

# SAÚDE DIGITAL E INTELIGÊNCIA ARTIFICIAL APLICADA À SAÚDE: LACUNAS REGULATÓRIAS, DESAFIOS E PERSPECTIVAS JURÍDICAS

## DIGITAL HEALTH AND ARTIFICIAL INTELLIGENCE: REGULATORY GAPS, CHALLENGES AND PERSPECTIVES

Fernando Aith <sup>1</sup>

### Resumo

Este artigo tem como objetivo identificar e analisar as lacunas regulatórias e os desafios jurídicos atuais no que se refere à saúde digital e ao uso aplicado da inteligência artificial (IA) na área da saúde. Os desafios regulatórios da saúde digital e da IA em saúde que se avizinham impõem ao Estado uma regulação eficaz capaz de garantir as condições necessárias ao desenvolvimento e disponibilização destas novas tecnologias aos indivíduos e à sociedade e, ao mesmo tempo, proteger a segurança e a saúde dos usuários destas novas tecnologias e da sociedade em geral. Analisa-se a necessidade de uma regulação do Estado eficiente sobre o uso das tecnologias digitais aplicadas à saúde, tendo como base os riscos e oportunidades da saúde digital e da inteligência artificial em saúde no Brasil. Após uma contextualização do tema, apresenta-se as lacunas e os desafios regulatórios da inteligência artificial aplicada à saúde no Brasil. Explora-se também os desafios jurídicos para a proteção de dados sensíveis e o conceito de vulnerabilidade digital. Apresenta-se ainda duas inovações regulatórias para a IA em saúde publicadas pela Organização Mundial de Saúde e pelo Parlamento da União Europeia: o Guia Ético para IA em Saúde (OMS) e o Regulamento Europeu para IA em Saúde (União Europeia). Ao fim, destaca-se três áreas que possuem lacunas regulatórias importantes e que representam desafios ao Estado e à sociedade no que se refere ao uso da inteligência artificial na área da saúde: (in)segurança, privacidade e discriminação.

**Palavras-chave:** Regulação. Saúde Digital. Direito da Saúde. Direito

---

<sup>1</sup> Professor Titular da Faculdade de Saúde Pública da Universidade de São Paulo (FSP/USP); Diretor Geral do Centro de Pesquisas em Direito Sanitário da USP (Cepedisa/USP); Editor Chefe da Revista de Direito Sanitário da USP.

Sanitário. Inteligência Artificial.

### **Abstract**

This article aims to identify and analyze current regulatory gaps and legal challenges regarding digital health and the use of artificial intelligence (AI) in healthcare. The regulatory challenges of digital health and AI in health that lies ahead requires the State to adopt effective regulation, capable of guaranteeing the necessary conditions for the development and availability of these new technologies to individuals and society and, at the same time, capable of protecting the safety and health of the users of these new technologies. The need for efficient State regulation on the use of digital technologies applied to health is analyzed in this paper, based on the risks and opportunities of digital health and artificial intelligence in health in Brazil. After contextualizing the topic, the gaps and regulatory challenges of artificial intelligence applied to health in Brazil are presented. The legal challenges for protecting sensitive data and the concept of digital vulnerability are also explored. Two regulatory innovations for AI in healthcare published by the World Health Organization and the Parliament of the European Union are also presented: the Ethical Guide for AI in Healthcare (WHO) and the European Regulation for AI in Healthcare (European Union). In the end, three areas that have important regulatory gaps and that represent challenges to the State and society with regard to the use of artificial intelligence in the health sector are highlighted: (in)security, privacy and discrimination.

## **1 INTRODUÇÃO**

O século XXI é o século da consolidação e evolução do mundo digital.

As inovações da vida moderna digital estão revolucionando também o setor saúde com suas múltiplas e variadas bases de dados digitais com informações sensíveis sobre a saúde dos indivíduos. Além disso, amplia-se com grande velocidade o uso do aprendizado de máquina automatizado e da inteligência artificial aplicada à saúde para fins diagnósticos e terapêuticos, ao mesmo tempo que as redes sociais digitais globais e altamente conectadas, controladas por grandes corporações digitais, começam a fazer circular uma quantidade infinita de dados e informações de saúde com também infinitos potenciais

econômicos.

Atualmente, no dia a dia dos sistemas de saúde ao redor do mundo é cada vez mais frequente nos depararmos com equipamentos médicos com inteligência artificial e capacidade de realizar cirurgias complexas apenas com a supervisão humana; dispositivos laboratoriais de diagnóstico que se utilizam da nuvem de dados digitais e da inteligência artificial para laudos diagnósticos conclusivos; bases de dados gigantes, organizadas e de “propriedade” de grandes grupos corporativos privados, com alto potencial de lucro em sua utilização (monetização das bases de dados digitais); dispositivos médicos capazes de realizar anamnese, diagnóstico e, ainda, fazer uma proposta terapêutica para o paciente; softwares de gestão e governança de serviços públicos e privados de saúde; aplicativos de internet que captam dados sensíveis das pessoas e prescrevem dicas ou orientações de comportamentos no campo da saúde física e mental etc.

Para além dos benefícios enormes que estas inovações do campo da saúde digital podem trazer, já está evidenciado que estes produtos, se não fiscalizados e desenvolvidos com ética e responsabilidade, podem produzir danos físicos, psicológicos e morais nos seus usuários, inclusive com resultado morte. Este conjunto abrangente de produtos e serviços de saúde que se utilizam das novas tecnologias digitais vem formando um campo de estudo que, genericamente, está sendo denominado como ‘saúde digital’.

No âmbito da saúde digital, a inteligência artificial destaca-se como um dos grandes temas a ser compreendido e regulado. Ferramentas de inteligência artificial (IA) servem para melhorar a qualidade, a segurança e a eficiência dos cuidados de saúde, e serão usadas para rastrear dados de pacientes, fazer triagem, ler imagens médicas, diagnosticar doenças, tomar decisões de tratamento, apoiar pacientes na promoção da saúde e fornecer cuidados primários, agudos, mentais e de longo prazo. Prevê-se que as inovações de IA não apenas ajudem, mas potencialmente substituam os cuidadores humanos, prestadores de serviços médicos, diagnosticadores e tomadores de decisão especializados.

Compreender os desafios regulatórios impostos à sociedade nesse momento mostra-se estratégico para que possamos usufruir o que estas inovações podem trazer de melhor, sem, contudo, expor os indivíduos e a sociedade como um todo a riscos desnecessários e, até, letais.

Estas novas tecnologias digitais em saúde agregam valor inestimável para a sociedade e para uma melhor proteção do direito à saúde na medida em que podem contribuir para a melhoria da qualidade dos serviços, para o aumento da acessibilidade aos serviços e produtos de saúde e para o aumento da capacidade humana de proteção da saúde individual e coletiva. No entanto, também trazem embutidos riscos sensíveis para os direitos de personalidade aplicados à saúde (intimidade, privacidade, liberdade, por exemplo), além dos próprios riscos associados aos produtos e serviços digitais, como o risco de usos abusivos destas tecnologias ou ainda usos equivocados com resultados maléficis para a saúde do paciente ou para a saúde coletiva.

O Estado brasileiro tem como função regular o setor saúde de forma abrangente e detalhada, visando garantir o respeito aos direitos fundamentais reconhecidos nas sociedades democráticas modernas. Além disso, o Estado tem o dever de desenvolver políticas sociais e econômicas para a garantia do direito à saúde, notadamente para a redução de riscos à saúde e para a promoção de acesso universal e igualitário às ações e serviços públicos de saúde.

