PRIVACIDADE NA COLETA DE DADOS PESSOAIS SENSÍVEIS DE PACIENTES: UMA ANÁLISE DO USO DA INTELIGÊNCIA ARTIFICIAL NA SAÚDE PÚBLICA

Elba Lúcia de Carvalho Vieira, Gustavo Alpoim de Santana, Ricardo Coutinho Mello e Zeny Duarte de Miranda

Resumo

A rápida expansão do uso da inteligência artificial tem trazido avanços em diversos aspectos da vida moderna. No entanto, é essencial considerar implicações relacionadas à privacidade dos dados pessoais de saúde. Este artigo visa abordar estas preocupações e analisar o atual cenário de uso da inteligência artificial na saúde pública brasileira. São discutidos impactos e desafios decorrentes dessa abordagem com base nas regulamentações existentes, como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. A coleta de dados pessoais sensíveis é uma prática comum na área da saúde, com o objetivo de melhorar a prestação de serviços e promover a saúde da população. Porém, o uso da inteligência artificial levanta preocupações, sendo necessário preservar a privacidade dos seus titulares em consonância com a LGPD. Anonimização de dados pessoais sensíveis, consentimento informado dos pacientes e proteção dos dados são alguns desafios. A utilização da inteligência artificial na saúde pública requer o armazenamento e o processamento de grandes quantidades de dados. É essencial, portanto, implementar medidas de segurança robustas para proteger esses dados contra acesso não autorizado, violações e ataques cibernéticos. Torna-se premente, portanto, a implementação de medidas que assegurem não somente proteção ao compartilhamento indevido, como também ao acesso não autorizado. A pesquisa foi conduzida por meio de revisão sistemática de literatura, abrangendo artigos científicos, relatórios governamentais e regulamentações relacionadas à privacidade e proteção de dados. A revisão inclui estudos publicados nos últimos cinco anos, com foco em abordagens de inteligência artificial e suas implicações para a privacidade dos pacientes. Os resultados indicam que a coleta de dados pessoais sensíveis de saúde é uma prática comum. No entanto, o uso da inteligência artificial requer acesso a dados dos pacientes, como histórico médico, resultados de exames, informações sobre doenças, entre outros, e isso levanta preocupações sobre a privacidade. As instituições governamentais têm o dever de criar políticas públicas e fornecer os investimentos necessários para que a inteligência artificial melhore o processo de tomada de decisões em benefício da população. As instituições de saúde pública têm o desafio de implementar políticas, procedimentos e medidas técnicas, visando a privacidade na coleta e armazenamento de dados pessoais sensíveis, especialmente, no que se refere à anonimização, consentimento e proteção dos dados.

Palavras-Chave: privacidade; saúde pública; inteligência artificial; dados pessoais sensíveis.

Introdução

O progresso tecnológico das últimas décadas tem provocado mudanças marcantes na maneira como conduzimos nossas vidas, nos comunicamos, adquirimos conhecimento e suprimos um crescente volume de requisitos e carências da vida em coletividade. Evidente nesse cenário é o advento de um mundo cada vez mais hiperconectado, saturado de plataformas digitais, que conferiu aos dados o papel central na configuração daquilo que é conhecido como sociedade digital.

> 'Vivemos hoje em um mundo de dados, gerados e tratados de forma intensa por humanos e máquinas sem haver por vezes uma tutela jurídica adequada do cidadão para garantir a segurança e o sigilo de suas informações ou para coibir abusos com relação ao tratamento dos seus dados pessoais". (Magrani 2019, p. 263)

Diante dessa conjuntura, emerge a percepção de que a inovação tecnológica e o consumo massivo de dados pessoais no ambiente online traz reflexões relevantes acerca de nossos padrões de conduta no contexto digital. Além disso, esse panorama traz desafios substanciais às organizações no que diz respeito à gestão dos dados pessoais sob sua tutela, particularmente diante das imposições regulatórias voltadas à preservação da privacidade e da proteção dos dados pessoais. Invariavelmente, passamos a conviver sob a ótica dos dados digitais. Nossas vidas traduzidas em dados digitais vão, aos poucos, sendo compiladas, armazenadas e processadas em grandes bases de dados de milhares de empresas ao redor do mundo, coletando dados pessoais para fornecimento de produtos e serviços direcionados ao consumidor.

Na perspectiva de um mundo guiado por dados, há reflexões relevantes a analisar, quanto aos desafios diante do crescente uso da Inteligência Artificial[1] (IA), associada à responsabilidade das organizações em proteger dados pessoais. Esta é uma questão primordial para que seja possível assegurar a privacidade dos indivíduos, considerando que "a privacidade é um direito humano, é um direito constitucional brasileiro e um direito humano digital, já que marcos regulatórios assim a consideram também na vida digital" (Vieira, 2019, p. 212).

> "Às novas formas de coleta e tratamento de informações, possibilitadas sobretudo pelo recurso a computadores, adicione-se a crescente necessidade de dados por parte das instituições públicas e privadas: como não é imaginável uma ação que vá de encontro a esta tendência, comum a todas as organizações sociais modernas, é necessário considerar de forma realista tal situação, analisando as transformações que causa na distribuição e no uso do poder pelas estruturas públicas e privadas." (Rodotà, 2008, p. 24)

O tratamento de dados pessoais sensíveis é um desafio para empresas, à luz da Lei Geral de Proteção de Dados Pessoais. Acrescente-se a isso, o uso, cada vez mais intenso, da Inteligência Artificial. Neste aspecto, a proteção de dados é um dos principais pilares, apesar de não ser o único, para se pensar no uso massivo da IA, principalmente no Brasil, ainda desprovido de uma regulamentação[2] verse sobre o tema.

