A SAÚDE DIGITAL: RESPONSABILIDADE ARTIFICIAL?

António Cruz Oliveira[1]
Tiago Branco da Costa[2]
https://doi.org/10.21814/uminho.ed.148.7

Resumo: Ao longo dos últimos anos a saúde passou a conhecer uma vertente cada vez mais digital, isto é, o acesso aos cuidados de saúde e a prestação dos mesmos passou a ser assegurada com recurso e através de meios (cada vez mais) digitais (e avançados). Este progresso permitiu-nos conhecer novas formas de assegurar o direito à saúde (e a sua proteção), mais acessíveis, mais céleres, mais eficientes, mais precisas e mais eficazes. Até aqui chegarmos – e ainda que, naquela época, o que a seguir se reproduzirá pudesse colher laivos de repúdio – beneficiámos de uma pandemia que, não tendo permitido mais, possibilitou, pelo menos, a aposta no mercado digital e na ciência dos dados com a chancela da União Europeia. A sua ação tem, *in universum*, ajudado a clarificar a importância e a dimensão deste novo mundo eletrónico,

[1] Assistente Convidado na Escola de Direito da Universidade do Minho. Advogado *In-house*. Doutorando em Ciências Jurídicas, na especialidade de Ciências Jurídicas Privatísticas, na Escola de Direito da Universidade do Minho. Investigador integrado do Centro de Investigação em Justiça e Governação (JusGov). aaoliveira@direito.uminho.pt.

[2] Assistente Convidado na Escola de Direito da Universidade do Minho. Doutorando em Ciências Jurídicas, na especialidade de Ciências Jurídicas Privatísticas, na Escola de Direito da Universidade do Minho. Bolseiro da Fundação para a Ciência e Tecnologia. Investigador integrado do Centro de Investigação em Justiça e Governação (JusGov). tiagobrancodacosta@direito.uminho.pt.

digital e disruptivo em que a saúde se desenvolve. Tentaremos, desta forma, compreender a aplicação do regime da responsabilidade civil no contexto da saúde digital, para o qual a inteligência artificial e a proteção dos dados pessoais vêm sendo convocados.

Sumário: 1. Saúde digital: considerações iniciais; 2. A IA ao serviço da saúde; 2.1. Potencialidades e desafios jurídicos; 2.2. A IA e a sua regulamentação no quadro europeu; 2.3. A responsabilidade civil pela utilização da IA na saúde; 3. A proteção de dados pessoais na saúde; 3.1. Os dados (pessoais?) como fonte de alimentação da IA; 3.2. A proteção dos dados pessoais no contexto da saúde digital: em particular na utilização da IA; 3.3. A responsabilidade civil pelo tratamento de dados pessoais no contexto da saúde digital; 4. Conclusões.

Palavras-chave: Dados pessoais; Inteligência artificial; Proteção de dados; Responsabilidade civil; Saúde digital.

1. Saúde Digital: considerações iniciais

In novissimis, a saúde tem conhecido e acentuado o seu cariz digital, *id est*, o acesso aos cuidados de saúde e a prestação destes passou a ser feita com recurso e através de meios (cada vez mais) digitais (e avançados). Este progresso permitiu-nos conhecer novas formas de assegurar o direito à saúde (e a sua consequente proteção), mais acessíveis, mais rápidas e mais eficientes[3]... A pandemia que enfrentámos recentemente, por um lado, e a aposta no mercado digital e nos dados que a União Europeia tem levado a cabo, por outro, ajudaram também a clarificar a importância e a dimensão deste novo "mundo" em que a saúde se desenvolve[4]. É, precisamente, este mundo – "eletrónico", digital e disruptivo – que, habitualmente, designamos como "saúde digital" ("*digital health*") ou "e-saúde" ("*e-health*")[5]. Contudo, *non in solo pane vivit homo*: impuseram-se também novos desafios, designadamente, no panorama jurídico, e no domínio da responsabilidade civil, *ad exemplum*. Com efeito, o propósito do nosso estudo é o de compreender a aplicação do regime da responsabilidade civil no contexto da saúde[6] digital, para o qual a inteligência artificial e a proteção dos dados pessoais têm sido convocados. Por essa razão, não é nossa intenção desenvolver, aqui, pormenorizadamente, o regime legal da inteligência artificial nem o da proteção de dados pessoais,

---

[3] *Vd.* entre outros, Fosch-Villaronga, Eduard, *Robots, healthcare, and the law – regulating automation in personal care*, New York, Routledge, 2021, p.172, "A critical functional component of most healthcare robot technology is the capacity to sense, track, and monitor patients and their activities. The process of monitoring and tracking elderly, disabled, and children may have various purposes. These include: alarming in case of detected abnormalities, conveying or facilitating the supervision or intervention of caregivers, generating data flows useful for diagnostics and therapy, and favouring a more adaptive and personalized interaction with other assistive technologies"; Pedro, Rute Teixeira, "Breves reflexões sobre a reparação de danos causados na prestação de cuidados de saúde com utilização de robots", em Silva, Eva Sónia Moreira da & Freitas, Pedro Miguel (eds.), *Inteligência artificial e robótica: desafios para o direito do século XXI*, Coimbra, GESTLEGAL, 2022, 151-185, pp.153 e ss..

[4] Cfr. Proposta de Regulamento IA, exposição de motivos, ponto 1.1., §1; e ainda Comissão Europeia, *COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES, Orientações para a Digitalização até 2030: a via europeia para a Década Digital*, Bruxelas, 09 de março de 2021, COM(2021) 118 final, pp.1-3.

[5] Entre outros, *vd.* Patrício, Miguel, "Uma breve nota sobre os desafios éticos da saúde digital («digital health»)", em *Revista Jurídica Luso-Brasileira*, ano 4 (2018), nº 6, pp.1-20, p.1.; Moreira, Eva Sónia, "Considerations about medical liability in the era of e-health", em Carvalho, Maria Miguel (ed.), *E.Tec Yearbook: Health Law and Technology*, Braga, JusGov - Research Centre for Justice and Governance School of Law - University of Minho, 2019, pp.25-36, p.26.

[6] Referimo-nos ao «contexto da saúde», no sentido de aqui incluir não só a prestação de cuidados de saúde, mas também outras atividades conexas (v.g. investigação clínica), que se sirvam da inteligência artificial e do tratamento de dados pessoais e que, por isso, também possam caber nesta análise.

(por manifesta impossibilidade) sem prejuízo das considerações introdutórias e das referências que se imponham a esse respeito.

Pretendemos, assim, no decurso das linhas que se seguem, abordar, naturalmente de forma sucinta e sistematizada, mas tão cuidada quanto possível, a interseção dos tópicos *supra* enunciados, no contexto sanitário, não perdendo nunca de vista, sob pena de antecipação de um juízo de culpabilidade inteiramente justificável, o quadro legal europeu que se desenha a respeito da temática ora em crise, sabendo que tal arrojo ficará, por ora, aquém do desenvolvimento que tal tópico nos merece.

Após, estaremos em condições de problematizar a questão a que nos propusemos responder: será a responsabilidade civil no contexto da saúde digital uma responsabilidade artificial?

2. A IA ao serviço da saúde

Nos Estados Unidos da América (E.U.A.), três em cada quatro pessoas, servem-se do *online* para beber informação sobre saúde. No velho continente, esse número reduz-se, sendo, todavia, suficientemente elucidativo dos tempos que correm: um em cada dois *homo sapiens* consomem infosaúde em linha[7]. Em Portugal, *exempli causa*, as receitas prescritas pelo clínico podem ser acedidas pelos seus destinatários através da aplicação eletrónica (*App*)[8] disponibilizada pelo SNS24, cujos *downloads* na *App* perfaziam, em julho de 2023, mais de 8,6 milhões de transferências[9]. Na era dos dados, uma entre as demais, o que nos revelam aqueloutros a que agora aludimos? A *big picture* parece-nos clara: a revolução digital e tecnológica em curso continua a transformar a sociedade em que vivemos e, no seu interior, alguns setores são, ao menos aparentemente, mais permeáveis à sua omnipresença, como parece suceder com os respetivos sistemas de saúde.

---

[7] Dados que se encontram disponíveis para consulta em WWW: <URL: https://health.google/intl/pt-BR_ALL/consumers/search/> [consultado em 01/08/2023].

[8] A qual integra os denominados Serviços Digitais SNS24, e os quais se encontram disponíveis para consulta em https://www.sns24.gov.pt/ [consultado em 01/08/2023]

[9] Informação que pode ser acedida e que se encontra disponível para consulta em WWW: <URL: https://expresso.pt/iniciativaseprodutos/projetos-expresso/5-decadas-de-democracia/2023-07-06-Como-esta-o-digital-a-mudar-o--acesso-a-saude--d0cb8d9c> [consultado em 01/08/2023].

A telessaúde, a inteligência artificial, a *Big Data*, os biossensores, os *wearables* clínicos e a *Internet of Health Things (IoHT)*, entre outros, convocam, além dos naturais rácios económicos – como a garantia de uma maior eficiência na promoção e prestação de cuidados de saúde[10] - um conceito maior: o de saúde digital ou *eHealth*. A sua representação não constitui, *ex mea sententia*, tarefa ultimada, podendo ser definida como o ecossistema de ferramentas e serviços que utilizam tecnologias de informação e comunicação centradas na melhoria dos cuidados de saúde proporcionados ao doente (pacientopocentrismo) e na gestão ótima do sistema de saúde como um todo[11].

With great innovations comes great challenges: *in casu*, apenas temos a pretensão de atender aos desafios jurídicos que o fenómeno disruptivo-digital faz erigir pela sua emersão. Constitui factualidade absolutamente incontornável que a novel realidade *supra* enunciada promove a estreia de eventos lesivos cuja debelação cumpre ao Direito, mormente, ao Direito da Responsabilidade Civil, acautelar. Se o intermediário na aferição do respetivo diagnóstico – a máquina algorítmica – falha, a quem pertencerá a responsabilidade? Em caso de manifesta discordância entre a "verdade" transmitida pelo algoritmo e a ciência do profissional de saúde médico, de que forma procederemos ao recorte ou delimitação do critério imputacional do dever de indemnizar? A (in)suficiência dos atuais (clássicos) modelos de responsabilidade civil é interrogação artificial? *Quid iuris* se o algoritmo utilizado por um qualquer sistema de IA aplicado à saúde for instruído com dados potencialmente discriminatórios?[12] Qual a relação que se estabelece entre os dados pessoais e a inteligência artificial em contexto de saúde? Verifica-se a

[10] No mesmo sentido, *vide* Pedro, Rute Teixeira, *Breves reflexões sobre a reparação de danos causados na prestação de cuidados de saúde...*, *op. cit.*, p.157 e Antunes, Henrique Sousa, *Direito e Inteligência Artificial*, Lisboa, Universidade Católica Portuguesa, 2020, p.15.

