

INTELIGÊNCIA ARTIFICIAL EM HOSPITAIS PÚBLICOS: DESAFIOS DA APLICAÇÃO DA LGPD E DA LEI DE ACESSO À INFORMAÇÃO NA GESTÃO DE DADOS SENSÍVEIS

Danillo Henrique Guimarães Souza¹
João Pedro Rodrigues Bragança Machado²
Leonardo Elias de Paiva³

RESUMO

Este trabalho analisa o uso da Inteligência Artificial (IA) em hospitais públicos brasileiros à luz da Lei Geral de Proteção de Dados (LGPD) e da Lei de Acesso à Informação. Destacam-se os desafios éticos e jurídicos no tratamento de dados pessoais e sensíveis, ressaltando o papel da legislação na garantia de segurança, transparência e responsabilização. O estudo também aborda a percepção social sobre a aplicação da IA na saúde pública, considerando riscos como violações de privacidade, consentimento inadequado e ataques cibernéticos, mas reconhecendo benefícios no diagnóstico, na triagem e na gestão hospitalar. Empregou-se uma metodologia de pesquisa bibliográfica com base em artigos científicos analisados qualitativamente, leis e doutrina majoritária. Os resultados indicam que há desafios éticos, jurídicos e sociais na aplicação da IA na saúde pública, com foco na proteção dos dados sensíveis. Conclui-se que a regulamentação dessa ferramenta, em consonância com a legislação brasileira, é essencial para equilibrar inovação tecnológica, eficiência hospitalar e proteção dos direitos fundamentais.

PALAVRAS-CHAVE: Inteligência Artificial; Lei Geral de Proteção de Dados; Lei de Acesso à Informação; Saúde Pública; Dados Sensíveis.

INTRODUÇÃO

A Inteligência Artificial (IA) consolidou-se como uma das maiores transformações tecnológicas do século XXI, influenciando não apenas a vida cotidiana, mas também áreas críticas como a saúde pública. Nos hospitais, a IA tem se mostrado capaz de auxiliar em diagnósticos, triagens e gestão de dados, otimizando processos e ampliando a eficiência dos serviços prestados.

Contudo, o tratamento de informações médicas, classificadas pela Lei Geral de Proteção de Dados (LGPD) como dados sensíveis, levanta debates éticos e jurídicos sobre privacidade, segurança e responsabilidade. Assim, torna-se indispensável analisar o uso da IA nos hospitais públicos à luz da legislação brasileira, ponderando seus benefícios e riscos, bem como os limites necessários para assegurar a proteção da dignidade e dos direitos fundamentais dos pacientes. Portanto, surge o

¹ Acadêmico do Curso de Direito da Faculdade Evangélica Raízes, Anápolis, Goiás, danilohgs25@gmail.

² Acadêmico do Curso de Direito da Faculdade Evangélica Raízes, Anápolis, Goiás, joaopedrobraganca23@gmail.com.

³ Professor Orientador. Mestre em Sociedade, Tecnologia e Meio Ambiente pela Faculdade UniEvangélica. Pós-Graduado em Direito Penal, Direito do Trabalho e Processo do Trabalho pelo Complexo Jurídico Damásio de Jesus, drleonardopaiva@outlook.com.

problema central que orienta esta pesquisa: como assegurar os dados sensíveis diante da crescente utilização de IA em hospitais públicos?

Este trabalho tem como objetivo geral analisar a utilização da IA no gerenciamento de dados pessoais sensíveis em hospitais públicos, considerando as implicações da LGPD e Lei de Acesso à Informação. Como objetivos específicos, busca-se: compreender o conceito de IA, dados pessoais e sensíveis; avaliar seu uso no suporte à gestão hospitalar de dados à luz da legislação brasileira; e entender como a sociedade enxerga o uso dessa ferramenta em hospitais públicos.

Foi adotada a metodologia de pesquisa bibliográfica, baseada na análise de artigos científicos publicados entre 2018 e 2025 nos fóruns e periódicos acadêmicos, compostos por pelo menos um autor com titulação de mestre ou doutor. A seleção do material ocorreu de forma qualitativa, priorizando trechos que contribuíssem para a compreensão, interpretação e aprofundamento do tema. Além disso, foram considerados trechos normativos da legislação vigente relacionada à proteção de dados, a fim de embasar juridicamente a discussão proposta.

A presente pesquisa foi estruturada em três tópicos principais. No primeiro, aborda-se Inteligência Artificial, Dados Pessoais e Sensíveis; no segundo, Uso da Ia nos Hospitais Públicos à Luz da Legislação Brasileira: Lei nº 13.709/18 e Lei nº 12.527/11; e por fim, Visão Social da Aplicação da Ia em Hospitais Públicos. A relevância deste estudo está na expansão da IA na saúde pública e na necessidade de conciliar o avanço tecnológico com a proteção dos direitos fundamentais. A partir disso, pretende-se contribuir com a discussão sobre os desafios e as oportunidades da incorporação ética e legal da IA no setor hospitalar público.

