AUSÊNCIA DE REGULAMENTAÇÃO DA IA PARA A PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS DE SAÚDE: ANÁLISE SOBRE DANOS AOS TITULARES.

Letícia Ramos Marinho[1]

RESUMO: A nova ordem social mundial vem sendo alterada e influenciada pelas novas tecnologias, em especial a Inteligência Artificial (IA). O uso cada vez intenso desta tecnologia, que se alimenta de todos os tipos de dados, incluindo dados pessoais, levanta questões significativas sobre privacidade e regulamentação. Este artigo se propõe a analisar este cenário, destacando a inexistência ou insuficiência de regulamentação da IA e suas influências nos direitos fundamentais da pessoa humana. A pesquisa foi realizada com base em uma revisão de literatura acadêmica e não acadêmica, estudos e regulamentações sobre Inteligência Artificial, regulamentações relacionadas à privacidade e proteção de dados pessoais, além de discussões em fóruns especializados compostos por profissionais especialistas nos temas da pesquisa.

Palavras-Chave: privacidade, dados pessoais sensíveis, inteligência artificial.

1 INTRODUÇÃO

Com o avanço contínuo das tecnologias de informação e comunicação (TICs), especialmente no campo da Inteligência Artificial, que demanda o uso de grandes volumes de dados pessoais e sensíveis, surgem questões fundamentais que afetam diretamente a vida dos cidadãos. Nesse contexto, é essencial discutir temas como o direito à privacidade, a proteção de dados pessoais sensíveis e a necessidade de regulamentações adequadas para garantir a proteção dos direitos fundamentais.

Embora a IA traga benefícios consideráveis, dependendo de sua aplicação, é inegável que, sem limites claros e regras bem estabelecidas — nas quais princípios como não discriminação e transparência sejam primordiais — os direitos fundamentais podem ser violados.

Ademais, é importante destacar os riscos relacionados à ausência de regulamentação no uso da IA, o que pode levar à violação de limites constitucionais, afetando diretamente a privacidade e a intimidade dos indivíduos.

Ao abordar os riscos e impactos para os titulares de dados pessoais sensíveis, especialmente na área da saúde, fica claro que esses riscos estão intimamente ligados às atividades que envolvem tais dados. No caso deste estudo, que se concentra nos dados pessoais sensíveis, como os dados de saúde, é impossível

[1] Graduanda em Direito pela Universidade Salvador (UNIFACS).

dissociar a prática de assistência à saúde da coleta, transformação, compartilhamento e armazenamento desses dados.

De maneira semelhante, como esse risco é intrínseco à própria atividade de assistência à saúde, trata-se de uma responsabilidade objetiva. Ou seja, qualquer lesão ao paciente — o titular dos dados — implica uma obrigação de reparação, independentemente de culpa.

Além disso, os avanços tecnológicos e científicos têm impactado de forma significativa o setor da saúde, mas também gerado grandes riscos, especialmente no que se refere à segurança dos dados pessoais sensíveis, ao direito à autodeterminação informada e ao direito fundamental à vida privada, inclusive no ambiente digital.

Para garantir a proteção desses direitos fundamentais, é imprescindível que exista uma regulamentação que estabeleça regras claras e que respeite os limites constitucionais. As atividades na área da saúde devem utilizar a Inteligência Artificial de maneira adequada, com propósitos, contextos e finalidades bem definidos.

Especialmente no que diz respeito aos dados pessoais sensíveis, como os dados de saúde, o uso da IA deve ser conduzido de forma a não causar danos ao indivíduo. Este ponto se torna ainda mais relevante quando consideramos o histórico de violações desses direitos, que resultaram em sofrimento humano significativo. Tais episódios impulsionaram a criação de medidas que assegurem que o desenvolvimento e o crescimento da tecnologia aconteçam dentro de limites éticos, respeitando os direitos fundamentais de todos.

2 ANÁLISE DA PRIVACIDADE NO CONTEXTO DE DADOS PESSOAIS SENSÍVEIS

De acordo com o artigo 5º da Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), dados pessoais são informações relacionadas a uma pessoa natural identificada ou identificável.

Por sua vez, dados pessoais sensíveis abrangem informações sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organizações de caráter religioso, filosófico ou político, além de dados relativos à saúde, à vida sexual, dados genéticos ou biométricos vinculados a uma pessoa natural, conforme disposto no artigo 5º da lei.

