

Inteligência artificial, privacidade e proteção de dados na saúde

Sofia B. Nunes¹, Rui Nunes¹

1. Faculdade de Medicina da Universidade do Porto, Porto, Portugal.

Resumo

A transição digital, especialmente no que tange a inteligência artificial, molda as relações entre pessoas e comunidades nos mais diferentes domínios de atividade. Este artigo aborda de modo estruturado e sistemático, a cibersegurança no que diz respeito à preservação de valores civilizatórios, tais como privacidade, ou proteção de dados pessoais na saúde, diante da transformação digital das sociedades contemporâneas. O artigo trabalha centralmente a hipótese da necessidade de estratégias claras de proteção de dados de saúde, dada sua especial sensibilidade, incluindo acesso, armazenamento e partilha por meio dos modernos sistemas digitais. Os autores sugerem a implementação de medidas criativas, que recorram a IA, para avaliar o impacto na privacidade quando do desenho, do desenvolvimento, da aquisição e da implementação de sistemas digitais. A exigência de estudos ou pareceres de impacto na privacidade seria excelente ferramenta de prevenção de fenômenos cibernéticos disruptivos.

Palavras-chave: Bioética. Segurança computacional. Inteligência artificial. Privacidade. Saúde.

Resumen

Inteligencia artificial, privacidad y protección de datos en salud

La transición digital, especialmente en lo que respecta a la inteligencia artificial, configura las relaciones entre personas y comunidades en los más diversos ámbitos de actividad. Este artículo pretende abordar de manera estructurada y sistemática, la ciberseguridad en lo relativo a la preservación de valores civilizatorios, como la privacidad o la protección de los datos personales de salud, ante la transformación digital de las sociedades contemporáneas. El artículo se centra en la hipótesis de la necesidad de estrategias claras para la protección de los datos de salud, dada su especial sensibilidad, incluido su acceso, almacenamiento e intercambio mediante los modernos sistemas digitales. Los autores sugieren la implementación de medidas creativas que recurran a la IA para evaluar el impacto sobre la privacidad durante el diseño, desarrollo, adquisición e implementación de sistemas digitales. La exigencia de estudios o dictámenes de impacto sobre la privacidad constituiría una excelente herramienta para prevenir fenómenos cibernéticos disruptivos.

Palabras clave: Bioética. Seguridad computacional. Inteligencia artificial. Privacidad. Salud.

Abstract

Artificial intelligence, privacy, and data protection in healthcare

The digital transition, particularly with regard to artificial intelligence, is shaping relationships among individuals and communities across a wide range of fields. This article aims to address, in a structured and systematic manner, cybersecurity as it relates to the preservation of civilizational values, such as privacy and the protection of personal health data, in the context of the digital transformation of contemporary societies. The article focuses primarily on the hypothesis that clear strategies for protecting health data are needed, given their particularly sensitive nature, including their access, storage, and sharing through modern digital systems. The authors suggest implementing creative measures that employ AI to assess privacy impacts during the design, development, acquisition, and implementation of digital systems. Requiring privacy impact studies or assessments would be an excellent tool for preventing disruptive cyber phenomena.

Keywords: Bioethics. Computer security. Artificial intelligence. Privacy. Health.

Declararam não haver conflito de interesse.

O advento da Quarta Revolução Industrial – essencialmente fruto da globalização e da era digital – veio alterar profundamente o modelo de desenvolvimento econômico e social das sociedades civilizadas (economia 4.0). A atual fase do desenvolvimento tecnológico pauta-se pela incorporação, na sociedade e na economia – nomeadamente na produção industrial –, de alargado conjunto de tecnologias de informação e comunicação, tais como a inteligência artificial (IA), a internet (internet das coisas), a robótica, entre outras. Virtualmente, todos os sistemas produtivos são afetados, incluindo o sistema de saúde, com elevado impacto na produtividade e no emprego (qualidade e quantidade) de novos modelos de negócio de base digital e em escala global. Historicamente, a evolução econômica, social e industrial se associa a diferentes evoluções tecnológicas – Indústria 1.0 e vapor de água e carvão; Indústria 2.0 e linhas de montagem baseadas na eletricidade; Indústria 3.0 e automatização; e Indústria 4.0 e internet e economia digital –, que implicaram o reequacionamento do desenvolvimento social e das relações políticas entre povos, Estados e nações¹.

A emergência e o desenvolvimento da inteligência artificial, ou mesmo a generalização da internet, vêm colocar o problema em novos termos. É possível falar até mesmo de economia 5.0, já que entramos agora em nova fase na qual importa otimizar a revolução digital, mas sempre a serviço das pessoas, da sociedade, da economia, da saúde e da promoção de um ambiente sustentável², e, simultaneamente, desenvolver sistemas de regulação e supervisão que permitam o pleno exercício de direitos inalienáveis dos cidadãos, como o direito à privacidade individual, inclusive no setor da saúde.

Trata-se de problema da maior atualidade e pertinência diante não apenas do crescimento descontrolado dessa tecnologia, mas também da falta de regulação transnacional de sua aplicação e utilização, que deve ser efetuada de acordo com princípios éticos universais, como autonomia individual ou justiça e equidade no acesso. Embora múltiplos países tenham avançado em leis e diretrizes sobre inteligência artificial, ainda não existe marco regulatório transnacional que garanta convergência e aplicabilidade global, o que mantém a questão em aberto e justifica a investigação aqui proposta.

Este artigo pretende abordar, de modo estruturado e sistemático, a cibersegurança no que diz respeito à preservação de valores civilizatórios, como privacidade, ou proteção de dados pessoais, diante da transformação digital das sociedades contemporâneas. Trabalha-se a hipótese da necessidade de estratégias claras de proteção de dados de saúde – incluindo acesso, armazenamento e compartilhamento –, tendo em vista sua especial sensibilidade. Importa também verificar se os médicos e demais profissionais de saúde adquiriram letramento adequado em IA e saúde digital para enfrentar exigências e desafios. Este estudo parte de revisão teórica para realizar análise documental, em que foram utilizados como critérios de seleção e discussão dos documentos analisados a relevância científica e o impacto destes nas políticas públicas nacionais e internacionais.

