

Inteligencia artificial, privacidad y protección de datos en salud

Sofia B. Nunes¹, Rui Nunes¹

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

Resumen

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.

Resumo

Inteligência artificial, privacidade e proteção de dados na saúde

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.

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.

Los autores declaran que no existe ningún conflicto de interés.

El advenimiento de la Cuarta Revolución Industrial — esencialmente resultado de la globalización y la era digital —, ha cambiado profundamente el modelo de desarrollo económico y social de las sociedades civilizadas (economía 4.0). La etapa actual del desarrollo tecnológico se caracteriza por la incorporación, en la sociedad y en la economía —en particular en la producción industrial—, de una amplia gama de tecnologías de la información y comunicación, como la inteligencia artificial (IA), internet (internet de las cosas), la robótica, entre otras. Prácticamente todos los sistemas de producción se ven afectados, incluido el sistema sanitario, con un impacto significativo en la productividad y en el empleo (calidad y cantidad) de los nuevos modelos de negocio digitales a escala global. Históricamente, la evolución económica, social e industrial se ha asociado con diferentes evoluciones tecnológicas: Industria 1.0 y vapor y carbón; Industria 2.0 y líneas de ensamblaje basadas en electricidad; Industria 3.0 y automatización; e Industria 4.0 e internet y economía digital, que han implicado una reevaluación del desarrollo social y de las relaciones políticas entre pueblos, Estados y naciones¹.

El surgimiento y desarrollo de la inteligencia artificial, o incluso el uso generalizado de internet, están planteando el problema desde una nueva perspectiva. Incluso se puede hablar de economía 5.0, puesto que estamos entrando en una nueva etapa en la que es importante optimizar la revolución digital, pero siempre al servicio de las personas, de la sociedad, de la economía, de la salud y de la promoción de un medio ambiente sostenible², y, simultáneamente, desarrollar sistemas de regulación y supervisión que permitan el pleno ejercicio de los derechos inalienables de los ciudadanos, como el derecho a la privacidad individual, incluso en el sector de la salud.

Se trata de un tema muy actual y relevante, dado no solo el crecimiento descontrolado de esta tecnología, sino también la falta de regulación transnacional de su aplicación y uso, que debería llevarse a cabo de acuerdo con principios éticos universales, como la autonomía individual o la justicia y la equidad en el acceso. Si bien varios países han avanzado en materia de leyes y directrices sobre inteligencia artificial, aún no existe un marco regulatorio transnacional que asegure la convergencia y la aplicabilidad a nivel mundial, lo que mantiene el tema abierto y justifica la investigación que aquí se propone.

Este artículo pretende abordar, de forma estructurada y sistemática, la ciberseguridad en lo que respecta a la preservación de valores civilizatorios, como la privacidad o la protección de datos personales, frente a la transformación digital de las sociedades contemporáneas. Se aborda la hipótesis de la necesidad de estrategias claras de protección de datos sanitarios —incluido el acceso, almacenamiento e intercambio—, teniendo en vista su sensibilidad especial. También es importante comprobar si los médicos y otros profesionales de la salud han adquirido los conocimientos adecuados en IA y salud digital para afrontar las demandas y los desafíos. Este estudio comienza con una revisión teórica para realizar un análisis documental, en el que los criterios para seleccionar y analizar los documentos analizados fueron su relevancia científica y su impacto en las políticas públicas nacionales e internacionales.

Sociedad digital global

McLuhan y Powers predijeron, hace algunas décadas, que el movimiento centrípeto inducido por la globalización cultural estaba transformando rápidamente el planeta en una verdadera “aldea global”³. Se entiende que esta evolución estuvo fuertemente impulsada por las nuevas tecnologías de la información y la comunicación (TIC), que se han convertido en parte integrante de la vida sociocomunitaria, especialmente entre las nuevas generaciones. Este determinismo tecnológico, dictado en parte por la enorme inversión de las sociedades civilizadas en alfabetización digital, recurre a la desmaterialización de los sistemas de información como paradigma de intervención. Internet, el correo electrónico, las redes sociales y las plataformas virtuales como la nube (*cloud*) han aportado beneficios evidentes a la humanidad en muchos ámbitos diferentes.

En el campo de la salud, la revolución digital se ha hecho sentir con fuerza, tanto en la gestión estratégica y operativa de las organizaciones (en los hospitales y en la atención primaria), como en la desmaterialización del proceso clínico (registro clínico electrónico), la prescripción médica (recetas digitales), la reserva de citas en línea para consultas y exámenes), o incluso en la e-salud, una nueva forma de interacción entre los pacientes y el sistema sanitario a través de la telemedicina⁴.

