contudo, compreendida no sentido da *accountability*. Em causa está, em rigor, a adoção de medidas técnicas e organizativas que se mostrem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade as regras do RGPD. Do mesmo passo, são colocados à disposição do responsável pelo tratamento de dados códigos de conduta elaborados nos termos dos artigos 40º e 41º RGPD, bem como procedimentos de certificação[16]. Prevêem-se, igualmente, outras regras, quais sejam a realização de *privacy impact assessements*, a notificação obrigatória das autoridades em caso de violação de dados pessoais e a nomeação de um encarregado de proteção de dados. Estabelecem-se, ainda, regras no sentido de

[15] EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 4 s.

[16] Ana Francisco Pinto DIAS, "Responsabilidade civil pelo tratamento de dados pessoais: a responsabilidade do *controller* por factos próprios e por factos de outrem", 1273

garantir a proteção dos dados pessoais desde a conceção, nos termos do artigo 25º RGPD.

Esta noção de *accountability* não faz apagar outras dimensões da responsabilidade. À responsividade a que agora se alude alia-se a responsabilidade. E, quanto a esta, somos confrontados com duas conceções distintas ao nível da disciplina europeia de proteção de dados.

Tal como já acontecia com a anterior legislação europeia na matéria, confrontamo-nos novamente com as noções de *data controller* (responsável pelo tratamento de dados) e *data processor* (subcontratante). Assumindo-se como peças centrais da regulamentação relativa aos dados pessoais, o responsável e o subcontratante oferecem-nos o desenho das relações que se estabelecem ou podem estabelecer entre aqueles que controlam ou executam uma operação de tratamento de dados, ao mesmo tempo que nos dotam de *critérios de determinação do responsável em caso de violação do direito à proteção de dados pessoais*. Lidamos, assim, com duas noções distintas de responsabilidade, a fazer rememorar, neste quadro, a lição de Honoré[17], que,

[17] Cf., para uma adequada compreensão dos diversos sentidos com que pode ser assumido o termo responsabilidade, H.L.A. HART, *Punishment and Responsability, Essays in the Philosophy of Law*, Oxford University Press, 1968, 210 s. Apresentam-se, aí, quatro sentidos para o termo *responsability*. A *role-responsability,* indicando que, se uma pessoa está investida num determinado cargo, lugar, estatuto, papel, fica adstrita a especiais deveres, alguns dos quais se prendem com a promoção do bem-estar dos outros ou a prossecução dos objetivos de uma dada organização; a *causal-responsability*, em cuja aceção o responsável se vem a identificar com o causador de um ato, pelo que não só os

apresentando uma taxonomia das diversas aceções de responsabilidade, fala, entre outras, da *role responsibility* e da

---

humanos, mas também as coisas, os animais ou os fenómenos não humanos podem ser considerados responsáveis (cf. p. 214); a *liability responsability*, que, ao contrário do sentido prévio, implica já uma assunção acerca do mérito da conduta, afastando-se do mecanicismo característico da visão da responsabilidade/causalidade, a implicar a responsabilidade como o desencadear de um efeito na realidade, tanto mais que a pessoa pode ser responsabilizada, neste sentido, pelos atos praticados por terceiros; a *capacity responsability,* intrinsecamente ligada à anterior, na medida em que a responsabilização do agente implica a existência de determinadas faculdades mentais e psicológicas sem as quais ele não se autodetermina, pelo que, em última instância, denotamos já o apelo a um dado sentido de liberdade sem a qual a primeira não pode ser
tematizada (cf. p. 226-227). Cf., ainda, sobre os vários sentidos do termo *responsibility,* H. L. A. HART, "Varieties of responsibility", *Law Quarterly Review*, 83, 1967, 346. No artigo citado, o autor apresenta a taxonomia referida. No que respeita, por exemplo, à *role responsibility*, salienta a dificuldade, por vezes sentida na apreciação do caso concreto, de determinação dos concretos deveres que oneram o sujeito em virtude da posição em que está investido. Acresce que inclui no conceito todas as obrigações que impendem sobre a pessoa como decorrência de um particular acordo firmado, entrando em considerações atinentes ao mundo contratual, tendo, não obstante, a cautela de, num esforço de compartimentação categorial, alertar que a assunção feita do termo responsabilidade não é confundível com aqueloutra de dever específico. A separá-los a consciência da complexidade e extensão da primeira, a implicar a conformação de uma *sphere of responsibility, requiring the exercise of discretion and care usually over a protracted period of time.* (cf. p. 347). Também, aí, claramente refere a interdependência entre os diversos sentidos da responsabilidade. Atendo-se ao direito já constituído, o autor considera que a *liability* está muitas vezes dependente da *causal responsibility* ou da *capacity responsibility.*

*liability*[18].

Se o conceito de responsável pelo tratamento de dados nos remete para uma ideia de responsabilidade enquanto assunção de um especial encargo, a implicar especiais deveres, que visam a salvaguarda dos dados pessoais alheios; o referido responsável pelo tratamento de dados pode tornar-se responsável, no sentido da *liability*, em caso de violação de algum ou alguns desses deveres. Fazendo-nos situar a montante ou a jusante do processo de tratamento de dados, as duas responsabilidades com que assim lidamos – responsabilidade pelo tratamento de dados e responsabilidade civil pela violação de dados pessoais – não deixam de apresentar entre si uma linha de continuidade, já que é a responsabilidade pelo tratamento de dados que, ao desenhar uma esfera de controlo associada a especiais deveres de cuidado que têm de ser assumidos, nos permite, *a posteriori,* determinar quem é o civilmente responsável.

Não se estranha, por isso, que o GT29 sobre a proteção de dados[19], ainda por referência à Diretiva 95/46/CE, venha sustentar que o conceito de responsável pelo tratamento de dados é um

---

[18] Para uma análise pormenorizada da relação entre a *role responsibility* e a *liability*, no contexto da proteção de dados, cf. Mafalda Miranda BARBOSA, "*Data controllers* e *data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil", *Revista de Direito Comercial*, 2018, 416-486 (="*Data controllers* e *data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil", *Revista da Banca, Bolsa e Seguros*, nº3, 2018, 147-216, que aqui acompanhamos de perto.

[19] Grupo de trabalho do artigo 29º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, fevereiro de 2010, 13 s.

conceito funcional, que visa atribuir responsabilidades àqueles que exercem uma influência de facto sobre os dados pessoais alheios. Numa outra formulação, lê-se no documento que todas as disposições que estabelecem condições para o tratamento lícito dos dados têm como destinatário o *controller*, sendo, por isso, ele o responsável pelos prejuízos sofridos devido ao tratamento ilícito dos dados, o que implica que a principal função do conceito seja a atribuição de responsabilidade[20].