[11] *Vide*, assim, HIMSS – Healthcare Information and Management Systems Society *cit.* por Isabel Guerra. *Cf.* Guerra, Isabel, *Telemedicina, relação médico-doente e aspetos deontológicos*, disponível para consulta em WWW: <URL: https://ordemdosmedicos.pt/telemedicina-relacao-medico-doente-e-aspectos-deontologicos/> [consultado em 23/07/2023]. No mesmo sentido, *vide*, entre outros, Comissão Europeia, *Saúde em linha (e-Saúde): Saúde e cuidados de saúde digitais*, *s.d.*, disponível para consulta em WWW: <URL: https://health.ec.europa.eu/ehealth-digital-health-and-care/overview_pt> [consultado em 23/07/2023]; Moreira, Eva Sónia, *Considerations about medical liability in the era of e-health...*, *op. cit.*, p.26.

[12] A este propósito, *vide*, *e.g.*, K.W. v. Armstrong, nº 14-35296 (9th Cir. 2015), disponível para consulta em WWW: <URL: https://law.justia.com/cases/federal/appellate-courts/ca9/14-35296/14-35296-2015-06-05.html> [consultado em 05/08/2023].

existência de mediana proporção entre a quantidade massiva de dados recolhidos e sua utilização, atenta a finalidade da primeira ação?

Ao longo das próximas fiadas procurar-se-á notar a conexão entre as questões colocadas pela maquinaria digital e as respostas oferecidas pela Ciência que a cata de acolher - a jurídica – reiterando, porém, que abundam as primeiras, e ainda escasseiam as segundas.

2.1. Potencialidades e Desafios Jurídicos

A primo tempore, cumprirá notar que, ao menos aparentemente, não se perspetiva simples a condição do *Ser negacionista*, nos dias que correm. Branquear o facto de tecnologia baseada em IA se constituir como instrumento auxiliar da ação humana na redefinição dos cuidados de saúde prestados (primários e hospitalares) ao doente/paciente-consumidor é tão credível como afirmar que o planeta terra adota formato plano. É, por isso, inquestionável que a susodita tecnologia aporta singular complementaridade no que ao diagnóstico e tratamento de enfermidades diz respeito, na disseminação e acesso a cuidados de saúde por banda dos mais vulneráveis – quer pela sua localização, quer pela sua patologia -, na instituição de farmacologia e medicina personalizada, na impressiva medicina de precisão (por via do cruzamento ciência genética e da bioinformática), na criação de dispositivos IoHT (autovigilância), desempenhando, outrossim, figura de relevo na predição e prevenção de surtos epidémicos (heterovigilância), quando ancorada em *Big Data*[13-14].

---

[13] *Vide*, a este título, Pereira, André G. Dias, "O médico-robô e os desafios para o Direito da Saúde: entre o algoritmo e a empatia", Lisboa, Gazeta de Matemática, Ano LXXX, nº 189, 2019, disponível para consulta em WWW: <URL: https://gazeta.spm.pt/fichaartigo?id=1527>, 30-34, p.30 [consultado em 05/08/2023]; Rocha, Miriam, "Virtualidades e limites do Direito face ao potencial discriminatório do uso da inteligência artificial", em Silva, Eva Sónia Moreira da & Freitas, Pedro Miguel (eds.), *Inteligência artificial e robótica: desafios para o direito do século XXI*, Coimbra, GESTLEGAL, 2022, 83-101, pp.86 e ss.; Pedro, Rute Teixeira, Rute Teixeira, *Breves reflexões sobre a reparação de danos causados na prestação de cuidados de saúde...*, *op. cit.*, pp.154 e ss., e Lobo, Marta Susana, "Responsabilidade Médica e Inteligência Artificial", *Lex Medicinae*, Revista Portuguesa de Direito da Saúde, Ano 20, nº 39 – Janeiro /Junho, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, 2023, disponível para consulta em WWW: <URL: http://www.centrodedireitobiomedico.org/publica%C3%A7%C3%B5es/revistas/revista-portuguesa-de-direito-da-sa%C3%BAde-lex-medicinae-ano-20-n%C2%BA-39-janeirojunho>, 73-91, pp. 83 e ss., [consultado em 05/08/2023].

[14] Revela-se de imperiosa referência, aludir à rede 5G. Esta última, pela sua velocidade e latência, permitirá disponibilizar faixas de frequência superiores à rede que a antecedeu (4G). Quer isto dizer que, no que à saúde digital

Da mesma sorte, não será "lícito" ao mais fiel seguidor desta nova "confissão" tecnológico-digital (IA) negar, à luz de tais desenvolvimentos, que aquela apresenta, à ciência jurídica, desafios próprios de uma era disruptiva: seja ao nível da conceção, registo e certificação de novos *wearables* clínicos assistidos por IA, ou pelo recurso, cada vez mais frequente, ao robô-assistente, o qual se encontra dotado de tal tecnologia, passando pela necessidade de subsumir o apontado desiderato tecnológico ao quadro legal vigente em matéria de recolha, tratamento e partilha de dados pessoais em ambientes colaborativos (*Big Data*), não esquecendo, *a limine*, a arquitetura que se pretende projetada para premunir a responsabilidade pelos danos causados por sistemas de inteligência artificial[15].

Ergo, são apenas alguns - e em traços gerais – os desafios que ora deslindamos, na certeza, porém, de que os mesmos se reconduzem a uma gota, num mar que não cessa de crescer.

2.2. A IA e a sua regulamentação no quadro europeu

In hoc tempore, têm assumido contido protagonismo as alterações aprovadas pelo Parlamento Europeu (PE), em 14 de junho de 2023, sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento sobre Inteligência Artificial) e que altera determinados atos legislativos da União (COM (2021) 0206) – visando as primeiras a promoção de uma IA centrada no ser humano, segura e transparente, ancorada na proteção da saúde e dos direitos fundamentais dos efeitos perversos que podem resultar

concerne, tal se traduz num tratamento mais célere dos pacientes, na expansão da utilização da telemedicina (em todas as suas modalidades, *eg.*, telecirurgia sem fios), maior eficiência no atendimento de casos urgentes, viaturas médicas de emergência mais conectadas, possibilitando um contacto mais estreito entre o doente e o clínico a partir do próprio veículo ou o recurso a novas terapêuticas para redução desse flagelo denominado ansiedade por via da realidade virtual. A este respeito vide a informação que se encontra disponível para consulta em WWW: <URL: https://portal5g.pt/temas/e-saude/> [consultado em 10/08/2023].

[15] *E.g.*, resultem aqueles da disponibilização, no mercado, de produtos defeituosos, condicionando, assim, a possibilidade de obter diagnósticos corretos e precisos, ou, em alternativa, resulte tal mácula de um *bug* na interconectividade do ecossistema digital, daí proliferando um verdadeiro evento adverso.

da sua utilização[16]. Voltaremos a este porto, após competente retrospetiva dos que lhe precederam.

A Indústria 4.0. ou quarta revolução industrial, como apelidada por Klaus Schwab[17], clama por um ímpeto reformador dos cânones regulatórios e jurídicos vigentes, aos quais o legislador europeu não tem sabido responder com a celeridade com que a rutura tecnológico-digital o assalta. *Rule or regulate to care*, *id est,* a necessidade de estabelecer o comando normativo como meio potenciador de superintendência, controlo e mitigação de riscos inerentes ao complexo ecossistema em que se move a IA, e aos danos emergentes do seu uso. Mas não só: a definição de um quadro legal, claro e uniforme, permitirá aos operadores económicos desenvolver, num ambiente de manifesta segurança jurídica, uma estratégia de inovação assente em tecnologia capacitada com IA, cuja principal beneficiada seja a sociedade, como coletivo uno. Não tendo ainda ultrapassado a barreira do debate legislativo-institucional, terá sido tal intenção a presidir às comunicações da Comissão Europeia (CE), datadas de 2018 e 2019, designada e respetivamente, a Comunicação da Comissão sobre IA para a Europa[18] e a Comunicação da Comissão subordinada à epígrafe do aumento da confiança numa IA centrada no ser humano[19-20].

---

[16] Neste sentido, *vide* a informação que encontra disponível para consulta em WWW: <URL: https://www.europarl.europa.eu/news/pt/press-room/20230609IPR96212/parlamento-negoceia-primeiras-regras-para-inteligencia-artificial-mais-segura> e em WWW: <URL: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PT.html>, [consultado em 10/08/2023]. Será esta última versão da Proposta de Regulamento IA que levaremos em linha de conta ao longo da nossa exposição.

[17] *Cf.* Schwab, Klaus, "The fourth Industrial Revolution: what it means, how to respond", *World Economic Forum*, 2016, disponível para consulta em WWW: <URL: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> [consultado em 06/08/2023].

[18] Cfr. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Inteligência artificial para a Europa*, Bruxelas, 25 de abril de 2018, COM(2018) 237 final, disponível para consulta em WWW: <URL: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018DC0237> [consultado em 06/08/2023.

[19] Cfr. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Aumentar a confiança numa inteligência artificial centrada no ser humano*, Bruxelas, 8 de abril de 2019, COM(2019) 168 final, disponível para consulta em WWW: <URL: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52019DC0168> [consultado em 06/08/2023].

[20] Detalhadamente, *vide*, Sousa, Susana Aires de, "Breves notas sobre a "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"", em *Direito em Mudança, A Proposta de Regulamento Europeu sobre Inteligência Artificial, Algumas Questões Jurídicas*, Suana Aires de Sousa (Coord.), 2023, disponível para consulta em WWW: <URL: https://www.uc.pt/site/assets/files/1184561/a_proposta_de_regulamento_ebook.pdf>, 1-14, pp.3 e ss. [consultado em 06/08/2023].

O intento daquela instituição europeia prosseguiu, desta feita, densificado no Livro Branco sobre a IA[21], documento onde seguiu ínsita a dilemática de procurar equilibrar os dois "fiéis da balança": *ex uno latere*, o intuito de proceder a uma abordagem normativa da tecnologia servida por IA, atentos os riscos associados ao seu emprego e, por outro, permitir que o progresso científico seja cultivado de forma sã, dentro das margens delimitadas pelos valores da União[22]. A construção do caminho aflorado não se fez sem a adoção de outros documentos de nomeado interesse, entre os quais notabilizamos a Resolução do Parlamento Europeu, de 16 de fevereiro de 2017[23], a Resolução do Parlamento Europeu, datada de 20 de outubro de 2020[24], e o Relatório apresentado pela Comissão Europeia ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social, datado de 19 de fevereiro de 2020[25].

O início da década marca o ponto de viragem: do plano conjetural ao primeiro projeto de tela legal sobre IA (dimensão da ação), substanciada na proposta de Regulamento sobre Inteligência Artificial[26]. Tal desiderato legislativo traduz o somatório das sinergias das instituições europeias para alcançar um feixe único e harmonizado de regras com o fito de regular a IA

---

[21] Cfr. Comissão Europeia, *Livro Branco sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança*, Bruxelas, 19 de fevereiro de 2020, COM(2020) 65 final, disponível para consulta em WWW: <URL: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en> [consultado em 06/08/2023].

[22] Cfr. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Aumentar a confiança numa inteligência artificial centrada no ser humano...*, *op. cit*., p. 1.

[23] Cfr. Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103 (INL)), disponível para consulta em WWW: <URL: www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.pdf> [consultado em 06/08/2023].