Sociedade digital global

McLuhan e Powers preconizaram, há algumas décadas, que o movimento centrípeto induzido pela globalização cultural estava rapidamente transformando o planeta em uma verdadeira “aldeia global”³. Entende-se que essa evolução foi fortemente estimulada pelas novas tecnologias de informação e comunicação (TIC), que se tornaram parte integrante da vida sociocomunitária, sobretudo nas novas gerações. Tal determinismo tecnológico, ditado parcialmente pelo enorme investimento das sociedades civilizadas no letramento digital, recorre à desmaterialização dos sistemas de informação como paradigma de intervenção. A internet, o *e-mail*, as redes sociais ou as bases virtuais como a nuvem (*cloud*) trouxeram óbvios benefícios à humanidade, e nos mais diferentes domínios.

Na saúde, a revolução digital foi intensamente sentida, quer na gestão estratégica e operacional das organizações (nos hospitais e na atenção primária), quer na desmaterialização do processo clínico (registo eletrónico de saúde), da prescrição médica (receitas digitais), da marcação de atos médicos (marcação on-line de consultas e exames), ou, ainda, na e-saúde, nova forma de interação dos pacientes com o sistema de saúde por meio da telessaúde⁴.

No Brasil e em Portugal (e na União Europeia), a coleta, o armazenamento e o envio de dados pessoais (imagem, sinal, vídeo) para análise mediante tecnologias de informação (*e-mail*, internet) têm implicações éticas e jurídicas específicas, reguladas, respectivamente, pela Lei Geral de Proteção de Dados Pessoais⁵ e pelo Regulamento Geral de Proteção de Dados⁶.

Em relação aos mais variados serviços – desde compras on-line, mobilidade e transportes (como Uber) a jogos e apostas, incluindo, obviamente, o *marketing* de produtos –, as plataformas digitais revolucionaram o modo como se efetuam negócios em escala global. Essa revolução inclui também a comunicação social, setor em que não apenas os *traditional media* (rádio, televisão, jornal, revistas) são hoje paulatinamente substituídos pelos *new media* (redes sociais, jornais digitais, *websites*, *mobile apps*, mundos virtuais, multimídia, jogos de computador e aplicações interativas), mas também ocorre importante mudança de paradigma.

Essa mudança se traduz em diferentes práticas culturais, mais baseadas na comunidade e em que a apreensão instantânea de informação, muitas vezes sem adequada apreciação crítica, pode originar círculos concêntricos de informação e, conseqüentemente, de formação de opinião, que distorcem a realidade e formam correntes de pensamento eventualmente deturpadas (de que o crescimento descontrolado de *fake news*, a desinformação, é bom exemplo). Na medicina, esse fenômeno pode ser especialmente complexo pelo impacto na saúde dos pacientes, a exemplo do discurso contrário à vacinação.

Na Europa, a enorme importância da transformação digital levou a Comissão Europeia a apresentar a inovadora “Agenda digital”⁷, um dos pilares estruturais da estratégia Europa 2030, intrinsecamente relacionada aos objetivos de crescimento da União Europeia. A ideia central da agenda é potencializar a utilização dinâmica das tecnologias de informação e comunicação de modo a estimular a inovação e o progresso econômico na União Europeia, a fim de criar um Mercado Digital Único na Europa. Criar serviços digitais de elevada qualidade, seja no trabalho, no lazer ou nos negócios, sem barreiras artificiais e com elevados níveis de proteção, é o desiderato desse mercado.

Ou seja, pretende-se, com essa evolução: melhorar o acesso de consumidores e empresas

(*geoblocking*, e-comércio e distribuição) às tecnologias; desenvolver redes digitais avançadas e serviços inovadores (mercado das telecomunicações, serviços de *media*, segurança informática); estimular a economia digital (economia dos dados, sociedade digital inclusiva, interoperabilidade e standardização, digitalização da indústria europeia); e garantir direitos e princípios digitais (de acordo com a Declaração Europeia sobre os Direitos e Princípios Digitais).

Também o Brasil tem ambiciosa agenda de transformação digital a caminho da era digital, que se pauta pelas seguintes metas⁸: melhorar a conectividade; aumentar a confiança nas tecnologias; desencadear a inovação digital; promover a transformação digital da economia; atualizar o marco regulatório para proteger dados de saúde e segurança da informação; e construir abordagem integral do governo (*whole-of-government*). Para isso, foi instituído grupo de trabalho voltado à gestão do Plano Brasileiro de Inteligência Artificial⁹, o que denota a preocupação existente na matéria.

Em decorrência da imparável evolução da tecnologia, surgem incontornáveis questões éticas que exigem reflexão e regulação na forma de legislação nacional e internacional. Tal legislação deve estar atenta aos direitos humanos e à sustentabilidade ambiental para que os direitos das gerações vindouras não sejam hipotecados, e para que o direito à saúde seja usufruído por todos em condições de equidade.

A transição digital molda de modo decisivo as relações entre pessoas e comunidades nos seus mais diferentes domínios. Virtualmente, nosso modo de vida está sendo reestruturado por essa revolução, e é necessário criar condições para perceber tal mudança e para estabelecer consciência crítica planetária sobre os desvios que podem ocorrer, exponenciados pela ausência de instituições formais em escala global capazes de regular muitas dessas atividades.