Em termos gerais, a conexão que assim se estabelece não é perturbadora. Diríamos, pelo contrário, que ela resulta clara em qualquer esquema de imputação. Na verdade, do ponto de vista delitual, porque o homem se concebe como pessoa, a responsabilidade que possa avultar, pela lesão, em regra culposa, de um direito ou de um interesse protegido através de uma disposição legal de proteção de interesses alheios, resulta da convolação de uma primitiva esfera de responsabilidade *pelo outro* numa esfera de responsabilidade *perante o outro*, sendo os deveres do tráfego que integram a primeira o que nos oferece o embrião da imputação objetiva que se há de estabelecer. Do ponto de vista contratual, embora com uma finalidade diversa e um fundamento axiológico também diferente, a compreensão de uma esfera de risco/responsabilidade – agora emergente da própria vinculação negocial – não nos fará andar muito longe destas ideias.

---

[20] Grupo de trabalho do artigo 29º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 7 s.
De notar, desde já, que o novo Regulamento Geral de Proteção de Dados vem considerar que os subcontratantes podem também ser responsabilizados em determinadas circunstâncias.

A novidade que o Regulamento Geral de Proteção de Dados nos oferece é a concretização, pelos deveres que estabelece e pela identificação dos obrigados por tais deveres, da referida *role responsibility*. Contudo, isto não nos resolve todos os problemas. De facto, não basta pensar numa esfera de responsabilidade a montante para que a imputação – e, portanto, a responsabilidade civil, a jusante – se possa afirmar, tanto mais que, neste âmbito, ela se define em abstrato pelo legislador. Assim, haveremos de analisar em que medida a lesão que ocorre se liga funcionalmente ao dever preterido, para o que teremos de confrontar a esfera de responsabilidade do *controller* com outras esferas de responsabilidade. É por isso que se torna particularmente importante – ou mesmo imprescindível – compreender as relações que se podem estabelecer entre o responsável pelo tratamento de dados e outros responsáveis pelo tratamento de dados ou entre o responsável pelo tratamento de dados e os subcontratantes. Do mesmo modo que é essencial contemplar a este, nível, os eventuais comportamentos de terceiros que possam surgir[21].

## 3. Sistemas automáticos de decisão e proteção de dados

Sendo certo que o ambiente digital suscita problemas acrescidos no que respeita aos dados pessoais, um especial consentimento haverá de ser obtido sempre que o tratamento de dados seja feito

[21] Sobre o ponto, com amplo desenvolvimento, Mafalda Miranda BARBOSA, "*Data controllers* e *data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil", 416 s.

de acordo com processos totalmente automatizados. De acordo com o artigo 22º/1 RGPD, «o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar».

Segundo o entendimento do GT29, a expressão direito é aqui usada em sentido impróprio. Quer isto dizer que não se atribui uma posição subjetiva de oposição a uma qualquer tentativa de tomada de decisão exclusivamente automatizada, mas se estabelece uma proibição genérica de decisões totalmente automatizadas, incluindo a definição de perfis, quando tais decisões produzam efeitos na esfera jurídica do titular dos dados ou o afetem significativamente de forma similar[22].

A proposta interpretativa parece ser autorizada pela articulação da norma com o teor do *considerandum* 71 e com a solução consagrada no nº2 do citado artigo 22º RGPD. Não cremos, porém, que os argumentos deponham no sentido da inexistência de um direito, sem que, contudo, tal implique uma discordância com a solução prático-normativa proposta pelo GT29. De facto, do que se trata é de reconhecer um direito em termos genéricos, que exclui *a priori* a possibilidade de uma tomada de decisão exclusivamente automatizada, e não um qualquer direito unicamente exercitável por reação ao comportamento do responsável pelo tratamento de dados.

[22] GT Artigo 29º, *Orientações sobre as decisões individuais automatizadas e a definição de perfis*, 22

Teleologicamente, a solução impõe-se com meridiana clareza. A utilização de algoritmos (quer na definição de perfis, quer na tomada de decisões automatizadas) caracteriza-se pela sua opacidade[23], analisada pelos autores de forma tripartida: opacidade corporativa, deliberadamente gerada como forma de resguardar os segredos de negócios das empresas que desenvolvem os algoritmos; opacidade cognitiva, resultante da incapacidade que as pessoas em geral (e o titular dos dados em especial) têm de entender o funcionamento do algoritmo e de perceber a linguagem que o mesmo utiliza[24]; e opacidade técnica, inerente ao recurso ao *deep learning*, inviabilizador da explicitação do percurso decisório do *software*, mesmo por parte dos seus programadores[25].

Nessa medida, porque a incolumidade dos direitos dos titulares dos dados pessoais não se pode garantir com o mero cumprimento de deveres de informação prestados pelo responsável pelo

[23] Cf. Jenna BURRELL, *How the machine thinks: understanding opacity in machine learning algorithms*, 2015, http://ssrn.com/abstract=2660674; F. PASQUALE, *The black box society*, Harvard University Press, 2015, 79 s.; Mariana Marques RIELLI, "Críticas ao ideal de transparência como solução para a opacidade de sistemas algorítmicos", *Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa* (coord. Mafalda Miranda Barbosa/Filipe Braga Netto/Michael César Silva/José Luiz de Moura Faleiros Júnior), Editora Foco, 2021, 440.

[24] Jenna BURRELL, *How the machine thinks: understanding opacity in machine learning algorithms*; Mariana Marques RIELLI, "Críticas ao ideal de transparência como solução para a opacidade de sistemas algorítmicos", 443.

[25] Jenna BURRELL, *How the machine thinks: understanding opacity in machine learning algorithms*; Mariana Marques RIELLI, "Críticas ao ideal de transparência como solução para a opacidade de sistemas algorítmicos", 443.

tratamento[26], há que proibir que certas decisões sejam tomadas por algoritmos, de forma totalmente automatizada[27].

É exatamente essa perspetiva que é assumida pelo artigo 22º/1 RGPD[28]. Importa, por isso, perceber que decisões são assimiladas pelo âmbito de relevância do preceito.

Desde logo, temos de estar diante de uma decisão. A este propósito, A. Barreto Menezes Cordeiro aduz que, "por decisão entende-se um ato, numa aceção não jurídica, que incida sobre um caso concreto e produza efeitos jurídicos relativamente a um ou mais titulares de dados específicos, quer seja a aceitação ou a recusa de um pedido, a sua caracterização, catalogação, atribuição de uma classificação, definição de perfil ou qualquer outra medida análoga produtora de um efetivo resultado"[29].

Tal decisão tem de ser *exclusivamente automatizada*, isto é, uma decisão que não envolva qualquer intervenção humana. Alerta, neste contexto, o GT29[30] que uma supervisão que não seja relevante, ou seja, que se conforme como um gesto meramente simbólico não é suficiente para afastar a qualificação. Assim, "se

---

[26] Lilian EDWARDS/Kichael VEALE, "Slave to the Algorithm? Why a "Right to an Explanation" is Probably not the Remedy You Are Looking For", *Duke Law & Technology Review*, 16, 2017, 18 s.