---

[1] Possibilidade de emular, nas máquinas, a capacidade humana de tomar decisões, algo pensado desde a década de 50.

[2] Está em trâmite, no Brasil, o Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233

> "O pilar fundamental da transformação digital é o conjunto de tecnologias avançadas, que incluem inteligência artificial, robôs, big data, realidade aumentada, internet das coisas e redes, que são os vetores que interligam praticamente tudo: sociedade, empresas e governos. Os potenciais benefícios das tecnologias digitais são múltiplos. Elas podem trazer inovação, eficiência, competitividade e redução de custos para a sociedade e a economia. Podem também tornar os serviços públicos mais transparentes, disponíveis e eficientes". (Gaetani e Almeida, 2023)

A sociedade digital caminha, a passos largos, no uso cada vez mais intenso de plataformas tecnológicas complexas com uso da IA, fazendo com que nossos rastros digitais sejam manipulados por uma indústria milionária de empresas de tecnologia, onde nossas interações digitais são coletadas em tempo real e correlacionadas à nossa identidade, é relevante o debate sobre a IA, junto à privacidade e proteção de dados. Igualmente importante são os desafios para as organizações, quanto às necessidades de proteção adequada aos dados pessoais, respeitando, no mundo real e no digital, a privacidade dos indivíduos.

TECNOLOGIAS DIGITAIS: CENÁRIO ATUAL NO BRASIL E NO MUNDO

Na era da sociedade digital, marcada pelo domínio online, dados pessoais são constantemente coletados, processados, armazenados, modificados, transmitidos e submetidos a uma variedade de outros processos de tratamento por organizações distribuídas em diversas regiões do globo.

Com o aumento de regulamentações relacionadas à privacidade e proteção de dados, a exemplo do "General Data Protection Regulation" (GDPR) que é a regulamentação de proteção de dados da União Europeia e também da "Lei Geral de Proteção de Dados Pessoais", a LGPD, aqui no Brasil, os desafios para proteção de dados pessoais aumentaram.

Isso ocorre em função das exigências legais que essas regulamentações estabelecem às organizações, principalmente na aplicação de medidas técnicas e administrativas de segurança, objetivando a adequação mínima e necessária nos cuidados e na preservação da privacidade dos indivíduos.

A LGPD surgiu como um impulso para o fortalecimento do tema da privacidade e proteção de dados no Brasil. O aumento de casos relativos ao vazamento de dados pessoais e de ataques cibernéticos constantes corroboraram com a evolução de legislações no mundo. Magrani (2019, p. 91) reforça que "o impulsionamento para uma maior proteção da privacidade, sobretudo no cenário online, adveio de acontecimentos relativos a vazamentos de informações e à edição de leis gerais para proteção de dados em países estrangeiros."

Com o propósito de aprofundar a análise, depara-se com a crescente adoção da Inteligência Artificial (IA), por meio dos serviços oferecidos por empresas já presentes no ambiente virtual global. Essas empresas, constantemente, coletam e processam dados pessoais, os quais serão empregados posteriormente. Esta forma de IA, que exerce uma certa influência sobre as vidas das pessoas, é constituída por algoritmos[3].

Na área de saúde também é crescente a preocupação com os riscos associados ao uso indevido de dados. Nessa direção, o Relatório Artificial Inteligence in Healthcare (European Parliamentary

[3] Em matemática e ciência da computação, um algoritmo é uma sequência finita de ações executáveis que visam obter uma solução para um determinado tipo de problema. (Silva, 2023)

Research Service, 2022) também adverte para sete principais riscos na utilização de IA na área de saúde: dano ao paciente devido a erros de IA; uso indevido de ferramentas médicas de IA; vieses na implementação de ferramentas de IA e perpetuação de desigualdades; falta de transparência; **questões de privacidade e segurança** (grifo nosso); lacunas na prestação de contas e obstáculos para a devida implementação.

Nesse contexto, compreender e realizar uma análise crítica dos desafios concernentes à salvaguarda de dados pessoais é imperativo, incluindo dados pessoais sensíveis, no cenário do crescente emprego da Inteligência Artificial.

A coleta de dados pessoais sensíveis é uma prática disseminada no campo da saúde, visto que a Inteligência Artificial demanda a coleta, o armazenamento e processamento de grandes bases de dados, surgem inquietações acerca da preservação da privacidade dos titulares desses dados à luz das diretrizes da LGPD.

No âmbito da Inteligência Artificial (IA), essa dinâmica se mantém, mas com particularidades. A rápida progressão dessa tecnologia, resultado de investimentos substanciais de gigantes do setor tecnológico, revela um avanço notável na criação de plataformas impulsionadas por IA. A Inteligência Artificial traz novas discussões, necessitando de diálogos e estudos significativos para sua regulação, minimizando riscos do uso inapropriado dos dados no mundo digital. A era impulsionada por dados digitais estabelece um patamar de risco renovado, especialmente quando se considera a possibilidade de má utilização desses dados, o que compromete a salvaguarda do direito à privacidade das pessoas.