Há uma tensão inerente aos sistemas de saúde de todo mundo, que coloca frente à frente os interesses do empreendedorismo privado e o interesse público a ser protegido por uma adequada regulação estatal. Esta tensão começa a ser verificada em maior escala atualmente no campo da saúde digital, especialmente em decorrência dos avanços que este campo obteve ao longo da pandemia da Covid-19. Encaixam-se neste cenário os atuais debates regulatórios que estão sendo travados na sociedade sobre o “*open health*”; sobre os ataques cibernéticos sofridos pelo Ministério da Saúde do Brasil (com consequências ainda desconhecidas); sobre o teletrabalho no campo da saúde; sobre a regulação de softwares como dispositivos médicos (este tema objeto de uma recém aprovada nova Resolução da ANVISA); sobre as “*fake news*” no campo da saúde, bastante destacadas pela Comissão Parlamentar de Inquérito do Senado que apurou crimes cometidos durante a Pandemia no Brasil; dentre outros temas com alto impacto para a saúde individual e coletiva.

Desde a simples segurança dos produtos e serviços que se utilizam da saúde digital, passando pela garantia de acesso às inovações tecnológicas que vão sendo incorporadas ao sistema de saúde, até o misterioso ambiente onde se desenvolvem e são testados os algoritmos de inteligência artificial em saúde, as funções regulatórias do Estado se

impõem de forma inequívoca. No entanto, embora alguns avanços já estejam sendo verificados no Brasil, ainda existem desafios significativos para desenvolver e organizar um ambiente regulatório claro, eficaz e coordenado para as tecnologias promissoras de saúde digital e inteligência artificial aplicadas à saúde. A Lei Geral de Proteção de Dados (LGPD) representou um importante avanço regulatório com impactos positivos sobre a saúde digital, mas é preciso continuar de forma permanente e altamente qualificada o processo de construção regulatória deste setor.

Considerando a incipiente legislação vigente no país sobre o tema, aliada à cada vez mais fragilizada organização institucional e de governança estatal para o eficiente exercício do poder regulatório estatal no campo da saúde digital, mostra-se imperioso que se coloque na agenda regulatória nacional a saúde digital, para que se possa construir um ambiente regulatório que seja capaz de, ao mesmo tempo, oferecer as bases necessárias para o desenvolvimento de novas tecnologias que sejam benéficas à sociedade e aos pacientes, e estabelecer os limites destas novas tecnologias no que se refere à plena proteção dos direitos fundamentais do ser humano, notadamente a integridade física e psicológica, a intimidade, a privacidade, a saúde e a liberdade.

Este artigo tem como objetivo identificar as perspectivas e os desafios regulatórios da saúde digital e da inteligência artificial aplicada na área da saúde. Os desafios regulatórios da saúde digital que se avizinham impõem ao Estado uma regulação eficaz capaz de garantir as condições necessárias ao desenvolvimento e disponibilização destas novas tecnologias aos indivíduos e à sociedade e, ao mesmo tempo, proteger a segurança e a saúde dos usuários destas novas tecnologias e da sociedade em geral.

## **2 RISCOS E OPORTUNIDADES DA SAÚDE DIGITAL E DA INTELIGÊNCIA ARTIFICIAL EM SAÚDE NO BRASIL: LACUNAS REGULATÓRIAS**

A regulação da IA aplicada à área da saúde deve buscar mitigar os riscos que estas novas ferramentas tecnológicas trazem à sociedade e aos indivíduos ou, pelo menos, definir regras relativas à responsabilidade civil e à indenização de vítimas envolvidas em conflitos associados ao uso dessas ferramentas.

A adoção de uma visão puramente jurídica sobre o tema da regulação da IA gera o risco de não se dar o devido valor às vantagens que essas mudanças sociais e tecnológicas podem trazer à sociedade e aos indivíduos. Deve-se buscar uma abordagem mais equilibrada sobre a regulação da IA em saúde, a partir de um modelo de governança flexível que incentive a rápida adoção de tecnologias de IA e, ao mesmo tempo, proteja a sociedade de forma equilibrada dos riscos potenciais que estas tecnologias trazem.

No que se refere aos riscos a serem abordados por uma regulação estatal, o primeiro risco a ser lembrado é o dos pacientes serem prejudicados diretamente pelas tecnologias de saúde da IA. Por exemplo, uma ferramenta de decisão de IA “mal treinada” pode cometer erros perigosos, como realizar um diagnóstico errado, prescrever o tratamento errado ou deixar de prescrever um tratamento promissor. Falhas regulatórias também podem prejudicar os pacientes de maneiras menos diretas (por exemplo, violando seus direitos de privacidade), ou mesmo em nível sistêmico (por exemplo, usando o escasso financiamento do SUS que deveria ser investido em outro lugar). A revolução da IA é uma oportunidade para o país repensar os seus atuais recursos de governança e, quem sabe, introduzir um modelo regulatório que rastreie as tecnologias ao longo de seu ciclo de vida (em oposição ao foco atual sobre a regulação pré-mercado).

Um segundo risco relacionado à introdução das ferramentas de IA no sistema de saúde brasileiro diz respeito ao objetivo constitucional de reduzir as desigualdades sociais e regionais (equidade). Existem diversos sub-riscos dentro desta categoria: o risco de viés algorítmico embutido nas ferramentas de IA; o risco de que as ferramentas de IA não recebam cobertura pública, o que significa que os pacientes mais ricos terão acesso exclusivo ou preferencial em comparação com os que não possuem recursos para acessar as novas tecnologias.

A iniquidade não é um problema inédito ou exclusivo da IA aplicada à saúde, sobretudo em um país histórica e estruturalmente desigual como o Brasil. A iniquidade sanitária estrutural manifesta-se no Brasil pelas diferenças entre os sistemas público e privado de saúde. Os processos e lógicas que regem a incorporação de uma nova tecnologia nos respectivos sistemas são diferentes: no sistema privado, aqueles que possuem mais recursos financeiros terão melhor e mais rápido acesso às novas tecnologias, inclusive as de IA; já no sistema público, a incorporação estará sujeita às contingências políticas do

Governo de turno e do Congresso Nacional, bem como a um processo técnico-político encampado pela Comissão Nacional de Incorporação de Tecnologias no Sistema Único de Saúde (CONITEC) e pelo Secretário de Ciência, Tecnologia, Inovação e Insumos Estratégicos em Saúde do Ministério da Saúde. A revolução da IA é uma oportunidade para um pensamento mais profundo e uma ação mais significativa sobre esses problemas de longa data.

O terceiro grande risco a ser destacado é o de que, em uma revolução tecnológica da magnitude desta que estamos vivendo, sempre haverá pontos cegos regulatórios. Ferramentas de IA trarão à tona novos pontos cegos, seja em decorrência da natureza da inovação, seja em decorrência da incapacidade estatal para identificar antecipadamente os riscos inerentes à IA em saúde. O ambiente regulatório atual não foi projetado com recursos humanos, computadores e equipes multisetoriais altamente qualificadas, necessários para uma eficiente regulação da IA aplicada à área da saúde. Esta realidade impõe a adoção de medidas imediatas de estruturação estatal para o desenvolvimento de suas capacidades regulatórias no setor. Se é verdade que a revolução da IA força uma profunda reconsideração da governança do sistema de saúde, esta é uma oportunidade bem-vinda.

### **3 DESAFIOS REGULATÓRIOS DA INTELIGÊNCIA ARTIFICIAL APLICADA À SAÚDE NO BRASIL**

As ferramentas de inteligência artificial (IA) podem melhorar a qualidade, a segurança e a eficiência dos serviços de saúde prestados nos sistemas de saúde modernos. Já estão sendo amplamente utilizadas para rastrear dados do paciente, fazer triagem, ler imagens médicas, diagnosticar doenças, fazer decisões de tratamento, apoiar os pacientes na promoção da saúde e fornecer cuidados em todos os níveis de atenção à saúde.

Uma vez que essas ferramentas vieram para ficar e serão cada vez mais presentes nos sistemas de saúde, importantes centros de pesquisa ao redor do mundo se dedicam a pensar em como fazer para que tais tecnologias sirvam para aperfeiçoar os ecossistemas de governança de sistemas de saúde para torná-los mais resolutivos e

eficazes. Flood e Régis<sup>2</sup> apresentam contribuições sobre os riscos, oportunidades e desafios da IA para a governança dos sistemas de saúde e para a efetivação do direito à saúde que podem ser bem aproveitadas para o cenário brasileiro.