[27] Nesse sentido, a proposta de CHESTERMAN, *Through a glass darkly: artificial intelligence and the problem of opacity*, 2020, http://ssrn.com/abstract=3575534

[28] Cf. Barreto Menezes CORDEIRO (coord.), *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº58/2019*, 220 s.

[29] A. Barreto Menezes CORDEIRO, "Decisões individuais automatizadas à luz do RGPD e da LGPD", 266.

[30] GT Artigo 29º, *Orientações sobre as decisões individuais automatizadas e a definição de perfis*, 22

alguém aplicar de forma sistemática perfis gerados automaticamente a pessoas sem ter qualquer influência efetiva no resultado, tratar-se-á […] de uma decisão tomada exclusivamente com base no tratamento automatizado"[31].

No mesmo sentido, A. Barreto Menezes Cordeiro sustenta que se "trata […] de um critério material e não de um critério formal, pelo que previsão […] tem-se por verificada sempre que a intervenção humana assuma contornos burocráticos, meramente confirmadores ou acríticos"[32].

Por outro lado, a decisão tem de produzir efeitos na esfera jurídica do titular dos dados ou de o afetar significativamente, de forma similar. A produção de efeitos na esfera jurídica refere-se à constituição, modificação ou extinção de relações jurídicas, mas também à afetação dos pressupostos de facto de exercício de um direito potestativo ou à lesão de um direito alheio ou de uma faculdade jurídica primária[33]. De acordo com o GT29, a decisão apenas será relevante se os efeitos tiverem um impacto grave[34].

A afetação significativa e similar dos interesses do titular do direito determina, igualmente, a proibição de decisões

---

[31] GT Artigo 29º, *Orientações sobre as decisões individuais automatizadas e a definição de perfis*, 23

[32] A. Barreto Menezes CORDEIRO, "Decisões individuais automatizadas à luz do RGPD e da LGPD", 267.

[33] A lesão de um direito alheio tem um potencial constitutivo de relações jurídicas. Entendemos, porém, que as hipóteses deveriam ser autonomizadas para melhor compreensão dos casos envolvidos.

[34] GT Artigo 29º, *Orientações sobre as decisões individuais automatizadas e a definição de perfis*, 23.

automatizadas. O GT29 considera que, "mesmo nos casos em que não há alterações nos seus direitos ou obrigações legais, o titular dos dados pode, contudo, sofrer um impacto suficiente para solicitar as proteções garantidas pela disposição em análise"[35].

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

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

A ideia de que a afetação tem de ser significativa implica, de acordo com a escalpelização oferecida pelo GT29, que a decisão afete "significativamente as circunstâncias, o comportamento ou as

[35] GT Artigo 29º, *Orientações sobre as decisões individuais automatizadas e a definição de perfis*, 23

escolhas das pessoas em causa"; tenha "um impacto prolongado ou permanente no titular dos dados", ou dê "origem a uma exclusão ou discriminação das pessoas"[36].

Em rigor, a explicitação das hipóteses apresentadas pelo grupo de trabalho, acompanhada dos exemplos que nos oferecem – "decisões que afetem a situação financeira de uma pessoa, designadamente a sua elegibilidade para obtenção de crédito; decisões que afetem o acesso de uma pessoa aos serviços de saúde; decisões que impeçam o acesso de uma pessoa a uma oportunidade de emprego ou a coloquem em séria desvantagem; decisões que afetem o acesso de uma pessoa à educação, como […] o ingresso em estabelecimentos de ensino superior"[37] –, pode envolver, em termos técnico-jurídicos, atenta a amplitude do conteúdo de alguns direitos subjetivos, uma efetiva violação de posições jus-subjetivas ativas. Por exemplo, tratando-se de decisões que afetem o acesso de uma pessoa à educação ou o ingresso no ensino superior, são lesadas dimensões que se integram no âmbito do direito ao livre desenvolvimento da personalidade, tornando-se, então, complexa a questão de saber se tais direitos se integram ou não no âmbito de tutela da proteção de dados.

A mesma opinião é partilhada por A. Barreto Menezes Cordeiro. Nas palavras do autor, "não vemos que decisões possam afetar significativamente de forma similar os titulares dos dados, mas que não produzam efeitos na sua esfera jurídica ou que vedam a sua

[36] GT Artigo 29º, *Orientações sobre as decisões individuais automatizadas e a definição de perfis*, 23
[37] GT Artigo 29º, *Orientações sobre as decisões individuais automatizadas e a definição de perfis*, 23

produção, ou seja, que não acionem a produção de efeitos jurídicos. De resto, os exemplos avançados pelo GT 29 relativos a esta segunda parte produzem, sem exceção, efeitos na esfera jurídica do titular"[38].

Problemática pode ser, a este nível, a questão da publicidade personalizada com base na definição de perfis, conduzindo ao fenómeno de *boxing* a que já nos referimos. O GT29, embora considere que o procedimento, em regra, não terá um impacto significativo nas pessoas, admite que ele possa ocorrer em função das características específicas de cada caso[39]. Designadamente, haveremos de ter em conta aspetos como "a dimensão intrusiva do processo de definição de perfis, nomeadamente o seguimento de pessoas em diferentes sítios Web, dispositivos e serviços; as expectativas e a vontade das pessoas em causa; a forma como o anúncio é apresentado; ou a utilização de vulnerabilidades conhecidas dos titulares de dados visados"[40].

A proibição não se aplica sempre que se verifique uma das hipóteses do artigo 22º/2 RGPD, ou seja, sempre que a decisão seja a) necessária para a execução ou a celebração de um contrato; b) autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os

[38] A. Barreto Menezes CORDEIRO, "Decisões individuais automatizadas à luz do RGPD e da LGPD", 268

[39] GT Artigo 29º, *Orientações sobre as decisões individuais automatizadas e a definição de perfis*, 24

[40] GT Artigo 29º, *Orientações sobre as decisões individuais automatizadas e a definição de perfis*, 24

direitos e liberdades e os legítimos interesses do titular dos dados; ou se c) baseie no consentimento explícito do titular dos dados.

