REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL

MARIANA BASTO MATOS*

Resumo: *A Inteligência Artificial (IA) tem vindo a ser introduzida na saúde como forma de auxiliar na tomada de decisão médica, introduzindo melhorias na prestação de cuidados. A sua implementação tem impacto direto na saúde do paciente ao nível da sensibilização para as patologias e sua monitorização.*
Procede-se a uma análise jurídica (europeia e nacional) sobre proteção de dados sensíveis e IA. O Regulamento (UE) 2016/679 do PE e do Conselho (RGPD) delimita a recolha, tratamento, acesso e uso de dados pessoais. A nível nacional, o RGPD necessita ser conjugado com a Lei n.º 58/2019 de 8 de agosto e a Lei n.º 12/2005 de 26 de janeiro. Relativamente à IA, analisa-se a Proposta de Regulamento do PE e do Conselho que estabelece regras harmonizadas em matéria de IA que está a ser discutida de modo a minorar os riscos associados ao seu uso.

Palavras-chave: *Inteligência Artificial; Legislação; Proteção de dados; Saúde.*

Abstract: *Artificial Intelligence (AI) has been introduced in healthcare to assist medical decision-making, and enable improvements in care delivery. Its implementation has a direct impact on the patient's health in terms of awareness of pathologies and their monitoring.*
A legal analysis (European and national) on the protection of sensitive data and AI is carried out. However, regulation (EU) 2016/679 of the EP and the Council (GDPR) limits the collection, processing, access, and use of personal data. At a national level, the GDPR needs to be combined with Law no. 58/2019 of August 8th and Law no. 12/2005 of January 26th. Regarding AI, the Proposal for a Regulation of the EP and the Council that establishes harmonised rules on AI is analysed, which is being discussed in order to reduce the risks associated with its use.

Keywords: *Artificial Intelligence; Legislation; Data protection; Health.*

1. APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA SAÚDE: VANTAGENS E DESVANTAGENS

Com o avanço da tecnologia, a Inteligência Artificial (IA) tem vindo a ser incorporada em diversos produtos e sistemas com o intuito de auxiliar na tomada de decisão médica, introduzindo melhorias na prestação de cuidados.

São inúmeros os dispositivos que auxiliam na monitorização dos dados em saúde. O caso mais flagrante é a presença de *wearables* no quotidiano, os quais permitem analisar a qualidade do sono, mas também os batimentos cardíacos, medem os níveis de glicose no sangue, o oxigénio, etc. Associada à IA, esta tecnologia permite aos médicos ter acesso a uma previsão da evolução do doente, adequar a medicação à distância, regulando as doses. Existem também robôs (caso Mabu) que recolhem dados sobre o estado clínico do paciente, interagindo com ele, enviam lembretes para a toma diária de medicação,

* Faculdade de Letras da Universidade do Porto/Escola Nacional de Saúde Pública. Email: marianamatos@me.com. ORCID: https://orcid.org/0009-0007-5727-6517.

ajudando-o desta forma a lidar com a sua patologia. Existem outros casos, como é o exemplo do robô em forma de foca que tem servido para ajudar pacientes com Alzheimer.

Associado à IA temos também o ChatGPT vocacionado para a área da saúde que poderá, eventualmente, auxiliar o médico na tomada de decisão. Todavia, a meu ver, este sistema deve ser utilizado com cautela por parte dos profissionais de saúde, na medida em que será sempre necessária a validação e confirmação das informações.

Existem estudos (Salvador et al. 2023) no sentido de verificar a possibilidade de utilizar a impressão digital como biomarcador para detetar a presença de patologias ou a eventualidade de se manifestar *a posteriori* uma doença neuropsiquiátrica. Refiram-se as consequências nefastas que a implementação deste projeto poderá ter ao nível da discriminação de pessoas que venham a sofrer de patologias desta índole. Para além disso, a previsão de possuir a doença num futuro próximo pode não se vir a manifestar e o paciente sofre com a notícia sem necessidade.

Para além dos exemplos acima consignados, não se pode descurar a presença e desenvolvimento do DeepMind utilizado para a análise automática de imagens no auxílio do diagnóstico e avaliação do quadro clínico dos pacientes. Estudos efetuados (Zaparolli 2022; Zaparolli 2021) demonstram que a taxa de assertividade é grande e a de erro reduzida comparativamente com os humanos na análise dos exames clínicos. Com os dados e imagens de diagnóstico previamente inseridos no sistema de IA, este recorre à aprendizagem automática, criando novos algoritmos. Através deste sistema é possível identificar patologias em estádios iniciais de cancros (por exemplo), auxiliando na prontidão na prestação de cuidados de saúde e consequente melhoria dos mesmos.