1. INTELIGÊNCIA ARTIFICIAL, DADOS PESSOAIS E SENSÍVEIS

A Inteligência Artificial é uma ferramenta de extrema relevância na atualidade. Muitos apontam para os seus benefícios nas funções diárias, seja no campo pessoal ou empresarial, facilitando e agilizando as tarefas. Por outro lado, destacam seus riscos, uma vez que a IA atua nas interações mais íntimas dos indivíduos, lidando com dados pessoais e sensíveis.

O estudo sobre a IA em hospitais públicos demonstra uma busca pela segurança dos pacientes no gerenciamento de seus dados pessoais e sensíveis à luz da legislação brasileira. Primeiramente é necessário expor o contexto histórico da criação e desenvolvimento dessa ferramenta, juntamente com alguns conceitos à respeito desses dados.

Stuart Russell traz a definição de inteligência artificial (IA) como o estudo dos métodos para fazer computadores se comportar de forma inteligente. Afirmar que, de modo geral, um computador é inteligente na medida em que faz a coisa certa ao invés da coisa errada. Conceitua a “coisa certa” como a ação mais propensa a atingir um objetivo, ou, em termos mais técnicos, a ação que maximiza uma utilidade esperada. Sustenta que a IA inclui tarefas

Ao longo da história, a busca por compreender e reproduzir as capacidades cognitivas humanas por meio de dispositivos artificiais tem fascinado os cientistas. Desde os primeiros questionamentos filosóficos sobre a natureza da inteligência até os avanços tecnológicos mais recentes, a ideia de criar máquinas que simulem aspectos do raciocínio humano tem sido uma constante.

O estudo sobre a IA ganhou força durante a Segunda Guerra Mundial, um período historicamente marcado pela devastação, mas também por expressivos avanços científicos e tecnológicos que redefiniram os rumos da humanidade. Apesar de seu contexto trágico e caótico, esse cenário contribuiu de forma decisiva para o desenvolvimento dessa tecnologia.

No ano de 1943, Warren S. McCulloch e Walter Pitts divulgaram o trabalho intitulado *A Logical Calculus of the Ideas Immanent in Nervous Activity*. Nesse estudo, eles abordaram o conceito de redes compostas por neurônios artificiais, concebidos de forma simplificada, capazes de realizar operações lógicas básicas. Posteriormente, serviu de base para o desenvolvimento das Inteligências Artificiais tradicionais (McCulloch; Pitts, 1943 *apud* Lage, 2022).

Após 1945, o contexto pós-guerra foi marcado pela intensa corrida tecnológica entre as potências globais da época. As pesquisas científicas se intensificaram nesse período, impulsionadas pela rivalidade geopolítica, forçando os países a investirem em tecnologias inovadoras.

O britânico Alan Turing publicou, em 1950, o artigo *Computing Machinery and Intelligence*. Nessa análise, apresentou o teste de Turing com o intuito de investigar se uma máquina poderia demonstrar capacidades cognitivas semelhantes às humanas (Turing, 1950 *apud* Lage, 2022).

Não obstante, é possível perceber que essa complexa ferramenta teve alguns marcos históricos. No entanto, foram nos últimos anos que a IA saltou de maneira significativa, fazendo com que os seres humanos se adequassem, tanto na maneira que a utilizam, quanto na sua regulamentação.

A IA clássica dos anos 1950 difere das técnicas atuais de *machine learning* e *deep learning*, que impõem novos desafios regulatórios. O *machine learning* permite que o computador aprenda sem programação explícita, de forma autônoma. Já o *deep learning*, sua subdivisão, utiliza algoritmos baseados em redes neurais artificiais que simulam o sistema neural biológico (Dourado; Aith, 2022).

Esse termo algoritmos, pode ser entendido como um conjunto finito de instruções para resolver problemas. Tal como uma receita de cozinha orienta o preparo de um prato. Algoritmos podem ser aplicados em cálculos de engenharia, processamento de dados ou planejamento de atividades (Sichman, 2021).

A crescente digitalização de processos e a globalização resultaram em uma produção massiva de dados, alterando profundamente a forma como decisões são tomadas. Nesse cenário, surge a necessidade de compreender e utilizar esses dados de maneira eficiente, o que levou ao desenvolvimento de novas ferramentas analíticas que utilizam esses algoritmos no gerenciamento destes dados massivos.

Estes dados massivos recebem o nome de *big data*, pois envolve o processamento de grandes volumes de dados para identificar padrões e extrair percepções relevantes. Diante da velocidade, diversidade e quantidade de informações geradas, torna-se indispensável adotar metodologias inovadoras, já que abordagens tradicionais não dão conta dessa complexidade (Sarlet; Molinaro, 2019).

É nesse ponto que os dados pessoais e sensíveis devem ser tratados com extrema cautela, pois embora a IA demonstre plena segurança, não é obstante que possa haver um vazamento de dados em eventual ocasião, principalmente em hospitais públicos. Para uma melhor compreensão, é necessário conceituar e diferenciar dados pessoais de dados pessoais sensíveis.