En Brasil y en Portugal (y en la Unión Europea), la recopilación, el almacenamiento y la transmisión

de datos personales (imagen, señal, vídeo) para su análisis mediante tecnologías de la información (correo electrónico, internet) tienen implicaciones éticas y legales específicas, reguladas, respectivamente, por la Ley General de Protección de Datos⁵ y por el Reglamento General de Protección de Datos⁶.

En lo que respecta a una amplia variedad de servicios —desde compras en línea, movilidad y transporte (como Uber) hasta juegos y apuestas, incluido, por supuesto, el *marketing* de productos—, las plataformas digitales han revolucionado la forma en que se hacen negocios a escala mundial. Esta revolución incluye también la comunicación social, sector en el que no solo los *traditional media* (radio, televisión, periódicos, revistas) son reemplazados poco a poco en la actualidad por los *new media* (redes sociales, periódicos digitales, sitios web, *mobile apps*, mundos virtuales, multimedia, juegos de computadora y aplicaciones interactivas), pero también se produce un importante cambio de paradigma.

Este cambio se traduce en prácticas culturales diferentes, más basadas en la comunidad, en que la asimilación instantánea de la información, a menudo sin una apreciación crítica adecuada, puede originar círculos concéntricos de información y, en consecuencia, de formación de opiniones, que distorsionan la realidad y forman corrientes de pensamiento que finalmente se deturpan (de las cuales el crecimiento descontrolado de las *fake news*, la desinformación, es un buen ejemplo). En medicina, este fenómeno puede ser especialmente complejo debido a su impacto en la salud de los pacientes, como lo demuestra la retórica antivacunas.

En Europa, la enorme importancia de la transformación digital ha llevado a la Comisión Europea a presentar la innovadora “Agenda digital”⁷, uno de los pilares estructurales de la estrategia Europa 2030, intrínsecamente relacionada con los objetivos de crecimiento de la Unión Europea. La idea central de la agenda es aprovechar el uso dinámico de las tecnologías de la información y comunicación para estimular la innovación y el progreso económico en la Unión Europea, con el fin de crear un Mercado Digital Único en Europa. El objetivo de este mercado es crear servicios digitales de alta calidad, ya sea para el trabajo, el ocio o los negocios, sin barreras artificiales y con altos niveles de protección.

En otras palabras, esta evolución tiene como objetivo mejorar el acceso de consumidores y empresas (*geoblocking*, e-comercio y distribución) a

las tecnologías; desarrollar redes digitales avanzadas y servicios innovadores (mercado de las telecomunicaciones, servicios de medios de comunicación, ciberseguridad); estimular la economía digital (economía de datos, sociedad digital inclusiva, interoperabilidad y estandarización, digitalización de la industria europea); y garantizar los derechos y principios digitales (en conformidad con la Declaración Europea sobre Derechos y Principios Digitales).

Brasil también cuenta con una ambiciosa agenda de transformación digital en su camino hacia la era digital, guiada por los siguientes objetivos⁸: mejorar la conectividad; aumentar la confianza en las tecnologías; impulsar la innovación digital; promover la transformación digital de la economía; actualizar el marco regulatorio para proteger los datos de salud y la seguridad de la información; y construir un enfoque integral del gobierno (*whole-of-government*). Para este propósito, se estableció un grupo de trabajo centrado en la gestión del Plan Brasileño de Inteligencia Artificial⁹, lo que denota la preocupación existente sobre el tema.

Como consecuencia de la imparable evolución de la tecnología, surgen inevitables cuestiones éticas que requieren reflexión y regulación en forma de legislación nacional e internacional. Dicha legislación debe tener en cuenta los derechos humanos y la sostenibilidad ambiental para que no se vean comprometidos los derechos de las generaciones futuras y para que todos disfruten del derecho a la salud en condiciones de equidad.

La transición digital está transformando decisivamente las relaciones entre las personas y comunidades en sus ámbitos más diversos. Prácticamente, nuestra forma de vida está siendo reestructurada por esta revolución, y es necesario crear las condiciones para percibir este cambio y establecer una conciencia crítica planetaria sobre las desviaciones que puedan producirse, exacerbadas por la ausencia de instituciones formales a escala mundial capaces de regular muchas de estas actividades.

La existencia de *big data*, es decir, la enorme cantidad de datos en diferentes formatos y recopilados de maneras muy diversas, ha revolucionado la forma en que los derechos individuales, considerados aspiraciones civilizatorias, se perciben y protegen en las sociedades contemporáneas. Nuestros datos personales están, de hecho, a merced de los sistemas digitales y de la inteligencia artificial, lo que hace necesario imponer los

principios bioéticos de autonomía, libertad individual, justicia y equidad.