No que concerne às vantagens da aplicação de IA na saúde, posso consignar que esta possibilita uma melhor análise e interligação dos dados do paciente ao longo da sua jornada na instituição de saúde, permitindo traçar o seu perfil desde a admissão até à alta. É possível prever a manifestação de doenças, na medida em que a IA recolhe dados, identifica padrões e prevê o risco destas. Tem sido utilizada como auxiliar na pesquisa médica e tomada de decisão clínica, já que facilita a monitorização dos dados dos pacientes, promovendo o diagnóstico e o tratamento dos mesmos. A utilização das informações em tempo real acompanhadas por estes sistemas torna possível avaliar os doentes crónicos e antecipar crises.

No que concerne às desvantagens, são inúmeras. Há um grande risco de fuga de informação, o que poderá pôr em causa a privacidade dos doentes, assim como propiciar a prática de crimes, nomeadamente a usurpação de identidade.

Cada vez mais, são frequentes as notícias de ciberataques e consequentes paragens de hospitais em virtude do bloqueio dos sistemas. Esta situação levanta problemas relativamente ao uso indevido de dados, na coleta de informações sensíveis, como são os dados em saúde, e que poderão ser vendidos mais tarde, beneficiando grandes grupos económicos (caso da indústria farmacêutica ou outras empresas na área da saúde que

através do perfil dos doentes tratados podem induzir a compra de produtos, aumentar os preços e influenciar as escolhas dos consumidores). Poderá haver uma intromissão nos sistemas dos dispositivos médicos, os quais podem estagnar as funções para as quais tinham sido programados, não debitando a medicação devida no momento certo ou até provocando a falência dos órgãos.

Podem ocorrer outras falhas nos sistemas de IA, gerando graves danos para os pacientes nos casos de erro no diagnóstico (quando se deposita toda a confiança nos sistemas para dar respostas, sem a verificação humana), administração de fármacos errados ou em doses inadequadas ou mesmo existindo uma falha no *software* dos robôs cirúrgicos, por exemplo.

Muitos sistemas de saúde estão perto do colapso, na medida em que os custos ligados à saúde são avultadíssimos e é necessário fazer uma gestão racional dos mesmos. Não podemos ignorar a existência de medicação na ordem dos milhares de euros, nomeadamente quando se trata de doenças raras, tratamentos oncológicos ou imunoterapia. No caso português, os hospitais públicos necessitam gerir as suas contas com base no orçamento que lhes é disponibilizado pelo Governo. É do conhecimento geral que os mesmos detêm um défice avultadíssimo em virtude dos preços pagos por GDH não serem atualizados nos últimos anos, sendo pago pelo Estado um valor abaixo do custo real. Com isto, pretendo alertar para o facto de se poder vir a recorrer à IA como forma de prever quais os doentes com uma maior probabilidade de terem um estilo de vida saudável, com menos complicações no pós-operatório ou ainda terem menos comorbilidades. O recurso a sistemas de IA deste nível poderá originar a seleção adversa de doentes, ignorando os que poderão acarretar mais custos aos hospitais. Esta realidade poderá ser transversal aos hospitais a nível mundial. Pense-se na importância que os Conselhos de Administração dos hospitais darão a sistemas desta índole quando realizarem *benchmarking*.

A IA alimenta-se de dados. A criação de bases de dados de saúde pode implicar situações graves de discriminação. Desde logo, o paciente portador de uma doença grave poderá ser vítima de discriminação não só na sociedade e no trabalho, mas também em outros contextos como, por exemplo, ver recusada a celebração de um contrato de seguro de saúde por parte da seguradora, em virtude da sua condição. Pode existir discriminação ao nível das adoções, em que as crianças poderão ser escolhidas consoante as características fisiológicas que os futuros pais gostariam de ver satisfeitas. Essa escolha pode decorrer dos registos patentes em bases de dados que recolham dados biométricos[1], por exemplo, podendo eventualmente gerar discriminações de raça e etnia.

[1] No Brasil, a identificação de bebés através da tecnologia INFANT.ID, desenvolvida pela Natosafe, está implementada em alguns hospitais. Este sistema recolhe a biometria neonatal, estabelece um vínculo biométrico, analisa-o e é efetuado um controlo. A INFANT. ID AUTH faz corresponder a biometria da mãe do bebé ao CPF e posteriormente analisa se a biometria do bebé é conforme com a da mãe. Cfr. Natosafe [s.d.].

As bases de dados com dados sensíveis podem vir a ser vendidas no mercado negro (algo que já aconteceu em diversos países) com todas as consequências que podem advir ao nível da segurança e privacidade dos titulares dos dados, bem como na influência das escolhas e indução da procura realizada pelas instituições de saúde e indústria farmacêutica. Urge a necessidade de proteger os titulares dos dados de eventuais intrusões.

A *Carta dos Direitos Fundamentais da União Europeia* (Parlamento Europeu, Conselho Europeu e Comissão Europeia 2016) no art.º 8.º/1 e 2 consagra que «todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito», reforçando a necessidade de um tratamento leal dos dados para fins específicos determinados, mediante o consentimento do seu titular, podendo consultá-los e retificá-los na eventualidade de existir alguma incongruência. O TFUE (*Tratado sobre o Funcionamento da União Europeia (versão consolidada)* 2012) reforça a ideia de proteção dos dados de carácter pessoal no art.º 16.º/1. A Convenção Europeia dos Direitos do Homem no art.º 8.º/1 estabelece que «qualquer pessoa tem direito ao respeito da sua vida privada» (Council of Europe [s.d.]). A proteção dos dados está também consagrada por via jurisprudencial (Cordeiro, coord., 2021, p. 64).