Hoje está evidente que, para que a IA aplicada à área da saúde seja socialmente benéfica, é preciso investir na estruturação do Estado para que este possa, de um lado, reforçar e induzir a inovação “boa” da IA e, de outro lado, impedir e proibir as inovações “ruins” em todo o sistema de saúde. Afinal, só faz sentido introduzir uma nova tecnologia no sistema de saúde se ela for benéfica ao paciente e à sociedade, levando-se em consideração sua segurança, qualidade e eficácia.

Nesse sentido, a função reguladora do Estado para que a IA em saúde seja utilizada em benefício dos pacientes e da sociedade é essencial e estratégica. Os caminhos para a adoção de tecnologias de IA promissoras podem ser prejudicados pela insegurança jurídica atualmente existente, causada pela ausência de clareza sobre as leis que se aplicam a esses novos produtos, em especial no que se refere ao respeito à privacidade ou às possíveis consequências no campo da responsabilidade civil.

Para que as tecnologias de inteligência artificial possam ser introduzidas nos sistemas de saúde de forma a contribuir com a melhoria da eficácia e da resolutividade dos serviços de saúde, é importante ter clareza regulatória e evidências sobre se (e como) as leis atuais precisam ser reformadas.

O Brasil enfrenta enormes desafios para estabelecer um ambiente regulatório claro e coordenado para tecnologias de IA promissoras. Compreender os riscos e oportunidades que tais tecnologias podem trazer é um exercício necessário para que o país possa identificar e superar positivamente esses desafios.

Observando-se o fenômeno da IA em saúde e suas implicações para o direito à saúde e outros direitos fundamentais, os principais desafios e questões que se apresentam atualmente para uma regulação eficiente nesta área podem ser assim sintetizados:

- i) O federalismo brasileiro e a jurisdição

---

<sup>2</sup> Régis, Catherine and Flood, Colleen M., AI and Health Law (February 1, 2021). in Florian Martin-Bariteau & Teresa Scassa, eds., Artificial Intelligence and the Law in Canada (Toronto: LexisNexis Canada, 2021), Available at SSRN: <https://ssrn.com/abstract=3733964>

fragmentada do Brasil sobre a saúde complicam a governança de inteligência artificial (IA) na área da saúde. Os resultados são camadas em cascata de governança e regulação e incerteza sobre se a totalidade regula suficientemente a IA em ambientes de saúde.

ii) Há incerteza quanto às principais questões legais, incluindo os requisitos legais em relação à privacidade e responsabilidade por lesões relacionadas à IA (por exemplo, o médico, o fabricante da tecnologia de IA, o hospital).

iii) As atuais estruturas do Ministério da Saúde e da Agência Nacional de Vigilância Sanitária (ANVISA) não são adaptadas para ferramentas que dependem de algoritmos em constante evolução. Há a necessidade de projetar uma nova estrutura que seja robusta e flexível.

iv) A adoção da IA na saúde deve ser eficiente e equitativa. É necessária uma orientação clara sobre as melhores práticas para processos justos de adoção de IA nos sistemas público e privado em saúde.

Dentre os deveres do Estado para a efetivação do direito à saúde no Brasil, organizar uma estrutura de governança e regulação da IA aplicada à saúde encontra-se entre os mais relevantes da atualidade.

#### **4 DADOS SENSÍVEIS E VULNERABILIDADE DIGITAL EM SAÚDE**

Outro grande desafio regulatório do sistema de saúde brasileiro para os próximos anos será o de regular adequadamente a coleta, o armazenamento, o tratamento, o uso, o comércio e a disponibilização dos dados digitais armazenados nas diversas plataformas e aplicativos digitais de saúde que estão em funcionamento e são amplamente difundidos no mercado. Os dados relacionados à saúde de uma pessoa são, via de regra, considerados como ‘dados sensíveis’, na medida em que reúnem informações que, tradicionalmente, encontram-se no campo dos direitos de

personalidade.

Dados típicos da personalidade da pessoa, tais como nome, endereço, idade, sexo, estado civil, gênero e cor, entre outros, são associados, nas plataformas e aplicativos digitais de saúde, a dados sensíveis e ultrassensíveis relacionados ao estado de saúde da pessoa, tais como hábitos alimentares, hábitos de exercício físico, condições de saúde, cirurgias já realizadas, medicamentos já usados e em utilização, exames diagnósticos laboratoriais, tratamentos realizados, doenças antigas e atuais etc. A depender do tipo de informação de saúde da pessoa, podemos dizer que são dados ultrassensíveis, que exigem grande proteção estatal, em nível igual ou ainda superior à proteção atualmente dada para os dados fiscais e bancários de um cidadão.

Nos tempos atuais, em que praticamente todas as ações cotidianas do dia-a-dia da vida estão mediadas por plataformas e aplicativos digitais, a quantidade de dados e informações pessoais de cada um de nós que está na posse de terceiros é enorme, gerando uma nova forma de vulnerabilidade que podemos classificar como ‘vulnerabilidade digital’.

A vulnerabilidade digital tem como causa não só a dimensão dos dados pessoais expostos a terceiros nas plataformas e aplicativos digitais, mas também a fragilidade dos cidadãos nestes tempos de revolução digital no que se refere ao recebimento diuturno de serviços digitais de saúde que podem, no final das contas, mais prejudicar do que beneficiar a saúde das pessoas. São os sites e aplicativos que vendem bem-estar, que vendem serviços diagnósticos e terapêuticos de saúde, que vendem produtos de saúde e medicamentos, enfim, que vendem a promessa de uma saúde melhor, mas que ainda não encontram um ambiente regulatório adequado para conformar suas práticas à necessária proteção dos usuários desses serviços digitais.

Finalmente, a vulnerabilidade digital em saúde está cada vez mais associada à fragilidade dos cidadãos em geral com relação ao recebimento direto, em seus dispositivos móveis digitais, de Fake News (notícias falsas, mentirosas) relacionadas à saúde. Ultimamente, as Fake News em saúde vêm provocando impactos individuais e coletivos visíveis no que se refere à vacinação obrigatória no país, mas não só. No Brasil, os efeitos das Fake News em saúde ao longo da pandemia foram devastadores (da cloroquina à vacina), assim como é muito comum atualmente a circulação de notícias falsas (positivas ou negativas) sobre um determinado produto, um determinado local ou um

determinado serviço de saúde, gerando danos e riscos à saúde individual e coletiva de difícil dimensionamento.

No campo da saúde, é bastante comum que políticas públicas de saúde organizadas pelo Estado cuidem de forma diferenciada dos grupos sociais em condição de vulnerabilidade. O conceito de vulnerabilidade vem sendo estudado e trabalhado por diversos autores, em uma constante busca por sínteses conceituais e diretrizes práticas para a transformação das dimensões comportamentais, sociais e político-institucionais. A vulnerabilidade digital é uma nova forma de vulnerabilidade, e deve ser trabalhada para que se entenda as diferentes suscetibilidades de indivíduos e grupos populacionais aos meios digitais, suscetibilidades agravadas pelos altos riscos de que os meios digitais sejam fontes de doenças e agravos à saúde com conseqüências indesejáveis, tais como sofrimento, limitação e morte. Assim, às tradicionais vulnerabilidades que o setor saúde já é obrigado a cuidar tradicionalmente somem-se as vulnerabilidades digitais, resultante das novas interações digitais a que estamos sujeitos em nosso dia a dia e, principalmente, dos produtos e serviços de saúde que se utilizam de meios digitais para serem vendidos, disponibilizados e publicizados.

Quando se trata de pessoas em condição de vulnerabilidade na área da saúde, tradicionalmente dois grupos são identificados: a vulnerabilidade por condições de saúde, que afeta aqueles que por alguma condição biológica ou do ciclo de vida necessitam de um cuidado mais específico e; as vulnerabilidades sócio-econômico-culturais, oriundas da condição de vida de um determinado grupo e/ou indivíduo, condição esta torna este grupo/indivíduo mais fragilizado socialmente e dependente de tratamento diferenciado a ser dado pelo Estado e pelo sistema público de saúde.