A existência de *big data*, ou seja, enorme quantidade de dados em diferentes suportes e captados de modos muito diversos, veio revolucionar o modo como os direitos individuais, considerados aspirações civilizatórias, são percebidos e protegidos nas sociedades contemporâneas. Nossos dados pessoais estão de fato à mercê dos sistemas digitais e da inteligência artificial, o que torna

necessário impor os princípios bioéticos de autonomia, liberdade individual, justiça e equidade.

Proteção de dados pessoais

De acordo com Tene e Polonetsky¹⁰, vivemos em uma era de *big data*. Os dados se tornaram a matéria-prima da produção, nova fonte de imenso valor econômico e social. Os avanços em mineração (*data mining*) e análise de dados e o aumento maciço do poder computacional e da capacidade de armazenamento de dados expandiram a quantidade de informação disponível para empresas, governos e indivíduos. Além disso, o número crescente de pessoas, dispositivos e sensores ligados por redes digitais revolucionou a capacidade de gerar, comunicar, compartilhar e acessar dados.

Os dados criam um enorme valor para a economia global, impulsionando inovação, produtividade, eficiência e crescimento. Ao mesmo tempo, como referem Omer Tene e Jules Polonetsky¹⁰, o “dilúvio de dados” é acompanhado de preocupações com a privacidade que podem provocar uma reação regulatória (*regulatory backlash*), atenuando a economia de dados e sufocando a inovação.

Percebe-se, então, que uma sociedade global digital evoca preocupações em diferentes níveis, sobretudo no que se refere a cibersegurança e controle e regulação do acesso a dados pessoais, incluindo os metadados, ou seja, dados que fornecem dados sobre outros dados. Estes são indispensáveis na comunicação e interação entre diferentes sistemas de inteligência artificial, e são úteis para descrever informação de qualquer natureza, seja médica, literária ou artística.

Esse conceito deve ser distinguido de *data lake* (incluindo *big data*), ou seja, coleções muito diversificadas de dados de diferentes proveniências, de forma estruturada ou não, que tendem a crescer exponencialmente com o desenvolvimento dos sistemas digitais. Os metadados são essenciais na pesquisa em medicina e ciências da vida, e já são correntemente utilizados por fornecerem informação detalhada de natureza demográfica, sobre tipo de amostras, métodos de processamento, entre outros. Também são sistematicamente utilizados na criação de formulários de relato de caso (*case report forms*), instrumento fundamental para o

desenvolvimento de ensaios clínicos de novos medicamentos para uso humano.

Nesse cenário, o quadro regulatório deve progressivamente implementar o conceito de dados FAIR (*FAIR data*), acrônimo para dados localizáveis (*findable*), acessíveis (*accessible*), interoperáveis (*interoperable*) e reutilizáveis (*reusable*). Esse conceito parte do princípio de que dados e metadados são acionáveis pelos sistemas digitais, uma vez que, devido ao volume, à complexidade e à rapidez de criação de dados desses sistemas, progressivamente confia-se neles para tratar dados. O primeiro passo é assegurar a localização de dados e metadados, componente essencial da FAIRificação dos dados, que devem ser acessíveis aos investigadores e sistemas computacionais, assim como as respectivas autorizações de acesso obtidas. Esta é condição essencial para uma IA de confiança, como sugere a Comissão Europeia¹¹.

Posto que a finalidade da estratégia FAIR é maximizar a reutilização de dados, a interoperabilidade de dados e sistemas é fundamental para otimizar sua análise, armazenamento e processamento. Na medicina e na pesquisa, dados FAIR não significam necessariamente dados abertos (*open data*), haja vista a sensibilidade dos dados de saúde. Porém, recorrer a eles apresenta inúmeras vantagens, como evitar duplicação de esforços, reutilizar dados para novas finalidades, alcançar o maior impacto possível com a investigação efetuada e contribuir para a replicabilidade e reprodutibilidade científica. Assim, a confiança da sociedade nas novas tecnologias cresce¹¹.

Portanto, é necessário identificar os principais problemas éticos referentes a coleta, armazenamento, análise, transferência e visualização de dados pessoais¹². E, ainda, se o “princípio da finalidade” na obtenção de dados é respeitado, de modo a tranquilizar a sociedade nesse aspecto, exigindo-se que o titular realize ato positivo claro que indique manifestação de vontade livre, específica, informada e inequívoca de que consente o tratamento de seus dados – mediante declaração escrita, inclusive em formato eletrônico, ou declaração oral, por exemplo. Destaca-se que o recém-criado “direito ao esquecimento” é reflexo da percepção generalizada de que os sistemas de informação não garantem eficazmente os direitos de cidadania. E, como referem Correia, Rego e Nunes¹³, este direito deve ser

progressivamente considerado na formulação de políticas públicas.

Na medicina, essa prática de consentimento é especialmente relevante e deve ser conhecida por médicos e outros profissionais de saúde na pesquisa em seres humanos¹⁴. O anexo apresenta exemplo de documento específico de consentimento ao tratamento de dados pessoais (conteúdo distinto do termo de consentimento livre e informado para participar em estudo/pesquisa, podendo, contudo, estar redigido no mesmo documento).

A generalização da IA na medicina também suscita questão mais vasta: a proteção da privacidade individual¹⁵, conceito que se relaciona, mas não se limita, à proteção de dados. Deverão ser considerados dados pessoais relativos à saúde todos aqueles que revelam informações sobre a saúde física ou mental de uma pessoa, incluindo informações sobre análises ou exames de parte do corpo ou de substância corporal, ou dados genéticos e amstras biológicas. Também são dados pessoais quaisquer informações sobre doença, deficiência, risco de doença, histórico clínico, tratamento clínico ou estado fisiológico ou biomédico.