Estas regras terão de, em matéria de proteção do consumidor, ser articuladas com outras pensadas ao nível europeu. Pensamos nas recentes alterações propostas ao quadro normativo, por via da proposta de Diretiva sobre o *enforcement* e modernização do direito europeu do consumidor. Introduzindo alterações nas Diretivas dos Direitos dos Consumidores (Diretiva 2011/83/UE); na Diretiva sobre cláusulas abusivas (Diretiva 93/13/CEE); na Diretiva dos preços (Diretiva 98/6/CE); na Diretiva sobre práticas comerciais desleais (Diretiva 2005/29/CE), esta nova proposta de diploma europeu não deixa de lado preocupações evidentes em matéria de proteção de dados. Assim, se, por um lado, reforça a obrigatoriedade de dar cumprimento ao RGPD, nos termos da proposta para a nova redação do nº4 do artigo 13º da Diretiva 2011/83/UE, por outro lado, parece alargar o âmbito da proteção que é devida. Designadamente, amplia-se o âmbito de relevância do diploma, tornando-o aplicável, também, aos contratos de fornecimento de conteúdos digitais que não sejam suportados por um meio tangível e aos contratos de fornecimento de serviços digitais, no quadro dos quais, o consumidor se obriga a fornecer dados pessoais ao profissional, exceto se os dados pessoais fornecidos pelo consumidor forem exclusivamente tratados pelo profissional com o propósito de fornecer o conteúdo digital. E, subsequentemente, reforçam-se os deveres de informação a cargo dos profissionais, para os ajustar aos modernos meios de comunicação, às especificidades deste tipo de contratos e aos perigos que o ambiente digital acarreta. Nos termos do *considerandum* 45 da proposta de diretiva, os profissionais podem

personalizar o preço das ofertas para consumidores específicos ou categorias específicas de consumidores, baseando-se em *automated decision-making and profiling of consumer behaviour*. Mas, nesse caso, devem informar claramente que os preços apresentados são personalizados com base nas decisões automatizadas, de modo a que o consumidor possa ter em conta o potencial risco da sua decisão de aquisição do produto. Estabelece-se, por isso, uma específica obrigação de informação nesta matéria, sem prejuízo da aplicação do RGPD, que determina que os titulares de dados não podem ser submetidos a automatizadas tomadas de decisão, incluindo através de *profiling*, e reforçam-se, assim, algumas das obrigações e direitos que já decorreriam do RGPD.

As soluções ditadas pelo direito comunitário (Diretiva UE 2019/2161) foram transpostas para o nosso ordenamento jurídico pelo DL nº 109-G/2021, de 10 de Dezembro. Assim, nos termos do artigo 4º/1, l), DL nº24/2014, antes de o consumidor se vincular a um contrato celebrado à distância ou fora do estabelecimento comercial, ou por uma proposta correspondente, o fornecedor de bens ou prestador de serviços deve indicar-lhe, em tempo útil e de forma clara e compreensível, para além de outras informações, que o preço foi personalizado com base numa decisão automatizada, quando tal ocorra.

Outras questões relacionadas com a publicidade comportamental devem-nos fazer refletir. As regras do consentimento são um importante instrumento para fazer face aos riscos que a nossa sociedade de informação arrasta para os titulares de dados pessoais. Contudo, podem não ser bastantes. Na verdade,

no momento em que presta o seu consentimento para a recolha de dados, por exemplo, ao navegar num determinado *site*, o consumidor pode não ter a consciência exata do impacto que o seu assentimento poderá ter no futuro, em termos de campanhas publicitárias. Devem, portanto, ser impostos determinados mecanismos que garantam a identificabilidade da publicidade com que o consumidor é "constantemente" invadido como verdadeira publicidade comportamental, relembrando-o da possibilidade de revogar o seu consentimento a qualquer tempo. A este propósito, poderia ser importante estabelecer a obrigatoriedade de uma revisão periódica do consentimento, adotando-se um mecanismo de *ongoing consent*[41]. Esta visão do problema estaria em linha com a regra segundo a qual devem ser oferecidas condições para a revogação do consentimento que tornam tão fácil esta opção como dar o próprio consentimento.

Particularmente relevantes a este ensejo são, igualmente, todas as situações que envolvem a recolha de *cookies* pelos prestadores de serviços. Tem-se entendido, na verdade, na senda das orientações emanadas pelo EDPB, que o acesso a determinados serviços e funcionalidades não pode ficar condicionado pelo consentimento do utilizador no que respeita à recolha de informação ou ao acesso a informação que já esteja alojada no seu equipamento. Em causa as chamadas *cookie walls*[42].

---

[41] Departamento de Proteção e defesa do consumidor, *Proteção de dados pessoais nas relações de consumo: para além da informação creditícia*, Brasília, 2010, 43 s.

[42] European Data Protection Board (EDBP), *Guidelines 05/2020 on consent under Regulation* 2016/679, 11, que aqui acompanhamos de muito perto.

Há, porém, que ter em conta as regras em matéria de comunicações eletrónicas[43]. O futuro *Regulamento ePrivacy*, que substituirá a diretiva 2002/58/CE, mantendo embora a regra de que apenas podem ser armazenados no equipamento do utilizador cookies com o seu consentimento, exceciona situações em que, tendo em conta certas finalidades, se pode prescindir dessa autorização, designadamente quando tal seja necessário para assegurar a navegabilidade no site ou para prestação de um serviço, numa linha de continuidade com o modelo anteriormente adotado.

Importa, portanto, articular os dois regimes[44]. Assim, sempre

---

[43] A este respeito, aliás, na ligação entre os consumidores e a proteção de dados, haveremos ainda de ter em conta algumas regras especiais: nos termos do artigo 13º-A Lei nº41/2004, está sujeito a consentimento prévio expresso do assinante que seja pessoa singular, ou do utilizador o envio de comunicações não solicitadas para fins de *marketing* direto, designadamente através da utilização de sistemas automatizados de chamada e comunicação que não dependam da intervenção humana (aparelhos de chamada automática), de aparelhos de telecópia ou de correio eletrónico, incluindo SMS (serviços de mensagens curtas), EMS (serviços de mensagens melhoradas) MMS (serviços de mensagem multimédia) e outros tipos de aplicações similares, o que não impede que o fornecedor de determinado produto ou serviço que tenha obtido dos seus clientes, no contexto da venda de um produto ou serviço, as respetivas coordenadas eletrónicas de contacto, possa utilizá-las para fins de *marketing* direto dos seus próprios produtos ou serviços análogos aos transacionados, desde que garanta aos clientes em causa, clara e explicitamente, a possibilidade de recusarem, de forma gratuita e fácil, a utilização de tais coordenadas, no momento da respetiva recolha, e por ocasião de cada mensagem, quando o cliente não tenha recusado inicialmente essa utilização.

[44] Cf. EDPB, *Opinion 5/2019 on the interplay between ePrivacy Directive and the GDPR*, 12-3-2019, 5 s. Para maiores desenvolvimentos, v., também, Catarina SILVA,

que as informações armazenadas constituam dados pessoais, aplica-se a título de regime-regra o regime das comunicações eletrónicas, e subsidiariamente o RGPD. Não sendo necessário o consentimento para a recolha e armazenamento de cookies, este não deve ser exigido à luz da disciplina da proteção de dados. Ao invés, se o consentimento for exigido nos termos do regime das comunicações eletrónicas, não poderá procurar-se o fundamento para o tratamento de dados pessoais, que aqueles envolvam ou em que aqueles se traduzam, numa condição de licitude diversa, de acordo com o artigo 6º RGPD[45].