No campo da saúde digital, estas vulnerabilidades são ainda mais potencializadas e conferem fragilidade aos usuários de sites e aplicativos de saúde, gerando especial impacto à saúde dos cidadãos que vivem em contextos sócio-etário-econômico-cultural mais precários e complexos. Esse caldo de vulnerabilidades clássicas associado à vulnerabilidade digital agrava ainda mais os desafios brasileiros no que se refere à promoção da equidade no campo da saúde.

Hoje no Brasil muito se discute sobre as iniquidades de saúde que atingem principalmente os grupos/indivíduos em condição de vulnerabilidade sócio-etária-econômica-cultural. A análise de alguns indicadores demográficos sociais do país nos permite perceber

claramente estas iniquidades e antever os perigos que esses grupos estão correndo nessa nova era da saúde digital.

As iniquidades no Brasil atingem a população de diversas formas. Considerando-se o nível de alfabetização como condição de vulnerabilidade, vê-se que ele se concentra na zona rural, com maiores proporções dentre a população indígena, parda e preta. Enquanto 5,62% da população branca que vive em centros urbanos é analfabeta, o mesmo problema atinge 10,32% da população preta e 8,35% da população parda que vivem em centros urbanos<sup>3</sup>.

O mesmo fenômeno de vulnerabilidade social de parcela específica de nossa população pode ser verificado em outros indicadores, como renda e moradia. De acordo com o IBGE, os rendimentos mensais dos brancos (R\$ 1.538) e amarelos (R\$ 1.574) se aproximaram do dobro do valor relativo aos grupos de pretos (R\$ 834), pardos (R\$ 845) ou indígenas (R\$ 735)<sup>4</sup>. Esses grupos tradicionalmente em condições vulneráveis certamente são também os mais vulneráveis no campo da saúde digital, expostos a serviços digitais picaretas ou ainda às Fake News com potencial de dano enorme à saúde individual e coletiva. Mas importa lembrar que, no que se refere à vulnerabilidade digital, mesmo os grupos sociais mais favorecidos encontram-se ou podem encontrar-se em situação de vulnerabilidade, já que serviços picaretas e as Fake News tem potencial de atingir a todos indistintamente.

Após as eleições norte-americanas que elegeram Donald Trump (2016), ficou evidente, ainda, o uso que os grandes conglomerados digitais do mundo podem fazer destes dados, e de que forma isso pode impactar comportamentos e escolhas individuais. A forma como a Cambridge Analytica usou e tratou os dados de milhões de usuários do Facebook para induzir de forma perniciosa o comportamento político dos cidadãos norte-americanos é uma pequena mostra do impacto que este tipo de tecnologia pode ter sobre a saúde individual e coletiva ao redor do mundo. O lado mais visível do perigo, que é a indução das pessoas em vulnerabilidade digital para o consumo de produtos e serviços de saúde, é apenas um exemplo do potencial de dano iminente que nos espreita.

---

<sup>3</sup> BRASIL. IBGE – Instituto Brasileiro de Geografia e Estatística. Censo 2010. 2010. Disponível em: <https://censo2010.ibge.gov.br/>

<sup>4</sup> BRASIL. IBGE – Instituto Brasileiro de Geografia e Estatística. Censo 2010. Disponível em: <https://censo2010.ibge.gov.br/>

Os dados sensíveis de saúde podem ser usados para diversos fins eticamente delicados e duvidosos, tais como: determinar quem vai ter um emprego ou não com base nas condições de saúde; definir qual o preço que uma pessoa pagará em seu plano de saúde; definir que tipo de condições de saúde serão admitidas nas políticas de imigração entre países; induzir uma pessoa a determinados comportamentos; etc.

Tudo isso já está acontecendo, e não podemos simplesmente ficar na praça dando milho aos pombos. Urge que a sociedade brasileira (e global) se organize para conter os infinitos riscos que a saúde digital nos impõe e nos irá impor em futuro não tão distante.

## **5 PERSPECTIVAS REGULATÓRIAS INTERNACIONAIS**

### **5.1 A OMS e o guia ético para a inteligência artificial na saúde**

A Organização Mundial de Saúde (OMS) lançou no início de 2024 o Guia para Modelos Multimodais de Inteligência Artificial para a Saúde<sup>5</sup>, oferecendo orientações éticas e de governança para o uso de IA em saúde nos diferentes Estados membros da Organização. O Brasil, como membro desta agência de saúde da ONU desde sua fundação, tem o dever de conhecer e observar essas diretrizes em seu território, zelando para a proteção dos seus habitantes no que se refere aos possíveis riscos que estas novas tecnologias podem trazer à sociedade e aos pacientes.

Conforme consta do documento da OMS, os Modelos Multimodais de Inteligência Artificial (MMIAs), embora relativamente novos e não suficientemente testados, estão produzindo um impacto enorme na sociedade em vários domínios, incluindo na área da saúde. Para ficar com o exemplo mais vistoso da disseminação do uso deste tipo de modelo de IA, vale lembrar que o Chat GPT tinha, em janeiro de 2023, apenas dois meses após seu lançamento, aproximadamente 100 milhões de usuários ativos no mês.

A OMS alerta ainda que, atualmente, várias empresas estão desenvolvendo MMIAs de forma integrada a aplicativos e produtos já amplamente utilizados, tais como os aplicativos de busca na Internet e aplicativos de serviços variados, e também em novos produtos e

---

<sup>5</sup> OMS - Organização Mundial de Saúde. 2024. Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models. Disponível em: <https://www.who.int/publications/i/item/9789240084759>

aplicativos. Há uma verdadeira corrida global, com vultosos investimentos públicos e privados, para o desenvolvimento de MMIA concorrentes. Mais recentemente vem emergindo os MMIA de código aberto, que surgem de forma mais rápida e barata do que aqueles desenvolvidos pelas maiores empresas, com potencial de uso e disseminação ainda maior.

De acordo com o guia da OMS, o advento dos MMIA está induzindo investimentos no setor e novos produtos estão sendo lançados em ritmo acelerado. A agência da ONU alerta que, embora os modelos multimodais de IA estejam sendo difundidos e usados amplamente, algumas empresas desenvolvedoras admitem que não entendem totalmente por que estes aplicativos/produtos geram certas respostas. Mesmo com a utilização de seres humanos para reforçar o aprendizado das máquinas, os MMIA podem gerar resultados que nem sempre são previsíveis ou controlados, como por exemplo a participação em “conversas” sem serem convidados, o que pode ser no mínimo desconfortável para os usuários, ou a publicação de conteúdo errado, enviesado ou defeituoso, mas bastante convincente e com alto potencial danoso.

A OMS alerta ainda que grande parte do apoio generalizado aos MMIA que existe em vários setores das sociedades modernas não deriva apenas do entusiasmo pela sua funcionalidade, mas também por afirmações não qualificadas e acríicas sobre o desempenho dos MMIA em publicações que não foram revisadas por pares.

Sabe-se hoje que os MMIA foram adotados ampla e rapidamente sem que os conjuntos de dados usados para treiná-los tenham sido divulgados, tornando difícil ou impossível saber, por exemplo: se os dados são tendenciosos; se os dados foram adquiridos legalmente e de acordo com as regras e princípios de proteção de dados; se o desempenho da tecnologia para resolver uma tarefa ou responder uma consulta reflete que ela foi treinada no mesmo problema ou, ao menos, em ou um problema semelhante; ou, ainda, se ela adquiriu a capacidade de resolver problemas. Outras preocupações sobre os dados usados para treinar os modelos multimodais, incluindo a consistência com as leis de proteção de dados, também são abordadas pelo documento da OMS.

Nesse sentido, o documento da OMS refere um estudo que descobriu que um grande modelo multimodal de linguagem, o GPT-3, pode, ao mesmo tempo, em comparação com humanos, produzir

informações precisas e mais fáceis de entender ou produzir “mais desinformação convincente”. O grande problema é que os humanos nem sempre conseguem distinguir o conteúdo gerado pelo MMIA de aquele gerado por um ser humano, nem tampouco se a informação é “precisa” ou se é “desinformação”.