Protección de datos personales

Según Tene y Polonetsky¹⁰, vivimos en una era de *big data*. Los datos se han convertido en la materia prima de la producción, una nueva fuente de inmenso valor económico y social. Los avances en la minería (*data mining*) y el análisis de datos, junto con el aumento masivo de la capacidad de procesamiento y almacenamiento de datos, han ampliado la cantidad de información disponible para empresas, gobiernos e individuos. Además, el creciente número de personas, dispositivos y sensores conectados por redes digitales ha revolucionado la capacidad de generar, comunicar, compartir y acceder a los datos.

Los datos generan un valor enorme para la economía mundial, una vez que impulsan la innovación, la productividad, la eficiencia y el crecimiento. A la vez, como señalan Omer Tene y Jules Polonetsky¹⁰, la “avalancha de datos” viene acompañada de preocupaciones sobre la privacidad que pueden provocar una reacción regulatoria (*regulatory backlash*), lo que frenaría la economía de los datos y sofocaría la innovación.

Así pues, resulta evidente que una sociedad digital mundial suscita inquietudes a distintos niveles, especialmente en lo que respecta a la ciberseguridad y al control y regulación del acceso a los datos personales, incluidos los metadatos, es decir, los datos que proporcionan información sobre otros datos. Estas herramientas son indispensables para la comunicación e interacción entre diferentes sistemas de inteligencia artificial, y resultan útiles para describir información de cualquier naturaleza, ya sea médica, literaria o artística.

Este concepto debe distinguirse del de *data lake* (que incluye el *big data*), es decir, colecciones de datos muy diversas procedentes de diferentes fuentes, estructuradas o no estructuradas, que tienden a crecer exponencialmente con el desarrollo de los sistemas digitales. Los metadatos son esenciales en la investigación en medicina y ciencias de la vida, y ya se utilizan habitualmente para proporcionar información detallada de carácter demográfico, como tipos de muestras, métodos de procesamiento, etc. También se utilizan sistemáticamente en la elaboración de formularios de informes de casos (*case*

report forms), una herramienta fundamental para el desarrollo de ensayos clínicos de nuevos fármacos para uso humano.

En este escenario, el marco regulatorio debería implementar progresivamente el concepto de datos FAIR (*FAIR data*), un acrónimo para datos localizables (*findable*), accesibles (*accessible*), interoperables (*interoperable*) y reutilizables (*reusable*). Este concepto se basa en el principio de que los datos y metadatos son activados por los sistemas digitales, una vez que, debido al volumen, a la complejidad y a la velocidad de creación de datos de estos sistemas, progresivamente se confía en ellos para procesar datos. El primer paso consiste en asegurar la ubicación de los datos y metadatos, un componente esencial de la FAIRificación de los datos, que deben ser accesibles para los investigadores y los sistemas informáticos, así como las autorizaciones de acceso correspondientes obtenidas. Esta es una condición esencial para una IA confiable, como sugiere la Comisión Europea¹¹.

Dado que el objetivo de la estrategia FAIR es maximizar la reutilización de datos, la interoperabilidad de datos y sistemas es fundamental para optimizar su análisis, almacenamiento y procesamiento. En medicina e investigación, los datos FAIR no implican necesariamente datos abiertos (*open data*), dada la sensibilidad de los datos de salud. Sin embargo, recurrir a ellos presenta numerosas ventajas, como evitar la duplicación de esfuerzos, reutilizar datos para nuevos fines, lograr el mayor impacto posible con la investigación realizada y contribuir a la replicabilidad y reproducibilidad científica. De este modo, crece la confianza de la sociedad en las nuevas tecnologías¹¹.

Por lo tanto, es necesario identificar los principales problemas éticos relacionados con la recopilación, el almacenamiento, el análisis, la transferencia y la visualización de datos personales¹². Además, si se respeta el “principio de finalidad” en la recopilación de datos, para tranquilizar a la sociedad al respecto, se requiere que el titular realice una acción afirmativa clara que indique una expresión de voluntad libre, específica, informada e inequívoca de que consiente el tratamiento de sus datos, ya sea mediante una declaración escrita, incluso en formato electrónico, o una declaración oral, por ejemplo. Cabe destacar que el recién creado “derecho al olvido” refleja la percepción generalizada de que los sistemas de información no

aseguran eficazmente los derechos de los ciudadanos. Y, como señalan Correia, Rego y Nunes¹³, este derecho debe tenerse en cuenta progresivamente en la formulación de políticas públicas.

En medicina, esta práctica de consentimiento es especialmente relevante y debe ser conocida por los médicos y por otros profesionales de la salud en la investigación con seres humanos¹⁴. El anexo presenta un ejemplo de un documento específico para el consentimiento al tratamiento de datos personales (contenido distinto del consentimiento libre, previo e informado para participar en un estudio/investigación, aunque puede estar incluido en el mismo documento).