A Lei Geral de Proteção de Dados (LGPD) divide as informações em dados pessoais e dados pessoais sensíveis. Dados pessoais é o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa. E os dados pessoais sensíveis são aqueles que, quando revelados, podem gerar algum tipo de discriminação (LNCC, 2024).

Nesta feita, a LGPD representa a base normativa para interpretação e aplicação ao presente estudo, que se desdobra em demonstrar a importância do tratamento de dados pessoais e sensíveis em hospitais públicos. Em seu artigo 5º é possível entender de forma mais concisa o que eles representam.

Art. 5º, I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável (Nome, CPF, Endereço, e-mail).

Art. 5º, II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Brasil, 2018).

A definição de dado pessoal sensível prevista na LGPD reforça a importância de avaliar com rigor o tratamento de informações em hospitais públicos por intermédio da IA, uma vez que o vazamento desses dados pode resultar em graves violações aos direitos fundamentais do paciente.

Diante do exposto, percebe-se que a proteção dos dados pessoais sensíveis no âmbito hospitalar não se limita a uma exigência legal, mas representa uma garantia essencial dos direitos do usuário. A LGPD, ao estabelecer parâmetros claros para o tratamento dessas informações, busca não apenas prevenir riscos de exposição indevida, mas também fomentar uma cultura de responsabilidade e confiança nessa relação profissional.

Consoante a essa premissa, um dos principais desafios no contexto brasileiro consiste em regulamentar o uso da IA de forma equilibrada, assegurando que sua aplicação não comprometa a agilidade nos atendimentos hospitalares. Ao mesmo tempo, é essencial estabelecer limites claros para que essa tecnologia não ultrapasse as fronteiras éticas em áreas críticas como a saúde.

O Brasil está em fase de debate sobre a regulamentação da inteligência artificial, com o Projeto de Lei nº 2338/2023. As discussões sobre a criação de um marco regulatório começaram em 2020, porém o projeto inicial foi modificado e reapresentado após a atuação de uma comissão de especialistas jurídicos formada em 2022. A proposta brasileira busca combinar elementos das legislações adotadas tanto pela União Europeia quanto pelos Estados Unidos no tratamento e processamento de dados por IA (Castro, 2024 apud Moretti; Zuffo, 2025).

No país, o estímulo ao desenvolvimento da IA ocorre de forma isolada em relação ao campo internacional, pois não há estratégia e tampouco foco em investir em pesquisas e inovações. É um país inerte, infelizmente, na posição de consumo de uma tecnologia que avança de maneira estrondosa (Carvalho, 2021).

Nos hospitais públicos, a utilização da IA em processos de atendimento, triagem e diagnóstico tem se mostrado uma ferramenta valiosa para otimizar e agilizar o trabalho dos profissionais de saúde. Contudo, sob a perspectiva do Direito, essa prática evidencia uma linha tênue entre os benefícios éticos do avanço tecnológico e os riscos de insegurança enfrentados pelo paciente.

2. USO DA IA NOS HOSPITAIS PÚBLICOS À LUZ DA LEGISLAÇÃO BRASILEIRA: LEI Nº 13.709/18 E LEI 12.527/11

A possibilidade de amparo da inteligência artificial pelo direito brasileiro, por meio da LGPD, encontra fundamento tanto em sua estrutura normativa quanto nas demandas contemporâneas da sociedade digital. Embora a LGPD não tenha sido elaborada com foco específico na regulação da IA, seu conteúdo oferece princípios e diretrizes fundamentais que podem ser aplicados ao uso dessas tecnologias, sobretudo quando envolvem o tratamento de dados pessoais sensíveis.

O uso da IA nos hospitais públicos é um assunto delicado, especialmente porque a Lei Geral de Proteção de Dados estabelece regras específicas para o tratamento de dados sensíveis. No Brasil, muitas empresas públicas que prestam serviços hospitalares utilizam essas ferramentas para acelerar o procedimento de atendimento, triagem e até mesmo no diagnóstico dos pacientes.

Em suas múltiplas formas de aplicação, vem atuando como um suporte cognitivo, quase como uma extensão do raciocínio humano no atendimento, diagnóstico de enfermidades, e na prestação de cuidados. Diante desse cenário, torna-se essencial que sua utilização seja constantemente

monitorada e orientada por profissionais humanos, de modo a preservar a integridade dos usuários (Nunes et al., 2022).

Deste modo, é plausível dizer que essa ferramenta, apesar de facilitar e agilizar o trabalho do profissional da saúde, deve ser administrada com extrema responsabilidade. Como já exposto, os dados pessoais sensíveis, se vazados, podem acarretar sérios problemas para a vida do paciente. Portanto, a LGPD, enquanto instrumento normativo de proteção, estabelece em seus dispositivos garantias voltadas à segurança desses dados.

Art. 46. Segurança dos Dados

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (Brasil, 2018).