A agência da ONU entende que nem os indivíduos nem os governos estão preparados para o lançamento de MMIA na escala que se avizinha. Expressa preocupação com o fato de que os indivíduos não foram treinados no uso eficaz destas novas tecnologias e podem não entender que as respostas nem sempre são precisas ou confiáveis, mesmo que um *chatbot* com tecnologia de modelo multimodal crie tal impressão nas pessoas.

A OMS avalia que os governos estão despreparados para enfrentar essa nova onda tecnológica. Regulamentos e leis escritas para governar o uso da IA podem não ser adequadas para enfrentar os desafios ou oportunidades associadas com os MMIA. Nesse sentido, a OMS entende como necessário o movimento da União Europeia para aprovar uma regulação específica para IA, inclusive incluindo dispositivos sobre o uso de MMIA no território europeu. Também destaca as ações de outros governos ao redor do mundo que estão desenvolvendo rapidamente novas leis ou regulamentos, ou instituíram proibições temporárias para estes produtos.

A estimativa é que, nos próximos anos, serão lançados mais produtos que se utilizam de MMIA, cada vez mais poderosos e com poder de introduzir novos benefícios, gerando novos desafios em termos de regulamentação. Neste ambiente dinâmico, a OMS elenca algumas orientações sobre ética e governança do uso dos MMIA na área da saúde.

A primeira orientação da OMS sobre ética e governança da IA para a saúde, publicada em 2021, examinou várias abordagens para aprendizado de máquina e diversas aplicações de IA na área da saúde, mas não especificamente a IA generativa ou os modelos multimodais. Quando publicada, não havia evidências de que a IA generativa e os MMIA estariam amplamente disponíveis tão cedo e seriam globalmente aplicados a cuidados clínicos, pesquisas em saúde e saúde pública.

O novo documento publicado neste início de 2024 apresenta princípios éticos e recomendações de governança da IA em saúde valiosos, que devem ser conhecidos por todos os atores envolvidos na

incorporação destas tecnologias aos sistemas de saúde, nos setores público e privado. Pode servir de importante base para futuras regulações a serem adotadas nos países membros da Organização, incluindo o Brasil.

O documento publicado pela OMS apresenta seis princípios éticos basilares para a IA na área da saúde:

**1. Proteger a autonomia:** garantir que os seres humanos continuem a controlar os sistemas de saúde e as decisões médicas; que os provedores têm as informações necessárias para usar sistemas de IA de forma segura e eficaz; que as pessoas entendem o papel que os sistemas de IA desempenham sobre os seus cuidados; que a privacidade e a confidencialidade dos dados são protegidas; que as informações utilizadas nos aprendizados de máquina sejam válidas e obtidas com consentimento, regulados por quadros jurídicos apropriados para a proteção de dados.

**2. Promover o bem-estar humano, a segurança humana e o interesse público:** garantir que os projetistas de IA atendem aos requisitos regulatórios de segurança, precisão e eficácia para usos ou indicações bem definidas; que medidas de controle de qualidade na prática e de melhoria da qualidade no uso da IA ao longo do tempo sejam adotadas; que a IA não seja usada se resultar em dano mental ou físico que poderia ser evitado pelo uso de uma prática ou abordagem tradicional ou alternativa.

**3. Garantir transparência, “explicabilidade” e inteligibilidade:** as tecnologias de IA devem ser inteligíveis ou compreensíveis para desenvolvedores, profissionais médicos, pacientes, usuários e reguladores; as informações sobre os produtos devem ser suficientes e publicadas ou documentadas antes do projeto ou implantação da IA; as informações devem facilitar consultas públicas e debate sobre como a IA é projetada e como deve ou não ser usada; a IA deve ser explicável de acordo com a capacidade daqueles a quem é

explicado.

**4. Promover a responsabilidade e a prestação de contas:** garantir que a IA seja usada sob condições apropriadas e por pessoas devidamente treinadas; que os pacientes e os médicos avaliam o desenvolvimento e a implantação da IA; que os princípios regulatórios são aplicados e que o algoritmo esteja sujeito à supervisão humana; que mecanismos apropriados estejam disponíveis para questionamento e para reparação de indivíduos e grupos que sejam prejudicados por decisões baseadas em IA.

**5. Garantir a inclusão e a equidade:** garantir que a IA seja concebida e partilhada para encorajar o uso e acesso mais amplo, apropriado e equitativo possível, independentemente de idade, sexo, identidade de gênero, renda, raça, etnia, orientação sexual, habilidade ou outras características; garantir que a IA não codifique preconceitos para a desvantagem de grupos identificáveis; zelar para que a IA seja monitorada e avaliada para identificar efeitos desproporcionais sobre grupos específicos de pessoas.

**6. Promover uma IA que seja responsiva e sustentável:** as tecnologias de IA devem promover a sustentabilidade dos sistemas de saúde e devem ser harmoniosas com os ambientes de trabalho.

Os princípios éticos e de governança de IA generativa e dos MMIAAs podem servir de base para a construção, no Brasil, de uma regulação indutora do desenvolvimento de tecnologias de IA em saúde que não causem danos e que sejam utilizadas sempre em benefício do sistema de saúde brasileiro e dos pacientes.

## **5.2 União Europeia e o regulamento europeu para a inteligência artificial**

No último dia 14 de junho o Parlamento Europeu aprovou definitivamente o Regulamento sobre Inteligência Artificial (“Artificial

Intelligence Act”)<sup>6</sup>. O texto regulamenta o uso da IA e considerou os avanços revolucionários recentes vistos nesse campo, em particular o desenvolvimento de modelos de fundação e IAs generativas, como ChatGPT, BARD, Midjourney e DALL-E. Ao incluir estes novos casos de uso de IA generativa, o projeto de regulamento propõe sujeitar esses sistemas a obrigações de segurança e qualidade, visando garantir o respeito aos direitos fundamentais (incluindo o direito à saúde), ao estado de direito, à cibersegurança e à proteção ambiental.

O projeto de regulamento europeu prevê medidas destinadas a regular a utilização da IA, criando uma nova estrutura de governança com o reforço dos poderes do Gabinete Europeu de IA para investigar infrações transfronteiriças e tem como objetivo harmonizar as regras a serem adotadas pelos países da União Europeia para a colocação no mercado, entrada em serviço e utilização de sistemas de IA nos países do bloco.

Dentre os temas que o regulamento visa harmonizar, destacam-se:

- i) as proibições de certas práticas de inteligência artificial;
- ii) a criação de requisitos específicos para sistemas de IA de alto risco e a definição de obrigações para os operadores desses sistemas;
- iii) o estabelecimento de regras de transparência harmonizadas para sistemas de IA destinados a interagir com indivíduos, sistemas de reconhecimento de emoções e sistemas de categorização biométrica e sistemas de IA utilizados para gerar ou manipular conteúdos de imagem, áudio ou vídeo e;
- iv) estabelecimento de regras de acompanhamento e vigilância do mercado.

O novo Regulamento Europeu para IA aplica-se a prestadores que colocam no mercado ou em serviço sistemas de IA na União Europeia (UE), independentemente de estarem lá estabelecidos ou num país de fora do bloco. O regulamento também se aplica aos utilizadores de sistemas de IA localizados no território da UE e aos fornecedores e

---

<sup>6</sup> União Europeia. EU Artificial Intelligence Act. 2024. Disponível em: <https://artificialintelligenceact.eu/ai-act-explorer/>

utilizadores de sistemas de IA localizados em países de fora do bloco, quando o produto produzido pelo sistema for utilizado na UE.