Organizações internacionais têm externado suas preocupações quanto aos riscos no uso da IA à privacidade. O desafio em implementar políticas, normas, procedimentos e medidas técnicas é crescente, tornando-se cada dia mais complexo, ante o surgimento de novas tecnologias, a exemplo da IA.

> "Os principais riscos para privacidade e segurança de dados em IA para assistência médica, incluindo compartilhamento de dados pessoais sem total consentimento informado, reaproveitamento de dados sem o conhecimento do paciente, violações de dados que podem expor informações confidenciais ou pessoais e o risco de danos - ou mesmo potencialmente fatais - ataques cibernéticos a soluções de IA, tanto em nível individual quanto hospitalar ou do sistema de saúde." (European Parliamentary Research Service, 2022, p. 2)

A Organização Mundial de Saúde[4] alerta que "[...] salvaguardar e proteger a privacidade individual não é apenas reconhecido como um requisito legal em muitos países, mas também é importante para permitir que as pessoas controlem informações confidenciais sobre si mesmas e a autodeterminação (respeito por sua autonomia) e para evitar danos". E segue expondo que "As organizações de direitos humanos têm interpretado e, quando necessário, adaptado direitos humanos existentes leis de direitos e padrões para avaliação de IA e estão revisando-os diante de os desafios e oportunidades associados à IA".

No Brasil, a adoção da IA no Sistema Único de Saúde (SUS) ainda é incipiente, todavia a o Ministério da Saúde está estudando formas de incorporar Inteligência Artificial (IA) a serviços públicos de saúde.

[4] World Health Organization (WHO). Ethics and governance of artificial intelligence for health. Disponível em: https://www.who.int/publications/i/item/9789240029200

A Lei Geral de Proteção de Dados Pessoais – LGPD – emerge como uma legislação que alarga o escopo da discussão acerca da manipulação de informações pessoais no Brasil.

Dados pessoais sensíveis e LEIS de privacidade e proteção de dados

A Lei Geral de Proteção de Dados Pessoais[5] (LGPD - Lei 13.709/18), no Brasil, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Além disso, a lei reconhece a promoção dos direitos humanos fundamentais, quando inclui o respeito à privacidade como um dos fundamentos da disciplina de proteção de dados pessoais[6], em consonância com a Declaração Universal de Direitos Humanos[7] (DUDH), a qual reforça o respeito à privacidade, quando ressalta que "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

Importante observar que a LGPD reforça, como um de seus princípios[8], o da não-discriminação, na hipótese da realização do tratamento de dados pessoais realizado por agente de tratamento, em que deve haver a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Este princípio denota a relevância adotada aos dados pessoais sensíveis, os quais devem ser respeitados e tratados adequadamente, através daqueles agentes de tratamento que coletam, usam, processam, armazenam ou realizam alguma outra atividade para fins justificados de suas atribuições, tal qual sustentado por Mulholland (2018, p.164), citando que "em relação ao princípio da não discriminação, fica vedada a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos. O legislador, ao relacionar o uso discriminatório às qualidades de ilicitude e abusividade, parece reconhecer a possibilidade de tratamento distintivo, desde que lícito e não abusivo".

Para fins conceituais e comparativos (Tabela 1), apresenta o que dizem as principais leis de privacidade e proteção de dados de alguns países, incluindo o Brasil, a respeito de dados pessoais sensíveis.

[5] Artigo 1º da Lei 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[6] Artigo 2º da Lei 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[7] ONU. Declaração Universal dos Direitos do Homem. Organização das Nações Unidas, 10.12.1948. Disponível em: https://nacoesunidas.org/

[8] Artigo 6º da Lei 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Tabela 1.

Dados pessoais sensíveis – definições comparadas

PAÍS	NOME DA LEI OU REGULAMENTO (ou similar)	CITADO EM	ANO	DESCRIÇÃO DE DADO PESSOAL SENSÍVEL
BRASIL	Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709)	Artigo 5o.	2018	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
UNIÃO EUROPEIA	General Data Protecting Regulation – GDPR	Considerandos 51 a 56	2016	Dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; Filiação sindical; Dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano; Dados relacionados com a saúde; Dados relativos à vida sexual ou orientação sexual da pessoa.
INGLATERRA	UK General Data Protecting Regulation - UK GDPR	Considerandos 51 a 56		Dados pessoais revelando origem racial ou étnica; Dados pessoais revelando opiniões políticas; Dados pessoais revelando crenças religiosas ou filosóficas; Dados pessoais revelando a filiação sindical; Dados genéticos; Dados biométricos (quando usados para fins de identificação); Dados relativos à saúde; Dados relativos à vida sexual de uma pessoa; e Dados sobre a orientação sexual de uma pessoa.
AUSTRÁLIA	The Privacy Act	Parte II - Interpretação Divisão 1 - Definições Gerais	1988	a) Informações ou uma opinião sobre um indivíduo: (i) origem racial ou étnica; ou (ii) opiniões políticas; ou (iii) filiação em associação política; ou (iv) crenças ou afiliações religiosas; ou (v) crenças filosóficas; ou (vi) associação a uma associação profissional ou comercial; ou (vii) filiação a um sindicato; ou (viii) orientação ou práticas sexuais; ou (ix) antecedentes criminais; isso também é informação pessoal; ou b) Informações de saúde sobre um indivíduo; ou c) Informações genéticas sobre um indivíduo que não sejam informações de saúde; ou d) Informações biométricas a serem usadas para fins de verificação biométrica automatizada ou identificação biométrica; ou e) Modelos biométricos.
JAPÃO	Act on the Protection of Personal Information	Artigo 2o.	2003	Informações pessoais de uma pessoa identificável quanto à raça, credo, condição social, histórico médico, antecedentes criminais, fato de ter sofrido dano por um crime, ou outros identificadores de seus equivalentes prescritos por Ordem do Gabinete como aqueles que requerem cuidados especiais para não causar discriminação injusta, preconceito ou outras desvantagens a essa
URUGUAI	Ley de Protección de Datos Personales	Artigo 4o.	2008	Dados pessoais que revelem origem racial e étnica, preferências políticas, convicções religiosas ou morais, afiliação sindical e informações relativas à saúde ou a vida sexual.
MÉXICO	Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Artigo 3o.	2010	Aqueles dados pessoais que afetem a esfera mais íntima de seu titular, ou cujo uso indevido possa dar origem a discriminação ou acarretar um risco grave para o mesmo. Em particular, são considerados sensíveis aqueles que possam revelar aspectos como origem racial ou étnica, estado de saúde presente e futuro, informação genética, crenças religiosas, filosóficas e morais, filiação sindical, opiniões políticas, preferência sexual.
COLÔMBIA	LEY ESTATUTARIA 1581	Artigo 5o.	2012	Aqueles que afetem a privacidade do Titular ou cujo uso indevido possa gerar discriminação, como os que revelem origem racial ou étnica, orientação política, convicções religiosas ou filosóficas, filiação a sindicatos, organizações sociais, direitos humanos ou que promovam os interesses de qualquer partido político ou que garantam os direitos e garantias dos partidos políticos da oposição, bem como dados relativos à saúde, vida sexual e dados biométricos