Ao realizar uma consulta médica de rotina em uma instituição de saúde, tanto o estabelecimento quanto o profissional responsável utilizam um prontuário eletrônico integrado aos diferentes setores e serviços do hospital. Considerando o grande volume de informações coletadas, a instituição tem direcionado investimentos crescentes ao processamento desses dados, visando não apenas otimizar a atuação dos profissionais de saúde, mas também aprimorar a qualidade do atendimento oferecido aos pacientes (Duarte et al., 2023).

Durante a consulta, o médico acessa o prontuário do paciente e verifica a precisão das informações registradas. A partir desse momento, todos os dados passam por análise e processamento, e ao término do atendimento, o profissional realiza observações personalizadas fundamentadas nas recomendações geradas pelos sistemas de inteligência artificial da instituição (Duarte et al., 2023).

Essa análise detalhada dos dados evidencia a importância crítica da precisão das informações processadas pelos sistemas de IA na saúde pública. Diferentemente de outras áreas, na medicina uma recomendação incorreta pode ter consequências gravíssimas. Neste ponto, apesar do art. 20 da LGPD mencionar especificamente sobre o tratamento automatizado dos dados, por conveniência também se desprende a garantia nas decisões médicas automatizadas.

Art. 20. Decisões Automatizadas

O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (Brasil, 2018).

A LGPD resguarda os segredos comerciais e industriais, e essa proteção deve ser levada em conta tanto na regulamentação infralegal quanto na análise de casos concretos. Esse amparo da LGPD pode até fomentar modelos empresariais baseados em algoritmos, mas deve considerar o equilíbrio

com relação ao direito à explicação em decisões automatizadas, de forma a respeitar os princípios éticos no uso da IA, em consonância com os direitos humanos. A própria Lei demonstra essa preocupação ao estipular a realização de auditorias quando houver suspeitas de discriminação (Dourado; Aith, 2022).

Como exposto, a Lei prevê o direito à revisão de decisões automatizadas, o que é particularmente relevante no contexto apresentado, em que algoritmos de IA influenciam ou determinam resultados com impactos significativos para os pacientes. Isso reforça a necessidade de responsabilização, explicabilidade e supervisão humana nas operações que utilizam essas ferramentas. Não obstante, a Lei de Acesso à Informação (Lei nº 12.527/11) garante a proteção e o controle de informações sigilosas, bem como das informações pessoais.

Art. 25. Informações Sigilosas

É dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção.

(...)

Art. 31. Informações Pessoais

O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem;

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem (Brasil, 2011).

Portanto, é dever do Estado controlar e proteger o acesso a informações sigilosas, assegurando que sua utilização ocorra de forma adequada e em conformidade com a legislação. No caso das informações pessoais, além de exigir respeito à intimidade, vida privada, honra, imagem e garantias individuais, a norma impõe limites claros quanto ao tempo de restrição de acesso e às condições de divulgação. Dessa forma, busca-se equilibrar a necessidade de transparência administrativa com a preservação dos direitos fundamentais, evitando abusos, usos indevidos ou violações à dignidade da pessoa humana.

Por conseguinte, a IA na saúde passa de uma ferramenta facilitadora para um problema complexo. Por isso é necessário que os hospitais públicos invistam em sistemas seguros, eficientes e ponderados, haja vista o conflito ético e profissional de um servidor público no manejo dessas ferramentas. Nesta feita, a doutrina pontua três princípios basilares norteadores no procedimento de segurança da informação.

Confidencialidade: Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas a quem é destinada;

Integridade: Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais; Disponibilidade: Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que eles necessitam dela para qualquer finalidade (Sêmola, 2014, p.43 *apud* Vasconcelos; Salib, 2021, p. 9).

Portanto, mesmo que a LGPD não regule diretamente a inteligência artificial expressamente em sua totalidade, ela oferece uma base jurídica importante para mitigar riscos, proteger direitos fundamentais e orientar o desenvolvimento ético da IA no Brasil. A lei estabelece princípios como a finalidade, necessidade, transparência, e segurança no tratamento de dados, que são especialmente relevantes em contextos em que sistemas automatizados tomam decisões baseadas em grandes volumes de informações pessoais (Brasil, 2018).

Art. 6º. Princípios

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (Brasil, 2018).

Um dos princípios mais importantes para o presente estudo é o princípio da transparência. Ele está presente tanto na Carta Magna, quanto nas demais leis, pois é de extrema relevância para o Direito, na medida em que determina que o Estado forneça informações precisas, claras e de forma facilitada a todo cidadão ou pessoa jurídica.

Art. 5º (...)

XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (Brasil, 1988).

Complementando esse dispositivo, a Lei de Acesso à Informação (Lei nº 12.527/2011) detalha condutas ilícitas que podem ensejar responsabilidade dos agentes públicos, como recusar ou atrasar o fornecimento de informações, fornecer dados de forma incorreta, incompleta ou imprecisa, agir com dolo ou má-fé, utilizar indevidamente ou ocultar informações sob sua guarda, impor sigilo para benefício próprio ou de terceiros e destruir documentos relacionados a possíveis violações de direitos humanos.