O objetivo geral declarado do regulamento é o de melhorar o funcionamento do mercado destas tecnologias, estabelecendo um quadro jurídico uniforme, em especial para o desenvolvimento, a colocação no mercado, a entrada em serviço e a utilização de sistemas de inteligência artificial no território da União Europeia (UE). As novas regras visam alinhar esses produtos aos valores da UE, no sentido de promover a adoção de uma inteligência artificial (IA) centrada no ser humano e fiável, assegurando simultaneamente um elevado nível de proteção da saúde, de segurança e dos direitos fundamentais.

O Parlamento Europeu parte do pressuposto de que a IA é formada por uma família de tecnologias em rápida evolução, que contribui para uma vasta gama de benefícios económicos, ambientais e sociais em todo o espectro de indústrias e atividades sociais. A utilização da IA pode proporcionar vantagens competitivas fundamentais às empresas e apoiar resultados social e ambientalmente benéficos, por exemplo nos cuidados de saúde, na medida em que possui o potencial de melhorar a previsão, otimizar a gestão e a destinação de recursos e personalizar as soluções digitais disponíveis para indivíduos e organizações.

O parlamento europeu destaca a necessidade de se criar e desenvolver um quadro jurídico com regras claras e harmonizadas em matéria de IA, capaz de promover o desenvolvimento, a utilização e a adoção da IA no mercado e que, ao mesmo tempo, capaz de proteger interesses públicos, como os da saúde, da segurança e da proteção dos direitos fundamentais, incluindo ainda interesses relacionados à proteção da democracia, do Estado de direito e do meio ambiente, tal como reconhecidos e protegidos pelo direito internacional e da UE.

### **5.2.1 Letramento em saúde**

Uma das principais estratégias de regulação adotadas pelo novo texto foi a de estabelecer regras para garantir o letramento em saúde. De acordo com o novo regulamento, para se obter os maiores benefícios dos sistemas de IA, protegendo simultaneamente os direitos fundamentais, a saúde e a segurança, e para permitir o controle democrático, o letramento em IA deve dotar os fornecedores, os implantadores e as pessoas afetadas com as noções necessárias para

tomar decisões informadas relativamente aos sistemas de IA.

As noções sobre letramento podem variar consoante o contexto e podem incluir: i) a compreensão da aplicação correta dos elementos técnicos durante a fase de desenvolvimento do sistema de IA; ii) as medidas a aplicar durante a sua utilização; iii) as formas adequadas de interpretação dos resultados do sistema de IA e; v) no caso das pessoas afetadas, o conhecimento necessário para compreender como as decisões tomadas com a ajuda da IA terão impacto sobre elas.

Nesse sentido, o letramento em IA deverá fornecer a todos os intervenientes relevantes na cadeia de valor da IA os conhecimentos necessários para garantir o seu funcionamento adequado e a sua aplicação correta. Além disso, a implementação generalizada de medidas de letramento em IA e a introdução de ações de acompanhamento adequadas poderão contribuir para melhorar as condições de trabalho e, em última análise, sustentar a consolidação e o caminho de inovação de uma IA segura, confiável, de qualidade e eficaz.

### **5.2.2 Proibições**

Um outro ponto importante que o Regulamento trata refere-se às proibições. O novo regulamento proíbe expressamente técnicas de manipulação baseadas na IA que sejam utilizadas para induzir comportamentos indesejados ou para enganar as pessoas, incitando-as a tomar decisões que subvertam e prejudiquem a sua autonomia, a sua tomada de decisões e as suas escolhas. Está expressamente vedada a colocação no mercado, a entrada em serviço ou a utilização de determinados sistemas de IA com o objetivo ou o efeito de distorcer materialmente o comportamento humano, por meio dos quais se possa causar danos significativos. Ficam proibidos, em particular, os sistemas de IA que possam causar impactos adversos suficientemente importantes na saúde física, psicológica ou financeira. Estes sistemas de IA são considerados particularmente perigosos e estão, portanto, proibidos no território europeu.

### **5.2.3 IA de alto risco**

Também foi dado um tratamento rigoroso para as IAs consideradas de alto risco pelo regulamento, que só deverão ser

colocados no mercado ou utilizados se cumprirem determinados requisitos obrigatórios, que garantam que tais tecnologias não representem riscos inaceitáveis para os interesses públicos estabelecidos pela legislação europeia e demais documentos normativos de proteção de direitos fundamentais.

Os sistemas de IA identificados como de alto risco são aqueles que têm um impacto prejudicial significativo na saúde, na segurança e nos direitos fundamentais das pessoas. Um exemplo de tecnologia considerada de alto risco pelo Regulamento é o dos robôs cada vez mais autônomos na produção industrial e na prestação de serviços, especialmente no contexto da assistência médica e nos cuidados pessoais. Estes robôs deverão ser capazes de operar e desempenhar as suas funções com segurança em ambientes complexos, sendo que, no setor da saúde, onde os riscos para a vida e a saúde são particularmente elevados, os sistemas de apoio às decisões humanas sobre diagnóstico e tratamento de saúde devem ser fiáveis e precisos.

O impacto adverso que pode ser causado pelo sistema de IA nos direitos fundamentais é de particular relevância para classificar um sistema de IA como de alto risco. Esses direitos incluem o direito à dignidade humana, o respeito pela vida privada e familiar, a proteção dos dados pessoais, a liberdade de expressão e de informação, a liberdade de reunião e de associação e a não discriminação, o direito à educação, a proteção do consumidor, os direitos dos trabalhadores, os direitos das pessoas com deficiência, igualdade de género, direitos de propriedade intelectual, direito a um recurso efetivo e a um julgamento justo, direito de defesa e presunção de inocência, direito a uma boa administração.

#### **5.2.4 Regras relativas ao uso da ia para acesso a serviços essenciais públicos ou privados**

Outra área em que a utilização de sistemas de IA merece atenção especial é seu uso para mediar o acesso e usufruto de determinados serviços e benefícios públicos e privados essenciais, necessários para que as pessoas participem plenamente na sociedade ou melhorem o seu nível de vida. Em particular, as pessoas que solicitam ou recebem prestações e serviços essenciais de assistência das autoridades públicas, nomeadamente serviços de saúde e/ou prestações de segurança social, são normalmente dependentes desses benefícios e

serviços e estão numa posição vulnerável em relação às autoridades responsáveis.

Com as novas regras estabelecidas, serão classificados de alto risco os sistemas de IA que forem utilizados para determinar se tais benefícios e serviços devem ser concedidos, negados, reduzidos, revogados ou reclamados pelas autoridades, incluindo se os beneficiários têm legitimamente direito a tais benefícios ou serviços. O regulamento entende que esses sistemas podem ter um impacto significativo na subsistência das pessoas e podem violar os seus direitos fundamentais, como o direito à proteção social, à não discriminação, à dignidade humana ou a um recurso efetivo, pelo que devem ser classificados como de alto risco.

O regulamento faz a ressalva de que, embora classificados como de alto risco, não é objetivo da nova norma impedir o desenvolvimento e a utilização de abordagens inovadoras na administração pública. Neste aspecto, o Parlamento Europeu faz o alerta de que os sistemas de IA utilizados para esses fins podem conduzir à discriminação entre pessoas ou grupos e perpetuar padrões históricos de discriminação, como os baseados na origem racial ou étnica, no gênero, na deficiência, na idade ou na orientação sexual, ou podem criar novas formas de impactos discriminatórios.

Além disso, o novo regulamento alerta que os sistemas de IA destinados a serem utilizados para avaliação de riscos e fixação de preços em relação a pessoas para seguros de saúde e de vida também podem ter um impacto significativo na subsistência das pessoas. Tais sistemas devem ser concebidos, desenvolvidos e utilizados de forma a evitar violações de direitos fundamentais que afetem gravemente a vida e a saúde das pessoas, incluindo a exclusão financeira e a discriminação.

### **5.2.5 IA para chamadas de emergência**

O regulamento também dedica dispositivos para regular os sistemas de IA utilizados na avaliação e classificação de chamadas de emergência efetuadas por pessoas, ou ainda para enviar ou estabelecer prioridade no envio de serviços de primeira resposta de emergência. As emergências expressamente mencionadas pelo Regulamento referem-se aos serviços públicos de segurança pública, de bombeiros e de saúde (socorro médico).