Destaca-se que a proteção de dados inclui dados genéticos, que, por sua própria natureza e porque implicam terceiras partes (familiares do caso *index*), merecem especial proteção. Dados genéticos são dados pessoais relativos às características genéticas, hereditárias ou adquiridas que resultem da análise de amostra biológica, nomeadamente da análise de cromossomos, ácido desoxirribonucleico (DNA) ou ácido ribonucleico (RNA), ou da análise de outro elemento que permita obter informações equivalentes¹⁶.

Portanto, é fundamental difundir a percepção, na sociedade em geral e na medicina em particular, de que a coleta e o tratamento de produtos biológicos (incluindo informação genética) devem ser claramente regulamentados e supervisionados, sempre no âmbito da criação de biobanco, ou seja, de banco de produtos biológicos.

O recurso a tecnologias que melhoram a privacidade, como encriptação, metadados, ou *user interface*, é hoje indispensável diante de novas tecnologias extrativas de dados, de escâner de corpo inteiro, ou de sequenciação de DNA de segunda geração. Sempre que possível, os dados

de saúde individuais devem ser anonimizados ou pseudonimizados para proteger a intimidade da pessoa. A aplicação da pseudonimização aos dados pessoais pode reduzir riscos para os titulares dos dados e ajudar os responsáveis pelo tratamento de dados a cumprirem suas obrigações de proteção, sobretudo a de proteger a privacidade individual, direito especialmente relevante, mas que, na cultura digital, tende a ser negligenciado.

De fato, a privacidade individual é direito fundamental que protege um dos valores mais marcantes de uma sociedade secular e pluralista, uma vez que pretende restringir o acesso não autorizado de terceiros – indivíduos, organizações ou do próprio Estado – à pessoa em suas múltiplas dimensões. Reinterpretando, assim, a visão de Coolley, citado por Adams, sobre a existência de um *right to be let alone*, ou seja, “direito a ser deixado em paz”¹⁷. Essa visão jurisprudencial do final do século XIX pretende afirmar que à pessoa humana é garantido o direito ao anonimato, a ser deixado sozinho e à reserva da intimidade individual, em qualquer contexto social, econômico, político, ou psicológico, devendo a legislação estipular claramente o quadro legal em que a privacidade pode ser condicionada¹⁸.

A privacidade individual é, no plano formal, direito relativamente novo, dado que a sociedade, nas múltiplas formas de organização e sujeita historicamente às mais diversas influências culturais, submeteu ancestralmente o ser humano aos desígnios coletivos e à satisfação das necessidades básicas de sobrevivência comunitária¹⁹. Contudo, as raízes desse direito podem estar na demarcação, na visão de Aristóteles, entre público e privado, ou seja, o *polis* e o *oikos*.

Na perspectiva de Solove²⁰, a preservação da privacidade exige que terceiros se abstenham de determinadas atividades que violem espírito, mente, paz, espaço físico ou corpo humano de uma pessoa. Esse direito encontra-se consolidado no art. 12 da Declaração Universal dos Direitos Humanos, que afirma claramente que *Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques*²¹. Progressivamente, o conceito de privacidade associou-se a formas

mais robustas de soberania individual, incluindo as seguintes dimensões:

- física: direito a decidir sobre o próprio corpo;
- mental: direito à liberdade cognitiva e moral, sem coação e com livre pensamento;
- de decisão: direito a tomar decisões sobre si próprio sem intromissão externa;
- informacional: direito a manter a informação pessoal reservada (incluindo dados pessoais), sendo necessário obter consentimento para acesso, utilização e armazenamento dessa informação; o segredo profissional (segredo médico) decorre dessa dimensão da privacidade;
- patrimonial: direito a obter, manter e gerir o patrimônio e a propriedade privada.

Daí a necessidade de implementar estratégias eficazes de cibersegurança, ou seja, proteger sistemas, programas e redes digitais contra ataques e interferências disruptivas no espaço digital. A cibersegurança visa proteger pessoas, instituições e sociedades do acesso indevido, da alteração ou da destruição de informação privilegiada, sendo a medicina e a saúde áreas especialmente sensíveis pela natureza privada dos dados pessoais.

Inteligência artificial e cibersegurança

Para implementar um programa eficaz de cibersegurança, é essencial que haja envolvimento ativo de todos os parceiros, com implementação de estratégia adequada e articulação eficaz de processos e de tecnologia. É necessário, portanto, conhecer as potencialidades da IA para prevenir ciberataques que recorrem a tecnologias intrusivas da privacidade, como computação onipresente, internet das coisas, dados de satélite, *blockchain*, criptomoeda, aprendizado de máquina, automação, tecnologia ambiental, tecnologia neurolinguística, tecnologia memética (estudo formal dos memes), tecnologia de grade, roubo de identidade, mineração de dados, cartões inteligentes, registradores de chaves e redes sem fio.

Deve-se, então, implementar medidas concretas de segurança física e lógica para prevenir os efeitos nocivos de ciberataques ou fenômenos extremos, como os *black swan events*, ou eventos cisne negro. Esse termo, cunhado por Taleb²²,

refere-se a fenômenos imprevisíveis, altamente improváveis, mas com significativo impacto nacional ou internacional, que só são reconhecidos *a posteriori*. A pandemia de covid-19 é exemplo recente de evento cisne negro e o recurso a IA em estratégias de cibersegurança pode permitir prevenir, ou pelo menos mitigar, o impacto devastador de futuras pandemias, não apenas na saúde dos pacientes, mas também no controle das mudanças radicais no comportamento do público e nas cadeias de suprimentos.

O setor da saúde, dada sua importância estratégica, é alvo prioritário de ciberataques, sobretudo se potencializados por IA, sendo necessário implementar testes de segurança para proteger eficazmente os dados pessoais e a privacidade dos pacientes. A cibersegurança na saúde é especialmente crítica porque hospitais e centros de saúde recorrem regularmente a tecnologias digitais em suas operações – a exemplo da telemedicina ou do prontuário eletrônico/registo de saúde eletrônico – em nível de *hardware*, *software* ou por meio da nuvem²³.