Lei de Acesso à Informação - Art. 32. Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar:

I - recusar-se a fornecer informação requerida nos termos desta Lei, retardar deliberadamente o seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa;

- II - utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;
- III - agir com dolo ou má-fé na análise das solicitações de acesso à informação;
- IV - divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal;
- V - impor sigilo à informação para obter proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem;
- VI - ocultar da revisão de autoridade superior competente informação sigilosa para beneficiar a si ou a outrem, ou em prejuízo de terceiros; e
- VII - destruir ou subtrair, por qualquer meio, documentos concernentes a possíveis violações de direitos humanos por parte de agentes do Estado (Brasil, 2011).

Assim, a legislação estabelece um conjunto normativo articulado que visa garantir transparência, responsabilização e proteção do interesse público, delimitando claramente os limites e obrigações dos agentes públicos no acesso à informação.

Em contrapartida, a LGPD prevê um conjunto de sanções administrativas relevantes para o caso de descumprimento das suas normas. Assim como os seres humanos se comunicam entre si, as inteligências artificiais também interagem digitalmente, permitindo a troca de informações entre sistemas. No entanto, essa comunicação automatizada pode resultar no compartilhamento inadvertido de dados pessoais, aumentando o risco de vazamentos de informações. Diante desse cenário, a LGPD estabelece medidas punitivas, incluindo advertências, multas, bloqueio ou eliminação de dados, visando assegurar a proteção da privacidade e a responsabilidade no tratamento de informações sensíveis. Conforme prevê a Lei Geral de Proteção de Dados:

- (...) Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
- I - advertência, com indicação de prazo para adoção de medidas corretivas;
 - II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
 - III - multa diária, observado o limite total a que se refere o inciso II;
 - IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
 - V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
 - VI - eliminação dos dados pessoais a que se refere a infração;
 - X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
 - XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (Brasil, 2011).

A LGPD, ao prever sanções no Art. 52, é essencial para o uso da IA em hospitais públicos, pois garante a proteção de dados sensíveis de saúde. As punições previstas funcionam como instrumentos de responsabilização, fortalecendo a confiança social e assegurando que o avanço

tecnológico ocorra em equilíbrio com os direitos fundamentais dos pacientes. No entanto, qual seria a autoridade nacional competente para aplicar essas sanções?

O tratamento de dados pessoais e sensíveis apresenta tamanha complexidade que se fez necessária a instituição de uma autarquia de caráter especial, com autonomia técnica e decisória, patrimônio próprio e sede no Distrito Federal: a Autoridade Nacional de Proteção de Dados (Brandão; Freitas; Dib, 2024).

Art. 55-A. Fica criada a Agência Nacional de Proteção de Dados – ANPD, autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, dotada de autonomia funcional, técnica, decisória, administrativa e financeira, com patrimônio próprio e com sede e foro no Distrito Federal (Brasil, 2018).

As funções da ANPD abrangem diversas atividades, entre as quais destaca: a formulação de políticas públicas e códigos de boas práticas, a proposição de iniciativas legislativas, a definição de padrões técnicos, a elaboração de relatórios anuais, a análise e fiscalização da adequação da proteção no tráfego internacional de dados, além da aplicação de sanções e da defesa dos dados pessoais, tanto por meio de ações coletivas quanto a partir de reclamações individuais (Possi, 2021 *apud* Brandão; Freitas; Dib, 2024).

Como se observou, os dados pessoais e sensíveis dos usuários dos serviços hospitalares públicos encontram-se resguardados e protegidos pela legislação brasileira. Entretanto, mostra-se relevante apresentar a percepção da sociedade sobre a gestão dessas informações quando realizada por meio da Inteligência Artificial.

3. VISÃO SOCIAL DA APLICAÇÃO DA IA EM HOSPITAIS PÚBLICOS

De acordo com a Organização Mundial da Saúde (OMS), a IA vêm transformando a medicina, a pesquisa científica e a saúde pública. Contudo, o ritmo acelerado desse avanço tecnológico desperta preocupações importantes, exigindo a observância de princípios éticos, regulamentações e normas sociais, sobretudo no que se refere ao acesso justo, à proteção da privacidade, à inclusão, à mitigação de preconceitos e à responsabilização. E se tratando de uma questão de alcance global, torna-se indispensável promover um amplo debate sobre a coleta, utilização e compartilhamento de dados vinculados a essas tecnologias, a fim de prevenir impactos mais sérios (Rodrigues, 2020).

Nesse contexto, percebe-se que a discussão sobre diretrizes éticas e sociais defendida pela OMS se relaciona diretamente com os riscos práticos identificados na aplicação da IA na saúde, mais especificamente em hospitais públicos. Questões como privacidade, consentimento e segurança digital deixam de ser apenas preocupações teóricas e passam a representar desafios concretos.