Os serviços de sistemas de triagem de doentes de cuidados de

saúde de emergência também são classificados como de alto risco, pois tomam decisões em situações muito críticas para a vida e a saúde das pessoas e de seus bens.

## **6 DESAFIOS REGULATÓRIOS DA INTELIGÊNCIA ARTIFICIAL EM SAÚDE: (IN)SEGURANÇA, PRIVACIDADE E DISCRIMINAÇÃO**

Avançar em um ambiente regulatório claro, transparente e eficaz sobre IA em saúde é um imperativo para o Brasil. O grande desafio regulatório da IA em saúde reside no equilíbrio entre garantir inovação e desenvolvimento da IA e, ao mesmo tempo, eliminar (ou reduzir) quaisquer resultados adversos da sua utilização. Para enfrentar este desafio, a inteligência humana deve ser capaz de decisões regulatórias sofisticadas.

Atualmente a regulação sobre a IA em saúde no Brasil é incipiente, quase inexistente. Existem algumas camadas de normas descoordenadas que podem impactar (positiva ou negativamente) a forma como a IA é usada no sistema de saúde brasileiro. As regulações atualmente existentes se espalham de forma desordenada pelos níveis federal, estadual e municipal, bem como pela autorregulação privada. Existem também regulações provenientes do direito civil e do direito contratual, ou ainda novas normas (LGPD, p.e.). Além disso, ao longo do tempo, os juízes desenvolverão jurisprudência que ajudará a orientar a forma de repartir a responsabilidade caso um paciente seja prejudicado como resultado da utilização (ou não utilização) de IA relacionada com a saúde.

Conforme apontado por Silva, Flood e Herder<sup>7</sup>, em diferentes cenários regulatórios (União Europeia, Inglaterra, Canada e Estados Unidos, por exemplo) vamos encontrar preocupações regulatórias imediatas sobre três temas relevantes que vêm causando violações a direitos e gerando riscos aos pacientes: segurança geral dos produtos; viés algorítmico e privacidade/segurança de dados pessoais.

---

<sup>7</sup> Michael Da Silva, Colleen M Flood, & Matthew Herder, "Regulation of Health-Related Artificial Intelligence in Medical Devices: The Canadian Story" (2022) 55:3 UBC L Rev 635. Disponível em: [https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=2047&context=scholarly\\_works](https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=2047&context=scholarly_works)

## 6.1 Segurança geral dos produtos com IA em saúde

No que se refere à segurança geral, as evidências científicas até agora existentes sobre o uso de inteligência artificial (IA) em saúde sugerem que muitas dessas inovações são mais eficazes que os humanos, fato que tem gerado grandes expectativas (e muita euforia) para o potencial benéfico que a IA pode trazer para o cuidado em saúde. No entanto, evidências também sugerem que a IA já comete e continuará cometendo erros, implicando em riscos relevantes aos pacientes.

Por exemplo, o IBM Watson for Oncology não foi treinado em dados reais de pacientes e fez recomendações de tratamento erradas. Descobriu-se que erros no funcionamento do dispositivo foram identificados antes de sua implementação na prática clínica, mas os desenvolvedores não divulgaram os problemas por mais de um ano<sup>8</sup>. Mais recentemente, descobriu-se que o *Epic Sepsis Model*, projetado para prever casos de sepse com base em registros eletrônicos de saúde, omite dois terços dos casos<sup>9</sup>. Espera-se que tais exemplos sejam raros, mas para que a IA possa garantir maior segurança e eficácia dos cuidados de saúde, os profissionais, os pacientes e o público devem poder confiar que os sistemas regulamentares (autorregulação e regulação estatal) eliminarão a IA insegura e ineficaz.

Outras questões de segurança estão relacionadas com a forma como os prestadores de cuidados de saúde interagem com as ferramentas de IA. Existem dois lados deste problema: subutilização e excesso de confiança. No que diz respeito à subutilização, os prestadores que não têm certeza sobre como a IA funciona podem estar relutantes em confiar e não estar dispostos a adotar uma IA que possa reduzir os erros médicos<sup>10</sup>. No que diz respeito à dependência excessiva, existem riscos se os fornecedores confiarem reflexivamente numa ferramenta de IA sem deliberarem, por exemplo, se esta foi

---

<sup>8</sup> Sara Gerke, Timo Minssen & Glenn Cohen, *DzEthical and Legal Challenges of Artificially Intelligence-Driven Healthcare* in Adam Bohr & Kaveh Memarzadeh, eds, *Artificial Intelligence in Healthcare* (Cambridge: Academic Press, 2020)

<sup>9</sup> Wong A, Otles E, Donnelly JP, et al. External Validation of a Widely Implemented Proprietary Sepsis Prediction Model in Hospitalized Patients. *JAMA Intern Med.* 2021;181(8):1065–1070. doi:10.1001/jamainternmed.2021.2626

<sup>10</sup> Risk Analytica, *The Case for Investing in Patient Safety in Canada* (2017). Disponível em: <https://www.bcit.ca/files/health/pdf/risk-analytica-2017-investing-in-patient-safety-in-canada.pdf>.

treinada em dados não representativos; nesses casos, o aconselhamento/diagnóstico da ferramenta para um determinado paciente pode não estar correto.

## 6.2 Viés algorítmico

A IA relacionada à saúde é projetada por humanos, que têm preconceitos explícitos e implícitos. Os algoritmos que os humanos desenvolvem podem, portanto, ser tendenciosos contra grupos/pacientes marginalizados. Os inovadores da IA fazem muitas escolhas de design que podem aumentar ou diminuir os riscos de enviesamento algorítmico, tais como decisões sobre se devem ou não prosseguir e desenvolver conjuntos de dados que são mais representativos, mas que podem ser mais dispendiosos ou de outra forma difíceis de obter. Mesmo conjuntos de dados representativos podem revelar-se problemáticos se, por exemplo, os dados forem originalmente recolhidos de forma a codificar preconceitos dos investigadores ou forem inseridos num algoritmo que codifica preconceitos e, conseqüentemente, tem impactos diferenciais<sup>11</sup>.

Também há a questão de saber se os conjuntos de dados são representativos. Já existe discriminação contra diferentes grupos (por exemplo, mulheres, populações racializadas, minorias sexuais e de género) nos cuidados de saúde<sup>12</sup>. A IA relacionada com a saúde pode ajudar, fornecendo recomendações que podem fazer com que os prestadores “verifiquem” os seus preconceitos/julgamentos inerentes. No entanto, a IA treinada com base em dados que sub-representam sistematicamente grupos devido à discriminação pode replicar os problemas de discriminação existentes, resultando em recomendações de IA que são inferiores para pacientes de populações marginalizadas<sup>13</sup>.

---

<sup>11</sup> Chen, Z. Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanit Soc Sci Commun* **10**, 567 (2023). <https://doi.org/10.1057/s41599-023-02079-x>

<sup>12</sup> Ayhan CHB, Bilgin H, Uluman OT, Sukut O, Yilmaz S, Buzlu S. A Systematic Review of the Discrimination Against Sexual and Gender Minority in Health Care Settings. *Int J Health Serv.* 2020 Jan;50(1):44-61. doi: 10.1177/0020731419885093. Epub 2019 Nov 4. PMID: 31684808. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/31684808/>

<sup>13</sup> McCradden, M.D., Stephenson, E.A. & Anderson, J.A. Clinical research underlies ethical integration of healthcare artificial intelligence. *Nat Med* **26**, 1325–1326 (2020). <https://doi.org/10.1038/s41591-020-1035-9>. Disponível em: <https://www.nature.com/articles/s41591-020-1035-9#citeas>

Isto poderia consolidar ou exacerbar as desigualdades existentes.