Ao longo das duas últimas décadas, hospitais em todo o mundo tornaram-se alvos de ataques cibernéticos, inclusive de natureza terrorista²⁴, como o ataque ao hospital Change Healthcare, nos Estados Unidos, em 2024, ou ao Hospital Clinic, em Barcelona, em 2023. Portanto, é fundamental desenvolver estratégias preventivas para proteger os dados pessoais dos pacientes. Na perspectiva de Lv e Piccialli²⁵, pode mesmo ser necessário recorrer a sistemas matemáticos avançados, como a tecnologia de privacidade diferencial, para proteger a identidade individual e os dados pessoais de saúde.

Além disso, o *hacking*, ou seja, o ato de identificar e explorar as fraquezas de um sistema ou de uma rede e, subsequentemente, acessar de forma não autorizada dados pessoais ou informações de uma organização, é frequente. Esse tipo de ação é realizada visando obter ganhos financeiros (acesso a cartão de crédito, por exemplo), realizar espionagem corporativa ou promovida por um Estado (para obter informações, por exemplo), e é mais facilitada pela tendência, eventualmente securitária, de videovigilância de espaços públicos ou no interior das organizações – entre as quais hospitais –, ou de monitorização on-line de diferentes atividades.

Essa tendência implica a implementação de complexos mecanismos de encriptação, crucial na proteção da privacidade e da segurança on-line, e ferramenta de grande interesse para proteger direitos fundamentais, como o direito à proteção da saúde. A encriptação, sobretudo se alavancada por inteligência artificial, assegura que pessoas e organizações possam compartilhar informação com segurança e liberdade, sem receio de que esta seja publicizada pelo Estado ou por organizações criminosas. Isso inclui informações sensíveis – como identidade de gênero, orientação sexual, estado de soropositividade para algumas doenças ou prognósticos reservados, como de oncologia –, assim como informações sensíveis nos setores privado e público de saúde (Sistema Único de Saúde ou Serviço Nacional de Saúde).

A abordagem da necessidade de implementar estratégias globais de cibersegurança, especialmente para responder à questão sobre a possibilidade de proteger a privacidade individual na sociedade digital e em ciberespaço alargado (universal no sentido literal do termo), carece de enquadramento conceitual adequado.

Este enquadramento deve fazer a interseção da segurança e da privacidade nas dimensões ontológica, epistemológica, metodológica e bioética, o que é especialmente relevante considerando a mudança de paradigma que hoje se evidencia²⁶. De fato, essa interseção propulsionada pela IA representa verdadeira mudança de paradigma, quer em perspectiva científica²⁷, quer em perspectiva epistemológica²⁸. Assim, entende-se que a problemática da cibersegurança na sociedade digital global será provavelmente um dos maiores desafios que a comunidade internacional enfrentará nas próximas décadas. A interface entre sociedade digital, privacidade e segurança global pode ser analisada na ótica do positivismo, podendo aprofundar-se esta análise através da apreciação deste paradigma em dimensões categoriais previamente selecionadas.

Em uma dimensão ontológica, segurança é necessidade objetiva, no plano do bem-estar pessoal e também da comunidade, sendo de primordial importância na ordem global e nas relações entre os diferentes estados. Já privacidade é direito formado pela consciência global, consensualizado por acordo mútuo entre as partes e ratificado por métodos aceitáveis por instituições

internacionais; é o oposto de direito enquanto valor social ou interpretação subjetiva do conceito de dignidade humana.

A dimensão epistemológica coloca em perspectiva a falta de segurança, enquanto realidade observável e fato incontestável relacionam-se com a verdade, também objetivável, da necessidade de proteção. Daí que se refira hoje a uma responsabilidade social global e coletiva de diferentes atores sociais em matéria de cibersegurança. Nesta dimensão, é realidade indesmentível a intromissão do Estado e seus organismos ou de empresas multinacionais, como a Big-AI (por motivos comerciais, securitários, de controle social, entre outros), na vida privada.

Já em uma dimensão metodológica, a evidência objetiva de falhas de segurança origina a necessidade de implementar estratégias de cibersegurança. Dada a hipótese de que só uma estratégia concentrada no nível da infraestrutura organizativa do Estado (ou em nível de governação supranacional) pode incrementar o nível de segurança digital, pode-se deduzir a necessidade de implementar estratégias integradas de cibergovernança. De fato, a violação reiterada da privacidade individual, fato constatável em falhas de cibersegurança, em diferentes níveis e em contextos muito diversos, suscita a necessidade de ampla discussão nacional e internacional acerca dessa temática. Eventualmente, será necessário implementar verdadeira ciberpolítica em nível transnacional, incluindo-se o envolvimento das Nações Unidas ou de outras organizações internacionais nessa regulação.

A bioética garantir a segurança, em especial na proteção de dados de saúde, é condição essencial para uma relação médico-paciente em que a confiança continue a ser elemento central do universo ético e autenticamente humano da entrevista clínica. Essa assunção torna-se imperativo ético de maior densidade quando os médicos se confrontam com sistemas digitais promovidos por IA, que os médicos apenas parcialmente controlam, dada a falta de explicação sobre a tecnologia. De fato, na medicina e nas ciências da saúde, a privacidade é valor bioético e direito fundamental na relação médico-paciente, pois se trata de direito inerente à pessoa humana, decorrente de sua identidade pessoal e da existência de um último reduto que deve estar salvaguardado de qualquer

intromissão externa. A proteção da privacidade é também pilar do dever de segredo médico e da própria moralidade interna da medicina.