Afigurou-se necessária a criação de um regulamento que regulamentasse a proteção dos dados no âmbito da U.E. e consequentemente nivelasse os EM na implementação da sua legislação sobre a temática. O RGPD (Parlamento Europeu e Conselho Europeu 2016) vem precisamente estabelecer as regras neste âmbito, salvaguardando não só a proteção dos dados, como o seu tratamento e a sua livre circulação (art.º 1.º/1).

2. PROTEÇÃO DE DADOS E TRATAMENTO DE DADOS DE SAÚDE

O RGPD visa defender os direitos e liberdades fundamentais das pessoas singulares, onde se inclui o direito à proteção dos dados tal como está consignado no art.º 1.º/2 e a promoção da livre circulação desses dados (art.º 1.º/3). O art.º 4.º/1) do RGPD entende que os dados pessoais são qualquer «informação relativa a uma pessoa singular identificada ou identificável». Uma pessoa singular é identificável quando possa ser identificada (direta ou indiretamente) por referência a um indicador, como seja um nome, número de identificação, dados de localização, elementos específicos da identidade física, genética, fisiológica, etc. Segundo o GT 29 a propósito da Diretiva 95/26/CE (anterior ao RGPD), ao analisar a definição constata-se a presença de quatro elementos não cumulativos: qualquer informação (inclui todos os aspetos que dizem respeito àquela pessoa, sendo que a proteção que lhe é conferida aplica-se independentemente da forma como foi recolhida e do suporte onde foi armazenada); relativa a[2]; pessoa singular e identificada ou identificável

[2] Pode ser analisada quanto ao conteúdo (a pessoa é o objeto de análise), finalidade (os dados recolhidos permitem aferir sobre o comportamento ou estatuto da pessoa) ou resultado (informação que apesar de não incidir sobre o conteúdo ou

(quando exista dado que, de modo inequívoco, identifique a pessoa). Os dados são relativos a pessoa determinável quando, à luz do princípio da razoabilidade, o responsável pelo tratamento da informação ou terceiros consiga ou possa identificar a identidade do titular desses dados (Considerando 26 e o art.º 4.º/1 do RGPD).

O Regulamento Geral de Proteção de Dados vem consagrar alguns princípios gerais no artigo 5.º, a saber: licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade, responsabilidade. Há, portanto, a apologia de um tratamento adequado, adotando-se medidas de segurança para proteger os dados sensíveis. No que concerne à lealdade, o princípio pugna para não serem obtidos ou tratados os dados através de meios ilegítimos ou por engano, sem o consentimento dos seus titulares. Com a transparência pretende-se garantir que os titulares dos dados sejam informados sobre o modo com estes são ou possam vir a ser tratados. A finalidade possui uma dupla vertente: não só de previsibilidade, mas também como garantia de segurança jurídica. Neste sentido, a limitação da finalidade prende-se não só com o prazo de conservação dos dados, mas também a pertinência e adequação dos mesmos. Relativamente à minimização dos dados, aqui está consagrado um mecanismo de imposição no sentido de que os dados pessoais recolhidos sejam pertinentes, adequados e limitados ao estritamente necessário ao cumprimento das finalidades que se pretendam alcançar através do seu tratamento. A exatidão tem a ver com o facto de os dados pessoais poderem ser atualizados e exatos. Com a limitação da conservação pretende-se garantir que o prazo para a conservação dos dados seja limitado ao mínimo, o que em muitas circunstâncias, tal não ocorre e as empresas utilizam-nos de forma vitalícia, algo que é necessário restringir.

Os titulares dos dados têm direito a obter, junto da entidade responsável pelo tratamento, a indicação sobre se os seus dados estão a ser utilizados e tratados, bem como a aceder aos mesmos (nos termos do artigo 15.º do RGPD). Podem também retificá-los sempre que se verifiquem incongruências ou que os mesmos se alterem (art.º 16.º do RGPD). O direito ao apagamento e ao esquecimento também foram consagrados no art.º 17.º/1 e n.º 2, respetivamente. No que concerne ao primeiro, o apagamento em sentido estrito verifica-se nas seguintes hipóteses: os dados estão a ser tratados de forma ilícita; o titular decide retirar o seu consentimento ou opõe-se ao seu tratamento; as informações deixaram de ser necessárias para a finalidade a que o tratamento se propunha ou necessitarem de ser apagadas em virtude de obrigações jurídicas decorrentes do Direito dos Estados-Membros ou do Direito europeu. O direito ao esquecimento a que se refere o n.º 2 do mesmo preceito está interligado com o apagamento das informações na Internet. Note-se que este princípio é deveras relevante num momento em que as pessoas

finalidade, permita retirar conclusões sobre os estes critérios) (Cordeiro, coord., 2021; Grupo de Trabalho de Proteção de Dados do Artigo 29.º 2007).

podem querer apagar os seus dados não só das redes sociais, como também da Internet. As pessoas podem efetivamente mudar de ideias relativamente à utilização dos seus dados e ao facto de estarem disponíveis *online*.