[24] Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime de responsabilidade civil aplicável à inteligência artificial (2020/2014 (INL)), disponível para consulta em WWW: <URL: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020IP0276> [consultado em 06/08/2023].

[25] Cfr. Comissão Europeia, *Relatório da Comissão ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu - Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica*, Bruxelas, 19 de fevereiro de 2020, COM(2020) 64 final, disponível para consulta em WWW: <URL: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52019DC0168> [consultado em 06/08/2023].

[26] Cfr. Comissão Europeia, *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*, Bruxelas, 21 de abril de 2021, COM(2021) 206 final, 2021/0106 (COD), disponível para consulta em WWW: <URL: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021PC0206> [consultado em 06/08/2023], doravante designado apenas por Proposta de Regulamento IA.

dentro de portas (União Europeia), almejando, *ad summam*, alcançar um elevado nível de proteção dos direitos fundamentais dos cidadãos europeus vinculados à União[27].

Desafortunada e inexplicavelmente, o famigerado Regulamento não se ocupou, *per se*, de aventar qualquer solução que pudesse contribuir para a discussão em torno da temática da responsabilidade civil por danos causados por sistemas dotados de IA, o que configura, salvo o devido respeito por diferente opinião, manifesto prejuízo no que à codificação e sistemática jurídicas diz respeito. A utilidade de tal proposta para o apontado efeito resultará da sua conjugação com uma outra: a proposta de Diretiva para a Responsabilidade Civil em assuntos de IA[28-29-30]. *Ad conclusum*, a proposta de quadro regulamentar em matéria de IA citada *supra* apresenta os seguintes caracteres: (i) garantir que os sistemas de IA disponibilizados no mercado cumprem os desígnios ético-legais que presidem à União dos 27; (ii) garantir a segurança jurídica como paradigma potencializador de atração de investimento e inovação no domínio da IA (iii) criar as condições necessárias para a melhoria dos mecanismos de boa governança e aplicação efetiva do *corpus juris* em vigor no concernente a matéria de direitos fundamentais (iv) possibilitar o desenvolvimento de um mercado único para as aplicações de IA legítimas, seguras e fiáveis[31]. A concretização dos nominados propósitos é disposta ao correr de doze títulos e outros tantos anexos, os quais materializam as

---

[27] *Idem,* pp. 2-19.

[28] Cfr. Comissão Europeia, *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial (Diretiva Responsabilidade da IA)*, Bruxelas, 28 de setembro de 2022, COM(2022) 496 final, 2022/0303 (COD), disponível para consulta em WWW: <URL: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52022PC0496&from=EN> [consultado em 06/08/2023], doravante designada apenas por Proposta de Diretiva Responsabilidade IA.

[29] Isto, sem esquecer a Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à responsabilidade decorrente dos produtos defeituosos - COM. (2022) 495 final – 2022/0302 (COD) - disponível para consulta em WWW: <URL: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52022AE4922> [consultado em 06/08/2023].

[30] Em perfeita comunhão com o que parece resultar da lição de Barbosa, Mafalda Miranda, "Ainda o futuro da Responsabilidade Civil pelos danos causados por Sistemas de IA", em *Revista de Direito da Responsabilidade*, Ano 5, 2023, disponível para consulta em WWW: <URL: https://revistadireitoresponsabilidade.pt/2023/ainda-o-futuro-da-responsabilidade-civil-pelos-danos-causados-por-sistemas-de-ia-mafalda-miranda-barbosa/>, 337-369, p. 363 [consultado em 06/08/2023].

[31] Cfr. Proposta de Regulamento IA, p.3.

obrigações impostas aos operadores económicos que produzam e disponibilizem e utilizem os seus sistemas de IA dentro da União Europeia[32].

Já no que tange à abordagem de tal proposta de Regulamento aos sistemas baseados em IA, uma última referência para sublinhar que a mesma é agora baseada no risco (título II, do Regulamento), apresentando uma estrutura de ordem decrescente: risco inaceitável (artigo 5º), risco elevado (artigo 6º) e risco mínimo.

Regressamos ao "porto" de partida, para reiterar a mensagem de raiz: a supressão das linhas do tempo pela evolução hipersónica do processo digital não possibilita discussões eternas sobre o Regulamento perfeito. A posição adotada pelo Parlamento Europeu recentemente, em face do Regulamento sobre Inteligência Artificial – impulsionada pelo advento da IA generativa[33] - é a prova disso mesmo. O Direito não precisará do Direito, mas a Sociedade sim; todos nós, cidadãos da União, carecemos daquela Ciência para a salvaguarda eficaz dos direitos absolutos que se encontram positivados no Direito dos Tratados Europeus como o último reduto de proteção (e de liberdade) da pessoa face aos efeitos nocivos que qualquer tecnologia baseada em IA possa desencadear.

2.3. A responsabilidade civil pela utilização da IA no contexto da saúde digital

Conforme oportunamente referido, a Comissão Europeia adotou, em 28 de setembro de 2022, uma Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à adaptação das regras da responsabilidade civil extracontratual à inteligência artificial (Diretiva Responsabilidade IA), com o claro propósito de, por aquela via, proceder a uma harmonização da legislação europeia neste particular, virtude da ausência de imperativos legais uniformes entre os Estados-Membros, atinentes à indemnização dos danos causados

[32] *E.g.*, *vide* o considerando 56, da Proposta de Regulamento IA.

[33] A IA generativa pode ser definida como um processo "automatizado que utiliza algoritmos para produzir, manipular ou sintetizar dados, muitas vezes sob a forma de imagens ou texto legível por humanos". O seu rosto mais popular são os complexos modelos do ChatGPT ou DALL-E. Cfr. Fruhlinger, Josh ,"O que é a IA generativa e como funciona?", 2023, artigo em linha, disponível para consulta em WWW: <URL: https://www.computerworld.com.pt/2023/03/14/o-que-e-a-ia-generativa-e-como-funciona/> [consultado em 07/08/2023].

por sistemas de IA. *Grosso modo*, as patentes discrepâncias entre os remédios que cada ordenamento jurídico oferece como meio debelatório da presente contenda – mormente, quando os mencionados sistemas de AI importem o confronto com bens jurídicos fundamentais, como a vida, a saúde, a integridade física e moral ou a identidade pessoal – serviriam apenas para potenciar uma crescente fragmentação decisória e não o inverso[34].

No ideário da intenção, tal esforço legislativo é, em qualquer circunstância, objeto do devido aplauso; no plano concreto, a nossa concordância fica por ali. A opção do legislador europeu por um modelo de responsabilidade civil subjetiva assente no juízo de censura sobre o concreto agente (culpa) pressupõe a adoção de um critério de natureza personalístico que, na hipótese sob julgo, não nos permitimos acompanhar. *Lato sensu*, a culpa consiste na imputação de um determinado facto ao agente; mais, *de jure condito*, dir-se-á que, regra geral, o instituto da responsabilidade civil supõe a culpa, a qual traduzirá a situação psicológica do agente para com o facto praticado[35]. A questão que, então, se coloca é a seguinte: que agente? O ente dotado de IA? Competirá a este ponderar o lado subjetivo da sua conduta? Esperamos, portanto, que o robô-assistente (dimensão física – *hardware*) que, incorporando tecnologia de IA que lhe proporciona 100% de autonomia para a função para a qual foi concebido e programado (dimensão digital), desampara, sem razão justificativa, o doente que carrega desde a viatura de emergência médica até ao bloco operatório, agravando, por consequência, a lesão do enfermo, devesse ter agido de modo diverso com base numa consciência que não possui? Não ignoramos que a proposta de Diretiva em apreço comporta uma inegável dimensão adjetiva temperada por uma variável substantiva, sendo, por tal, aplicável a ações de responsabilidade civil extracontratual por danos causados por sistemas de IA sempre que tais demandas sejam propostas ao abrigo de

[34] *Cf.* Proposta de Diretiva Responsabilidade IA, pp. 5-6.

[35] Por todos, *vide*, entre outros, Costa, Mário J. Almeida, *Direito das Obrigações*, 12.ª Edição, revista e atualizada, Coimbra, Almedina, 2014, pp. 578 e ss; Varela, J. Antunes, *Das Obrigações em Geral*, volume I, 10ª ed., revista e atualizada, Coimbra, Almedina, 2000, pp.566 e ss.; Faria, J. Ribeiro de; Vasconcelos, Miguel Pestana; e Pedro, Rute Teixeira, *Direito das Obrigações*, Volume I, 2ª edição – reimpressão 2021, Coimbra, Almedina, 2020, pp. 436 e ss.; Barbosa, Mafalda Miranda, *Lições de Responsabilidade Civil*, Princípia Editora, 1ª Edição, 2017, pp. 227 e ss; e Cordeiro, António Menezes, *Tratado de Direito Civil VIII – Direito das Obrigações, Gestão de Negócios, Enriquecimento sem Causa, Responsabilidade Civil*, Reimp. da 1ª Edição do Tomo III da parte II de 2010, Coimbra, Almedina, 2017, pp. 435 e ss.

regimes de responsabilidade culposa (artigo 1º, da Proposta de Diretiva IA)[36], aliviando, de uma banda, o ónus da prova do lesado, pela introdução de uma presunção de causalidade (artigo 4º, da Proposta de Diretiva IA), facultando, por outra, célere acesso, por parte daquele, a elementos de prova (artigo 3º, da Proposta de Diretiva IA). Porém, as nuances introduzidas por tal Proposta, complementada, *summo rigore*, pela Proposta de Diretiva 2022/0302 (COD), referente à responsabilidade decorrente de produtos defeituosos, em nada alteram a questão de facto: a ausência de consciência de si, ou de representação de um dado estado mental, torna o ente dotado de IA suscetível de lhe ver ser assacado um juízo de "reprovabilidade pessoal"?[37] Cremos que não. Ao nosso robô assistente faltam-lhe, entre outras, e para além do natural domínio da consciência, a imaginação, a criatividade, o sentimento e a mundividência espiritual próprias do *ser de carne e osso*[38-39].

Na ótica do legislador europeu, o repto lançado pela IA é, assim, resolúvel com a pedra filosofal da presunção (de causalidade), a qual parece encontrar-se gizada para tribunais alimentados pela denominada IA forte,

---

[36] Cfr. Proposta de Diretiva Responsabilidade IA, p. 13.

[37] Varela, J. Antunes, *Das Obrigações em Geral*..., *op. cit*., p.566.

[38] Tampouco aderimos a uma ideia de pampsiquismo, ou seja, recondutora da animização dos vários elementos da natureza. Por diferentes palavras, a consciência é uma característica fundamental, senão básica, do mundo/matéria física. Com maior detalhe, vide, Curado, J. M., "Bombarda e a Consciência I", em *Jornal de Ciência Cognitivas*, 2005, disponível para consulta em WWW: <URL: https://repositorium.sdum.uminho.pt/bitstream/1822/3746/1/JCC%20BOMBARDA%20E%20A%20CONSCIENCIA.pdf> [consultado em 07/08/2023].