Algumas das principais preocupações da segurança na proteção de dados são: confidencialidade, a fim de prevenir acesso não autorizado, evitar *sniffing* (monitorização de dados e controle de tráfico ilegais), limitar o compartilhamento de credenciais de acesso e promover maior controle de acesso por meio da criptografia; e integridade, a fim de prevenir modificação não autorizada de dados, promover assinaturas digitais, validação de dados, codificação e métodos consistência interna ou evitar falha de equipamentos, ataques ou *ransomware*.

É fundamental prever essa possibilidade de falta de segurança na proteção de dados melhorando sua detecção e prevenindo ocorrências futuras. Por motivos muito distintos, desde garantia de autenticidade dos dados (especialmente importante em setores como saúde, em que muita informação sem qualquer base científica circula na internet e nas redes sociais) até manutenção da integridade da informação (no sentido de garantir armazenamento sem possibilidade de acesso não autorizado), é importante definir regras claras e políticas internacionais coerentes. A política de mercado único digital na União Europeia é exemplo concreto da necessidade de partilhar dados entre os diferentes estados, mas, também, de implementar políticas coerentes e estruturadas em matéria de segurança²⁹.

Existem situações de ameaça à segurança cognitiva e estrutural. Existe, ainda, o risco não desprezível de falência total das infraestruturas críticas, como sugere Myriam Dunn: *As piores consequências dos riscos criados pelas tecnologias de informação e comunicação manifestam-se na possível falha das chamadas infraestruturas críticas, que são sistemas e ativos cuja incapacidade ou destruição teria um impacto debilitante na segurança nacional e no bem-estar econômico e social de um Estado. Impulsionados por uma preocupação crescente com a potencial vulnerabilidade das sociedades em rede, juntamente com um número crescente de perturbações no domínio cibernético, muitos países tomaram medidas para compreender melhor as vulnerabilidades e ameaças às suas infraestruturas (de informação) e propuseram medidas para a proteção desses ativos*³⁰.

Naturalmente, trata-se de problema global, mas também de foco de preocupação de cada país. Assim, aconselha-se que cada país proponha e implemente estratégia nacional de cibersegurança, mas sempre em articulação com outros países interessados em implementar tais políticas. É fato que quase toda população valoriza o ciberespaço, implícita ou explicitamente, dada sua ubiquidade, escala e intangibilidade³¹. Considerando também o nível de literacia digital das populações enquanto consumidores, incluindo os pacientes, essa ação é de primordial importância³², e inclui a responsabilidade partilhada de diferentes *stakeholders*, de modo a originar um sistema complexo e inter-relacionado de cibersegurança.

Em qualquer caso, dada a inexistência de instituições internacionais legitimadas pela ordem global que regulem eficazmente essas práticas³³, parece importante continuar a promover esta reflexão com base em pressupostos teóricos e metodológicos adequados. Assim, independentemente de tal regulação ser efetuada à margem da soberania tradicional do Estado ou rejeitando qualquer excepcionalidade do ciberespaço³⁴, podem ser encontradas soluções devidamente fundamentadas e que concretizem as mais elevadas aspirações civilizatórias nesse domínio – por exemplo, e como referimos em outro estudo³⁵, enquadrando a inteligência artificial de confiança no âmbito mais lato dos Objetivos de Desenvolvimento Sustentável das Nações Unidas.

A inteligência artificial tem a capacidade de revolucionar a cibersegurança, dado que permite: analisar rapidamente largas quantidades de dados; detectar anomalias e vulnerabilidades do sistema (tais como padrões de comportamento); reagir em tempo real, sinalizando comportamentos suspeitos; automatizar processos repetitivos, liberando os funcionários para outras tarefas; priorizar riscos e detectar instantaneamente a possibilidade de *malware* e de intrusões antes de acontecerem; e diminuir o erro humano.

A cibersegurança tradicional repousa na análise manual, em que a detecção baseia-se na assinatura (*signature-based detection*), um dos sistemas de detecção básicos de segurança. Ela identifica comportamentos maliciosos por meio da pesquisa de uma lista de indicadores conhecidos e tem sido razoavelmente efetiva em ameaças conhecidas. Não responde, porém, a ameaças novas ou desconhecidas.

As organizações cibercriminosas já investiram massivamente na IA para que esta lançasse ciberataques a determinadas organizações, e o setor da saúde não é exceção. Apesar disso, o potencial da IA em proteger os sistemas digitais é ilimitado. Devido a sua rapidez, efetividade e eficiência, ela aumenta substancialmente a produtividade das equipes de segurança, nomeadamente diante de novas formas de ciberataque, como *malware* ou novos vetores de *scripting*.

A segurança de dados biométricos – dados referentes a características humanas específicas que permitem identificar um indivíduo – também é considerada de enorme relevância. Os sistemas e processos de identificação biométrica recorrem à identificação e comparação de dados físicos ou comportamentais, realizadas por complexos sistemas digitais, agora exponenciados pela inteligência artificial. Incluem o recurso a impressões digitais, reconhecimento facial, dados genéticos, análise de voz, varredura da íris ou análise da palma da mão. No plano comportamental, a identificação biométrica recorre, por exemplo, à análise do modo como alguém anda ou de suas expressões faciais.

Ela é utilizada recorrentemente para controlar assiduidade na gestão das organizações, fiscalizar acesso – a fim de promover cibersegurança e impedir acesso não autorizado a computadores e outros sistemas digitais –, e geralmente é prova de identidade pessoal. No Brasil, a identificação biométrica é fortemente regulada pela Lei Geral de Proteção de Dados Pessoais⁵ (LGPD); na Europa, pelo Regulamento Geral de Proteção de Dados⁶ e pelo AI Act¹⁵, dado o potencial de abuso e violação de direitos fundamentais. Outros países têm produzido iniciativas regulatórias, diretrizes e leis que abordam ética, transparência, segurança e responsabilidade na IA, ainda que com diferentes enfoques: leis vinculativas (Coreia do Sul), diretrizes administrativas (Japão) ou legislação específica para danos e privacidade (Estados Unidos).