O direito à oposição também é bastante relevante na medida em que os titulares podem opor-se ao tratamento dos seus dados (art.º 21.º/1 do RGPD. Podem ainda revogar o seu consentimento quando o entenderem nos termos do art.º 7.º/3 do RGPD. Por último, convém referir que o tratamento de dados pessoais pode estar sujeito a restrições nos termos do art.º 18.º do RGPD.

Para efeitos de dados relativos à saúde considera-se aqueles são os «pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde» (art.º 4.º/15) RGPD (Deodato 2017). Estes dizem respeito à saúde do seu titular e não às doenças de que possa vir a padecer. Neste sentido, estes dados incluem-se nos sensíveis, englobando as informações relativas à saúde mental ou física das pessoas singulares passadas, presentes e até futuras. Menezes Cordeiro dá como exemplo deste tipo de dados as informações que sejam recolhidas durante a inscrição ou realização da prestação de cuidados de saúde, podendo ser qualquer número (o de utente, por exemplo) ou símbolo que permita identificar o seu titular de forma inequívoca no que concerne à prestação de cuidados (Cordeiro, coord., 2021, pp. 95-96). Parece existir uma mistura entre os dados administrativos (requeridos para se realizar a admissão dos doentes nas instituições hospitalares) e os dados de saúde. A anotação do art.º 4.º/15 do RGPD (Cordeiro, coord., 2021, pp. 95-96) remete-nos para o art.º 2.º da Lei n.º 12/2005, para efeitos da qual se considera informação de saúde «todos os dados que estejam direta e indiretamente ligados à saúde».

O RGPD não define o que são dados pessoais especiais, apenas se socorre do art.º 9.º/1 para elencar taxativamente os dados especiais. O art.º 4.º do RGPD densifica as categorias: dados biométricos, genéticos e os relativos à saúde.

O art.º 9.º/1 do RGPD consagra a proibição do tratamento de dados que revelem a origem ética ou racial, bem como as opiniões políticas e convicções religiosas, os dados genéticos, os dados biométricos destinados a identificar inequivocamente o seu titular e, ainda os dados relativos à saúde, vida sexual ou orientação sexual. Estão patentes duas tipologias: a que se prende com o resultado que advém do tratamento desses dados e a segunda (dados genéticos, biométricos, relativos à saúde, etc.) tem a ver com a categoria de dados.

A proibição do art.º 9.º/1 do RGPD pode ser afastada mediante o consentimento de forma inequívoca do seu titular nas situações consagradas no art.º 9.º/2, nomeadamente para efeitos de medicina preventiva ou do trabalho, diagnóstico médico, prestação de cuidados ou tratamentos de saúde nos termos do art.º 9.º/2/h) RGPD (Cordeiro, coord., 2021, p. 140; Monge 2020), por motivos de interesse público no domínio da saúde pública (art.º 9.º/2/i) RGPD), para fins de arquivo de interesse público, fins de investigação científica

ou histórica (art.º 9.º/2/j) RGPD). Não podemos descurar o facto de o tratamento dos dados de saúde ter que respeitar o princípio da proibição do excesso (na sua vertente da proporcionalidade e razoabilidade e o princípio da finalidade (nos termos do art.º 5.º/b) do RGPD). O uso dos dados sensíveis deve acontecer nas circunstâncias em que não haja outra solução mais indicada, como forma de se respeitar o princípio da proporcionalidade e o da minimização dos dados (art.º 5.º do RGPD).

A nível nacional, a Lei n.º 58/2019, de 8 de agosto, assegura execução do RGPD. Consagra que o acesso a dados pessoais se rege pelo princípio da necessidade de conhecer a informação (art.º 29.º/1). O artigo 29.º/2 da Lei n.º 58/2019 regula o tratamento dos dados de saúde e dados genéticos apenas consagra que nos casos previstos no art.º 9.º/2/h) do RGPD há o dever de confidencialidade e sigilo para quem tem acesso aos dados relativos à saúde e os trata (art.º 29.º/2, 4 e 5), sob pena de ser aplicado o art.º 51.º da Lei n.º 58/2019 no caso de o profissional incorrer na violação deste dever. O acesso deve ser realizado exclusivamente sob a forma eletrónica (art.º 29.º/3 da Lei n.º 58/2019) e o titular dos dados deve ser notificado de qualquer acesso aos seus dados pessoais (art.º 29.º/6). Relativamente ao processo clínico do doente, este pode consultar o histórico de acessos aos seus dados através do SNS24.