Os principais riscos associados à privacidade e à segurança de dados no uso da IA para a assistência médica envolvem questões como o compartilhamento de informações pessoais sem o devido consentimento informado, a reutilização de dados sem o conhecimento do paciente, além de possíveis violações que podem expor dados sensíveis. Soma-se a isso a ameaça de ataques cibernéticos direcionados a soluções de IA, capazes de provocar danos significativos, e até mesmo fatais, tanto em nível individual quanto público (European Parliamentary Research Service, 2022, *apud* Vieira et al., 2025).

Diante desse cenário, pode-se imaginar o caso de uma paciente submetida a um exame de mama, por exemplo. É inquestionável que os dados obtidos nesse contexto possuem caráter altamente sigiloso e, caso venham a ser expostos, podem acarretar não apenas constrangimento à vítima, mas também sérios impactos psicológicos e emocionais. A gravidade da situação torna-se ainda maior quando envolve pacientes em idade infantil, ampliando os riscos e potenciais traumas decorrentes da violação da privacidade e dignidade da pessoa humana.

Portanto, cabe ao profissional da saúde agir de maneira transparente observando os princípios basilares da relação médico-paciente. Isso implica respeitar a autonomia do paciente, garantir a confidencialidade das informações compartilhadas e assegurar que as decisões clínicas sejam sempre pautadas pela ética e pelo melhor interesse do indivíduo assistido.

Como salientado, em setores como navegação ou entretenimento, erros de IA geram incômodo, mas na saúde pública é a vida do paciente que está em perigo. Por esse motivo, cada nova solução dessa ferramenta aplicada à medicina precisa comprovar a robustez e a confiabilidade de seus algoritmos, de modo a garantir a devida segurança e confiança em sua utilização (Zaparolli, 2022).

Para exemplificar a aceitação da IA por pacientes em diferentes contextos hospitalares, apresenta-se a seguir um estudo com 39 participantes. Foi conduzida por pesquisadores com titulação de mestre e doutor: Evelise S. Duarte, Fagner Sutel de Moura, Leonardo Pestillo de Oliveira e Lucas França Garcia, em um artigo acadêmico intitulado *Aspectos bioéticos da utilização de sistemas de inteligência artificial no campo da saúde: um estudo exploratório*, 2023. A seguir, apresenta-se um trecho adaptado do experimento.

No cenário 1, a pesquisa investigou a percepção dos participantes sobre o uso de sistemas de IA em consultas médicas de rotina. Os resultados indicaram que a maior preocupação estava com a privacidade e confidencialidade dos dados (92,3%), seguida pela responsabilidade profissional e institucional (71,8%) e pelo consentimento informado (66,7%).

No cenário 2, a pesquisa avaliou a percepção dos participantes sobre o uso de sistemas de IA em dispositivos inteligentes de monitoramento (ex: smartphones ou relógios). As principais preocupações foram a privacidade e confidencialidade dos dados (76,9%), seguidas pelo consentimento informado na coleta desses dados (66,7%) e pela responsabilidade pelas recomendações geradas pelos aplicativos (48,7%).

No cenário 3, a pesquisa investigou a percepção dos participantes sobre o uso de sistemas de IA no processamento e interpretação de exames laboratoriais e imagem. As maiores preocupações foram responsabilidade e confiança (79,5% cada), seguidas por riscos associados à atividade e pela privacidade e confidencialidade dos dados processados pelos sistemas de IA (33,3% cada).

No cenário 4, a pesquisa analisou a percepção dos participantes sobre o uso de sistemas de IA na interpretação de exames quando surgem achados secundários, com ou sem significado clínico (ex: tumor benigno ou maligno). As principais preocupações foram a confiança nos resultados (84,6%), seguida da responsabilidade associada a esses achados (74,4%) culminados à privacidade e confidencialidade dos dados (Duarte et al., 2023, p. 270).

Os participantes da pesquisa demonstraram compreender o funcionamento dos sistemas de IA e suas principais aplicações, reconhecendo ainda que seu uso pode modificar a relação médico-paciente e ampliar a análise especializada das condições clínicas. Mas no campo ético, destacaram preocupações com a privacidade, confidencialidade dos dados, o processo de consentimento informado e a definição de responsabilidades no uso da IA, especialmente em consultas de rotina, aplicativos de dispositivos inteligentes e no processamento de exames laboratoriais e de imagem (Duarte et al., 2023).

De maneira geral, os quatro cenários analisados evidenciam que, embora os participantes reconheçam o potencial dessa ferramenta em diferentes contextos da saúde, ainda prevalecem algumas preocupações. Esses achados revelam que a aceitação da IA no ambiente médico-hospitalar depende não apenas de sua eficiência técnica, mas também da garantia de segurança, transparência e responsabilização no uso dos dados dos pacientes.

Para prevenir questões éticas relacionadas ao uso da inteligência artificial na área médica, é fundamental definir diretrizes firmes e bem estruturadas que assegurem a transparência e a confiança nas decisões apoiadas por IA. O ponto central dessa estratégia é deixar claro qual é a função desses sistemas inteligentes no processo de decisão clínica (Amaro; Nakaya; Rizzo, 2024).