[39] Neste sentido, colham-se, de igual sorte, os lapidares ensinamentos de Sónia Moreira da Silva. Questiona a distinta Autora, se, *e.g.*, fará sentido que um "agente autónomo seja titular de direitos de personalidade? Faz sentido que seja titular do direito à vida, à integridade física, à imagem, à honra... à semelhança de um ser humano? Como defender a existência, por exemplo, de um direito à auto-determinação ou um direito ao livre desenvolvimento da personalidade de uma máquina? Atribuir a uma máquina um estatuto jurídico que se assemelhe ao do ser humano é coisificar o ser humano, é diminuir o ser humano, é atentar contra a sua dignidade (...)". Comungamos ainda de posição idêntica quanto à analogia de base estribada pela Autora, mormente, no que concerne ao facto do nosso ordenamento jurídico não ter criado estatuto similar ao do *homo sapiens* relativamente aos animais, não obstante existirem sólidos indícios de senciência em animais. Concluir que alguns destes seres vivos possuem a capacidade de experimentar sensações de forma consciente não os torna, *ipso facto*, sujeitos de direitos e obrigações. – *Cf*. Silva, Eva Sónia Moreira da, "IA e Robótica: a caminho da personalidade jurídica?", em Oliveira, A. Sofia Pinto & Jerónimo, Patrícia (Coord.), *Liber Amicorum Benedita Mac Crorie*, Volume II, Braga, Uminho Editora, 2022, p.548; *vide* ainda, na esteira do exposto, Barbosa, Mafalda Miranda, "O futuro da responsabilidade civil desafiada pela inteligência artificial: as dificuldades dos modelos tradicionais e caminhos de solução", em *Revista de Direito da Responsabilidade*, Ano 2, 2020, disponível para consulta em WWW: <URL: https://revistadireitoresponsabilidade.pt/2020/o-futuro-da-responsabilidade-civil-desafiada-pela-inteligencia-artificial-as-dificuldades-dos-modelos-tradicionais-e-caminhos-de-solucao-mafalda-miranda-barbosa/>, p.310 e ss. [consultado em 08/08/2023]; Maia, Ana Rita, "A Responsabilidade Civil na Era da Inteligência Artificial – Qual o caminho?", em *Revista Julgar*, 2021, disponível para consulta em WWW: <URL: http://julgar.pt/a-responsabilidade-civil-na-era-da-inteligencia-artificial-qual-o-caminho/>, p.33, e Humphrey, Nicholas, *Senciência: a invenção da consciência*, Bertrand Editora, 2023, pp.222-223.

ou ASI (*Artificial Super Intelligence)*[40]. Além de enformar de um pendor marcadamente assimétrico[41], aparenta confundir, bebendo de melhores palavras, a apreciação 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"[42].

Recuperamos o acarinhado robô-assistente como representação das dificuldades que, neste campo, se apresentam como fraturas expostas. Arredada a possibilidade de atribuição de personalidade jurídica eletrónica a entes despersonalizados, cumprirá determinar, nessa conformidade, o agente sobre o qual recairá a obrigação de indemnizar. O comportamento (positivo ou negativo) a partir do qual é infligida a lesão ao doente – *id est*,

---

[40] *Vide,* pormenorizadamente, Silva, Eva Sónia Moreira da, *IA e Robótica: a caminho da personalidade jurídica?..., op. cit.*, p.538.

[41] O quadro jurídico para o exercício da contraprova por parte do lesante/demandado é notoriamente desproporcional, compreendendo-se mal como pretende o legislador transnacional acautelar um ambiente digitalmente seguro e transcendentalmente apetecível para o investimento da Indústria tecnológica na União, assegurando-lhe, por via de tal Proposta de Diretiva, que, em caso de evento lesivo, a mesma parte já em desvantagem no que ao juízo imputacional do facto ao agente diz respeito. Caso contrário, vejamos: dispõe o artigo 4º, nº 1, da Proposta de Diretiva IA que, sob "reserva dos requisitos estabelecidos no presente artigo, os tribunais nacionais presumem, para efeitos da aplicação das regras de responsabilidade a uma ação de indemnização, 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": (a) "O demandante demonstrou ou o tribunal presumiu, nos termos do artigo 3º, nº 5, 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"; (b) "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"; (c) 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". Numa temática de cariz iminentemente técnico, com uma complexidade ainda não totalmente descortinada, caberá ao intérprete-julgador presumir um qualquer nexo causal? O "facto culposo" atribuído ao demandado deriva do "incumprimento de um dever de diligência previsto no direito da União ou no direito nacional". Quedamo-nos, por ora, interrogados: a que dever de diligência se reporta o legislador? Terá debruçado o seu pensamento sobre o critério do *reasonable doctor,* do profissional de saúde médio ou do bom pai de família? Desconhecendo a *ratio essendi* da referida cogitação, qualquer daqueles deverá ser objeto de competente revisão, uma vez que a sua enunciação apresenta uma conexão incindível com a natureza humana. Do mesmo modo, se a intenção daqueloutro redunda no estabelecimento de um novo dever de diligência, ilustrativamente, o do *reasonable computer standard*, somos a entender que a sua formulação não é geneticamente compatível com um modelo assente na responsabilidade civil delitual, porquanto perspetivado para a máquina e não para o Homem. *Vide*, a respeito da vertente temática, Antunes, Henrique Sousa, "Inteligência Artificial e Responsabilidade Civil: Enquadramento", em *Revista de Direito da Responsabilidade*, Ano 1, 2019, disponível para consulta em WWW: <URL: https://revistadireitoresponsabilidade.pt/2019/inteligencia-artificial-e-responsabilidade-civil-enquadramento/>, p. 153 [consultado em 08/08/2023] e Abbot, Ryan, «The Reasonable Computer: Disrupting the Paradigm of Tort Liability», em *George Washington Law Review*, Volume 86, nº 1, 2018, disponível para consulta em WWW: <URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2877380>, p.37 [consultado em 08/08/2023.

[42] Cfr. Barbosa, Mafalda Miranda, Ainda o futuro da Responsabilidade Civil pelos danos causados por Sistemas de IA..., *op. cit.*, p.363.

o facto daquele robô interromper a sua marcha deixando cair aparatosamente o paciente - é atribuível ao fabricante, ao programador ou ao utilizador (prestador dos cuidados de saúde)? *In secondo luogo*, a ação desencadeada pelo robô resulta da aprendizagem do mesmo quando em contacto com o ambiente que o rodeia?[43]

A resposta à primeira questão requer um "fumo branco" que ainda não raia. Assim, a geometria variável de agentes a quem pode ser assacada alguma espécie de responsabilidade aliada à complexidade e negritude algorítmica que animam a estrutura física robotizada dificultam a concreta identificação daqueles que deram causa ao dano[44]. Daqui resulta que daquela miríade de sujeitos poderá advir a "desproteção indevida do doente"[45], personagem esta que deveria permanecer alheia aos efeitos contraproducentes da tecnologia que, ao menos aparentemente, a visa beneficiar.

A segunda questão tem chamado à colação, não raras vezes, o comando legal previsto, pelo nº 2, do artigo 493º, do Código Civil. Nesse sentido, todo aquele que, no exercício de uma atividade perigosa, por sua própria natureza ou pela natureza dos meios utilizados, causar dano a outrem, está obrigado a repará-lo, salvo se lograr demonstrar que envidou todas as providências exigidas pelas circunstâncias com o fim de o prevenir. Na hipótese em equação, a condição evolutiva imprevisível da espécie robótica em crise (robô assistente), e os riscos que dali podem emergir para a saúde e integridade física dos doentes, em virtude da real capacidade de autoaprendizagem da máquina, permitirá concluir que a utilização de tais geringonças encerra perigosidade bastante que justifique a aplicação da presunção vertida no normativo citado[46]. Operando esta última, recairá sobre o prestador de cuidados de saúde a obrigação de proceder à reparação dos danos produzidos no exercício da atividade especialmente perigosa, salvo se ilidir a dita presunção, *de lege lata*.

Se no vertente caso, tendemos a aderir ao entendimento proposto, a verdade é que não descuramos que o emprego casuístico da vertente solução

---

[43] No apontado sentido, *vide*, Pedro, Rute Teixeira, *Breves reflexões sobre a reparação de danos causados na prestação de cuidados de saúde...*, *op. cit.*, pp.160-161.

[44] *Ibidem*, pp. 176-177.

[45] *Ibidem*, p. 177.

[46] *Ibidem*, p. 174.

não promove a tão desejada harmonização do sistema jurídico como um todo, até porque se afigura de complexo cotejo, o recorte das situações de perigosidade efetiva envolvendo *robots*[47].

Até que o nosso humilde saber mature em sentido diverso, e não refutando, em circunstância alguma, que o entendimento agora propugnado enverede por caminho distinto, continuamos a pugnar, acompanhando outros, antes de nós[48], pela necessidade do legislador europeu ou, na sua ausência, o legislador nacional, prefigurar a previsão de um cenário assente na responsabilidade objetiva, como *iter* mais eficaz no combate e prevenção dos complexos riscos multipolares emergentes da utilização de sistemas baseados em IA.

3. A proteção de dados pessoais na saúde

Será possível prestar cuidados de saúde sem proceder ao tratamento de dados? Toda a informação tratada em contexto de saúde será, necessariamente, considerada informação relativa a uma pessoa identificada ou identificável? Os dados pessoais tratados em contexto de saúde serão sempre considerados dados pessoais de categorias especiais? Qual a relação que se estabelece entre os dados pessoais e a inteligência artificial em contexto de saúde?

Estas são algumas das questões que, frequentemente, emergem no contexto da prestação de cuidados de saúde e às quais tentaremos, de forma sumária, dar resposta ao longo dos próximos capítulos. Se, por um lado, os avanços significativos da tecnologia têm permitido alcançar mais e melhores resultados, por outro lado também tomámos consciência de que, num contexto cada vez mais digital, o tratamento de dados pessoais, alinhado com a estratégia europeia para os dados, deve respeitar os princípios e regras basilares nesta matéria, mormente os prescritos pelo Regulamento Geral

[47] *Cf.* Barbosa, Mafalda Miranda, I*nteligência Artificial: entre a utopia e a distopia, alguns problemas jurídicos*, Coimbra, GESTLEGAL, 2021, pp. 88-89.

[48] *Idem*, pp. 97 e ss.; Barbosa, Mafalda Miranda, *Ainda o futuro da Responsabilidade Civil pelos danos causados por Sistemas de IA..., op. cit.*, p.369; e Pedro, Rute Teixeira, *Breves reflexões sobre a reparação de danos causados na prestação de cuidados de saúde..., op. cit.*, p. 175.

sobre a Proteção de Dados (RGPD)[49]. Com efeito, a Comissão Europeia, por altura da apresentação de «Uma Agenda Digital para a Europa»[50], assinalou a falta de confiança dos cidadãos em matéria de proteção da privacidade e segurança e, por conseguinte, o impacto negativo no desenvolvimento do mercado digital. Por essa razão, em 2012, sublinhando o papel crucial da Diretiva 95/46/CE[51], lançou o repto de se proceder à atualização do quadro legal europeu referente à proteção de dados pessoais[52]. Mais tarde, em 2015, através da «Estratégia para o Mercado Único Digital na Europa»[53], a Comissão reconhecendo que a economia mundial estava a tornar-se digital, apontou várias oportunidades no domínio dos serviços digitais, dos quais fazia parte a saúde em linha.