Conforme estabelecido no artigo 5º, inciso LXXIX, da Constituição Federal do Brasil, a proteção dos dados pessoais é assegurada como um direito fundamental, indispensável para uma vida digna, especialmente no contexto da era digital. Esse direito foi reconhecido com a Emenda Constitucional nº 115, de 2022.

Importante destacar que a LGPD não considera esse rol de dados sensíveis como taxativo. Isso significa que, dependendo do contexto, determinados dados pessoais podem ser classificados como sensíveis. Conforme Teffé (2022), relativo ao entendimento se trata de rol taxativo ou exemplificativo:

> [...] não esclareceu o que seriam dados sensíveis em termos conceituais, não definiu suas espécies nem se posicionou quanto à qualidade de seu rol: se taxativo ou exemplificativo.

De forma similar, o Regulamento (EU) 2016/679, do Parlamento Europeu e do Conselho, denominado *Genaral Data Protection Regulation* (GDPR), que regulamenta a proteção de dados pessoais no âmbito dos países da União Europeia, também define dados pessoais como qualquer informação que possa identificar uma pessoa física, direta ou indiretamente.

A LGPD, inspirada no GDPR, compartilha muitas semelhanças com o regulamento europeu. Um reflexo disso é o acordo de cooperação firmado entre a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) do Brasil e a autoridade europeia, o Comité Europeu para a Proteção de Dados (CEPD), visando a troca de experiências, aprendizado mútuo e apoio em investigações de incidentes relacionados a vazamentos de dados pessoais e outras questões que envolvam a de proteção de dados pessoais e os direitos dos seus titulares.

Ambos, a LGPD e o GDPR, não apenas definem o que são dados pessoais e dados pessoais sensíveis, mas também regulamentam as hipóteses de tratamento desses dados, estabelecendo "bases legais" que autorizam o tratamento dos dados pessoais. Essas bases legais, presentes nos artigos 7º e 11º da LGPD, indicam as situações em que o tratamento de dados é permitido, sendo consideradas as "autorizações" dadas aos agentes de tratamento (controlador e operador de dados pessoais), sejam pessoas físicas ou jurídicas que tratam dados com fins econômicos.

Um aspecto relevante da LGPD é que o artigo 11º da lei estabelece as permissões específicas para o tratamento de dados pessoais sensíveis. O legislador reconheceu a maior vulnerabilidade desses dados, conferindo-lhes uma proteção jurídica mais robusta. Por isso, o artigo 11º restringe significativamente as hipóteses

em que pessoas físicas ou jurídicas podem tratar dados sensíveis, impondo limites e exigindo cuidados adicionais para garantir a proteção dos direitos dos titulares.

Assim, é possível conceituar dados sensíveis segundo Stefano Rodotá apud Chiara Teffé (2022):

> [...] dados sensíveis são aqueles relativos à saúde e a vida sexual, às opiniões e ao pertencimento étnico ou racial, com uma lista semelhante às encontradas nas normas relativas a casos de discriminação. Assim, somos confrontados com algo que vai além da simples proteção da vida privada e se apresenta como defensor da mesma igualdade entre pessoas.

Conforme apontado por Santana, Vieira, Miranda e Mello, "o conceito de dados sensíveis deve ser compreendido em função do tratamento que é dado a eles. Ou seja, dados sensíveis são considerados como tal não apenas por sua natureza intrinsecamente pessoal, de maneira a priori, mas também em razão do uso e da finalidade a que são destinados, por meio de um tratamento que pode acarretar um risco de discriminação abusiva" (Mulholland, 2021).

Rodotá (2008) propõe uma categorização distinta para os dados sensíveis, argumentando que eles devem receber proteção especial contra o risco de circulação, devido ao seu potencial de serem utilizados de forma discriminatória.

A Lei Geral de Proteção de Dados (LGPD), no artigo 1º, estabelece de forma clara que seu objetivo é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. Dessa forma, fica evidente que as legislações de proteção de dados em vigor no Brasil e em outros países demonstram uma preocupação em definir de maneira específica os dados pessoais sensíveis, diferenciando-os dos dados pessoais comuns. As leis de privacidade e proteção de dados desses países, conforme apontado por Santana, Vieira, Miranda e Mello, consideram as informações relacionadas à saúde de um indivíduo como dados pessoais sensíveis.