Além da Lei Geral de Proteção de Dados e da Lei de Acesso à Informação, é visível a preocupação do corpo legislativo em desenvolver outra norma que aborde esse tema especificamente, como o projeto de lei mencionado no início. Dessa forma, seria possível impor um limite para o uso da IA, contudo, vale ressaltar que esse limite não pode prejudicar o desenvolvimento tecnológico, bem como o amparo da privacidade dos pacientes.

CONCLUSÃO

O presente trabalho demonstrou que a Inteligência Artificial, ao mesmo tempo em que se apresenta como uma ferramenta estratégica para a modernização da saúde pública, suscita desafios éticos, jurídicos e sociais de grande relevância. A utilização da IA em hospitais públicos possibilita avanços significativos na gestão hospitalar, no diagnóstico clínico e na otimização dos atendimentos,

contribuindo para a eficiência dos serviços prestados. Contudo, tais benefícios devem ser cuidadosamente ponderados diante dos riscos relacionados ao tratamento de dados pessoais e sensíveis, cuja proteção constitui direito fundamental assegurado pela Constituição Federal e regulamentado pela Lei Geral de Proteção de Dados (LGPD).

Verificou-se que a LGPD, embora não tenha sido criada especificamente para disciplinar a inteligência artificial, fornece bases normativas sólidas para mitigar riscos e orientar seu uso em conformidade com os princípios da finalidade, necessidade, transparência e segurança. A articulação da LGPD com a Lei de Acesso à Informação também revela a preocupação do ordenamento jurídico em equilibrar a proteção da privacidade com a garantia de transparência administrativa. Nesse cenário, destaca-se o papel da Autoridade Nacional de Proteção de Dados (ANPD), responsável pela regulamentação, fiscalização e aplicação de sanções em casos de descumprimento das normas.

A análise evidenciou ainda que a visão social acerca da aplicação da IA em hospitais públicos está marcada por preocupações quanto à privacidade, ao consentimento informado, à responsabilidade profissional e à confiabilidade dos sistemas. Os estudos revisados indicam que a aceitação da tecnologia depende diretamente da capacidade de assegurar segurança, transparência e explicabilidade no tratamento dos dados, de modo a não fragilizar a relação médico-paciente nem comprometer a dignidade humana.

Por fim, conclui-se que o avanço da Inteligência Artificial na saúde pública brasileira deve caminhar de forma paralela à criação de um marco regulatório específico, capaz de conciliar inovação tecnológica e respeito aos direitos fundamentais. É imprescindível que o Estado, as instituições hospitalares e a sociedade civil atuem conjuntamente para construir diretrizes éticas e jurídicas claras, que garantam a utilização responsável e segura da IA. Dessa forma, será possível potencializar seus benefícios sem abrir margem para violações de direitos, consolidando um uso justo, eficiente e humanizado dessa tecnologia no âmbito hospitalar.

ARTIFICIAL INTELLIGENCE IN PUBLIC HOSPITALS: CHALLENGES IN APPLYING THE GENERAL DATA PROTECTION LAW AND THE ACCESS TO INFORMATION LAW IN THE MANAGEMENT OF SENSITIVE DATA

ABSTRACT

This study analyzes the use of Artificial Intelligence (AI) in Brazilian public hospitals in light of the General Data Protection Law (LGPD) and the Access to Information Law. It highlights the ethical and legal challenges involved in processing personal and sensitive data, emphasizing the role of legislation in ensuring security, transparency, and accountability. The research also examines the social perception of AI implementation in public healthcare, considering risks such as privacy

violations, inadequate consent, and cyberattacks, while acknowledging its benefits in diagnosis, triage, and hospital management. A bibliographical research methodology was employed, based on qualitative analysis of scientific articles, legislation, and major legal doctrines. The results indicate that ethical, legal, and social challenges persist in the application of AI in public health, particularly regarding the protection of sensitive data. It is concluded that regulating this technology in accordance with Brazilian law is essential to balance technological innovation, hospital efficiency, and the protection of fundamental rights.

KEYWORDS: Artificial Intelligence; General Data Protection Law; Access to Information Law; Public Health; Sensitive Data.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [s.d.]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 de abril de 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 12 de abril de 2025.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. **Lei de Acesso à Informação**. Brasília, DF: Presidente da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 10 de setembro de 2025.

BRANDÃO, Sonia Darque do Nascimento; FREITAS, João Paulo Bezerra de; DIB, Rebeca Dantas. Regulação de dados pessoais na era digital e os desafios no setor público de saúde. **Revista Delos**, Curitiba, v.17, n.62, p. 01-23, 2024. Disponível em: <https://ojs.revistadelos.com/ojs/index.php/delos/article/view/3203>. Acesso em: 12 de abril de 2025.