Deste modo, depois de dar à luz o RGPD, em 2016; de apresentar, em 2017, o processo de construção de uma economia europeia dos dados[54]; de ser publicado, em 2018, o Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia[55]; de apresentar, em 2020, a «Segunda Agenda Digital para a Europa»[56]; de lançar, em 2021, as «Orientações para a Digitalização até 2030: a via europeia para a

[49] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), OJ L 119, 04 de maio de 2016, pp.1–88.

[50] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Uma Agenda Digital para a Europa*, Bruxelas, 19 de maio de 2010, COM(2010)245.

[51] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, OJ L281, 23.11.1995, pp. 31-50.

[52] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Proteção da privacidade num mundo interligado: Um quadro europeu de proteção de dados para o século XXI*, Bruxelas, 25 de janeiro de 2012, COM(2012)9 final, p. 2.

[53] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Estratégia para o Mercado Único Digital na Europa*, Bruxelas, 06 de maio de 2015, COM(2015)192 final.

[54] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Construir Uma Economia Europeia Dos Dados*, Bruxelas, 10 de janeiro de 2017, COM(2017) 9 final.

[55] OJ L 303, 28 de novembro de 2018, pp. 59-68.

[56] Comissão Europeia, *Shaping Europe's digital future* [Construir o futuro digital da Europa], Luxemburgo, 19 de fevereiro de 2020, disponível em: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_pt#documentos [consultado em 11.08.2023].

Década Digital»[57]; de ser publicada, em 2022, a «Declaração Europeia sobre os Direitos e Princípios Digitais para a Década Digital»[58]; em maio de 2022, a Comissão Europeia lançou o espaço europeu de dados de saúde (EEDS)[59], apresentando a «Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde»[60-61]. Este espaço comum europeu congrega as necessidades de progresso e evolução, no que respeita à forma e aos meios através dos quais os cuidados de saúde são prestados às pessoas na União, bem como a necessidade de facilitar o controlo dos dados pessoais pelos cidadãos, designadamente através do reforço dos seus direitos.

Sem prejuízo de todos os avanços, iniciativas, propostas e diplomas apresentados no contexto europeu, mantém-se viva a preocupação com a proteção de dados, tendo em conta a experiência europeia recente que demonstrou que sem a confiança dos cidadãos no mercado europeu e nos seus operadores, bem como nas instituições da UE, o futuro do mercado digital claudicará.

Em particular no domínio saúde, constata-se uma maior preocupação relativamente ao tratamento de dados pessoais, o que se justifica, essencialmente, por três razões. Em primeiro lugar, os dados pessoais tratados em contexto de saúde não assumem todos a mesma natureza. Com efeito, aqueles que mais importam para as finalidades de saúde são, por princípio, os dados relativos à saúde – "*dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem*

---

[57] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Orientações para a Digitalização até 2030: a via europeia para a Década Digital*, Bruxelas, 09 de março de 2021, COM(2021) 118 final.

[58] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, que estabelece uma Declaração Europeia sobre os Direitos e Princípios Digitais para a Década Digital*, Bruxelas, 26 de janeiro de 2022, COM(2022) 27 final.

[59] Disponível em https://ec.europa.eu/commission/presscorner/detail/pt/ip_22_2711 [consultado em 06/08/2023].

[60] Comissão Europeia, Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde, Estrasburgo, 03 de maio de 2022, COM(2022) 197 final, 2022/0140(COD).

[61] Cfr. Costa, Tiago Branco da, "O altruísmo (económico?) de dados: breves considerações sobre o espaço europeu de dados de saúde e a proteção de dados pessoais", em Oliveira, A. Sofia Pinto & Jerónimo, Patrícia (Coord.), *Liber Amicorum Benedita Mac Crorie*, Volume II, Braga, Uminho Editora, 2022, pp. 613-622.

informações sobre o seu estado de saúde" –, que são considerados dados de categorias especiais e, portanto, merecedores de uma tutela acrescida[62-63].

Em segundo lugar, porque os dados elencados no nº 1 do artigo 9º – *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* – estão historicamente associados a experiências e acontecimentos sociais que marcaram, profundamente, a forma como encaramos a dignidade humana e a proteção do indivíduo face ao "tratamento (abusivo) de informações que lhe digam respeito"[64]. Por esta razão, o legislador europeu optou por proibir, por princípio, o tratamento deste tipo de dados pessoais. Contudo, ciente de que o seu tratamento pode ser precioso em determinados contextos (de que prestação de cuidados de saúde constitui exemplo) cuidou de estabelecer, a título excecional, um conjunto de situações que poderão justificar o sobredito tratamento[65].

Em terceiro lugar, porque, para além dos dados relativos à saúde, os dados genéticos e os dados biométricos podem também ser preciosos em contexto de saúde, e estes, por oferecerem informações únicas sobre o titular dos dados, podem constituir um perigo acrescido para a sua esfera privada

---

[62] Cfr. artigo 9º do RGPD. Esta tutela tem que ver com o grau de privacidade de que gozam estes dados, *i.e.*, os dados pessoais em questão referem-se à esfera íntima do indivíduo. A este respeito, *Vd.* Vasconcelos, Pais de, *Direitos de Personalidade*, reimpressão da edição de 2006, Coimbra, Almedina, 2017, p. 80, "Tem sido tentado um critério de determinação do conteúdo do direito à privacidade assente sobre a distinção de três esferas concêntricas: a esfera da vida íntima, a esfera da vida privada e a esfera da vida pública. Na esfera da vida íntima compreender-se-ia o que de mais secreto existe na vida pessoal, que a pessoa nunca ou quase nunca partilha com outros, ou que comunga apenas com pessoas muitíssimo próximas, como a sexualidade, a afetividade, a saúde, a nudez; na esfera da privacidade, que é já mais ampla, incluir-se-iam aspetos da vida pessoal, fora da intimidade, cujo acesso a pessoa permite a pessoas das suas relações, mas não a desconhecidos ou ao público; a esfera pública abrangeria tudo o mais, aquilo a que, na vida de relação e na inserção na sociedade, todos têm acesso".

[63] Por todos, *Vd.* Gómez Sánchez, Yolanda, "Categorías especiales de datos personales: los datos de origen étnico o racial, los datos genéticos, los datos biométricos, los datos relativos a la salud, los datos relativos a la vida sexual y la orientación sexual (comentario al artículo 9.1 RGPD)", em Troncoso Reigada, Antonio (dir.), *Comentario al Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Tomo I, Navarra, Thomson Reuters, 2021, pp. 1041-1063.

[64] Cfr. Alves, Joel A., *O Novo Modelo de Proteção de Dados Pessoais Europeu - Da Heterorregulação à Autorregulação Publicamente Regulada*, Coimbra, Almedina, 2021, p.24; A este respeito, *Vd.* Dupré, Catherine, *The age of dignity*, Oxford and Portland, HART, 2015, pp. 53 e ss..

[65] Cfr. artigo 9º nº 2 do RGPD.

(sobretudo quando inseridos no mercado digital e aliados a uma tecnologia como a inteligência artificial)[66].

Não obstante, o regime da proteção de dados não conhece significativos desvios quando estamos perante a sua aplicação no contexto da saúde. Senão vejamos: (i) os princípios gerais contidos no artigo 5º do RGPD- *licitude*, *lealdade e transparência*, *limitação das finalidades*, *minimização dos dados*, *exatidão*, *limitação da conservação*, *integridade e confidencialidade* e *responsabilidade*[67] – continuam a ter plena aplicação; (ii) os direitos dos titulares dos dados são igualmente válidos[68]; (iii) os deveres a que o prestador de cuidados de saúde, enquanto responsável pelo tratamento de dados, se encontra adstrito também se verificam presentes[69].

Ainda assim, há que considerar o princípio da necessidade de conhecer (a informação), consagrado no artigo 29º da LERGPD[70], de acordo com o qual, no âmbito do tratamento de dados relativos à saúde e de dados genéticos, o acesso deve limitar-se ao estritamente necessário, atenta a finalidade do tratamento. Conforme assinala A. Barreto Menezes Cordeiro[71], não seria necessário o legislador nacional acolhê-lo na lei de execução, já que o mesmo

---

[66] *Vd.* Comité Europeu para a Proteção de Dados, *Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo*, adotadas em 29 de janeiro de 2020, disponível em https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_pt, p.18 [consultado em 06/08/2023]. "A utilização de dados biométricos, mais concretamente o reconhecimento facial, implica riscos acrescidos para os direitos dos titulares dos dados. É crucial que o recurso a este tipo de tecnologias se faça no devido respeito pelos princípios da licitude, da necessidade, da proporcionalidade e da minimização dos dados, tal como estabelecido no RGPD. Embora a utilização destas tecnologias possa ser considerada particularmente eficaz, os responsáveis pelo tratamento devem, antes de mais, avaliar o seu impacto nos direitos e liberdades fundamentais e ponderar a utilização de meios menos intrusivos para atingir a finalidade legítima do tratamento".

[67] A respeito dos princípios, *vd.*, por todos, Terwangne, Cécile de, "Article 5. Principles relating to processing of personal data", em Kuner, Christopher, et. al. (ed.), *The EU General Data Protection Regulation (GDPR) – A Commentary*, United Kingdom, Oxford University Press, 2020, pp.309-320; Cordeiro, A. Barreto M., *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*, Coimbra, Almedina, 2021, pp. 101-107.

[68] Por todos, v*d.* Vrabec, Helena U., *Data Subject Rights under the GDPR*, Uited Kingdom, Oxford University Press, 2021, pp.64 e ss.; Cordeiro, A. Barreto Menezes, *Direito da Proteção de Dados: À luz do RGPD e da Lei nº 58/2019*, Coimbra, Almedina, 2020, pp. 256 e ss..

[69] Cfr. Moniz, Graça Canto, *Manual de Introdução à Proteção de Dados Pessoais*, Almedina, 2023, pp. 205 e ss.

[70] Lei nº 58/2019, de 08 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (doravante designada apenas por LERGPD).

[71] Cfr. Cordeiro, A. Barreto Menezes, *Direito da Proteção de Dados, op.cit.,* p. 253.

decorre do princípio da minimização dos dados e concretiza, de certo modo, o princípio da integridade e da confidencialidade[72].

Ademais, no nº 6, do citado artigo 29º, da LERGPD, consagrou-se um novo dever que recai sobre o responsável pelo tratamento dos dados – o de "*notificar o titular dos dados de qualquer acesso realizado aos seus dados pessoais* e de *assegurar a disponibilização desse mecanismo de rastreabilidade e notificação*".

Por outro lado, o legislador nacional tratou também de regulamentar as bases de dados ou registos centralizados de saúde[73], permitindo que os dados relativos à saúde sejam organizados em bases de dados ou registos centralizados assentes em plataformas únicas, desde que estas plataformas cumpram os requisitos de segurança e de inviolabilidade e, por sua vez, os dados sejam tratados para efeitos das finalidades legalmente previstas no RGPD e na legislação nacional[74].