A Lei n.º 12/2005, de 26 janeiro, relativa à informação genética pessoal e informação de saúde define o que se entende por informação de saúde como toda a informação «direta ou indireta ligada à saúde, presente ou futura, de uma pessoa viva ou falecida» (art.º 2.º). Note-se a inovação do quadro legislativo nacional face ao europeu, na medida em que também contempla os dados da pessoa falecida. A informação de saúde (dados clínicos, resultados de exames, análises, intervenções e diagnóstico) é propriedade da pessoa. Assim, as unidades de saúde são depositárias da informação e não podem usá-la para outros fins que não os da prestação de cuidados e investigação em saúde (art.º 3.º/1). O tratamento da informação vem consagrado no art.º 4.º desta lei, sendo que a informação médica consta no art.º 5.º e as informações genéticas, bem como as suas bases de dados e teste, devem ser analisadas articulando-se o art.º 6.º a 9.º deste diploma com o DL n.º 131/2014, de 29 de agosto.

3. CAMINHO PERCORRIDO PELA UE NO SENTIDO DE REGULAR A IA

A UE tem trabalhado nos últimos anos de modo a dar orientações e legislar sobre a IA. Desta forma, foram várias as comunicações emanadas, caso da da Comissão sobre a Inteligência Artificial para a Europa (Estratégia de IA) de abril de 2018 ou a Comunicação da Comissão sobre Aumentar a Confiança numa Inteligência Artificial centrada no ser humano, 2019. Ainda podemos vislumbrar a consagração de Orientações Éticas para uma inteligência artificial de confiança (abril de 2019) elaboradas pelo Grupo Independente de Peritos de Alto Nível, criado pela Comissão Europeia, ou ainda o

White Paper sobre a Inteligência Artificial. O *Livro Branco sobre a Inteligência Artificial* enuncia um conjunto de benefícios que a IA pode trazer aos cidadãos, empresas e para serviços de interesse público, não descurando também os inúmeros riscos que lhe estão associados (Comissão Europeia 2020, pp. 12-14). Apresenta a possibilidade de serem criados dois ecossistemas, um voltado para a excelência ao longo da cadeia de valor, integrando os sectores público e privado, e outro ao nível da confiança no que concerne ao cumprimento das regras da UE, gerando confiança nos utilizadores da IA e garantindo segurança jurídica (Comissão Europeia 2020, p. 3). Esboçou-se uma abordagem baseada no risco, a qual tem sido aprofundada na proposta.

Em abril de 2021, apareceu a Proposta de Regulamento sobre inteligência artificial (*AI Act*). Entretanto surgiu uma nova versão desta em dezembro de 2022, designada de Proposta de Regulamento do PE e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento de Inteligência Artificial) e altera determinados atos legislativos da União (Parlamento Europeu e Conselho Europeu 2021). Centra a sua abordagem nos diferentes graus de risco para os Direitos Fundamentais. Prevê os seguintes níveis: inaceitável (aquele em que as suas práticas são proibidas em virtude de violarem os direitos fundamentais e a segurança nos termos do art.º 5.º), elevado (no qual o art.º 6.º consagra as regras para a classificação destes sistemas), limitado (em que está subjacente o imperativo de transparência, nos termos do art.º 52.º) e, por último, o risco mínimo ou sem risco (o qual não levanta problemas de maior complexidade).

Relativamente à organização sistemática da proposta, esta divide-se em XII títulos, sendo que o I é relativo à aplicação do diploma, objetivos e definições; o II referente a práticas proibidas; o III prevê o sistema de risco elevado indicando não só as regras e sua classificação, mas também os requisitos e deveres a serem cumpridos, bem como um plano de gestão/avaliação de risco. Segue-se o título IV, o qual pugna pela obrigação de transparência aplicável aos fornecedores e utilizadores de determinados sistemas de IA; o V relativo a medidas de apoio à inovação; o VI com questões de governação e criação do Comité Europeu para a IA; o VII é dedicado a base de dados europeias relativas ao sistema de IA com elevado risco. O título VIII consagra medidas de acompanhamento e vigilância dos sistemas após a comercialização, bem como a partilha de informação e a fiscalização do mercado; o IX vem alertar para a necessidade de se criar códigos de conduta no âmbito da IA. O título X estipula regras sobre a confidencialidade dos dados; o XI menciona poderes delegados na Comissão; e, por último, no título XII surgem as disposições transitórias. A proposta conta ainda com IX anexos, os quais preveem diplomas com o intuito de os harmonizar com o novo Regulamento, mas também é apresentado um elenco de sistemas de risco elevado (segundo os ditames do art.º 6.º) no Anexo III. O art.º 48.º do Regulamento refere uma declaração de conformidade, a qual vem exposta no Anexo V e o VI menciona o procedimento de avaliação da conformidade realizada a partir do controlo interno (art.º 17.º do Regulamento). O Anexo VII

trata da conformidade baseada na avaliação dos sistemas de gestão de qualidade e na avaliação da documentação técnica, também ainda decorrente do art.º 17.º. Os dados que devem ser apresentados para registar operadores e sistemas de IA de risco elevado tal como consta no art.º 51.º vêm consagrados no Anexo VIII.