Elaborado pelos autores (com base nas leis e regulamentações de privacidade e proteção de dados de cada país – tradução nossa)

Diante do exposto, é evidente que as legislações mencionadas revelam uma inquietação em distinguir entre os conceitos de dados pessoais sensíveis (em contraposição aqueles reconhecidos meramente como dados pessoais). Isso se dá devido à possível manifestação de efeitos discriminatórios e prejudiciais aos titulares desses dados, decorrentes do manuseio impróprio ou inadequado, especialmente quando associados à identidade de indivíduos.

> "O conceito de dados sensíveis deve ser funcionalizado de acordo com o tratamento que é concedido a eles. Significa sustentar que dados sensíveis são qualificados como tais não só por conta de sua natureza intrinsecamente personalíssima, de forma apriorística, mas devido ao uso e finalidade que é concedido a esse dado por meio de um tratamento que pode gerar uma potencialidade discriminatória abusiva". (Mulholland, 2021, p.3)

Além disso, importante observar que dados de saúde (que são dados pessoais sensíveis) são caracterizados pelo GDPR[9] como "todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro."

Inteligência artificial

O termo Inteligência Artificial (IA) foi cunhado pelo professor John McCarthy, da Universidade de Stanford, durante seminário apresentado no Dartmouth College, na cidade de Hanover (New Hampshire, EUA) em 1956. Naquela época, conforme Prado (2023), já havia diversas teorias de simulação de linguagem, complexidade, redes neurais e aprendizado de máquinas e esse termo fora adotado para designar os sistemas computacionais que empregavam tais teorias.

Em uma definição histórica tem-se que a IA existe "quando uma máquina é capaz de imitar a inteligência humana ou mesmo superá-la para realizar uma determinada tarefa, como previsão ou raciocínio". (European Parliamentary Research Service, 2022, p. 2).

Nas últimas décadas, sugiram inúmeras definições do termo IA que, de certa forma, convergem para máquinas capazes de emular a inteligência humana, ou seja, refere-se "ao desempenho por programas de computador de tarefas comumente associadas a seres inteligentes" (World Health Organization, 2021, p. 4, tradução nossa).

Nessa direção, o Escritório de Inteligência Artificial do Serviço Digital do Governo do Reino Unido (United Kingdom, 2021, p.6) define IA como a utilização de tecnologia digital para a criação de sistemas capazes de realizar tarefas que normalmente foram concebidas para exigir inteligência humana e essencialmente "é um campo de pesquisa que engloba filosofia, lógica, estatística, ciência da computação, matemática, neurociência, linguística, psicologia cognitiva e economia". (United Kingdom, 2021, p. 6, tradução nossa).

Para o referido Escritório, a IA está em constante evolução e envolve geralmente máquinas que utilizam dados estatísticos para encontrar padrões em um grande volume de dados; e possuem a habilidade de executar tarefas repetitivas sem a necessidade de constante intervenção humana.

Deve-se ressaltar que em uma definição específica, o Conselho de Inteligência Artificial da Organização para Cooperação e Desenvolvimento Econômico (OCDE) recomenda e afirma que:

[9] Regulamento Geral de Proteção de Dados (General Data Protecting Regulation – GDPR) da União Europeia. Considerando 35. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

> "Um sistema de IA é um sistema baseado em máquina que pode, para um determinado conjunto de objetivos definidos pelo homem, fazer previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais. Os sistemas de IA são projetados para operar com diferentes níveis de autonomia." (OCDE, 2019 como citado por World Health Organization, 2021, p. 4, tradução nossa)

O fundamento da IA são os algoritmos que carregam instruções para rápida análise e transformação de dados em conclusões, informações ou outros resultados. Os algoritmos analisam grandes quantidades de dados e a capacidade de analisar esses dados alimentam rapidamente a IA. Berton (2021, p.21) acrescenta que

> A IA possui várias subáreas, as principais estão relacionadas ao Aprendizado de Máquina (AM), do inglês, Machine Learning (ML) com várias aplicações nos processos de reconhecimento e detecção de padrões; ao Processamento de Linguagem Natural (PLN) que visa trabalhar a comunicação utilizando a linguagem verbal e textual; nos casos de aplicações baseadas em Visão Computacional; que visa o reconhecimento de objetos além da robótica que trabalha com agentes físicos que por meio de sensores e atuadores se tornam capazes de interferir no mundo real.(Berton, 2021, pp. 21-22).