Na medicina e ciências da vida, a identificação biométrica é hoje utilizada regularmente na investigação científica e na saúde pública para realizar controle epidemiológico. Prevê-se que, impulsionada pela IA, a identificação biométrica possa não

apenas garantir a segurança dos dados pessoais, mas promover cuidados médicos mais precisos e personalizados³⁶.

Considerações finais

O artigo buscou avaliar uma das dimensões essenciais da cibersegurança, o impacto da IA na proteção de dados pessoais e da privacidade individual na medicina e na sociedade em geral. A cibersegurança de dados pessoais pode ter múltiplas dimensões valorativas no futuro próximo. Isto é, pode-se evoluir da abordagem positivista sobre a preservação da privacidade pessoal (e, portanto, da integridade individual) na ótica tradicional das relações entre o indivíduo e a sociedade (por exemplo, os Estados, o sistema de saúde, as grandes multinacionais da indústria farmacêutica) para uma distinta dinâmica em que a sociedade promove esse tipo de interação de acordo com princípios bioéticos universais.

Em conclusão, é necessário implementar medidas criativas, que recorram à IA, para avaliar o impacto na privacidade e na proteção de dados quando do desenho, desenvolvimento, aquisição e implementação de sistemas digitais. Exigir estudos ou pareceres de impacto na privacidade seria uma excelente maneira de prevenir fenômenos cibernéticos disruptivos que ameacem a percepção social dos benefícios da IA. De qualquer forma, a transição digital e, em particular, a inteligência artificial devem estar sempre sob supervisão humana (*human in the loop*), e os valores civilizatórios universalmente partilhados devem ser sempre considerados durante sua aplicação.

A medicina e demais profissões da saúde devem estar totalmente comprometidas em todo o processo de implementação de sistemas de IA na área (*physician in the loop*), garantindo que a tecnologia seja ferramenta de auxílio à decisão médica e não viole os direitos fundamentais dos pacientes. Isso implica que na formação médica sejam implementadas estratégias educativas e de letramento em tecnologias digitais para que os médicos estejam totalmente incluídos na transição digital e dela sejam elemento nuclear.

Referências

1. Rawls J. The law of peoples. The idea of public reason revisited. Boston: Harvard University Press; 1999.
2. Mafi A, Holmes S. Artificial intelligence risks becoming an environmental disaster. *BMJ* [Internet]. 2025 [acesso 13 jan 2025];388. DOI: 10.1136/bmj.r505
3. McLuhan M, Powers B. The global village. New York: Oxford University Press; 1989.
4. Cornford T, Klecun-Drabowska E. Ethical perspectives in evaluation of telehealth. *Camb Q Healthc Ethics* [Internet]. 2001 [acesso 13 jan 2025];10(2):161-9. DOI: 10.1017/s0963180101002079
5. Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União* [Internet]. Brasília, 15 ago 2018 [acesso 21 jan 2025]. Disponível: <https://tinyurl.com/456hda6y>
6. Parlamento Europeu. Regulamento 2016/679. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados. *Jornal Oficial da União Europeia* [Internet]. Bruxelas, p. 119-52, 4 maio 2016 [acesso 20 abril 2025]. Disponível: <https://tinyurl.com/23bx67r3>
7. Década digital da Europa [Internet]. Bruxelas: Comissão Europeia; 2024 [acesso 8 jan 2025]. Disponível: <https://tinyurl.com/5ccnpamn>
8. Organisation for Economic Co-operation and Development. A caminho da era digital no Brasil [Internet]. Paris: OECD Publishing; 2020 [acesso 20 abr 2025]. DOI: 10.1787/45a84b29-pt
9. Brasil. Resolução CITDIGITAL nº 2, de 8 de maio de 2025. Institui Grupo de Trabalho para a gestão do Plano Brasileiro de Inteligência Artificial. *Diário Oficial da União* [Internet]. Brasília, ed. 87, p. 2, 12 maio 2025 [acesso 7 nov 2025]. Seção 1. Disponível: <https://tinyurl.com/4ttxy9wd>
10. Tene O, Polonetsky J. Privacy in the age of big data: a time for big decisions. *Stanford Law Review Online* [Internet]. 2012 [acesso 8 jan 2025];63:63-9. p. 63. Tradução livre. Disponível: <https://tinyurl.com/5n7wwpht>
11. High-Level Expert Group on Artificial Intelligence. Ethics guidelines for trustworthy AI. Brussels: European Commission; 2019.
12. Nicolaidou IL, Georgiades C. The GDPR: new horizons. In Synodinou TN, Jouglex P, Markou C, Prastitou T, editors. *EU Internet Law – Regulation and Enforcement*. Berlin: Springer; 2017. p. 3-18.
13. Correia M, Rego G, Nunes R. Gender transition: is there a right to be forgotten? *Health Care Anal* [Internet]. 2021 [acesso 20 abril 2025];29:283-300. DOI: 10.1007/s10728-021-00433-1
14. Lekadir K, Frangi AF, Porras AR, Glocker B, Cintas C, Langlotz CP *et al*. FUTURE-AI: international consensus guideline for trustworthy and deployable artificial intelligence in healthcare. *BMJ* [Internet]. 2025 [acesso 8 jan 2025];388:e081554. DOI: 10.1136/bmj-2024-081554
15. European Union. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. Brussels: European Union [Internet]; 2023 [acesso 20 abril 2025]. Disponível: <https://tinyurl.com/3pvh64h4>
16. Nunes R. *GeneÉtica*. Coimbra: Almedina; 2013.
17. Adams R. The right to be let alone. *Fla Law Rev* [Internet]. 1965 [acesso 3 mar 2025];17(4):597-608. Disponível: <https://tinyurl.com/y4dva5ck>
18. Warren SD, Brandeis LD. The right to privacy. *Harv Law Rev* [Internet]. 1890 [acesso 3 mar 2025];4(5):193-220. Disponível: <https://tinyurl.com/dvww5kbx>
19. Prosser W. Privacy. *Calif Law Rev* [Internet]. 1960 [acesso 3 mar 2025];48:383-423. DOI: 10.2307/3478805
20. Solove DJ. A taxonomy of privacy. *Univ PA Law Rev* [Internet]. 2006 [acesso 3 mar 2025];154(3):477-560. Disponível: <https://bit.ly/4wodnF>
21. United Nations. Universal Declaration of Human Rights (1948) [Internet]. New York: United Nations; 2006 [acesso 12 ago 2026]. Disponível: <https://bit.ly/3SN7B9A>