As práticas de IA são proibidas (Título III) quando violem valores como a dignidade humana, igualdade, liberdade e direitos fundamentais. Incluem-se os sistemas de IA que tenham em vista manipular a população, podendo causar danos físicos ou psicológicos à pessoa manipulada ou a terceiros; a implementação de serviços ou sistemas de IA no mercado que explorem vulnerabilidades, tendentes a alterar comportamentos (art.º 5.º/1 e 2). A colocação em serviços ou sistemas de IA avaliações ou classificações da credibilidade de pessoas singulares com base no seu comportamento social, características pessoais ou de personalidade em que a classificação conduzirá ao tratamento desfavorável ou mesmo prejudicial de grupos ou pessoas singulares em contextos sociais, diversos daqueles em que os dados foram gerados ou recolhidos (art.º 5.º/1/c) da Proposta), também está vedada. Para além disto, é considerada prática proibida a identificação biométrica à distância em tempo real, em espaços públicos acessíveis ao público para a manutenção da ordem pública [art.º 5.º/1/d)], salvo as exceções consignadas nos n.ºs 2, 3 e 4 do mesmo preceito.

Nos sistemas de IA que criam risco elevado (nomeadamente para a saúde, direitos fundamentais ou segurança de pessoas singulares), apesar de serem autorizados no mercado europeu, é obrigatório o cumprimento de requisitos determinados e a uma avaliação da conformidade *ex ante*. Assim, para o sistema ser considerado como de risco elevado, não se tem em conta apenas a função desempenhada pelo sistema de IA, mas também as modalidades e as finalidades com que este é utilizado. Segundo o art.º 6.º/1, para efeitos de risco elevado, consideram-se os sistemas de IA usados como componente de segurança de produto (art.º 6.º/a) e Anexo II). No anexo II consideram-se sistemas de AI de elevado risco os algoritmos usados como sistemas de segurança, nomeadamente de dispositivos médicos e dispositivos médicos para diagnóstico *in vitro*. No considerando 32 e no art.º 6.º/b), articulado com o Anexo III, é considerado para este efeito o sistema de IA autónomo, cuja finalidade represente risco elevado para a segurança e saúde ou prejuízo para os direitos fundamentais, tendo em consideração a gravidade dos danos. Neste anexo inclui-se a identificação biométrica e categorização de pessoas singulares, acesso a serviços públicos essenciais e privados, gestão da migração, asilo e controlo das fronteiras.

Tal como foi mencionado, os sistemas de IA de risco elevado podem funcionar no mercado europeu, no entanto necessitam de cumprir requisitos obrigatórios horizontais como forma de garantir uma IA de confiança. Assim, a avaliação e certificação dos produtos cumprem dois tipos de regulação: um relativo à testagem, documentação e prestação de informações antes da sua colocação no mercado e, num momento posterior, o controlo, a manutenção dos registos e as informações relativas a anomalias e incidentes graves durante a vida do algoritmo na fase de pós-comercialização. A avaliação de conformidade

consta do art.º 19.º da Proposta, sendo que esta fica a cargo do fornecedor que a realizará por sua responsabilidade, salvo nos sistemas de IA usados para identificação biométrica à distância de pessoas em que, caso o sistema não seja proibido, deve contar com um organismo notificado durante o processo (Considerandos 64 e 65). Presume-se que os sistemas de IA de risco elevado estão em conformidade com as normas harmonizadas (art.º 40.º e 43.º) ou na ausência destas, dever-se-á aplicar o art.º 41.º.

A avaliação de conformidade é feita com base no controlo interno (art.º 43.º/1/a) e Anexo VI), em que o fornecedor avalia o cumprimento de todos os requisitos obrigatórios e técnicas aplicáveis, consolida a documentação técnica (art.º 11.º e Anexo IV) que ficará à disposição dos organismos notificados (autoridade de supervisão) pelo prazo de 10 anos (art.º 50.º). Todavia, o procedimento de avaliação de conformidade poderá também ser baseado na avaliação do sistema de gestão de qualidade (art.º 17.º) e na avaliação da documentação técnica com a participação do organismo notificado (art.º 43.º/1/b) e Anexo VII) com acesso à informação (nomeadamente o disposto no ponto 4.3 do Anexo VII) pelo período estipulado no art.º 50.º da Proposta. Este último procedimento deve ser utilizado quando: o fornecedor aplicar parcialmente; não aplicar as normas harmonizadas do art.º 40.º ou nos casos em que tais normas não existam ou as especificações não estiverem disponíveis conforme o art.º 41.º. No final da avaliação, o organismo notificado, se verificar que o sistema de IA tem condições para funcionar, aprova um certificado, o qual tem duração máxima de 5 anos (art.º 44.º/2), podendo ser prorrogado por iguais períodos após nova reavaliação. Se o sistema de IA deixou de cumprir os requisitos, o organismo pode recusar, suspender ou restringir o certificado, tendo que fundamentar a sua recusa (art.º 44.º/3).