Atualmente, torna-se crescente o emprego de IA em diversos campos do conhecimento e a área da saúde desponta como uma das mais promissoras. O Serviço de Pesquisa do Parlamento Europeu (European Parliamentary Research Service, 2022), aponta que entre as principais áreas de aplicação de IA na medicina e na assistência médica estão: a prática clínica; a pesquisa biomédica; a saúde pública e a administração de sistemas de saúde (Tabela 2).

Tabela 2

Domínios	**Subáreas**	**Principais aplicações**
Prática Clínica	Radiologia, patologia digital, emergência médica, cirurgia, predição de riscos, intervenções adaptativas, cardiologia, nefrologia, hepatologia, saúde mental.	O potencial para a aplicação da IA no cenário clínico é enorme e varia desde a automação de processos diagnósticos para tomada de decisão terapêutica e pesquisa clínica. Os dados necessários para o diagnóstico e tratamento vem de muitas fontes, incluindo notas clínicas, testes de laboratório, dados de farmácia, imagens médicas e informações genômicas.
Pesquisa Biomédica	Pesquisa clínica, descoberta de medicamentos, testes clínicos.	A pesquisa biomédica parece se beneficiar mais das soluções derivadas da IA em comparação com a clínica aplicações, com avanços recentes também mostrando aplicações promissoras de IA no conhecimento clínico recuperação. Por exemplo, os principais recursos de conhecimento médico já estão usando algoritmos de ML para classificar os resultados da pesquisa, incluindo algoritmos que aprendem continuamente com o comportamento de pesquisa dos usuários (Fiorin et al., 2018 como citado por European

		Parliamentary Research Service, 2022, p. 10, tradução nossa)
Saúde Pública	Identificação e prevenção de doenças e epidemias etc.	Todas as aplicações de outros domínios que contemplem os sistemas de saúde públicos de cada país ou região. Identificação de dados demográficos específicos ou localizações geográficas onde há prevalência de doenças ou comportamentos de alto risco; vigilância epidemiológica digital.
Administração de Sistemas de Saúde	Codificação, agendamento e marcação de exames e consultas, detecção de frades, gerenciamento do fluxo de pacientes, auditoria.	Os sistemas de saúde são caracterizados por um fluxo de trabalho administrativo pesado com uma grande diversidade de atores e instituições, incluindo pacientes, profissionais de saúde, instalações e organizações de saúde, instalações de imagem, laboratórios , farmácias, pagadores e reguladores. Há, portanto um grande potencial de aplicação da IA dentro desse ambiente administrativo pesado que incluem, entre muitos outros aspectos; o tempo gasto na recuperação de reembolso financeiro; a entrada de dados em vários sistemas de informação baseados em práticas; o processamento de informações de hospitais e outros provedores; e o auxílio aos pacientes e usuários na navegação em sistemas de sáude fragmentados, por exemplo.

Principais domínios de aplicação da IA na medicina e na assistência médica Fonte: Elaboração própria (com base no Relatório Artificial Inteligence in Healthcare, European Parliamentary Research Service, 2022)

Nessa perspectiva, as plataformas de IA apresentam a capacidade de proporcionar respostas complexas em intervalos de tempo reduzidos, aprimorar continuamente a qualidade de serviços oferecidos à população, ler grandes volumes de bases de dados e realizar análises preditivas abrangentes em áreas diversas como saúde, educação, segurança pública, entre outros segmentos.

> “Nos últimos anos, verifica-se uma explosão no número de aplicações e serviços voltados para a área de saúde, o que inclui, por exemplo, o uso de inteligência artificial para diagnósticos e predições; softwares que fazem o acompanhamento e orientam o tratamento de doenças; e aplicativos de controle menstrual ou de cuidados durante a gravidez. A saúde tornou-se em vários aspectos um produto, havendo táticas cada vez mais agressivas para se coletar dados sensíveis dessa natureza”. (Teffé, 2022, p.89)

Por outro lado, apesar dos inúmeros benefícios proporcionados pelo uso da IA, há preocupações relevantes, quanto aos riscos à privacidade dos indivíduos, em especial, sobre os dados pessoais sensíveis, estes que podem causar discriminação e preconceito aos seus titulares, dados estes que devem ter tratamento e proteção diferenciados e robustos.