Nesse sentido, Teffé (2022) destaca a relevância do livre desenvolvimento da personalidade como um direito fundamental, cuja finalidade é assegurar que cada indivíduo possa escolher sua forma de viver, se desenvolver e se expressar, conforme seu próprio projeto de vida. Ela também enfatiza que garantir o livre desenvolvimento da personalidade é uma responsabilidade do Estado e da sociedade, que devem adotar medidas políticas e ações concretas para viabilizar esse desenvolvimento. Ao proteger os dados pessoais, assegura-se, portanto, a liberdade, a igualdade e a integridade tanto do indivíduo quanto da coletividade.

Rodotá (2008) define a privacidade de forma precisa como o direito de manter o controle sobre as próprias informações. O autor descreve a esfera privada como o conjunto de ações, comportamentos, opiniões, preferências e dados pessoais sobre os quais o indivíduo deseja exercer controle exclusivo. Assim, a privacidade pode ser entendida como a "proteção das escolhas de vida contra qualquer forma de controle público ou estigmatização social", em um contexto marcado pela "liberdade das escolhas existenciais".

É essencial compreender que a definição de dados pessoais sensíveis é determinante, ou seja, ela estabelece quais informações exigem maior proteção, dada a sua capacidade de causar danos significativos aos titulares em certos contextos sociais e políticos.

Conforme Scott Skinner-Thompson, citado por Chiara Teffé (2022), a ausência de uma proteção adequada à privacidade resulta em danos concretos, especialmente para comunidades marginalizadas. Estas comunidades enfrentam, historicamente, marginalização, discriminação de diversas formas, assédio e violência, como é o caso de minorias como negros, homossexuais e transexuais.

Portanto, como afirmam Mulholland e Kremer, também citados por Chiara Teffé (2022), é imprescindível adotar um olhar atento à diversidade ao tratar da tutela dos dados sensíveis, de modo que o Direito assegure os princípios da igualdade material e da não discriminação.

É fundamental destacar que o tratamento de dados pessoais sensíveis por parte de empregadores, recrutadores, seguradoras, planos de saúde e órgãos governamentais pode resultar em violação de direitos, nos casos em que os dados pessoais sensíveis não tenham o adequado tratamento e as adequadas medidas de proteção e segurança. A Constituição de 1988 assegura o princípio da não discriminação em razão de origem, raça, sexo, cor, idade ou qualquer outra forma de discriminação.

O direito à antidiscriminação pode ser compreendido, conforme Roger Rios (2020) como uma proteção essencial contra práticas discriminatórias que impactam a dignidade e os direitos individuais dos cidadãos.

> A discriminação enfrentada pelo direito da antidiscriminação é, portanto, tomada por uma perspectiva mais substantiva que formal: importa enfrentar a desigualdade prejudicial e injusta, pois nem sempre a adoção de tratamentos distintos se revela maléfica, sendo mesmo tantas vezes exigida, como alerta a dimensão material do princípio da igualdade (o de tratar

> igualmente os iguais e desigualmente os desiguais na medida de suas desigualdades).

Chiara Teffé (2022), destaca a existência de duas modalidades de discriminação: a direta e a indireta. A discriminação direta ocorre de forma intencional e consciente, enquanto a indireta se manifesta por meio de atitudes aparentemente neutras, mas que geram impactos prejudiciais, mesmo sem a intenção de discriminar, afetando indivíduos e grupos marginalizados.

Ambas as modalidades de discriminação (direta e indireta), se espalham por toda a estrutura organizacional, perpetuando privilégios e desigualdades. Esse tipo de discriminação pode atingir dados pessoais sensíveis, seja por ações humanas ou por decisões automatizadas feitas por máquinas, resultando em consequências negativas para indivíduos e grupos hipervulneráveis, como crianças e idosos.

Dada a grande possibilidade de que dados pessoais sensíveis sejam tratados de maneira a causar danos irreparáveis, é importante observar que, em 1990, a Organização das Nações Unidas (ONU) emitiu as *Diretrizes para a Regulamentação de Arquivamento de Dados Pessoais Computadorizados*, com o objetivo de prevenir a discriminação e a violação de interesses, direitos e liberdades dos indivíduos.

A proteção reforçada para dados pessoais sensíveis se justifica pelo fato de que esses dados revelam informações cruciais sobre o passado, o presente e o futuro de um indivíduo. Esse aspecto é de extrema relevância e está presente tanto na LGPD quanto no GDPR. No *considerando 51* do GDPR, é destacado que esses dados merecem proteção especial devido à sua natureza sensível, pois podem representar riscos significativos para os direitos e liberdades dos indivíduos. Esse ponto é reafirmado no *considerando 71*, conforme tratado por Chiara Teffé (2022), em sua obra, que enfatiza a necessidade de uma proteção jurídica rigorosa para dados que possuem tal sensibilidade.