Contudo, porque o consentimento é exigível para a recolha de *cookies*, dele não pode ficar dependente o acesso a um qualquer serviço, sob pena de faltar a nota de liberdade que deve revestir a autorização legitimadora. Repare-se, ademais, que sempre que seja necessário o consentimento para a dita recolha e armazenamento de *cookies*, são aplicáveis os requisitos impostos pelo RGPD.

## 4. Proteção de dados e inteligência artificial: problemas específicos

Todas as soluções que, perfuntoriamentde, fomos assinalando podem não ser bastantes para lidar com os problemas que a

"A utilização de cookies e a (in)suficiência dos requisitos aplicáveis ao consentimento", *Anuário de Proteção de dados*, 2021, 10 s.

[45] Catarina SILVA, "A utilização de cookies e a (in)suficiência dos requisitos aplicáveis ao consentimento", 11.

inteligência artificial comunica ao nível da proteção de dados.

Entre muitos desses problemas, alguns dos quais possivelmente não diagnosticados, tal a velocidade com que os algoritmos se vão desenvolvendo, importa sublinhar alguns.

Desde logo, tendo os algoritmos potencial para gerar novos dados a partir dos que foram inicialmente transmitidos, coloca-se o problema de saber se o fundamento de licitude do tratamento que deles seja feito é suficiente ou não para abarcar esta segunda geração de dados.

Por outro lado, o modo de funcionamento da máquina, baseado no estabelecimento de correlações estatísticas – que estão muito longe de representar relações de causalidade –, pode estar na base de corrupção de dados que, posterior e sequencialmente, poderão ser utilizados como matéria prima para a aprendizagem algorítmica. Quer isto dizer que, para além do potencial de discriminação que os algoritmos encerram, eles exponenciam a possibilidade de se chegar a soluções erradas, eventualmente lesivas de direitos alheios, agravando-se, assim, um problema atinente aos vieses de programação que possam já existir[46].

Acresce a tudo isto que nem sempre é fácil, atenta a autonomia e a opacidade dos sistemas, perceber quais os conjuntos de dados efetivamente utilizados na aprendizagem algorítmica. Pense-se, a este propósito e com especial acuidade, nos algoritmos, como o

[46] Este problema pode ocorrer também a partir de dados não pessoais. Basta para tanto que, a partir de dados pessoais, se gerem dados anonimizados que, não o sendo, podem gerar um problema de corrupção – suscitando problemas de responsabilidade – ou um problema de discriminação/manipulação.

ChatGPT, que imitam linguagem natural, criando textos, conversas, gerando fotografias falsas de um imenso realismo, elaborando códigos de programas de computador, escrevendo ensaios ou roteiros de filmes, entre muitas outras potencialidades, ou seja, os chamados LLM (*large language models*). Trata-se de um sistema treinado, através da análise de biliões de palavras, para prever, num enunciado linguístico, a palavra seguinte, a partir da compreensão das frases, de modo a poder, posteriormente, dar resposta a perguntas ou criar histórias, de tal sorte que do *input* inicial – a traduzir-se nas palavras que compõem a questão colocada – pode gerar-se automaticamente, como *output*, um texto, sendo igualmente capaz, na sua versão 4, de analisar imagens e compreendê-las como se fossem entradas em texto. Simplesmente, não obstante as potencialidades que encerra, as tentativas de correção de muitos erros detetados e a ampliação de funções, o sistema parece marcado pela falta de transparência quer quanto ao modo de funcionamento, quer quanto aos dados que são utilizados, tendo levado inclusivamente a autoridade italiana em matéria de proteção de dados a bloquear a sua utilização[47]. Em causa está, segundo a autoridade italiana, a ausência de uma base jurídica que justifique a recolha em massa de dados que são utilizados para

[47] Em rigor, os problemas já detetados com base no funcionamento do ChatGPT levam-nos mais longe: pense-se no caso do senhor belga que, depois de ter interagido durante duas semanas com um chatbot, cometeu suicídio, incentivado pelas palavras que ia recebendo da aplicação. Por um lado, o chatbot mostra-se, pela aprendizagem desregulada, apto a produzir textos radicais, eivados muitas vezes de discurso de ódio; por outro lado, a pessoa, mais vulnerável ou não, pode ser permeável a manipulações emocionais, criando a sensação interior de que está efetivamente a desenvolver uma interação subjetiva.

treinar o algoritmo.

Num outro plano, as dificuldades comunicam-se à eventual concretização de uma pretensão indemnizatória. Na verdade, ainda que no tocante aos dados pessoais se parta, nos termos do artigo 82º RGPD, de uma presunção de culpa, esta poder ser facilmente ilidida pela prova do cumprimento de todas as regras decorrentes do regulamento. Lidando com sistemas autónomos, as lesões podem ser causadas pela corrupção de dados provocada pelo funcionamento algorítmico. E, nessa medida, as lesões deixam de poder ser imputadas ao *controller*, mesmo tendo em conta que ele pode responder pelos atos do *processor*, exceto se convocarmos, para fundamentar a responsabilidade, um regime diverso daquele que assenta no RGPD ou na disciplina privatística do Código Civil. É este um dos principais problemas da existência de dados de segunda geração que podem ou não ser dados pessoais, atenta a possível anonimização que deles venha a ser feita, a suscitar problemas atinentes não só à culpa como à causalidade.

Mas o problema pode também ser causado com base nos dados de primeira geração: ou porque com base neles se podem criar *deep fake news*, ou porque podem conduzir a hipóteses de discriminação, ou porque podem gerar situações de manipulação (ideológica ou emocional), suscitando-se o problema de saber a quem pode ser imputada a lesão.

Por outro lado, na medida em que um dos perigos associados à utilização de sistemas de inteligência artificial para o tratamento de dados passa pela eventual manipulação que possa ocorrer, exponenciada pela larga escala de funcionamento dos algoritmos, pode não ser discernível a existência de um dano que, polarizado

no sujeito individualmente considerado, assuma gravidade suficiente para justificar a tutela do direito[48].

## 5. O caminho de solução

Os problemas que se denotam tornam evidente que não é bastante a existência de um regulamento geral de proteção de dados, sendo imperioso disciplinar a inteligência artificial.

A proposta de um Regulamento do Parlamento Europeu e do Conselho, tendo em conta a necessidade de adoção de regras uniformes em matéria de inteligência artificial[49], oferece-nos uma abordagem baseada no risco, definindo três grandes níveis.