> “[...] a capacidade de tratamento de dados pessoais das mais diversas ordens vem aumentando exponencialmente, principalmente devido ao advento de tecnologias avançadas de inteligência artificial, com o uso de algoritmos sofisticados e com a

> possibilidade de aprendizado por máquinas (machine learning).” (Mulholland, 2018, p.173)

Para Instituições públicas de saúde, as quais lidam diariamente com dados pessoais sensíveis, os desafios são ainda maiores, dado que estas dependem, diretamente, de políticas públicas protetivas, além de investimentos adequados que sejam capazes de promover segurança e proteção para as infraestruturas técnicas, com medidas e ações que possam, sobremaneira, manter a proteção aos dados pessoais sensíveis e o respeito à privacidade de seus titulares, seja através da coleta, processamento, armazenamento ou toda e qualquer forma de tratamento dos dados pessoais sensíveis.

MEDIDAS PARA MITIGAÇÃO DE RISCOS À PRIVACIDADE

Foram analisadas algumas medidas técnicas, a começar pela anonimização e pseudononimização. A LGPD[10] define dado anonimizado como “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” e anonimização como “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo”.

Este conceito é reafirmado por BIONI (2020, p.191) quando diz que “A antítese do conceito de dado pessoal seria um dado anônimo, ou seja, aquele que é incapaz de revelar a identidade de uma pessoa” e por COTS e OLIVEIRA (2018, p.141) quando complementa que “há duas formas de anonimizar os dados pessoais: a primeira é eliminar a possibilidade de identificação sem que se pretenda a reversão do procedimento; a segunda, também conhecida como pseudoanonimização, consiste em tornar indisponíveis os dados que permitiriam a identificação por meio de técnicas como a encriptação”, sobre as possibilidades de tornar um dado pessoal em dado anônimo, quando assim for necessário, para que se mantenha a privacidade de seus titulares.

Para a LGPD[11], anonimização e pseudonimização são medidas técnicas a serem consideradas por instituições de saúde:

> “Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas”. (LGPD, 2018)

Já o GDPR[12] considera que a aplicação da pseudononimização aos dados pessoais “pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento e os seus subcontratantes a cumprir as suas obrigações de proteção de dados”.

---

[10] Artigo 5º da Lei 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[11] Artigo 13º da Lei 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[12] Regulamento Geral de Proteção de Dados (General Data Protecting Regulation – GDPR) da União Europeia. Considerando 28. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

Nesse sentido, o "Parecer 05/2014 sobre técnicas de anonimização" foi escrito pelo Grupo de Trabalho de Proteção de Dados pertencente ao European Comission[13] – EC (Órgão da União Europeia), em trabalho relativo ao tema no GDPR, o qual traz várias abordagens com o objetivo de ter uma "estratégia para colher os benefícios dos 'dados abertos' para as pessoas e a sociedade em geral, reduzindo, simultaneamente, os riscos para as pessoas em causa", considerando a aleatorização[14] e a generalização[15] como principais técnicas de anonimização de dados pessoais.

Neste rol de medidas, a pseudoanonimização utiliza técnicas como a criptografia[16], as quais podem tornar indisponíveis os dados pessoais, priorizando e respeitando a privacidade de seus titulares.

Uma outra medida técnica analisada foi o consentimento. A LGPD[17] o define como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Já o GDPR[18] define que "o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito".

Consentimento é também considerado pela LGPD[19] como uma das suas dez hipóteses legais, quando especifica em um de seus artigos que o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular.

Nessa circunstância, a hipótese legal do consentimento não necessariamente prevalecerá diante das demais hipóteses legais.

> "Informações, indicadores de saúde e orientações científicas devem ser a base para a formulação de políticas de saúde. Entende-se que uma adequada política pública para os vários problemas de saúde enfrentados pela população [...] necessita de uma estrutura de informações segura e confiável, que sustente e direcione as tomadas de decisão. Para tanto, com a LGPD em vigor, diversos protocolos e bancos de dados geridos pela Administração Pública deverão ser adequados à norma, para que se garanta seu uso regular e o desenvolvimento de políticas públicas e de ações mais eficientes e que atendam integralmente às necessidades da população". (Teffé, 2022, p.91)

Assim, é relevante observar que será necessário o consentimento do titular de dados pessoais nos casos em que um agente de tratamento não possuir justificativas, dentro de uma das hipóteses legais

---

[13] EC. European Comission. Grupo de trabalho de proteção de dados do Artigo 29.o. 0829/14/PT GT216. Parecer 05/2014 sobre técnicas de anonimização. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-re- commendation/files/2014/wp216_pt.pdf].

[14] Família de técnicas que altera a veracidade dos dados a fim de eliminar a estreita ligação entre os dados e a pessoa. Se os dados forem suficientemente imprecisos já não poderão ser relacionados com uma pessoa específica. É passível de proteger contra ataques ou riscos de inferência e pode ser combinada com técnicas de generalização a fim de fornecer garantias de privacidade mais sólidas. (European Comission. Grupo de trabalho de proteção de dados do Artigo 29.o. 0829/14/PT GT216. Parecer 05/2014 sobre técnicas de anonimização.)

[15] Generalizar, ou diluir, os atributos dos titulares dos dados através da alteração da respetiva esca- la ou ordem de grandeza (isto é, uma região em vez de uma cidade, um mês em vez de uma semana). (European Comission. Grupo de trabalho de proteção de dados do Artigo 29.o. 0829/14/PT GT216. Parecer 05/2014 sobre técnicas de anonimização.)

[16] Ciência que escreve mensagens de forma cifrada ou em código e que pode tornar indisponível a identificação do titular de um dado pessoal.