Após a avaliação de conformidade, os fornecedores devem ainda registar os sistemas de IA de risco elevado numa base de dados pública, em que os dados serão tratados pela Comissão Europeia (art.º 60.º da Proposta).

Após estes procedimentos, a Proposta prevê ainda deveres de acompanhamento após a introdução do sistema no mercado, obrigando assim os fornecedores a informarem as autoridades nacionais sobre as anomalias ou incidentes ocorridos que violem o direito nacional e europeu em matéria de direitos fundamentais, quando deles tiverem conhecimento ou forem retirados do mercado (art.º 62.º). Deve haver um plano de acompanhamento pós-comercialização nos termos dos arts. 3.º/25 e 61.º da Proposta.

Refira-se que, nos Considerandos 71 e 72, incentiva-se a criação de ambientes controlados de experimentação e teste de sistemas de IA na fase de desenvolvimento e pós-comercialização, garantindo-se desta forma a conformidade com os direitos fundamentais, reforçando a segurança jurídica.

Relativamente aos deveres de comportamento e requisitos obrigatórios a cumprir nos sistemas de IA de elevado risco para minorar os riscos, destacam-se os seguintes: criação e manutenção de um sistema de gestão de qualidade (art.º 17.º), procedimentos

de gestão e governação de dados (art.º 10.º e Considerando 44), sistema permanente de gestão de risco (art.º 9.º), garantia de transparência e prestação informações (art.º 13.º e Considerando 7), manutenção de registos (art.º 12.º e Considerando 46), supervisão humana (art.º 14.º e Considerando 48), exatidão, solidez e cibersegurança (art.º 15.º e Considerandos 49 e 50). As ideias que são vertidas ao longo destes artigos aparecem inicialmente nos Considerandos supramencionados. Desta forma, a Proposta introduz os assuntos nos Considerandos, demonstrando qual é a posição adotada, mas também os riscos que estão inerentes a sistemas de IA de risco elevado, sendo posteriormente desenvolvidos nos artigos citados.

Pelo exposto supra, verifica-se que as instituições europeias estão de olhos postos na evolução dos sistemas de IA, sabem da progressiva introdução destes na vida quotidiana e como tal precisam de a regular. Por um lado, pretendem salvaguardar os interesses, direitos fundamentais e segurança do titular dos dados. Por outro, apesar de os sistemas de risco elevado poderem causar consequências nefastas, a sua realidade é iminente, daí que possam circular no mercado europeu desde que cumpram determinados requisitos. Por este motivo, concentrei a minha atenção em descrever brevemente alguns dos ditames que precisam ser observados.

CONCLUSÃO

São inúmeras as vantagens que se podem retirar da introdução de sistemas de IA na área da saúde. Todavia não podemos descurar a existência de riscos que lhe estão subjacentes e que podem pôr em causa não só a segurança jurídica das pessoas singulares, mas também a violação de direitos fundamentais. Desta forma e, após uma breve alusão a ambos os cenários, verifica-se que a IA se alimenta de dados, os quais podem ficar desprotegidos aquando da implementação destes sistemas. A criação do Comité Europeu para a Proteção de Dados denota claramente uma tentativa comunitária de salvaguardar os direitos, liberdades e garantias dos cidadãos, bem como de criar algumas barreiras à recolha selvagem e desmesurada de dados sem o consentimento dos seus titulares. Assim sendo, o RGPD vem no sentido de se criar uma proteção de âmbito supranacional de modo a tentar nivelar os direitos dos cidadãos no que concerne à recolha, tratamento e utilização dos seus dados.

A Lei n.º 58/2019, de 8 de agosto, foi emanada com o intuito de assegurar a execução do RGPD a nível nacional. Este diploma prevê no art.º 29.º o tratamento de dados de saúde e dados genéticos, assegurando que o acesso aos dados pessoais deve estar enformado não só pelo princípio da necessidade de conhecer a informação, mas também devem ser tratados com base no dever de confidencialidade. Os profissionais encarregados desse tratamento têm de agir de acordo com o dever de sigilo. São ainda mencionadas as bases de dados (art.º 30.º), diploma que deve ser analisado conjuntamente com a Lei n.º 12/2005, de 26 de janeiro, relativo à proteção e confidencialidade da informação

genética, assim como a criação de bases de dados neste âmbito. Não se pode descurar a necessidade de articular a legislação europeia com a nacional, devendo a mesma ser analisada em simultâneo.

Verifica-se que as instituições europeias têm trabalhado no sentido de definir um quadro legislativo coeso em matéria de IA, lutando pela salvaguarda dos direitos fundamentais e da segurança jurídica dos cidadãos. Tentam ainda assegurar simultaneamente um espaço com um «ecossistema de confiança» como menciona o *Livro Branco sobre a Inteligência Artificial*, no sentido de promover a inovação, mas criando um sentimento de confiança por parte dos seus utilizadores.