Nos termos do artigo 5º, proíbem-se determinadas atividades que, implicando a utilização da inteligência artificial, envolvem um *risco considerado inaceitável*: sistemas de inteligência artificial que devolvem técnicas subliminares que afetem a consciência de uma pessoa, de modo a que, condicionando o seu comportamento, lhe possam causar um dano físico ou psicológico; que explorem alguma das vulnerabilidades de um específico grupo de pessoas devido à sua idade, fragilidade física ou mental, de modo a que, condicionando o seu comportamento, lhe possam causar um dano

[48] Este problema leva intencionada a questão de saber se os danos não patrimoniais decorrentes da lesão de dados pessoais podem ser sempre indemnizados ou se têm de obedecer aos requisitos que os diversos ordenamentos jurídicos estabelecem para aceder ao patamar da ressarcibilidade.
[49] COM (2021) 206 final, de 21-4-2021

físico ou psicológico; que sejam colocados ao serviço das autoridades públicas para avaliar ou classificar as pessoas singulares, durante um determinado período de tempo, tendo em conta as suas características ou o seu comportamento social; que envolvem sistemas de identificação biométrica, em espaços acessíveis ao público, para efeitos de cumprimento da lei, exceto se tal for absolutamente imprescindível para prosseguir uma das finalidades prevista na al. d), do nº1, do artigo 5º.

Paralelamente, configuram-se os chamados *sistemas de alto risco*, relativamente aos quais é imposto o cumprimento rigoroso de diversos deveres, antes de poderem ser colocados no mercado. Tais deveres orientam-se no sentido da supervisão humana e da disponibilização de informação.

Os sistemas são qualificados como de alto risco, se cumprirem cumulativamente dois requisitos: o sistema de inteligência artificial destinar-se a ser utilizado como componente de segurança de um produtor ou se for ele próprio um produto, abrangido pela legislação de harmonização enumerada no Anexo II; e o produto ser submetido a uma avaliação de conformidade de terceiros, com vista à colocação no mercado do produto nos termos da legislação contida no Anexo II. Os sistemas de inteligência artificial identificados no Anexo III são igualmente considerados sistemas de alto-risco. Este elenco pode ser atualizado pela Comissão. Trata-se, nesse caso, de sistemas que envolvem um risco para a saúde ou a segurança ou um risco de um impacto adverso em direitos fundamentais, se esse risco é, tendo em conta a sua severidade e a probabilidade de ocorrência, equivalente ou superior ao risco de lesão colocado pelos sistemas de inteligência artificial já referenciados no dito anexo III.

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

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

Na Orientação Geral de 6 de dezembro de 2022, estabelece-se a posição provisória do Conselho sobre a proposta de Regulamento, constituindo-se a base para a preparação das negociações com o Parlamento Europeu

Com o novo documento, reforça-se a ideia de estabelecimento de regras harmonizadas para a colocação no mercado, a colocação em serviço e a utilização de sistemas de IA; a regra da proibição de certas práticas de IA; regra da subordinação dos sistemas de IA de risco elevado a requisitos específicos, consagrando-se obrigações para os operadores de tais sistemas; estabelecem-se regras de transparência para certos sistemas de IA e regras no tocante à fiscalização e vigilância do mercado e à governação.

Do ponto de vista subjetivo, o regulamento aplicar-se-á a fornecedores que coloquem no mercado ou coloquem em serviço sistemas de IA no território da União, independentemente de estarem fisicamente presentes ou estabelecidos na União ou num

país terceiro; a utilizadores de sistemas de IA que estejam fisicamente presentes ou estabelecidos na União; a fornecedores e utilizadores de sistemas de IA que estejam fisicamente presentes ou estabelecidos num país terceiro, se o resultado produzido pelo sistema for utilizado na União; a importadores e distribuidores de sistemas de IA; a fabricantes de produtos que coloquem no mercado ou coloquem em serviço um sistema de IA juntamente com o seu produto e sob o seu próprio nome ou marca; a mandatários dos prestadores, que estejam estabelecidos na União.

Prevendo-se algumas exclusões no que respeita ao âmbito de aplicação, importa sublinhar que o mesmo não será aplicável aos utilizadores que sejam pessoas singulares que utilizam sistemas de IA no âmbito de uma atividade puramente pessoal de caráter não profissional, com exceção do artigo 52º.

Em paralelo, no tocante aos sistemas de inteligência artificial de finalidade geral, isto é, aos sistemas de inteligência artificial cujo fornecedor, independentemente da forma em que tenha sido colocado no mercado ou colocado em serviço, inclusive como software de fonte aberta preveja que desempenha funções de aplicação geral, como o reconhecimento de imagem e de fala, a reprodução de áudio e vídeo, a deteção de padrões, a resposta a perguntas, a tradução, entre outras, podendo ser utilizado em múltiplos contextos e podendo ser integrado em vários outros sistemas de IA, consagra-se um regime privilegiado, sendo apenas aplicáveis as obrigações previstas no artigo 4º-B, devendo respeitar, designadamente, os requisitos estabelecidos no título III, do capítulo II, quando estejam em causa sistemas de IA de risco elevado.

Continua, assim, a estruturar-se a regulamentação com base em diversos níveis de risco.

Nos termos do artigo 5º, continuam a ser proibidos os sistemas de IA de risco inaceitável:

sistema de IA que empregue técnicas subliminares que contornem a consciência de uma pessoa com o objetivo ou efeito de distorcer substancialmente o seu comportamento de uma forma que cause ou seja razoavelmente suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa;

sistema de IA que explore quaisquer vulnerabilidades de um grupo específico de pessoas associadas à sua idade, deficiência ou situação socioeconómica específica, com o objetivo ou efeito de distorcer substancialmente o comportamento de uma pessoa pertencente a esse grupo de uma forma que cause ou seja razoavelmente suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa;

e sistemas de IA para efeitos de avaliação ou classificação 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 conduz a um tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos das mesmas em contextos sociais não relacionados com os contextos nos quais os dados foram originalmente gerados ou recolhidos ou conduz a um tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos das mesmas que é injustificado ou desproporcionado face ao seu comportamento social ou à gravidade do mesmo;

sistemas de identificação biométrica à distância em tempo real em espaços acessíveis ao público por autoridades policiais ou em nome destas para efeitos de manutenção da ordem pública, salvo se essa utilização for estritamente necessária para alcançar objetivos precisos estabelecidos no artigo 5º/1, d), devendo neste caso obedecer-se aos requisitos previsos nos restantes números do citado artigo 5º.

No que respeita aos sistemas de IA de alto risco, os quais continuam a ser definidos de acordo com os mesmos parâmetros. Quanto a eles, deve ser criado, implantado, documentado e mantido um sistema de gestão de riscos em relação a sistemas de IA de risco elevado, entendido como um processo iterativo contínuo, planeado e executado ao longo de todo o ciclo de vida de um sistema de IA de risco elevado. A ideia é identificar e analisar os riscos conhecidos e previsíveis mais suscetíveis de ocorrer ao nível da saúde, da segurança e do impacto nos direitos fundamentais; avaliar outros riscos que possam surgir e adotar as medidas adequadas de gestão de riscos que possam ser razoavelmente atenuados ou eliminados durante o desenvolvimento ou a conceção do sistema ou através da prestação de informações técnicas adequadas.