[17] Artigo 5º da Lei 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[18] Regulamento Geral de Proteção de Dados (General Data Protecting Regulation – GDPR) da União Europeia. Considerando 32. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

[19] Artigo 7º da Lei 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

especificadas na LGPD, para que possa realizar o tratamento de determinado dado pessoal (sensível ou não).

Resultados

A adoção de medidas de segurança robustas torna-se fundamental, visando a salvaguarda desses dados contra potenciais incidentes de acesso não autorizado, violações e ataques cibernéticos. Assim, a implementação de ações que não apenas assegurem a contenção de compartilhamento inadequado, mas também resguardem o acesso não autorizado, assume um papel de destaque.

A LGPD não apenas exige a implementação de medidas protetivas, mas também reforça o direito à privacidade dos indivíduos. O ingresso da Inteligência Artificial traz à tona novos debates nesse campo, demandando um diálogo e investigações substanciais para sua devida regulamentação. Esse processo visa mitigar os perigos da utilização indevida de dados no contexto do universo digital.

À luz do que foi apresentado, é possível concluir que as medidas técnicas de anonimização e pseudoanonimização de dados representam instrumentos estabelecidos na legislação brasileira e global, delineando orientações destinadas a orientar Organizações, sobretudo aquelas ligadas à saúde. Essas medidas têm o potencial de atuar como mecanismos protetivos em relação aos dados pessoais sensíveis.

No Brasil, Instituições como a Agência Nacional de Saúde Suplementar (ANS), o Ministério da Saúde, o Sistema Único de Saúde (SUS), secretarias especializadas, hospitais públicos e médicos da rede pública têm o compromisso de realizar o tratamento de dados pessoais sensíveis de saúde da população de forma adequada e segura. Dado que estas Instituições lidam com grandes bases de dados pessoais da população na rede pública de saúde, o cenário face a este compromisso é desafiador, porém, não impossível.

Considerações Finais

Inúmeros obstáculos surgem à medida que enfrentamos inovações tecnológicas de crescente complexidade, sendo a utilização massiva da Inteligência Artificial uma das mais proeminentes. Contudo, o desafio que possivelmente se destaca como o mais crucial é o estabelecimento de uma governança eficaz para o tratamento adequado de dados pessoais sensíveis, em especial dados de saúde, juntamente com a salvaguarda da privacidade e da proteção dessas informações, em sintonia com a aplicação da Inteligência Artificial.

As leis de proteção de dados pessoais em diversos países no mundo, têm o potencial de contribuir significativamente para um controle mais rigoroso sobre a utilização indiscriminada das informações pessoais, devido à imposição de diretrizes obrigatórias para as organizações quanto à proteção de dados e segurança da informação.

A Lei Geral de Proteção de Dados Pessoais (LGPD), vigente no Brasil, segue essa mesma tendência. A expectativa reside no aprendizado das organizações em tratar os dados de maneira mais responsável, o que resultaria na mitigação de riscos e na redução de incidentes relacionados a violações de dados. Por consequência, isso pode ser fator determinante para manter a proteção da privacidade dos indivíduos.

No Brasil, as instituições governamentais, encarregadas de moldar políticas públicas, estão progredindo na direção de estabelecer leis e regulamentações que promovam o aprimoramento do ecossistema de proteção à privacidade. Torna-se crucial acompanhar de perto essa evolução, enquanto não se deve afastar a igual responsabilidade do Governo em prover recursos financeiros

essenciais às Instituições para garantir a utilização transparente e segura de novas tecnologias, como a inteligência artificial. Essa abordagem visa o benefício de toda a população.

Por outro lado, entidades de saúde pública enfrentam o desafio de estabelecer políticas, protocolos e medidas técnicas destinadas a garantir a preservação da privacidade durante a coleta e armazenamento de informações sensíveis de indivíduos. Esse desafio é particularmente caracterizado na abordagem de tópicos como anonimização, consentimento e salvaguarda de dados pessoais.

Referências

Act on the Protection of Personal Information. Disponível em: [https://www.japaneselawtranslation.go.jp/en/laws/view/4241/em]

BARTECH, **Cristoph et al. An Introduction to Ethics in Robotics and AI** (SpringerBriefs in Ethics). Basiléia(Suiça): Springer Nature, 2021.

BERTON, Lilian. **Noções sobre IA.** In: VALÉRIO NETTO, Antonio; BERTON, Lilian; TAKAHATA, André. Ciência de Dados e a Inteligência Artificial na Área de Saúde. São Paulo: Editora dos Editores, 2021. 224p.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BIONI, Bruno. **Compreendendo o conceito de anonimização e dado anonimizado**. Escola Paulista da Magistratura. Cadernos Jurídicos. Ano 21 - Número 53 - Janeiro-Março/2020. Direito Digital e proteção de dados pessoais. São Paulo, 2020. Disponível em: [http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Cad-Juridicos_n.53.pdf]. Acesso em 20/8/2023.

BRASIL. **Lei n. 13.709 de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais**. Brasília, 2018. Disponível em: [http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm]. Acesso em 19/7/2023.

COTS, Marcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: Thomson Reuters Brasil, 2018.

DATA PRIVACY BR. **Contribuição à consulta pública a Estratégia Brasileira de Inteligência Artificial.** São Paulo; Reticências Creative Design Studio, 2020.

EC. European Comission. **Grupo de trabalho de proteção de dados do Artigo 29.o. 0829/14/PT GT216**. **Parecer 05/2014 sobre técnicas de anonimização**. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf]. Acesso em 25/7/2023.