El uso generalizado de la IA en la medicina también plantea una cuestión más amplia: la protección de la privacidad individual¹⁵, un concepto que está relacionado con la protección de datos, pero que no se limita a ella. Se considerarán datos personales de salud todos los datos que revelen información sobre la salud física o mental de una persona, incluida la información sobre análisis o exámenes de parte del cuerpo o de sustancias corporales, o datos genéticos y muestras biológicas. Los datos personales incluyen aun cualquier información sobre enfermedad, discapacidad, riesgo de enfermedad, historia clínica, tratamiento clínico o estado fisiológico o biomédico.

Cabe resaltar que la protección de datos incluye los datos genéticos, que, por su propia naturaleza y porque involucran a terceros (miembros de la familia del caso *index*), merecen una protección especial. Los datos genéticos son datos personales relativos a características genéticas, hereditarias o adquiridas, que resulten del análisis de una muestra biológica, en particular del análisis de cromosomas, ácido desoxirribonucleico (ADN) o ácido ribonucleico (ARN), o del análisis de otro elemento que permita obtener información equivalente¹⁶.

Por lo tanto, es fundamental difundir la idea, en la sociedad en general y en la medicina en particular, de que la recogida y el procesamiento de productos biológicos (incluida la información genética) deben estar claramente regulados y supervisados, siempre en el marco de la creación de un biobanco, es decir, un banco de productos biológicos.

El uso de tecnologías que mejoran la privacidad, como el cifrado, los metadatos o la interfaz de usuario, es ahora indispensable ante las nuevas tecnologías de extracción de datos, los escáneres corporales completos, o la secuenciación

de ADN de segunda generación. Siempre que sea posible, los datos de salud individuales deben anonimizarse o pseudonimizarse para proteger la privacidad personal. La aplicación de la pseudonimización a los datos personales puede reducir los riesgos para los titulares de los datos y ayudar a los responsables del tratamiento de datos a cumplir con sus obligaciones de protección, especialmente la obligación de proteger la privacidad individual, un derecho particularmente relevante que tiende a descuidarse en la cultura digital.

En efecto, la privacidad individual es un derecho fundamental que protege uno de los valores más significativos de una sociedad laica y pluralista, ya que tiene como objetivo restringir el acceso no autorizado de terceros —individuos, organizaciones o el propio Estado— a la persona en sus múltiples dimensiones. Reinterpretar, por lo tanto, la opinión de Coolley, citada por Adams, sobre la existencia de un *right to be let alone*, es decir, “el derecho a ser dejado en paz”¹⁷. Esta postura jurisprudencial de finales del siglo XIX pretende afirmar que a la persona humana se le asegura el derecho al anonimato, a ser dejado en paz y a la privacidad de la intimidad individual, en cualquier contexto social, económico, político o psicológico, y que la legislación debe estipular claramente el marco jurídico en el que puede condicionarse la privacidad¹⁸.

La privacidad individual es, en términos formales, un derecho relativamente nuevo, dado que la sociedad, en sus múltiples formas de organización e históricamente sujeta a las más diversas influencias culturales, ha sometido ancestralmente a los seres humanos a designios colectivos y a la satisfacción de las necesidades básicas de supervivencia de la comunidad¹⁹. Sin embargo, las raíces de este derecho pueden radicar en la demarcación, según Aristóteles, entre lo público y lo privado, es decir, la *polis* y el *oikos*.

Desde la perspectiva de Solove²⁰, preservar la privacidad requiere que terceros se abstengan de ciertas actividades que violen el espíritu, la mente, la paz, el espacio físico o el cuerpo humano de una persona. Este derecho se encuentra consolidado en el artículo 12 de la Declaración Universal de los Derechos Humanos, que afirma claramente que *Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección*

de la ley contra tales injerencias o ataques²¹. Gradualmente, el concepto de privacidad se ha asociado con formas más sólidas de soberanía individual, incluyendo las siguientes dimensiones:

- física: derecho a decidir sobre el propio cuerpo;
- mental: derecho a la libertad cognitiva y moral, sin coacción y con libre pensamiento;
- de decisión: el derecho a tomar decisiones sobre uno mismo sin interferencia externa;
- informacional: derecho a mantener la información personal reservada (incluidos los datos personales), que requiere consentimiento para el acceso, uso y almacenamiento de dicha información; el secreto profesional (confidencialidad médica) se deriva de esta dimensión de la privacidad;
- patrimonial: derecho a obtener, mantener y gestionar el patrimonio y la propiedad privada.