---

[72] *Vd.* ainda Costa, Tiago Branco da, "O tratamento de dados pessoais na prestação de cuidados de saúde: a caminho da reconfiguração da relação jurídica estabelecida entre o prestador de cuidados de saúde e o paciente?", em Fonseca, Isabel Celeste M. & Bujosa Vadell, Lorenzo M. (coord.), *SOCIEDADE, DIREITO(S) E TRANSIÇÃO DIGITAL – II Encontro Ibérico de Doutorandos em Direito da Universidade do Minho e da Universidade de Salamanca*, Braga, Centro de Investigação em Justiça e Governação, Escola de Direito da Universidade do Minho, 2021, 3-25, pp.17-18. Sobre a sua concretização, estabeleceu o legislador que as medidas e os requisitos técnicos mínimos de segurança devem ser aprovados por portaria dos membros do Governo responsáveis pelas áreas da saúde e da justiça, que deve regulamentar, nomeadamente, as seguintes matérias: (a) estabelecimento de permissões de acesso aos dados pessoais diferenciados, em razão da necessidade de conhecer e da segregação de funções; (b) requisitos de autenticação prévia de quem acede; e (c) registo eletrónico dos acessos e dos dados acedidos (cfr. artigo 29º, nº 7, da LERGPD).

[73] Cfr. artigo 30º da LERGPD.

[74] Cfr. Comissão Nacional de Proteção de Dados, Parecer nº 20/2018, Processo nº 6275/2018, 02 de maio de 2018, pp. 29v. e ss., onde se assinala que "Esta norma surge sem qualquer enquadramento justificativo, designadamente na exposição de motivos, que permita compreender a razão de ser da sua previsão. Este artigo não define os aspetos essenciais do tratamento de dados para que possa ser tida como legitimadora do tratamento: desde logo, não define quem é ou pode ser responsável por tais bases de dados, nem as finalidades das mesmas. O teor aberto da norma permitiria a qualquer entidade, pública ou privada, ou pessoa singular criar uma base de dados de saúde centralizada, o que não pode ser o resultado pretendido pelo legislador nacional, por contrariar a proteção específica e reforçada exigida pelo nº 1 do artigo 9º do RGPD para os dados de saúde. A estas objeções acresce ainda o risco que a centralização de informação clínica sempre importa: o evidente valor económico dos dados de saúde (de grande utilidade para laboratórios farmacêuticos e para seguradoras, por exemplo) é potenciado exponencialmente com a centralização dos mesmos (pela amplitude e maior facilidade de relacionamento da informação), sendo correspondentemente acompanhado pelo aumento do risco de violação dos dados pessoais. (...) É que o risco para os direitos e liberdades dos cidadãos da existência de um tratamento com estas características é suscetível de causar danos com tal intensidade, em especial no que respeita à possibilidade de dar origem a discriminação, a prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, ou a quaisquer outros prejuízos importantes de natureza económica ou social, que não podem ser tolerados". Cfr. Cordeiro, A. Barreto M., *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*, Coimbra, Almedina, 2021, pp. 626-627.

Por fim, mas não menos importante, a questão da investigação científica conhece novidades em relação ao regime geral consagrado no RGPD: (i) os direitos de acesso, retificação, limitação do tratamento e de oposição podem ser comprimidos, na medida do necessário, se forem suscetíveis de tornar impossível ou prejudicar gravemente a realização dos fins da investigação; e (ii) o consentimento para o tratamento de dados para fins de investigação científica pode abranger diversas áreas de investigação ou ser dado unicamente para determinados domínios ou projetos de investigação específicos[75].

3.1. Os dados (pessoais?) como fonte de alimentação da IA

Conforme se assinala, expressamente, no novo considerando 2-A, da Proposta de Regulamento IA, "a inteligência artificial depende frequentemente do tratamento de grandes volumes de dados, e de muitos sistemas e aplicações de IA para o tratamento de dados pessoais", pelo que estas duas realidades são indissociáveis. Por esta razão, considerou a União Europeia que uma das bases para o Regulamento IA terá de ser, necessariamente, o artigo 16º do TFUE[76], e que terá de ser respeitado o direito fundamental à proteção de dados pessoais[77]. Aliás, se o objetivo é criar uma inteligência artificial centrada no ser humano, não poderia ser outra a opção.

Toda a informação relativa a uma pessoa singular identificada ou identificável é considerada, à luz do RGPD, um dado pessoal[78]. Dentro deste universo, o legislador cuidou de distinguir, desde logo, entre dados de categorias gerais e dados de categorias especiais[79], estabelecendo disciplinas distintas para o tratamento dos dados de cada uma dessas categorias. Ademais, dentro

---

[75] Cfr. Martín Uranga, Amelia, "Protección de datos y fomento de la investigación cientifica: la necesidad de un equilíbrio adecuado (comentario al artículo 9.2.j) RGPD)", em Troncoso Reigada, Antonio (dir.), *Comentario al Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Tomo I, Navarra, Thomson Reuters, 2021, pp. 1219-1248.

[76] "Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". *Vd.* considerandos 2º-A e 2º-B da Proposta de Regulamento IA.

[77] *Idem*, *Ibidem*. A este respeito, veja-se o considerando 45-A da Proposta de Regulamento IA, onde se diz, aliás, que "o direito à privacidade e à proteção de dados pessoais deve ser garantido ao longo de todo o ciclo de vida do sistema de IA".

[78] Cfr. artigo 4º, nº 1, do RGPD.

[79] Cfr. artigo 9º, do RGPD.

delas, agrupou alguns tipos de dados e definiu-os – em especial para o contexto da saúde, *dados genéticos*[80], *dados biométricos*[81], *dados relativos à saúde*[82].

No âmbito da utilização da inteligência artificial, a biometria assume uma especial dimensão, sobretudo quando aliada a uma medicina de precisão ou personalizada[83], razão pela qual a Proposta de Regulamento IA dedica parte do seu texto a esta questão. Apesar da remissão para o RGPD[84], o legislador, nesta última versão, não deixou de acrescentar um novo conceito – *dados baseados na biometria*[85]. Em suma, estes dados baseados na biometria "podem, ou não, permitir a identificação ou confirmar a identificação única de uma pessoa singular"[86], pelo que poderão sujeitar-se, ou não, ao regime legal esboçado para o tratamento de dados de categorias especiais[87]. De qualquer modo, não é despiciendo lembrar o entendimento perfilhado pelo Comité Europeu para a Proteção de Dados CEPD, a respeito da classificação dos dados como biométricos:

> *"Para que o tratamento seja considerado um tratamento de categorias especiais de dados pessoais (artigo 9º), é necessário que os dados biométricos sejam tratados «para identificar uma pessoa de forma inequívoca». Em suma, à luz do artigo 4º, ponto 14, e do artigo 9º* [do RGPD], *há que ter em conta três critérios:*
>
> *– a natureza dos dados: dados relacionados com as características físicas, fisiológicas ou comportamentais de uma pessoa singular,*

---

[80] Cfr. artigo 4º, nº 13, do RGPD.

[81] Cfr. artigo 4º, nº 14, do RGPD.

[82] Cfr. artigo 4º, nº 15, do RGPD.

[83] *Vd.* Nunes, Rui, *Ensaios em bioética*, Brasília, Conselho Federal de Medicina (CFM), 2017, p.199, que se refere à «medicina 4P» - "Trata-se da possibilidade criada pela análise do genoma humano de implementar sistemática e articuladamente a Medicina Preditiva, a Medicina Preventiva e a Medicina Participativa contribuindo para nova filosofia, segundo a qual o doente é parceiro verdadeiramente ativo porque geneticamente informado sobre os cuidados de saúde que pode e deve receber, ou seja, uma Medicina Personalizada".

[84] Cfr. artigo 3º, §1, ponto 33, em articulação com o considerando 7, da Proposta de Regulamento IA.

[85] *Vd.* artigo 3º §1, ponto 33-A – "dados resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular" –, em articulação com o considerando 7 da Proposta de Regulamento IA – "Os dados baseados na biometria são dados adicionais resultantes de um tratamento técnico específico relacionado com os sinais físicos, fisiológicos ou comportamentais de uma pessoa singular, como expressões faciais, movimentos, frequência cardíaca, voz, digitação ou marcha", que podem, ou não, permitir a identificação ou confirmar a identificação única de uma pessoa singular".

[86] *Idem*.

[87] Cfr. Considerando 24 da Proposta de Regulamento IA.

– o meio e a forma de tratamento: dados «resultantes de um tratamento técnico específico»,
– a finalidade do tratamento: os dados devem ser utilizados para identificar uma pessoa de forma inequívoca."

Assim se compreende que a barreira entre «dados biométricos» e «dados baseados na biometria» pode ser ténue. A par disto, temos também de considerar outros termos associados à biometria (e que implicam, necessariamente, o tratamento de dados biométricos e, em alguns casos, de outros "dados sensíveis"): «identificação biométrica»[88], «verificação biométrica»[89], «categorização biométrica»[90] e «sistema de identificação biométrica à distância[91].

Neste sentido, e ciente do risco que estas operações de tratamento de dados podem representar para os titulares dos dados, o legislador europeu, de entre várias, veio a acolher a proibição de colocação no mercado, de colocação em serviço ou de utilização de sistemas de categorização biométrica,

---

[88] *Vd.* artigo 3º, §1, ponto 33-B – "o reconhecimento automatizado de características humanas físicas, fisiológicas, comportamentais e psicológicas para efeitos de determinação da identidade de uma pessoa, comparando os dados biométricos dessa pessoa com os dados biométricos de pessoas armazenados numa base de dados (identificação «um para muitos»)", em articulação com o considerando 7-A da Proposta de Regulamento IA – "A definição de «identificação biométrica» usada neste regulamento deve ser entendida como o reconhecimento automatizado de características humanas físicas, fisiológicas, comportamentais e psicológicas, tais como o rosto, o movimento dos olhos, as expressões faciais, a forma do corpo, a voz, a fala, a marcha, a postura, a frequência cardíaca, a pressão arterial, o odor, a força dos dedos ao digitar, reações psicológicas (raiva, angústia, tristeza, etc.) com o objetivo de verificar a identidade de um indivíduo, comparando os dados biométricos desse indivíduo com dados biométricos de indivíduos armazenados numa base de dados (identificação de um-para-muitos), independentemente do seu respetivo e prévio consentimento".

[89] *Vd.* artigo 3º, §1, ponto 33-C – "a verificação automatizada da identidade de pessoas singulares através da comparação de dados biométricos de uma pessoa com dados biométricos previamente fornecidos (verificação «um para um», incluindo a autenticação)".

[90] *Vd.* artigo 3º, §1, ponto 35 – "a classificação de pessoas singulares em categorias específicas, ou a dedução das suas características e atributos com base nos seus dados biométricos ou dados baseados em biometria, ou que possam ser inferidas a partir desses dados", em articulação com o considerando 7-B da Proposta de Regulamento IA – "A definição de «categorização biométrica» utilizada neste regulamento deve ser entendida como a inserção de indivíduos em categorias específicas, ou o processo de inferir as suas características e atributos, como o género, sexo, idade, cor do cabelo, cor dos olhos, tatuagens, origem étnica ou social, saúde, capacidade mental ou física, traços comportamentais ou de personalidade, características da linguagem, religião, ou pertença a uma minoria nacional, ou orientação sexual ou política, com base nos seus dados biométricos ou de base biométrica, ou que possam ser razoavelmente inferidos a partir desses dados".