Antes da colocação do sistema no mercado ou da colocação em serviço, deve ser elaborada a documentação técnica do sistema de alto risco. Ao mesmo tempo, o próprio sistema, que deve permitir a máxima transparência possível na sua utilização, deve permitir tecnicamente o registo automático de eventos ao longo do seu ciclo de vida. No que respeita à transparência, torna-se particularmente importante a obrigação de acompanhamento do sistema das instruções de utilização, num formato digital ou outro adequado,

que incluam informações concisas, completas, corretas e claras que sejam pertinentes, acessíveis e compreensíveis para os utilizadores, nos termos do artigo 13º. Acresce que os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de tal modo que possam ser eficazmente supervisionados por pessoas singulares durante o seu período de utilização.

Para além dos requisitos de conceção, prevêem-se obrigações que recaem sobre os fornecedores do sistema de alto risco, nos termos do artigo 16º. Além desses deveres, os fornecedores têm ainda de criar um sistema de gestão de qualidade que assegure a conformidade do sistema com as regras do regulamento IA (artigo 17º), de manter uma série de documentação disponível (artigo 18º), de manter os registos gerados automaticamente pelos sistemas de IA, desde que estejam sob o seu controlo por força de uma disposição contratual com o utilizador ou de uma disposição legal (artigo 20º), de adotar as medidas corretivas necessárias para repor a conformidade do sistema em questão ou proceder à retirada ou recolha do mesmo, quando tenham motivos para considerar que um sistema de IA de risco elevado que foi colocado no mercado ou em serviço não está em conformidade com o Regulamento IA (artigo 21º). Preveem-se, ainda, deveres de informação e de cooperação com as autoridades competentes (artigo 22º e 23º).

Consagram-se, igualmente, deveres para os mandatários, os quais devem ser designados, por mandato escrito, sempre que o sujeito que disponibiliza o seu sistema de IA no mercado da União e esteja estabelecido fora dela (artigo 25º); para os importadores (artigo 26º); para os distribuidores (artigo 27º); bem como para os utilizadores (artigo 28º). Quanto a estes, devem, entre outras obrigações específicas, utilizar os sistemas de acordo com as

instruções de utilização que os acompanham e atribuir a supervisão humana a pessoas singulares que possuam as competências, a formação e a autoridade necessárias.

Num terceiro nível de regulamentação, continuamos a prever obrigações específicas de transparência – estas são aplicáveis a *sistemas de risco limitado*.

Nos termos do artigo 52º, os fornecedores devem assegurar que os sistemas de IA destinados a interagir com pessoas singulares sejam concebidos e desenvolvidos de maneira que aquelas sejam informadas de que estão a interagir com um sistema de IA, salvo se tal se revelar óbvio do ponto de vista de uma pessoa singular razoavelmente informada, atenta e advertida, tendo em conta as circunstâncias e o contexto de utilização. Do mesmo modo, os utilizadores de um sistema de categorização biométrica devem informar sobre o funcionamento do sistema as pessoas a ele expostas; os utilizadores de um sistema de reconhecimento de emoções devem informar sobre o funcionamento do sistema as pessoas a ele expostas; e 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.

Consagram-se, também, sistemas de testagem obrigatórios, sujeitos a diversos requisitos; deveres de acompanhamento pós-comercialização, devendo os fornecedores criar e documentar um sistema de acompanhamento pós-comercialização que seja

proporcionado aos riscos do sistema de IA de risco elevado; e deveres de comunicação de quaisquer incidentes graves às autoridades de fiscalização do mercado dos Estados-membros onde tal incidente ocorrer.

Pese embora a importância da proposta de regulamento, o mesmo parece já estar obsoleto, atenta a evolução exponencial da inteligência artificial. Em causa está, designadamente, a emergência dos modelos LLM. Estando em causa um sistema de uso geral suscitam-se, desde logo, problemas no tocante ao controlo do seu funcionamento. Na verdade, se as obrigações definidas são proporcionais ao nível de risco definido e se os sistemas que apresentam um risco inaceitável devem ser banidos, os sistemas de risco elevado podem funcionar com restrições e mediante o cumprimento de rigorosos deveres. Quer isto dizer que, no tocante aos sistemas de uso geral, só se forem qualificados como sistemas de elevado risco é que ficam submetidos a uma maior supervisão e a restrições regulamentares. E a dificuldade no momento presente passa exatamente por qualificar a inteligência artificial generativa, de que é exemplo o ChatGPT, como sendo um sistema de elevado risco, atentos os anexos da proposta de regulamento, quando são óbvios os perigos que acarreta, quais sejam o acesso a dados pessoais que podem ser tratados fora das condições de legitimação para os quais foram transmitidos, a exposição de dados a terceiros, em função de bugs que se podem verificar, a proliferação de *fake news* e *deep fake news*, por força da atividade criativa do sistema, a manipulação ideológica ou emocional.

Não se nega, é certo, que as obrigações constantes do artigo 52º se aplicam igualmente aos sistemas de uso geral, de tal sorte que devem ser cumpridos deveres de informação no sentido de

esclarecer que as pessoas estão a interagir com um sistema de IA, bem como deveres no sentido de clarificar que alguns conteúdos foram gerados ou manipulados artificialmente e no sentido de informar sobre o funcionamento do sistema que permita o reconhecimento de emoções ou o reconhecimento biométrico.

Simplesmente, a despeito dos deveres de informação ou de aviso a que haja lugar, é possível que a pessoa sinta que age com uma entidade subjetiva, construindo um vínculo imaginário, mas perigoso, que a torna especialmente vulnerável às mensagens difundidas pelo algoritmo e especialmente permeável a lesões que venha a sofrer por meio dele. Com a agravante de, sendo os dados potenciadores da lesão criados pelo próprio algoritmo, se tornar particularmente difícil a imputação delitual.

Dir-se-ia, quanto à relação entre os dados pessoais usados ou gerados pela inteligência artificial e a responsabilidade civil, que as dificuldades são de dois tipos: em primeiro lugar, os dados que permitem o funcionamento da inteligência artificial podem sofrer uma corrupção, podendo não ser viável descobrir-se a sua origem ou não sendo o utilizador, distribuidor ou fabricante responsável por eles; em segundo lugar, os dados gerados pelo sistema autónomo, podendo eles próprios não ser fiáveis, podem resultar dos processos automáticos de autoaprendizagem.