### **6.3 Segurança, privacidade e proteção**

Muitos temem que a coleta de *big data* por governos ou empresas multinacionais (por exemplo, Google, IBM, Facebook) produza inevitavelmente violações de privacidade. Há justo receio do uso de dados pessoais de saúde por diferentes instituições para, por exemplo, recusar seguros, aumentar cobranças devido a riscos de saúde identificados nessas bases de dados ou, ainda, afetar negativamente as oportunidades de emprego. Apesar dos riscos, o uso de *big data* continua a ser necessário para construir uma IA segura e eficaz e para mitigar os riscos de enviesamento algorítmico.

As preocupações com a privacidade são ainda mais complicadas por questões relacionadas à segurança cibernética. Mesmo quando os titulares de dados e os utilizadores adquirem dados de forma justificada, devem proteger os dados de caírem nas mãos de pessoas que não possuem razões legítimas de acesso aos mesmos. O sistema de saúde brasileiro é, na prática, operado por uma infinidade de diferentes intervenientes e entidades (hospitais sem fins lucrativos, clínicas privadas, pequenos consultórios gerais, SUS, grandes cadeias de farmácias etc.) com capacidades variadas para garantir sistemas seguros.

Do ponto de vista da segurança, as preocupações com a privacidade podem tornar mais difícil a construção de inovações em IA a partir de dados agregados que sejam representativos das populações que irão servir. Os membros de comunidades indígenas, negras e outras comunidades que foram marginalizadas podem opor-se à partilha de dados devido a abusos históricos e atuais dos seus dados por parte de governos e empresas privadas. Ao mesmo tempo, existe o risco de erro no diagnóstico e no tratamento se não forem incluídos dados dessas populações.

A “desidentificação” de dados, na qual as informações de identificação são eliminadas, reduz os riscos de privacidade, mas nem sempre é possível. Também existe o risco, com grandes conjuntos de dados envolvidos na maioria dos projetos de IA relacionados com a saúde, de “reidentificação” e utilização indevida por intervenientes

menos escrupulosos<sup>14</sup>.

Diferentes países estão desenvolvendo normas de melhores práticas para proteger os dados utilizados na IA, e mesmo normas básicas de cibersegurança podem ajudar a minimizar estes riscos. Mas os riscos permanecem. Os inovadores também podem enfrentar desafios na aquisição de dados representativos de restrições excessivas de privacidade e/ou das múltiplas camadas de restrições que operam nos níveis federal, estadual e privado.

No Brasil, ao mesmo tempo em que o uso da IA em saúde vem crescendo exponencialmente nos sistemas público e privado, a regulação sobre esses novos produtos avança a passos de tartaruga, expondo profissionais, pacientes e a sociedade como um todo a riscos que podem violar direitos humanos em cascata, a começar pelo direito à saúde.

Para que possamos usufruir dos benefícios da IA em saúde, sobretudo no âmbito do SUS, uma regulação eficaz é certamente mais salutar para a inovação e o desenvolvimento da IA em saúde no país do que uma selva desregulada, habitada por aventureiros com as intenções mais variadas, em grande parte pautadas pelo lucro.

## 7 CONSIDERAÇÕES FINAIS

A saúde digital já é uma realidade em nosso país. Está presente nas compras feitas em farmácias (qual seu CPF?); nos telesserviços de saúde (telemedicina, telepsicologia, telefisioterapia etc.); nas consultas médicas (cadastros, prontuários); nos aplicativos que “vendem” saúde e bem-estar; em cada “like” dado em assuntos relacionados à saúde e bem-estar; em cada busca no Google sobre serviços de saúde.

O Governo Federal, por meio da Secretaria Nacional de Informação e Saúde Digital do Ministério da Saúde (SEIDIGI/MS), vem desenvolvendo importantes ações de indução no campo da saúde digital, voltadas à capacitação de gestores, trabalhadores e usuários no planejamento, uso e incorporação de produtos e serviços de informação e tecnologia da informação e comunicação – TIC (telessaúde, infraestrutura de TIC, desenvolvimento de software, interoperabilidade,

---

<sup>14</sup> Cohen IG, Mello MM. HIPAA and Protecting Health Information in the 21st Century. JAMA. 2018 Jul 17;320(3):231-232. doi: 10.1001/jama.2018.5630. PMID: 29800120. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/29800120/>

integração e proteção de dados e disseminação de informações). Essas medidas tendem a ampliar, ainda mais, a abrangência e uso da saúde digital no país.

Ao mesmo tempo em que assistimos à transformação digital do sistema de saúde brasileiro, que atinge tanto os serviços públicos ofertados pelo Sistema Único de Saúde (SUS) quanto os serviços privados de saúde, constatamos uma ainda frágil e incipiente regulação estatal sobre este enorme setor econômico em ascensão. O descompasso entre a rapidez da incorporação da saúde digital ao dia-a-dia dos serviços de saúde e a morosidade da regulação estatal sobre esta nova realidade expõe a sociedade brasileira, como um todo, a riscos de saúde conhecidos e desconhecidos, além de apresentar importantes questões éticas e jurídicas relacionadas aos direitos humanos fundamentais. Urge, portanto, que o Brasil organize uma política regulatória sobre a saúde digital, para que as inovações tecnológicas digitais sejam incorporadas ao sistema de saúde brasileiro de forma racional, benéfica aos pacientes e em respeito aos princípios e objetivos constitucionais do direito à saúde e do SUS.

## REFERÊNCIAS

Ayhan CHB, Bilgin H, Uluman OT, Sukut O, Yilmaz S, Buzlu S. A Systematic Review of the Discrimination Against Sexual and Gender Minority in Health Care Settings. *Int J Health Serv.* 2020 Jan;50(1):44-61. doi: 10.1177/0020731419885093. Epub 2019 Nov 4. PMID: 31684808. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/31684808/>

BRASIL. IBGE – Instituto Brasileiro de Geografia e Estatística. Censo 2010. 2010. Disponível em: <https://censo2010.ibge.gov.br/>

Chen, Z. Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanit Soc Sci Commun* **10**, 567 (2023). <https://doi.org/10.1057/s41599-023-02079-x>

Cohen IG, Mello MM. HIPAA and Protecting Health Information in the 21st Century. *JAMA.* 2018 Jul 17;320(3):231-232. doi: 10.1001/jama.2018.5630. PMID: 29800120. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/29800120/>

McCadden, M.D., Stephenson, E.A. & Anderson, J.A. Clinical research underlies ethical integration of healthcare artificial intelligence. *Nat Med* **26**, 1325–1326 (2020). <https://doi.org/10.1038/s41591-020-1035-9>. Disponível em: <https://www.nature.com/articles/s41591-020-1035-9#citeas>

Michael Da Silva, Colleen M Flood, & Matthew Herder, "Regulation of Health-Related Artificial Intelligence in Medical Devices: The Canadian Story" (2022) 55:3 UBC L Rev 635. Disponível em: [https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=2047&context=scholarly\\_works](https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=2047&context=scholarly_works)

OMS - Organização Mundial de Saúde. 2024. Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models. Disponível em: <https://www.who.int/publications/i/item/9789240084759>

Régis, Catherine and Flood, Colleen M., AI and Health Law (February 1, 2021). in Florian Martin-Bariteau & Teresa Scassa, eds., *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada, 2021), Available at SSRN: <https://ssrn.com/abstract=3733964>

Risk Analytica, The Case for Investing in Patient Safety in Canada (2017). Disponível em: <https://www.bcit.ca/files/health/pdf/risk-analytica-2017-investing-in-patient-safety-in-canada.pdf>.

Sara Gerke, Timo Minssen & Glenn Cohen, *DzEthical and Legal Challenges of Artificially Intelligence-Driven Healthcare* in Adam Bohr & Kaveh Memarzadeh, eds, *Artificial Intelligence in Healthcare* (Cambridge: Academic Press, 2020)

União Europeia. EU Artificial Intelligence Act. 2024. Disponível em: <https://artificialintelligenceact.eu/ai-act-explorer/>

Wong A, Otlés E, Donnelly JP, et al. External Validation of a Widely Implemented Proprietary Sepsis Prediction Model in Hospitalized Patients. *JAMA Intern Med*. 2021;181(8):1065–1070. doi:10.1001/jamainternmed.2021.2626