> A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizados, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicção, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas.

O considerando 85 do GDPR também destaca que, caso não sejam adotadas as medidas de segurança apropriadas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas, incluindo a perda de controle sobre seus dados pessoais, limitação de seus direitos, discriminação, roubo ou usurpação de identidade, prejuízos financeiros, reversão não autorizada de pseudonimização, danos à reputação, perda de confidencialidade de dados protegidos por sigilo profissional, ou qualquer outra desvantagem econômica ou social.

Teffé (2022) destaca que, embora os modelos e fórmulas matemáticas ofereçam vantagens, eles apresentam limitações, especialmente quando se trata de traduzir aspectos complexos da natureza humana em critérios objetivos. Assim, decisões automatizadas podem violar direitos fundamentais, porém, seus efeitos podem ser minimizados ou evitados, caso sejam observados parâmetros éticos e constitucionais no uso das tecnologias que fazem tais decisões automatizadas. Nesse contexto, a matemática e cientista de dados Cathy O'Neil, citada por Teffé (2022), alerta que opiniões humanas estão embutidas nos algoritmos, de modo que eles tendem a automatizar o status quo.

O'Neil defende que, para garantir a justiça nos algoritmos, é necessário fiscalizá-los, corrigi-los e aprimorá-los. Além disso, ela ressalta que o princípio da não discriminação deve ser incorporado desde a concepção dos sistemas de inteligência artificial, em conformidade com os princípios do *privacy by design* e *privacy by the default*.

Outro ponto importante refere-se ao tratamento de dados pessoais sensíveis no contexto da inteligência artificial. É fundamental que o desenvolvimento dessa tecnologia seja orientado por princípios e valores éticos, com o objetivo de alcançar suas finalidades, mas sempre respeitando e protegendo os direitos humanos. Para isso, é essencial minimizar o uso de dados e informações tratadas, adotando, por exemplo, técnicas de anonimização. Além disso, deve-se utilizar ferramentas tecnológicas que garantam, por padrão, a transparência em relação aos critérios empregados nas decisões automatizadas.

O avanço tecnológico é um processo inevitável, assim como o uso de dados pessoais sensíveis no contexto dessa evolução. Contudo, é fundamental que esse progresso e o crescente emprego dessas informações sejam conduzidos dentro dos princípios e limites previstos pela Constituição, artigo 5°, inciso LXXIX, assegurando a proteção dos direitos fundamentais. Esses direitos devem ser tratados como bens

jurídicos a serem tutelados, como defende Danilo Doneda (2021), cujo objetivo é proporcionar ao ordenamento jurídico uma maneira eficaz de conciliar os interesses envolvidos e os valores que ele reflete.

> Para o direito privado, especificamente, umas das abordagens possíveis seria o reconhecimento da natureza de bem jurídico à informação e, a partir disso, a disponibilização dos instrumentos do direito de propriedade para a sistematização do tema.

Doneda (2021) alerta sobre a forma como essas informações circularão dentro dos centros de processamento de dados, sendo um requisito essencial para a construção da "datasphere" — um conjunto de informações que engloba dados sobre nós e nossas ações.

> Uma vez que os eventos cotidianos de nossas vidas são sistematicamente armazenados em um formato legível por uma máquina. Esta informação ganha uma vida toda própria. Ela ganha novas utilidade. Ela se torna indispensável em operações comerciais. E ela usualmente é transmitida de um computador a outro, e entre o setor privado e o governo.

Compreender o que são dados pessoais sensíveis é fundamental para que o ordenamento jurídico possa atuar de forma mais eficaz em sua proteção. Esses dados devem ser avaliados levando em conta a natureza e as características da informação pessoal, bem como o contexto em que será feito o seu tratamento.

Além disso, é necessário considerar os interesses específicos do responsável pelo tratamento, os destinatários potenciais dos dados, a finalidade e o propósito para os quais eles serão processados. Isso inclui verificar se há a intenção de inferir ou tratar atributos sensíveis, as condições do tratamento, as relações que podem ser estabelecidas com outras informações disponíveis sobre o titular ou o grupo a que ele pertence, as possibilidades tecnológicas atuais, e o impacto no livre desenvolvimento da personalidade do indivíduo.