De ahí la necesidad de implementar estrategias eficaces de ciberseguridad, es decir, de proteger los sistemas, programas y redes digitales contra ataques e interferencias disruptivas en el espacio digital. La ciberseguridad tiene como objetivo proteger a las personas, las instituciones y las sociedades del acceso, la alteración o la destrucción no autorizados de información privilegiada, y la medicina y la atención sanitaria son áreas particularmente sensibles debido a la naturaleza privada de los datos personales.

Inteligencia artificial y ciberseguridad

Para implementar un programa de ciberseguridad eficaz, es fundamental contar con la participación activa de todas las partes, mediante la implementación de una estrategia adecuada y una coordinación efectiva de los procesos y la tecnología. Por lo tanto, es necesario conocer las potencialidades de la IA para prevenir ciberataques que utilizan tecnologías que atentan contra la privacidad, como la computación omnipresente, el internet de las cosas, los datos satelitales, *blockchain*, las criptomonedas, el aprendizaje automático, la automatización, la tecnología ambiental, la tecnología neurolingüística, la tecnología memética (el estudio formal de los memes), la tecnología de grid, el robo de identidad, la minería de datos, las tarjetas inteligentes, los registradores de pulsaciones de teclas y las redes inalámbricas.

Por lo tanto, deben implementarse medidas de seguridad física y lógica concretas para prevenir los efectos nocivos de los ciberataques o de

fenómenos extremos, como los *black swan events*, o eventos cisne negro. Este término, acuñado por Taleb²², se refiere a fenómenos impredecibles y altamente improbables, pero con un impacto nacional o internacional significativo, que solo se reconocen *a posteriori*. La pandemia de COVID-19 es un ejemplo reciente de un evento cisne negro, y el uso de la IA en las estrategias de ciberseguridad puede ayudar a prevenir, o al menos a mitigar, el impacto devastador de futuras pandemias, no solo en la salud de los pacientes, sino también en el control de cambios radicales en el comportamiento público y las cadenas de suministro.

Dada su importancia estratégica, el sector sanitario es un objetivo prioritario de los ciberataques, especialmente aquellos potenciados por la IA. Por lo tanto, es necesario implementar pruebas de seguridad para proteger eficazmente los datos personales y la privacidad de los pacientes. La ciberseguridad en la salud es especialmente crítica porque los hospitales y centros de salud utilizan habitualmente tecnologías digitales en sus operaciones, como la telemedicina o los historiales clínicos/registros de salud electrónicos, ya sea a nivel de *hardware*, *software*, ya sea en la nube²³.

En las últimas dos décadas, los hospitales de todo el mundo se han convertido en objetivos de ciberataques, incluidos ataques terroristas²⁴, como el ataque al hospital Change Healthcare en los Estados Unidos, en el 2024, o al Hospital Clínic de Barcelona, en el 2023. Por lo tanto, es fundamental desarrollar estrategias preventivas para proteger los datos personales de los pacientes. Desde la perspectiva de Lv y Piccialli²⁵, incluso puede ser necesario recurrir a sistemas matemáticos avanzados, como la tecnología de privacidad diferencial, para proteger la identidad individual y los datos personales de salud.

Además, el hacking, es decir, el acto de identificar y explotar vulnerabilidades en un sistema o red y, posteriormente, obtener acceso no autorizado a datos personales o a información de una organización, es frecuente. Este tipo de acción se lleva a cabo con el objetivo de obtener beneficios económicos (acceso a tarjetas de crédito, por ejemplo), realizar espionaje corporativo o es promovida por un Estado (para obtener información, por ejemplo), y se ve facilitada por la tendencia, a veces por razones de seguridad, de la videovigilancia de espacios públicos o del interior

de organizaciones, incluidos los hospitales, o por la monitorización en línea de diferentes actividades.

Esta tendencia implica la implementación de complejos mecanismos de cifrado, cruciales para proteger la privacidad y la seguridad en línea, y una herramienta de gran interés para proteger derechos fundamentales, como el derecho a la protección de la salud. El cifrado, especialmente cuando se utiliza con inteligencia artificial, asegura que las personas y las organizaciones puedan compartir información de forma segura y libre, sin temor a que el Estado o las organizaciones criminales la hagan pública. Esto incluye información sensible, como la identidad de género, la orientación sexual, el estado de seropositividad para ciertas enfermedades o pronósticos confidenciales, como los relacionados con la oncología, así como información sensible en los sectores de salud privado y público (Sistema Único de Salud o Servicio Nacional de Salud).

El enfoque para abordar la necesidad de implementar estrategias mundiales de ciberseguridad, especialmente para tratar la cuestión de cómo proteger la privacidad individual en la sociedad digital y en el ciberespacio extendido (universal en el sentido literal del término), carece de un marco conceptual adecuado.