EUROPEAN PARLIAMENTARY RESEARCH SERVICE, EPRS. **Artificial Inteligence in Healthcare:** applications, risks, and ethical and societal impacts. Panel for the Future of Science and Technology. Scientific Foresight Unit STOA). European Union, 2022. Disponível em:< https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)72951>. Acesso em: 12 nov. 2022.

GAETANI, Francisco e ALMEIDA, Virgílio. **Devagar com o andor e com a automação**. Departamento de Ciência da Computação. Notícia. Valor Econômico publica artigo de professor do DCC. Disponível em:[https://dcc.ufmg.br/valor-economico-publica-artigo-de-professor-do-dcc/]. Acesso em 20/8/2023.

Lei de Proteção de Dados Pessoais (LEY DE PROTECCION DE DATOS PERSONALES). Disponível em: [https://www.impo.com.uy/bases/leyes/18331-2008]

Lei Federal de Proteção de Dados Pessoais em Posse dos Indivíduos (LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES). Disponível em:https://www.gob.mx/cms/uploads/attachment/file/123648/Ley_Federal_de_Protecci_n_de_Datos_Personales_en_Posesi_n_de_los.pdf]

LEY ESTATUTARIA 1581. Disponível em: [http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html]

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da Hiperconectividade**. Disponível em: [http://eduardomagrani.com/wp-content/uploads/2019/07/Entre-dados-e-robo%CC%82s-Pallotti-13062019.pdf]. Acesso em 20/7/2023.

MULHOLLAND, Caitilin. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18)**. Faculdade de Direito de Vitória - FDV. Revista de Direitos e Garantias Fundamentais. V. 19, n.3, set./dez. 2018. Disponível em: [https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603]. Acesso em 23/7/2023.

MULHOLLAND, Caitilin. **Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018)**. Disponível em: [https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensíveis.pdf]. Acesso em 20/7/2023.

ONU. **Declaração Universal dos Direitos do Homem**. Organização das Nações Unidas, 10.12.1948. Disponível em: [https://nacoesunidas.org/]. Acesso em 19/8/2023.

Oyadomari, Winston, Costa, Ramon Silva e Ribeiro, Manuella Maia. **Perspectivas da sociedade brasileira em relação à privacidade e à proteção de dados pessoais.** In: CETIC.BR/ NIC.BR. Proteção de dados pessoais: privacidade e confiança no ambiente digital. Panorama Setorial da Internet. Número 2. Junho, 2023. Ano 15. Disponível em: [https://www.cgi.br/media/docs/publicacoes/6/20230727104116/psi-ano-xv-n-2-protecao-de-dados-pessoais.pdf]. Acesso em: 19/8/2023.

Regulamento Geral de Proteção de Dados (General Data Protecting Regulation – GDPR). Disponível em: [https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679]

Regulamento Geral de Proteção de Dados da Inglaterra (UK General Data Protecting Regulation - UK GDPR). Disponível em: [https://www.gov.uk/data-protection]

RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SILVA, Adriana. Algoritmos. Glossário de Inteligência Artificial. I2ai, 2001. Disponível em: 2ai.org/content/glossary/?gclid=Cj0KCQjw84anBhCtARIsAISI-xe-Nd8LdHal1mjio_bXb1OydjS13RqRCCpNm-r_PAr11JLhxvo_aZYaAolTEALw_wcB#cap5. Acesso em: 16 jul. 2023

SUBRAHMANYA, S.V.G; SHETTY, D.K; PATIL, V.; HAMEED, B.M.Z; PAUL, R.; SMRITI, K.; NAIK, N.; SOMANI, B.K. The role of data science in healthcare advancements: applications, benefits, and future prospects. **Irish Journal of Medicine Science**. 2022 Aug;191(4):1473-1483. doi: 10.1007/s11845-021-02730-z. Epub 2021 Aug 16. PMID: 34398394; PMCID: PMC9308575. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9308575/pdf/11845_2021_Article_2730.pdf. Acesso em: 12 nov. 2022.

TEFFÉ, Chiara Spadaccini de. **Dados Pessoais Sensíveis: qualificação, tratamento e boas práticas**. 1. ed. São Paulo: Foco, 2022. 304 p.

The Privacy Act. Disponível em: [https://www.oaic.gov.au/privacy/privacy-legislation]

UNITED KINGDOM. **A Guide to using artificial inteligence in the public sector**. Office for Artificial Inteligence, Government Digital Service, United Kingdom, 2020. Disponível em:< https://www.gov.uk/government/publications/a-guide-to-using-artificial-intelligence-in-the-public-sector>. Acesso em: 12 nov. 2022.

VALÉRIO NETTO, Antonio; BERTON, Lilian; TAKAHATA, André. **Ciência de Dados e a Inteligência Artificial na Área de Saúde.** São Paulo: Editora dos Editores, 2021. 224p.

VIEIRA, Elba Lúcia de Carvalho. Capítulo 6 – **A proteção de dados desde a concepção (by design) e por padrão (by default).** In: LGPD – Lei Geral de Proteção de Dados Pessoais. Manual de Implementação. São Paulo: Thomson Reuters Brasil, 2019.

WORLD HEALTH ORGANIZATION. Ethics and governance of artificial inteligence for health: WHO guidence. **World Heath Organization**: Geneva, 2021. Disponível em: https://www.who.int/publications/i/item/9789240029200. Acesso em: 12 nov. 2022.