[91] *Vd.* artigo 3º, §1, ponto 36 – "sistema de IA concebido para identificar pessoas singulares à distância por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência, sem que o responsável pela implantação do sistema de IA saiba antecipadamente se a pessoa em causa estará presente e pode ser identificada, excluindo os sistemas de verificação", em articulação com o considerando 8 da Proposta de Regulamento IA.

que categorizam as pessoas singulares de acordo com atributos ou características sensíveis ou protegidos, ou com base nesses atributos ou características inferidos[92]. Todavia, esta proibição pode resultar afastada quando estejamos perante "sistemas de IA concebidos para serem utilizados para fins terapêuticos aprovados com base no consentimento informado específico das pessoas que lhes são expostas ou, se for caso disso, do seu tutor legal"[93]. De todo o modo, ainda que não abrangidos pelas proibições previstas no artigo 5º da Proposta de Regulamento IA, devem ser classificados como de risco elevado os sistemas de IA concebidos para serem utilizados na identificação biométrica de pessoas singulares, assim como os sistemas de IA concebidos para serem utilizados para inferir sobre as características pessoais de pessoas singulares com base na biometria ou em dados biométricos, incluindo sistemas de reconhecimento de emoções[94].

Claro está que a inteligência artificial não se alimenta apenas de dados pessoais, embora, neste particular, seja essa a utilização que nos importa, sem ignorarmos, porém, que a "divisão exata entre dados pessoais e não pessoais nestes conjuntos de dados está a tornar-se cada vez mais ténue, devido à evolução tecnológica", designadamente no que se refere aos dados relativos à saúde[95]. Neste sentido, quando estejam em causa dados pessoais (ou um conjunto de dados que não permita a destrinça entre dados pessoais e dados não pessoais[96]), não poderemos deixar de chamar à colação o regime legal da proteção de dados pessoais.

---

[92] Cfr. artigo 5º, nº 1, alínea b-A), da Proposta de Regulamento IA.

[93] *Idem*.

[94] Cfr. considerando 33-A, da Proposta de Regulamento IA.

[95] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu e ao Conselho – Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados não pessoais na União Europeia*, Bruxelas, 29 de maio de 2019, COM(2019) 250 final, p.11. Sobre a questão da convivência entre dados pessoais e dados não pessoais no contexto do mercado da União, *vide*, entre outros, Masseno, Manuel David, "Na borda: dados pessoais e não pessoais nos dois regulamentos da União Europeia", *CYBERLAW, Revista Científica sobre Cyberlaw do Centro de Investigação Jurídica do Ciberespaço (Cijic) da Faculdade de Direito da Universidade de Lisboa*, vol. 1, nº 9, 2020, pp. 12-31; Costa, Tiago Branco da, *O altruísmo (económico?) de dados..., op. cit.*, pp. 613-643.

[96] Neste sentido, cfr. considerando 2º-A, da Proposta de Regulamento IA, onde se afirma que os Regulamentos (UE) 2016/679 e (UE) 2018/1725, a Diretiva (UE) 2016/680 e a Diretiva 2002/58/CE "constituem a base para um tratamento dos dados sustentável e responsável, nomeadamente nos casos em que os conjuntos de dados contêm uma combinação de dados pessoais e não pessoais".

3.2. A proteção dos dados pessoais no contexto da saúde digital: em particular na utilização da IA

No que concerne à proteção de dados no contexto da saúde digital, em particular quando falamos da introdução da inteligência artificial no contexto da saúde, devemos ter presente, para facilitar a nossa exposição os diversos momentos da relação estabelecida entre o prestador de cuidados de saúde (responsável pelo tratamento dos dados) e a pessoa em contexto de saúde (titular dos dados): (i) aquando da recolha dos dados; (ii) durante a relação entre o responsável pelo tratamento e o titular dos dados; (iii) término da relação entre o responsável pelo tratamento e o titular dos dados. De entre os três, selecionaremos, os dois primeiros, que apresentam, no nosso entendimento, maiores desafios.

No primeiro momento assinalado, antevemos dificuldades ou desafios relacionados, desde logo, com a questão da licitude do tratamento dos dados. Será que a utilização deste tipo de sistemas de IA poderá estar abrangida pela condição de licitude referente à prestação de cuidados de saúde? Será que esta ferramenta de IA é indispensável àquela prestação de cuidados de saúde? Ou pelo contrário dependerá da adesão voluntária da pessoa em contexto de saúde (titular dos dados)?

De seguida, e com igual relevo, o cumprimento dos deveres de informação que recaem sobre o responsável pelo tratamento dos dados pode sair prejudicado. Com efeito, quando pensamos na introdução e utilização de tecnologia conhecida pela sua opacidade e falta de transparência, por um lado, e com a necessidade de informar detalhadamente o titular dos dados, de entre outros elementos, da existência de decisões automatizadas, incluindo a definição de perfis, bem como da lógica subjacente, importância e consequências de tal tratamento para o titular dos dados, por outro lado, impõe-se a seguinte questão: como poderá o responsável pelo tratamento dos dados assegurar o cumprimento deste seu dever de informação, concretamente no que respeita à lógica subjacente ao sistema de IA e às suas consequências, quando, concomitantemente, se assume que poderá haver uma utilização indevida do mesmo, resultante de comportamentos humanos ou de interações com outros sistemas?[97]

[97] Cfr. Andrade, Francisco, "Análise crítica de alguns aspetos da proposta de regulamento europeu para a inteligência artificial", em Silva, Eva Sónia Moreira da & Freitas, Pedro Miguel (Eds.), *Inteligência artificial*

Mas esta não é a única questão que poderá surgir neste contexto, uma vez que o artigo 52º da Proposta de Regulamento IA cuidou de estabelecer obrigações de transparência, que deverão ser respeitadas pelos fornecedores e pelos utilizadores dos sistemas de IA. Opacidade, ininteligibilidade não rimam com segurança e confiança, mas têm, necessariamente, de rimar com responsabilidade.

No que diz respeito ao segundo momento e, portanto, ao decurso da relação, devemos ter presente a importância das medidas técnicas e organizativas que os fornecedores e utilizadores dos sistemas de IA devem adotar com vista a garantir a integridade e a confidencialidade dos dados pessoais tratados[98]. Conforme já tivemos oportunidade de referir, a proteção de dados deve ser garantida ao longo de todo o ciclo de vida do sistema de IA, pelo que os princípios da minimização de dados e da proteção desde a conceção e por defeito são fundamentais[99]. Atento o contexto em que operamos, não deixa de causar alguma dúvida e inquietação o desenvolvimento e a utilização de um sistema de inteligência artificial (que quanto mais e melhores dados recolher, melhor resultados poderá oferecer), ao mesmo tempo que se tenta dar cumprimento, por exemplo, ao princípio da minimização dos dados.

Ainda a este respeito, afigura-se relevante a manutenção de registos (em relação aos sistemas de IA de risco elevado), que permitam rastrear o funcionamento do sistema de IA, já que estes devem ser concebidos e desenvolvidos de forma a permitir a supervisão humana ("ferramentas de interface homem-máquina)[100]. Do mesmo modo, quando pensamos em sistemas autónomos, capazes de gerar respostas e de apresentar novos resultados com base no

e robótica: desafios para o direito do século XXI, Coimbra, GESTLEGAL, 2022, p.332, "o sistema de Inteligência Artificial pode ter a sua utilização (comportamento) alterada por interações quer com humanos, quer com outros sistemas de Inteligência Artificial. No entanto, estranha-se a referência a "outros sistemas razoavelmente previsíveis". É que se torna evidente que o grande problema na atuação dos sistemas de Inteligência Artificial será precisamente a alteração comportamental decorrente de interações (sobretudo, as não previsíveis) com humanos ou outros sistemas autónomos de Inteligência Artificial. A este respeito, seria até mais do que conveniente uma qualquer referência aos estados cognitivos e intencionais do software ou à consideração das razões que podem levar o software a atuar de um determinado modo".

[98] Cfr. Considerando 45-A da Proposta de Regulamento IA, onde se acrescenta que "Essas medidas devem incluir não só a anonimização e a cifragem mas também a utilização de tecnologias cada vez mais disponíveis, que permitem a introdução de algoritmos nos dados e a obtenção de informações valiosas sem a transmissão entre as partes ou a cópia desnecessária dos próprios dados em bruto ou estruturados".

[99] Neste sentido, cfr. considerando 45 da Proposta de Regulamento IA.

[100] Cfr. artigos 12º e 13º da Proposta de Regulamento IA.

conjunto de dados recolhidos e tratados, pela interação com o homem ou com a máquina (ou outros sistemas de IA) também não deixa de ser preocupante a questão da segurança dos dados, pelo que se prescreve (ainda que em relação aos sistemas de IA de risco elevado) a necessidade de garantir a (exatidão, solidez e) cibersegurança do sistema, impedindo tentativas de terceiros não autorizados de alterar a utilização do sistema ou desempenho, atendendo às circunstâncias e aos riscos de cada caso[101].

3.3. A responsabilidade civil pelo tratamento de dados pessoais no contexto da saúde digital

Um dos princípios basilares em matéria de tratamento de dados pessoais é o princípio da responsabilidade, de acordo com o qual o responsável pelo tratamento dos dados é responsável pelo cumprimento de todos os princípios consagrados no artigo 5º do RGPD (e demais regras que os concretizam), pela demonstração desse cumprimento[102], e ainda pelo ressarcimento dos danos que possam resultar da violação do RGPD.

A par deste princípio (e porque o seu conteúdo, como se explicou, contende com todos os demais), o princípio da integridade e da confidencialidade sujeita o responsável pelo tratamento dos dados ao tratamento de forma segura, isto é, mediante a necessária proteção contra o tratamento não autorizado ou ilícito, a perda, a destruição ou danificação acidental. Esta segurança do tratamento deve ser assegurada pela adoção das medidas técnicas e organizativas adequadas a assegurar e comprovar que o tratamento dos dados é feito em conformidade com o RGPD[103]. Assim, para o que aqui nos importa, este princípio da responsabilidade implica para o responsável pelo tratamento dos dados: (i) tratar dados de forma segura, adotando para o efeito as medidas técnicas e organizativas adequadas à proteção contra o tratamento não autorizado ou ilícito, a perda, a destruição ou danificação acidental; (ii) registar todas as atividades de tratamento sob a sua responsabilidade; (iii) comprovar o cumprimento das regras referentes ao tratamento

[101] Cfr. Artigo 15º da Proposta de Regulamento IA.

[102] Cfr. artigo 5º, nº 2, em articulação com o artigo 82º, do RGPD.

[103] *Vd.* Artigo 24º do RGPD.

dos dados; (iv) responder pelos danos causados aos titulares em virtude da violação do RGPD.