Este marco debe realizar la intersección de la seguridad y la privacidad en las dimensiones ontológica, epistemológica, metodológica y bioética, lo cual es especialmente relevante considerando el cambio de paradigma que se evidencia en la actualidad²⁶. De hecho, esta intersección impulsada por la IA representa un verdadero cambio de paradigma, tanto desde una perspectiva científica²⁷ como desde una perspectiva epistemológica²⁸. Por lo tanto, se entiende que la cuestión de la ciberseguridad en la sociedad digital mundial probablemente será uno de los mayores desafíos a los que se enfrentará la comunidad internacional en las próximas décadas. La interacción entre la sociedad digital, la privacidad y la seguridad mundial puede analizarse desde una perspectiva positivista, y este análisis puede desarrollarse aún más examinando este paradigma en dimensiones categóricas previamente seleccionadas.

Desde una perspectiva ontológica, la seguridad es una necesidad objetiva, tanto en términos de bienestar personal como de bienestar comunitario, y reviste una importancia primordial en el orden mundial y en las relaciones entre los diferentes

Estados. La privacidad, por otra parte, es un derecho que surge de la consciencia mundial, acordado mediante el consentimiento mutuo entre las partes y ratificado por métodos aceptables para las instituciones internacionales; es lo opuesto a un derecho entendido como valor social o como interpretación subjetiva del concepto de dignidad humana.

La dimensión epistemológica sitúa la falta de seguridad en perspectiva, como una realidad observable y un hecho innegable, relacionado con la verdad igualmente objetiva de la necesidad de protección. De ahí la referencia actual a una responsabilidad social mundial y colectiva de los diferentes actores sociales en materia de ciberseguridad. En este contexto, la intromisión del Estado y sus agencias, o de empresas multinacionales como la Big-AI (por motivos comerciales, de seguridad, de control social y otros), en la vida privada es una realidad innegable.

Desde un punto de vista metodológico, la evidencia objetiva de fallas de seguridad crea la necesidad de implementar estrategias de ciberseguridad. Partiendo de la hipótesis de que solo una estrategia centrada en la infraestructura organizativa del Estado (o en el nivel de gobernanza supranacional) puede aumentar el nivel de seguridad digital, se puede deducir la necesidad de implementar estrategias integradas de cibergobernanza. De hecho, la reiterada violación de la privacidad individual, un hecho evidente en las brechas de ciberseguridad a diferentes niveles y en contextos muy diversos, plantea la necesidad de un amplio debate nacional e internacional acerca de este tema. En última instancia, será necesario implementar una ciberpolítica genuina a nivel transnacional, incluyendo la participación de las Naciones Unidas u otras organizaciones internacionales en esta regulación.

La bioética que garantiza la seguridad, especialmente en la protección de los datos de salud, es una condición esencial para una relación médico-paciente en la que la confianza sigue siendo un elemento central del universo ético y auténticamente humano de la entrevista clínica. Esta premisa se convierte en un imperativo ético de mayor importancia cuando los médicos se enfrentan a sistemas digitales impulsados por IA que solo controlan parcialmente, dada su falta de comprensión de la tecnología. En efecto, en medicina y ciencias de la salud, la privacidad es un valor bioético y un derecho fundamental en la relación médico-paciente, ya que es un derecho inherente a la persona humana, derivado de su

identidad personal y de la existencia de un refugio final que debe ser protegido de cualquier intrusión externa. La protección de la privacidad es también una piedra angular del deber de confidencialidad médica y de la moral intrínseca de la medicina.

Algunas de las principales preocupaciones de seguridad en la protección de datos son la confidencialidad, para prevenir el acceso no autorizado, evitar *sniffing* (monitoreo ilegal de datos y control de tráfico), limitar el intercambio de credenciales de acceso y promover un mayor control de acceso mediante el cifrado; y la integridad, para prevenir la modificación no autorizada de datos, promover firmas digitales, validación de datos, codificación y métodos de consistencia interna, o evitar fallos en los equipos, ataques o *ransomware*.

Es fundamental predecir este potencial de violaciones de seguridad de datos mejorando su detección y previniendo futuras incidencias. Por una amplia gama de razones, desde garantizar la autenticidad de los datos (algo especialmente importante en sectores como el de la salud, donde circula mucha información sin base científica en internet y en las redes sociales) hasta mantener la integridad de la información (en el sentido de garantizar su almacenamiento sin posibilidad de acceso no autorizado), es importante definir normas claras y políticas internacionales coherentes. La política del mercado único digital en la Unión Europea es un ejemplo concreto de la necesidad de compartir datos entre diferentes Estados, pero también de implementar políticas coherentes y estructuradas en materia de seguridad²⁹.