CARVALHO, André Carlos Ponce de Leon Ferreira. Inteligência Artificial: riscos, benefícios e uso responsável. **Estudos Avançados**, São Paulo, v.35, n. 101, p. 21-35, 2021. Disponível em: <https://doi.org/10.1590/s01034014.2021.35101.003>. Acesso em: 12 de abril de 2025.

DUARTE, Evelise Scaraboto; MOURA, Fagner Sutel de; OLIVEIRA, Leonardo Pestillo de; GARCIA, Lucas França. Aspectos bioéticos del uso de sistemas de inteligencia artificial en el campo de la salud: un estudio exploratorio. **Revista de Bioética y Derecho**, [S. l.], n. 57, p. 263–285, 2023. Disponível em: <https://revistes.ub.edu/index.php/RBD/article/view/35146>. Acesso em: 11 agosto de 2025.

DOURADO, Daniel de Araujo; AITH, Fernando Mussa Abujamra. A regulação da inteligência artificial na saúde no Brasil começa com a Lei Geral de Proteção de Dados Pessoais. **Revista de Saúde Pública**, São Paulo, v. 56, p. 56-80, 2022. Disponível em: <https://doi.org/10.11606/s15188787.2022056004461>. Acesso em: 12 de abril de 2025.

LAGE, Fernanda de Carvalho. Manual de Inteligência artificial no Direito Brasileiro. 2 ed, São Paulo: JusPodvum, 2022. Disponível em: https://juspodivmdigital.com.br/cdn/arquivos/jus2235_previa-do-livro.pdf. Acesso em: 04 de junho de 2025.

LNCC, Laboratório Nacional de Computação Científica. Qual a diferença entre dados pessoais e sensíveis?. **Ministério da Ciência, Tecnologia e Inovações**, 2024. Disponível em: <https://www.gov.br/lbcc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/campanha-lgpd/2024/qual-a-diferenca-entre-dados-pessoais-e-dados-sensiveis>. Acesso em: 10 de setembro de 2025.

MORETTI, Juliano Lazzarini; ZUFFO, Milena Maltese. LGPD e inteligência artificial: um estudo comparado. **Direito Internacional e Globalização Econômica**, São Paulo, v. 13, n. 13, p. 21-42, 2025. Disponível em: <https://revistas.pucsp.br/index.php/DIGE/article/view/69370>. Acesso em: 12 de abril de 2025.

NUNES, Heloá da Conceição; GUIMARÃES, Rita Miranda Coessens; DADALTO, Luciana. Desafios bioéticos do uso da inteligência artificial em hospitais. **Revista Bioética**, Brasília, v. 30, n. 01, p. 82-93, 2022. Disponível em: https://revistabioetica.cfm.org.br/revista_bioetica/article/view/2644. Acesso em: 12 de abril de 2025.

RODRIGUES, Paula Marques. A Inteligência Artificial Médica e o uso de dados pessoais no atendimento aos pacientes. **Migalhas**, 2020. Disponível em: <https://www.migalhas.com.br/depeso/325245/a-inteligencia-artificial-medica-e-o-uso-de-dados-pessoais-no-atendimento-aos-pacientes>. Acesso em: 18 de agosto de 2025.

SARLET, Gabrielle Bezerra Sales; MOLINARO, Carlos Alberto. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 13, n. 41, p. 183-212, 2020. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/811>. Acesso em: 12 de abril de 2025.

SICHMAN, Jaime Simão. Inteligência Artificial e Sociedade: avanços e riscos. **Estudos Avançados**, São Paulo, v. 35, n. 101, p. 37-50, 2021. Disponível em: <https://www.scielo.br/j/ea/a/c4sqqrthGMS3ngdBhGWtKhh>. Acesso em: 5 de junho de 2025.

VIEIRA, Elba Lúcia de Carvalho; SANTANA, Gustavo Alpoim de; MELLO, Ricardo Coutinho; MIRANDA, Zeny Duarte de. Privacidade na coleta de dados pessoais sensíveis de pacientes: uma análise do uso da inteligência artificial na saúde pública. **Revista Fontes Documentais**, [S. l.], v. 7, n. Edição especial, p. e722414, 2025. Disponível em: <https://periodicos.ufba.br/index.php/RFD/article/view/66395>. Acesso em: 15 agosto de 2025.

VASCONCELOS, Charles Rogério; SALIB, Marta Luiza Leszczynski. Lei Geral De Proteção De Dados Pessoais: Desafios e impactos para o Poder Público. **TCE-RO**. p.1-25, 2021. Disponível em: https://lgpd.tcero.tc.br/wp-content/uploads/2021/07/TCC-Charles-Roge%CC%81rio-Vasconcelos_TCE-RO.pdf. Acesso em: 17 de setembro de 2025.

ZAPAROLLI, Domingos. A Inteligência Artificial chega à Saúde. **PesquisaFapesp**, 2022. Disponível em: <https://revistapesquisa.fapesp.br/a-inteligencia-artificial-chega-a-saude/>. Acesso em: 18 de agosto de 2025.