No que tange à responsabilidade civil pela violação do RGPD, devemos começar por assinalar a amplitude da responsabilidade que resulta, desde logo, do termo empregue pelo legislador no artigo 82º do RGPD – *tratamento que viole o regulamento*. A pergunta que se impõe é: o que significa violar o RGPD? Apesar da relação que estabelecemos entre o princípio da responsabilidade e o direito de indemnização e responsabilidade consagrado no artigo 82º, a violação ao regulamento não deve ser apenas entendida como uma violação dos princípios fundamentais consagrados no artigo 5º do RGPD. Ainda que possamos estar perante uma situação em que a infração ao regulamento não consubstancie, pelo menos de forma direta e evidente, uma infração aos princípios fundamentais do artigo 5º, a mesma deve ser considerada relevante para efeitos de apuramento da responsabilidade civil ao abrigo do artigo 82º do RGPD[104].

Sem prejuízo do que acabámos de referir, o próprio RGPD tratou de estabelecer uma "isenção" a esta responsabilidade, nos casos em que o responsável pelo tratamento dos dados (ou o subcontratado) provar que *não é de modo algum responsável pelo evento que deu origem aos danos*[105]. Se estamos perante (i) um evento; (ii) ilícito, na medida em que viola o RGPD; (iii) que causa danos[106]; e (iv) há um nexo causal entre o evento e os danos; então, demonstrar que *não é de modo algum responsável pelo evento que deu origem*

---

[104] Cfr. Coelho, Cristina Pimenta, "Anotação ao artigo 82º", em Pinheiro, Alexandre Sousa (coord.), *Comentário ao Regulamento Geral de Proteção de Dados*, Almedina, 2018, pp. 635-636; Cordeiro, A. Barreto Menezes, *Direito da Proteção de Dados...*, *op. cit.*, p. 383, "O campo de aplicação material do artigo 82º compreende, para além de violações dos RGPD, todos os outros tratamentos – na mesma aceção ampla – que violem os atos delegados e de execução adotados nos termos do RGPD, bem como o Direito dos Estados-Membros que dê execução a regras do RGPD".

[105] Cfr. artigo 82º do RGPD.

[106] A este respeito, *vd.* Tribunal de Justiça da União Europeia, Acórdão de 04 de maio de 2023, Processo C-300/21, *UI contra Österreichische Post AG*, onde se afirma que: "A simples violação das disposições deste regulamento não é suficiente para conferir um direito de indemnização"; "Os artigos 77.° e 78.° do RGPD (...) preveem vias de recurso interpostos numa ou contra uma autoridade de controlo, em caso de alegada violação deste regulamento, sem que aí seja mencionado que o titular dos dados deve ter sofrido um «dano» ou um «[prejuízo]» para poder interpor esses recursos, contrariamente aos termos utilizados no referido artigo 82.° no que respeita às ações de indemnização"; "Não é menos verdade que a interpretação assim acolhida não pode ser entendida no sentido de que um titular dos dados, afetado negativamente pela violação do RGPD, esteja dispensado de demonstrar que essas consequências negativas constituem um dano imaterial"; "[O artigo 82º opõe-se a uma] norma ou a uma prática nacional que subordina a indemnização de um dano imaterial, na aceção desta disposição, à condição de o dano sofrido pelo titular dos dados atingir um certo grau de gravidade".

aos danos só pode significar que o responsável pelo tratamento, para ficar isento de responsabilidade, tem de demonstrar que não agiu de forma dolosa, nem negligente. No entanto, nos casos em que se verifique a intervenção de terceiros (*v.g.* acesso ilegítimo), poderá ser possível (pelo menos em tese) acionar a sua responsabilidade civil e/ou penal.

Ainda no que se refere à responsabilidade civil, deve-se sublinhar que o titular dos dados está duplamente protegido, na medida em que poderá acionar diretamente o responsável pelo tratamento dos dados e/ou o subcontratado[107], pois estamos perante uma responsabilidade solidária[108]. No entanto, conforme assinala Mafalda Miranda Barbosa[109], "lidando com sistemas autónomos, as lesões podem ser causadas pela corrupção de dados provocada pelo funcionamento algorítmico", pelo que a expectativa de ressarcimento do titular dos dados poderá sair gorada à luz do regime legal constante do RGPD ou do Código Civil.

4. Conclusões

O fenómeno disruptivo-digital em curso – uma espécie de *El niño tecnológico* – augura uma transformação perpétua da sociedade em que vivemos e, no seu seio, alguns setores são, inelutavelmente, mais permeáveis à sua presença, como claramente parece ser o caso do setor da saúde. O ecossistema de ferramentas e serviços que utilizam tecnologias de informação e comunicação centradas na melhoria dos cuidados de saúde proporcionados ao doente e na gestão ótima do sistema de saúde como um todo fazem hoje parte integrante do universo clínico. Neste particular, apesar da inegável complementaridade no que respeita ao diagnóstico e tratamento de enfermidades, na disseminação e acesso a cuidados de saúde por banda dos mais vulneráveis, na instituição de farmacologia e medicina personalizada, na

[107] Cfr. artigo 82º, do RGPD.

[108] Sem prejuízo do eventual direito de regresso entre o responsável pelo tratamento de dados e subcontratado. Neste sentido, *Vd.* Coelho, Cristina Pimenta, *Anotação ao artigo 82º..., op. cit*, p. 637.

[109] Barbosa, Mafalda Miranda, "Proteção de dados e inteligência artificial (também a propósito do ChatGPT)", em *Revista de Direito Comercial*, 2023, 753-802, disponível em: https://www.revistadedireitocomercial.com/protecao-de-dados-e-inteligencia-artificial, [consultado em 11.08.2023], p.788; e ainda, a respeito da Diretiva Responsabilidade da IA, pp. 799 e ss..

impressiva medicina de precisão, na criação de dispositivos IoHT, ou na predição e prevenção de surtos epidémicos, emergem da utilização das TIC desafios ímpares no concernente à conceção, registo e certificação de novos *wearables* clínicos assistidos por IA, no uso e recurso crescente à robótica baseada na mesma tecnologia, sem olvidar as dificuldades que se vêm fazendo sentir no que diz respeito à subsunção do apontado desiderato tecnológico ao quadro legal vigente em matéria de recolha, tratamento e partilha de dados pessoais em ambientes colaborativos (*Big Data*).

Nesta senda, a União Europeia tem procurado pôr em prática uma abordagem normativa da tecnologia servida por IA, atentos os riscos associados ao seu emprego, tentando, concomitantemente, permitir que o progresso científico seja cultivado de forma sã, dentro das margens delimitadas pelos valores da União. Destacam-se, assim, a proposta de Regulamento sobre Inteligência Artificial, bem como a proposta de Diretiva para a Responsabilidade Civil em assuntos de IA.

No que tange à responsabilidade civil pela utilização da IA no setor da saúde, e sem prejuízo dos avanços que se venham a registar neste contexto, pugnamos, por ora, pela necessidade do legislador europeu ou, na sua ausência, o legislador nacional, prefigurar a previsão de um cenário assente na responsabilidade objetiva, como *iter* mais eficaz no combate e prevenção dos complexos riscos multipolares emergentes da utilização de sistemas baseados em IA.

Sem prejuízo do que resulta expresso, não nos negamos, todavia, a colocar o "dedo na ferida". O modelo de responsabilidade civil projetado para os danos advindos da utilização de sistemas de AI é, por agora, uma realidade retórica. Tem cabido ao intérprete construir o que pode, servindo-se do que tem. Por uso de diferente verbo, a inteligência artificial tem merecido, por aquele a quem compete legislar, uma resposta artificial.

A falta de confiança dos cidadãos em matéria de proteção da privacidade e segurança e, por conseguinte, o impacto negativo no desenvolvimento do mercado digital deram o mote para a reforma do quadro legal atinente à proteção de dados pessoais na União.

O regime da proteção de dados oferecido pelo RGPD não conhece significativos desvios quando estamos perante a sua aplicação no contexto da saúde: (i) os princípios gerais contidos no artigo 5º – *licitude*, *lealdade e*

transparência, *limitação das finalidades*, *minimização dos dados*, *exatidão*, *limitação da conservação*, *integridade e confidencialidade* e *responsabilidade* – continuam a ter plena aplicação; (ii) os direitos dos titulares dos dados são igualmente válidos; (iii) os deveres a que o prestador de cuidados de saúde, enquanto responsável pelo tratamento de dados, se encontra adstrito também se verificam presentes. Todavia, o tratamento de dados pessoais em contexto de saúde, designadamente quando associados a tecnologias de IA, merece particular atenção, mormente pela natureza dos dados que frequentemente são objeto de tratamento. Com efeito, no âmbito da utilização da inteligência artificial, a biometria assume uma especial dimensão, sobretudo quando aliada a uma medicina de precisão ou personalizada, o que poderá ser preocupante, uma vez que os dados biométricos (tal como os dados genéticos) oferecem informações únicas sobre o titular dos dados.

Antevemos que a introdução e a utilização de tecnologia conhecida pela sua opacidade e falta de transparência poderá colocar desafios ao nível dos deveres de informação (existência de decisões automatizadas, incluindo a definição de perfis; lógica subjacente, importância e consequências do tratamento de dados para o titular dos dados); quando se assume, designadamente, a possibilidade de utilização indevida dos sistemas de IA, resultante de comportamentos humanos ou de interações com outros sistemas. Ao mesmo tempo, as medidas técnicas e organizativas que os fornecedores e utilizadores dos sistemas de IA devem adotar com vista a garantir a integridade e a confidencialidade dos dados pessoais tratados serão fundamentais, já que a proteção de dados deve ser garantida ao longo de todo o ciclo de vida do sistema de IA.

O princípio da responsabilidade consagrado no RGPD implica para o responsável pelo tratamento dos dados: (i) tratar dados de forma segura, adotando para o efeito as medidas técnicas e organizativas adequadas à proteção contra o tratamento não autorizado ou ilícito, a perda, a destruição ou danificação acidental; (ii) registar todas as atividades de tratamento sob a sua responsabilidade; (iii) comprovar o cumprimento das regras referentes ao tratamento dos dados; (iv) responder pelos danos causados aos titulares em virtude da violação do RGPD. Contudo é necessário ponderar a aplicação dos regimes legais constantes do RGPD e do Código Civil, no sentido de perceber se os mesmos são aptos a responder aos desafios colocados pela IA.

Em suma: "a inteligência artificial deve ser uma ferramenta ao serviço das pessoas e uma força positiva para a sociedade com o objetivo final de aumentar o bem-estar dos seres humanos"[110], pelo que o nosso justificado receio se deve prender não propriamente com o aparecimento e desenvolvimento destas novas tecnologias, mas antes com as causas a que as mesmas podem servir[111].

[110] Cfr. Proposta de Regulamento IA, exposição de motivos, ponto 1.1., §2.

[111] Na expressão de Alves, Joel A., *O Novo Modelo de Proteção de Dados Pessoais Europeu..., op. cit.,* p. 23, "a lógica de "domínio total" preconizada por regimes como o Third Reich veio a atingir o seu máximo expoente, demonstrando ao mundo que tudo é possível – mormente, quando o progresso da ciência e da técnica é colocado ao serviço das causas erradas".