Existen situaciones que amenazan la seguridad cognitiva y estructural. También existe el riesgo, nada insignificante, de una falla total de las infraestructuras críticas, como sugiere Myriam Dunn: *Las peores consecuencias de los riesgos que generan las tecnologías de la información y comunicación se manifiestan en la posible falla de las denominadas infraestructuras críticas, que son sistemas y activos cuya inoperatividad o destrucción tendría un impacto devastador en la seguridad nacional y en el bienestar económico y social de un Estado. Impulsados por la creciente preocupación por la vulnerabilidad potencial de las sociedades en red, junto con un número creciente de interrupciones en el dominio cibernético, muchos países han tomado medidas para comprender mejor las vulnerabilidades y amenazas a sus infraestructuras (de información) y han propuesto medidas para proteger estos activos*³⁰.

Naturalmente, se trata de un problema mundial, pero también de un motivo de preocupación para cada país. Por lo tanto, se recomienda que cada país proponga e implemente una estrategia nacional de ciberseguridad, pero siempre en coordinación con otros países interesados en implementar dichas políticas. Es un hecho que casi toda la población valora el ciberespacio, implícita o explícitamente, dada su ubicuidad, escala e intangibilidad³¹. Considerando también el nivel de alfabetización digital de las poblaciones como consumidores, incluidos los pacientes, esta acción es de suma importancia³², e incluye la responsabilidad compartida de diferentes *stakeholders*, con el fin de crear un sistema de ciberseguridad complejo e interconectado.

En cualquier caso, dada la falta de instituciones internacionales legitimadas por el orden mundial que regulen eficazmente estas prácticas³³, parece importante seguir promoviendo esta reflexión sobre la base de supuestos teóricos y metodológicos apropiados. Así pues, independientemente de que dicha regulación se lleve a cabo fuera de la soberanía tradicional del Estado o rechazando cualquier excepcionalidad del ciberespacio³⁴, se pueden encontrar soluciones debidamente justificadas que hagan realidad las más altas aspiraciones civilizatorias en este ámbito; por ejemplo, y como mencionamos en otro estudio³⁵, enmarcando la inteligencia artificial confiable dentro del ámbito más amplio de los Objetivos de Desarrollo Sostenible de las Naciones Unidas.

La inteligencia artificial tiene el potencial de revolucionar la ciberseguridad, ya que permite analizar rápidamente grandes cantidades de datos; detectar anomalías y vulnerabilidades del sistema (como estándares de conducta); reaccionar en tiempo real, señalando conductas sospechosas; automatizar procesos repetitivos, dejando a los empleados libres para otras tareas; priorizar riesgos y detectar instantáneamente la posibilidad de *malware* e intrusiones antes de que ocurran; y reducir el error humano.

La ciberseguridad tradicional se fundamenta en el análisis manual, en el que la detección se basa en la firma (*signature-based detection*), uno de los sistemas básicos de detección de seguridad. Este sistema identifica comportamientos maliciosos mediante la búsqueda en una lista de indicadores conocidos y ha demostrado ser razonablemente eficaz contra amenazas conocidas. Sin embargo, no responde a amenazas nuevas o desconocidas.

Las organizaciones cibercriminales ya han invertido mucho en IA para lanzar ciberataques contra organizaciones específicas, y el sector sanitario no es una excepción. A pesar de ello, el potencial de la IA para proteger los sistemas digitales es ilimitado. Gracias a su velocidad, efectividad y eficiencia, aumenta sustancialmente la productividad de los equipos de seguridad, especialmente ante nuevas formas de ciberataque, como el *malware* o los nuevos vectores de *scripting*.

La seguridad de los datos biométricos —datos relacionados con características humanas específicas que permiten identificar a un individuo— también se considera de enorme importancia. Los sistemas y procesos de identificación biométrica se basan en la identificación y comparación de datos físicos o de conducta, llevada a cabo por sistemas digitales complejos, ahora mejorados por la inteligencia artificial. Incluyen el uso de huellas dactilares, reconocimiento facial, datos genéticos, análisis de voz, escaneo del iris o análisis de la palma de la mano. En lo que respecta a la conducta, la identificación biométrica utiliza, por ejemplo, el análisis de la forma de andar de una persona o sus expresiones faciales.