Atualmente está a ser discutida a Proposta que estabelece as regras harmonizadas em matéria de IA. Verifica-se que o PE e o Conselho optaram por seguir as linhas defendidas no Livro Branco e manter uma abordagem baseada no risco, estabelecendo para o efeito quatro tipologias: risco inaceitável, elevado, limitado e mínimo ou sem risco. O primeiro contempla as práticas proibidas em virtude da violação dos direitos fundamentais e segurança. O risco elevado é aquele a que a Proposta mais dedica espaço, precisamente pelo facto de a implementação destes sistemas de IA poder causar riscos à segurança, sendo fulcral criar condições e estabelecer requisitos de mitigação destes riscos.

A Proposta também consagra requisitos ao nível da documentação, qualidade dos dados, transparência e rastreabilidade, sendo imprescindível a supervisão humana ao longo da vida do sistema. O PE e o Conselho vieram ainda estabelecer relações regulatórias *ex ante* ao nível da prestação de informações, documentação e testagem e *ex post* no sentido de reforçar o controlo, a manutenção dos registos e prestação de informações sobre as anomalias ou incidentes relevantes que ocorram durante a vida do algoritmo e após a sua entrada no mercado.

Para concluir, resta apenas mencionar que a UE tem percorrido um caminho inovador, onde tem sido pioneira na discussão destas temáticas. Resta-nos esperar e acompanhar as discussões, alterações e consequente aprovação do Regulamento sobre a IA.

REFERÊNCIAS

ALVES, Joel A., 2021. *O Novo modelo de proteção de dados pessoais europeu*. Coimbra: Almedina.

COMISSÃO EUROPEIA, 2020. *Livro Branco sobre a inteligência artificial: uma abordagem europeia virada para a excelência e a confiança* [Em linha] [consult. 2023-10-06]. Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1.

CORDEIRO, A. Barreto Menezes, coord., 2021. *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*. Coimbra: Almedina.

COUNCIL OF EUROPE, [20--]. *Convenção Europeia dos Direitos do Homem* [Em linha] [consult. 2023-09-08]. Disponível em: www.conventions.coe.int.

DEODATO, Sérgio, 2017. *A Proteção dos dados pessoais de saúde*. Lisboa: UCP Editora.

GRUPO DE TRABALHO DE PROTECÇÃO DE DADOS DO ARTIGO 29.º, 2007. *Parecer 4/2007 sobre o conceito de dados pessoais* [Em linha] [consult. 2023-09-08]. No. WP136. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf.

MONGE, Cláudia, 2023. Proteção de dados e tratamento de dados de saúde: algumas questões. Em: Domingo Soares FARINHO, Francisco Paes MARQUES, e Tiago Fidalgo de FREITAS, eds. *Direito da Proteção dos Dados*, pp. 349-402. Coimbra: Almedina.

MONGE, Claúdia, 2020. Proteção de dados de saúde nos hospitais públicos. *Revista de Direito Administrativo*. Lisboa: AAFDL. Maio-ago., **3**(8), 81.

NATOSAFE, [20--]. INFANT.ID – *Born to be unique* [Em linha] [consult. 2023-09-14]. Disponível em: https://natosafe.com.br.

PARLAMENTO EUROPEU, CONSELHO EUROPEU, e COMISSÃO EUROPEIA, 2016. Carta dos Direitos Fundamentais da União Europeia. *Jornal Oficial da União Europeia* [Em linha] [consult. 2023-09-07]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR.

PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2021. Proposta do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial e altera determinados atos legislativos da União. *Jornal Oficial da União Europeia* [Em linha] [consult. 2023-11-19]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206.

PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016. Regulamento (UE) 2016/679 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). *Jornal Oficial da União Europeia* [Em linha] [consult. 2023-11-19]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679.

PORTUGAL. Leis, decretos, etc., 2019. Lei n.º 58/2019. *Diário da República I Série*. 2019-08-08, (151), 3-40.

SALVADOR, Raymond, et al., 2023. Fingerprints as Predictors of Schizophrenia: a Deep Learning Study. *Schizophrenia Bulletin* [Em linha]. **49**(3), 738-745 [consult. 2023-11-19]. Disponível em: https://doi.org/10.1093/SCHBUL/SBAC173.

Tratado sobre o Funcionamento da União Europeia (versão consolidada). *Jornal Oficial da União Europeia* [Em linha] 2012 [consult. 2023-11-19]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12012E/TXT.

ZAPAROLLI, Domingos, 2022. A Inteligência Artificial chega à saúde. *Revista Pesquisa Fapesp* [Em linha]. (322) [consult. 2023-11-15]. Disponível em: https://revistapesquisa.fapesp.br/a-inteligencia-artificial-chega-a-saude.

ZAPAROLLI, Domingos, 2021. Diagnósticos digitais. *Revista Pesquisa Fapesp* [Em linha]. (305) [consult. 2023-11-15]. Disponível em: https://revistapesquisa.fapesp.br/diagnosticos-digitais.