22. Taleb N. The black swan: the impact of the highly improbable. New York: Random House; 2008.
23. Nunes R. Healthcare as a universal human right: sustainability in global health [Internet]. Milton Park: Routledge; 2022 [acesso 3 mar 2025]. Disponível: <https://bit.ly/4wLo9xq>
24. Chen G, Jin G. Insights from evidence-based medicine method for building security systems against terrorist attacks in hospitals. J Multidiscip Healthc [Internet]. 2023 [acesso 3 mar 2025];16:4133-7. DOI: 10.2147/JMDH.S426166
25. Lv Z, Piccialli F. The security of medical data on internet based on differential privacy technology. ACM Trans Internet Technol [Internet]. 2021 [acesso 3 mar 2025];21(3):1-18. DOI: 10.1145/3382769
26. Banks M. The inter-paradigm debate. In: Light M, Groom AJR, editors. International relations: a handbook of current theory. London: Francis Pinter; 1985. p. 12-13.
27. Kuhn T. The structure of scientific revolutions. Chicago: The University of Chicago Press; 1970.
28. Popper K. Conjeturas e refutações. Coimbra: Almedina; 2003.
29. Digital single market policy. Europe 2020 Strategy [Internet]. Brussels: European Commission; 2018 [acesso 3 mar 2025]. Disponível: <https://bit.ly/4q9ZFeW>
30. Dunn M. A comparative analysis of cybersecurity initiatives worldwide. International Telecommunications Union. Genève: WSIS Thematic Meeting on Cybersecurity; 2005. p. 3. Tradução livre.
31. Choucri N, Madnick S, Ferwerda J. Institutions for cyber security. International responses and global imperatives. Inf Technol Dev [Internet]. 2014 [acesso 3 mar 2025];20(2):96-121. DOI: 10.1080/02681102.2013.836699
32. Miedema TE. Engaging consumers in cyber security. Journal of Internet Law [Internet]. 2018 [acesso 3 mar 2025];21(8):3-15.
33. Keohane R. International institutions: two approaches. Int Stud Q [Internet]. 1988 [acesso 3 mar 2025];32(4):379-96. DOI: 10.2307/2600589
34. Santos L. Regulação do ciberespaço: cesuristas e tradicionalistas. Janus [Internet]. 2015 [acesso 3 mar 2025];6(1):93-107. Disponível: <https://bit.ly/4qe10By>
35. Nunes R, Nunes S. Reliable Artificial Intelligence: The 18th Sustainable Development Goal. Journal of Ethics and Legal Technologies [Internet]. 2024 [acesso 3 mar 2025];6(2):1-19. DOI: 10.14658/pupj-JELT-2024-2-2
36. Nunes R, Nunes S. Inteligência artificial: uma ponte para o futuro da medicina. Rev. bioét. (Impr.) [Internet]. 2025 [acesso 30 out 2025];33(2):24-34. DOI: 10.1590/1983-803420254115PT

Sofia Nunes – Doutora – asnunes@med.up.pt

 0000-0002-7182-9890

Rui Nunes – Doutor – ruinunes@med.up.pt

 0000-0002-1377-9899

Correspondência

Sofia Nunes – Al. Prof. Hernâni Monteiro, 4200-319. Porto, Portugal.

Contribuições dos autores

Sofia Nunes: conceitualização; investigação; metodologia; recursos; supervisão; visualização; redação – rascunho original; redação – revisão e edição.

Rui Nunes: conceitualização; investigação; metodologia; recursos; supervisão; visualização; redação; rascunho original; redação – revisão e edição.

Disponibilidade de dados: Todos os dados utilizados ou gerados na pesquisa estão integralmente descritos e apresentados no corpo do artigo.

Editora responsável: Dilza Teresinha Ambrós Ribeiro

Recebido: 18.5.2025

Revisado: 21.5.2026

Aprovado: 1.6.2026

Anexo

DECLARAÇÃO DE CONSENTIMENTO

(nome completo), titular da
Carteira de Identidade Nacional/do Cartão de Cidadão nº _____, declaro que confiro a

(nome da organização), de forma livre e inequívoca, o consentimento
para o tratamento dos meus dados pessoais constantes do _____ (nome do estudo), que
decorrerá no _____ (nome do local onde será realizado o estudo), bem como
ao tratamento subsequente desses dados no âmbito desta finalidade.

Confirmando que fui informado(a) de que tenho direito de solicitar acesso aos meus dados pessoais, requerer
sua retificação, apagamento e sua portabilidade, e que para qualquer dúvida ou reclamação respeitante
a dados pessoais devo enviar um correio eletrônico para o Encarregado de Proteção de Dados da

(nome da organização), para o endereço de correio eletrônico _____,
bem como que tenho o direito de reclamação para a Autoridade Nacional de Proteção de Dados/
Comissão Nacional de Proteção de Dados.

Confirmando ter lido as Políticas de Privacidade da _____ (nome da organização), que se
encontram em (sítio da internet).

(local), (data)

(Assinatura igual à constante no documento de identificação)