Se utiliza con frecuencia para controlar la asistencia en la gestión organizativa, para supervisar el acceso —con el fin de promover la ciberseguridad y prevenir el acceso no autorizado a ordenadores y otros sistemas digitales— y, por lo general, se utiliza como prueba de identidad personal. En Brasil, la identificación biométrica está fuertemente regulada por la Ley General de Protección de Datos⁵ (LGPD); en Europa, por el Reglamento General de Protección de Datos⁶ y por el AI Act¹⁵, dado el potencial de abuso y violación de derechos fundamentales. Otros países han elaborado iniciativas regulatorias, directrices y leyes que abordan la ética, la transparencia, la seguridad y la responsabilidad en la IA, aunque con enfoques diferentes: leyes vinculantes (Corea del Sur), directrices administrativas (Japón) o legislación específica sobre daños y privacidad (Estados Unidos).

En medicina y ciencias de la vida, la identificación biométrica se utiliza habitualmente en la investigación científica y en la salud pública para el control epidemiológico. Se prevé que, impulsada por la IA, la identificación biométrica no solo

puede garantizar la seguridad de los datos personales, sino también promover una atención médica más precisa y personalizada³⁶.

Consideraciones finales

Este artículo trató de evaluar una de las dimensiones esenciales de la ciberseguridad: el impacto de la IA en la protección de datos personales y la privacidad individual en la medicina y en la sociedad en general. La ciberseguridad de los datos personales podría tener múltiples dimensiones de valor en un futuro próximo. Es decir, es posible evolucionar desde el enfoque positivista para preservar la privacidad personal (y por lo tanto la integridad individual) según la perspectiva tradicional de la relación entre el individuo y la sociedad (por ejemplo, los Estados, el sistema de salud, las grandes empresas farmacéuticas multinacionales) hacia una dinámica distinta en la que la sociedad promueve este tipo de interacción de acuerdo con principios bioéticos universales.

En conclusión, es necesario implementar medidas creativas, utilizando IA, para evaluar el impacto en la privacidad y la protección de datos durante el diseño, desarrollo, adquisición e implementación de sistemas digitales. Exigir estudios o evaluaciones del impacto en la privacidad sería una excelente manera de prevenir fenómenos cibernéticos disruptivos que amenacen la percepción pública de los beneficios de la IA. En cualquier caso, la transición digital y, en particular, la inteligencia artificial deben estar siempre bajo supervisión humana (*human in the loop*), y los valores civilizatorios universalmente compartidos deben tenerse siempre en cuenta durante su aplicación.

La medicina y otras profesiones sanitarias deben comprometerse plenamente durante todo el proceso de implementación de sistemas de IA en la práctica (*physician in the loop*), para asegurar que la tecnología sirva como herramienta de apoyo a la toma de decisiones médicas y no viole los derechos fundamentales de los pacientes. Esto implica que deben implementarse estrategias educativas y de alfabetización digital en la formación médica para que los médicos se integren plenamente en la transición digital como un elemento central.

Referencias

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 [acceso 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 [acceso 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/4wodtnF>
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 – Doctora – asnunes@med.up.pt

 0000-0002-7182-9890

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

 0000-0002-1377-9899

Correspondência

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

Contribución de los autores

Sofia Nunes: conceptualización; investigación; metodología; recursos; supervisión; visualización; redacción - borrador original; redacción - revisión y edición.

Rui Nunes: conceptualización; investigación; metodología; recursos; supervisión; visualización; redacción - borrador original; redacción - revisión y edición.

Disponibilidad de los datos: Todos los datos utilizados o generados en la investigación se describen y presentan íntegramente en el cuerpo del artículo.

Editora responsable: Dilza Teresinha Ambrós Ribeiro

Recibido: 18.5.2025

Revisado: 21.5.2026

Aprobado: 1.6.2026

Anexo

DECLARACIÓN DE CONSENTIMIENTO

(nombre completo), titular de la Cédula de Identidad Nacional/de la Tarjeta de Ciudadano n.º _____, declaro que otorgo a _____ (nombre de la organización), de forma libre e incuestionable, el consentimiento para el procesamiento de mis datos personales que constan en el _____ (nombre del estudio), que se llevará a cabo en _____ (nombre del lugar en el que se realizará el estudio), así como al procesamiento posterior de dichos datos en el ámbito de este propósito. Confirmando que he sido informado(a) de que tengo derecho a solicitar acceso a mis datos personales, a solicitar su rectificación, supresión y portabilidad, y que para cualquier pregunta o queja relacionada con datos personales debo enviar un correo electrónico al Responsable de Protección de Datos de _____ (nombre de la organización), a la dirección de correo electrónico _____, así como que tengo derecho a presentar una queja ante la Autoridad Nacional de Protección de Datos/ Comisión Nacional de Protección de Datos. Confirmando que he leído la Política de Privacidad de _____ (nombre de la organización), que se encuentra en (sitio web).

(lugar), (fecha)

(Firma igual a la del documento de identificación)