Ora, também quanto a este ponto, as propostas europeias parecem ficar aquém do que seria desejável. Depois da proposta de um primeiro modelo em que se diferenciavam hipóteses de responsabilidade objetiva e de responsabilidade subjetiva, tendo em conta o nível de risco associado a cada um dos sistemas de inteligência artificial, parece seguir-se agora no sentido da primazia

da responsabilidade por culpa.

Nos termos da Diretiva Responsabilidade da IA, cuja proposta foi adotada pela Comissão em setembro, e de acordo com o artigo 4º/1, os tribunais nacionais presumem o nexo de causalidade entre o facto culposo do demandado e o resultado produzido pelo sistema de IA ou a incapacidade do sistema de IA de produzir um resultado, se estiverem preenchidas todas as seguintes condições: o demandante demonstrou ou o tribunal presumiu a existência de culpa do demandado, ou de uma pessoa por cujo comportamento o demandado é responsável, consistindo tal no incumprimento de um dever de diligência previsto no direito da União ou no direito nacional diretamente destinado a proteger contra o dano ocorrido; pode-se considerar que é razoavelmente provável, com base nas circunstâncias do caso, que o facto culposo influenciou o resultado produzido pelo sistema de IA ou a incapacidade do sistema de IA de produzir um resultado; o demandante demonstrou que o resultado produzido pelo sistema de IA ou a incapacidade do sistema de IA de produzir um resultado deu origem ao dano.

Os termos da presunção, ilidível, concitam-nos as maiores dúvidas. Desde logo, não se percebe o que se presume na hipótese de o lesado demonstrar que o resultado produzido pelo sistema de IA ou a incapacidade do sistema de IA de produzir um resultado deu origem ao dano e de ser razoavelmente provável, com base nas circunstâncias do caso, que o facto culposo influenciou o resultado produzido pelo sistema de IA ou a incapacidade do sistema de IA de produzir um resultado. Por outro lado, confunde-se a análise do âmbito de proteção do dever incumprido, a permitir uma presunção baseada na imputação, com uma ideia de probabilidade que nos aponta ainda para uma visão causalista e fisicista e com uma ideia

de dificuldade probatória.

Esta conclusão é confirmada pelas restantes regras em matéria de presunção de causalidade.

Assim, no caso de uma ação de indemnização intentada contra um fornecedor de um sistema de IA de risco elevado sujeito aos requisitos estabelecidos no título III, capítulos 2 e 3, do Regulamento Inteligência Artificial ou uma pessoa sujeita às obrigações do fornecedor nos termos do artigo 24º ou do artigo 28º, nº 1, do Regulamento Inteligência Artificial, a primeira condição só é cumprida se o autor da ação tiver demonstrado que o fornecedor ou, se for caso disso, a pessoa sujeita às obrigações do fornecedor não cumpriu algum dos seguintes requisitos estabelecidos nos referidos capítulos, tendo em conta as medidas tomadas e os resultados do sistema de gestão de riscos. A saber: o sistema de IA é um sistema que utiliza técnicas que envolvem o treino de modelos com dados que não foram desenvolvidos com base em conjuntos de dados de treino, validação e teste que cumprem os critérios de qualidade; o sistema de IA não foi concebido e desenvolvido de maneira que cumpra os requisitos de transparência; o sistema de IA não foi concebido e desenvolvido de maneira que permita uma supervisão eficaz por pessoas singulares durante o período de utilização do sistema de IA; o sistema de IA não foi concebido e desenvolvido de maneira que alcance, tendo em conta a finalidade prevista, um nível apropriado de exatidão, solidez e cibersegurança; ou as medidas corretivas necessárias não foram imediatamente tomadas para assegurar a conformidade do sistema de IA com as obrigações estabelecidas no Regulamento Inteligência Artificial.

Por seu turno, no caso de uma ação de indemnização intentada contra um utilizador de um sistema de IA de risco elevado sujeito aos requisitos estabelecidos no título III, capítulos 2 e 3, do Regulamento Inteligência Artificial, a primeira condição é cumprida se o demandante provar que o utilizador não cumpriu as suas obrigações de utilizar ou controlar o sistema de IA em conformidade com as instruções de utilização que o acompanham ou que expôs o sistema de IA a dados de entrada sob o seu controlo que não são pertinentes tendo em conta a finalidade prevista do sistema.

Além disso, no caso de uma ação de indemnização relativa a um sistema de IA de risco elevado, o tribunal nacional não pode aplicar a presunção prevista no nº 1 se o demandado demonstrar que estão razoavelmente acessíveis ao demandante elementos de prova e conhecimentos especializados suficientes para provar o nexo de causalidade; e, no caso de uma ação de indemnização relativa a um sistema de IA que não seja um sistema IA de risco elevado, a presunção estabelecida só é aplicável se o tribunal nacional considerar que é excessivamente difícil para o demandante provar o nexo de causalidade.

O enfoque da solução é probatória e orienta-se pela proteção do lesado. Repare-se, aliás, que se prevê a possibilidade de se contestar uma ação de responsabilidade quando baseada numa presunção de causalidade, que não ultrapassa o plano do ser, o que nos mostra a fragilidade da ponderação baseada na probabilidade.

Ora, se em geral o problema da causalidade não pode continuar a ser perspetivado segundo uma relação de causa-efeito, devendo

antes ser compreendido em termos imputacionais[50], torna-se insustentável aderir à posição tradicional, de que ainda é tributária a proposta europeia em matéria de responsabilidade civil pela IA, quando em causa estejam danos causados por sistemas autónomos. A opacidade e a autonomia da máquina inviabilizam as mais das vezes a prova da ligação de que se cura.

Os problemas parecem, contudo, ir além das dificuldades em sede causal. É que, mesmo solucionada a questão por outra via, sem a previsão de uma hipótese de responsabilidade objetiva, torna-se, em muitos casos, inviável indemnizar o lesado.

Quer no quadro da proposta europeia – na qual se exige a prova do não cumprimento ou a presunção do não cumprimento de um dever de diligência –, quer no quadro do entendimento que propomos a propósito da causalidade, que só funciona a partir do momento em que se edifica uma esfera de risco/responsabilidade que, se não é desenhada a priori pelo legislador, tem de emergir a partir da violação de deveres no tráfego, deixará de haver responsabilidade em todas as situações em que, não tendo sido preterido qualquer dever, a lesão resulta da corrupção de dados gerada pelo próprio algoritmo com base na aprendizagem que fez a partir de milhões de dados e da natureza das correlações estatísticas que elabora, as quais são suscetíveis de gerar enviesamentos discursivos.

Mafalda Miranda Barbosa

---

[50] Cf. Mafalda Miranda BARBOSA, *Do nexo de causalidade ao nexo de imputação. Contributo para a compreensão da natureza binária e personalística do requisito causal ao nível da responsabilidade civil extracontratual*, Princípia, 2013