Também é essencial avaliar a potencialidade do tratamento de dados sensíveis para se tornar um instrumento de estigmatização ou discriminação ilícita ou abusiva, conforme discutido na obra de Chiara Teffé.

Doneda citado por Teffé (2022), aborda a questão da categoria dos dados sensíveis, em que destaca:

> A elaboração desta categoria e de disciplinas específicas a ela aplicadas não foi isenta de críticas, como a que afirma que é impossível, em última análise, definir antecipadamente os efeitos do tratamento de uma informação, seja ela da natureza que for. Desta forma, mesmo dados não qualificados como sensíveis, quando submetidos a um determinado tratamento, podem revelar aspectos sobre a personalidade de alguém, podendo levar a práticas discriminatórias. Afirma-se, em síntese, que um dado, em si, não é perigoso ou discriminatório - mas o uso que ele se faz pode sê-lo. [...] deve-se ter em conta que o próprio conceito de dados sensíveis atende à uma necessidade de delimita uma área na qual a probabilidade de utilização discriminatória da

> informação é potencialmente maior – sem deixarmos de reconhecer que há situações onde tal consequência pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se prestes a fins legítimos e lícitos.

É importante destacar a necessidade de garantir maior proteção aos dados sensíveis, especialmente considerando que nem todos eles estão explicitamente definidos. Dependendo do contexto e da finalidade do tratamento, dados pessoais podem se tornar sensíveis e, portanto, requerer uma proteção mais rigorosa.

Esse ponto é abordado na obra de Teffé (2022), que exemplifica como dados inicialmente não sensíveis podem ser inferidos como tal. Por exemplo, um controlador pode inferir a etnia de uma pessoa a partir de seu histórico educacional ou até mesmo do seu sobrenome ou local de nascimento, sugerindo sua raça.

Assim, a distinção entre dados pessoais gerais e dados pessoais sensíveis torna-se falha, uma vez que, com o uso de Big Data "*é um dos aspectos do campo da ciência de dados que trata de outros aspectos, como estratégias para extração, transformação e carga dos dados, modelagem, construção e avaliação de algoritmos descritivos e preditivos, visualização de grandes quantidades de dados e deploy dos modelos em ambientes de produção para a tomada de decisão, entre outros*.", e análises avançadas, qualquer dado pode, em potencial, ser transformado em sensível. Teffé observa, com base em pesquisas da Universidade de Cambridge, que registros digitais de comportamento, como as curtidas no Facebook, podem ser usados para prever, de forma automática e precisa, atributos pessoais sensíveis.

Outro fenômeno relevante destacado por Teffé é a *datificação*, que se refere ao processo de transformar a vida e as relações de uma pessoa em dados. A datificação converte a experiência humana em informações que circulam por diversas plataformas, serviços, aplicativos, bancos de dados e dispositivos de hardware. Essas informações são organizadas de maneira que possam ser registradas, monitoradas e analisadas, permitindo a extração de novos dados e a realização de análises preditivas sobre os indivíduos. Esse processo facilita a realização de inferências sensíveis, muitas vezes sobre aspectos privados e pessoais dos sujeitos, ampliando o alcance e o impacto do tratamento de dados.

Logo, os dados que se deixa de forma voluntária ou não, são rastros e objetos de análise, tanto para o setor privado, quanto para o público. Fazer inferências e correlações, são importantes não há que se discutir para uma realidade tecnológica que a cada dia ganha mais espaço na vida das pessoas, entretanto, é também é

indiscutível que as mesmas inferências e correlações também podem ser usadas para manipular e influenciar indivíduos, com distorções de autoestima ou até deturpação de narrativas. Como observa Teffé (2022):

> [...] tutelar dados sensíveis e tratamentos de caráter sensível significa proteger a pessoa contra discriminação abusiva ou ilícitas, assegurar igualdade material no seu tratamento e permitir o livre desenvolvimento da sua personalidade, levando-se em conta suas diferenças e características particulares.

Os dados pessoais relacionados à saúde, nesse contexto, são talvez os mais vulneráveis, que possuem altos graus de sensibilidade e criticidade, considerando que expõem o indivíduo em uma condição de fragilidade, revelando informações sensíveis sobre seu estado físico e mental. Na obra de Teffé, o conceito de dado de saúde, conforme definido pelo *General Data Protection Regulation* (GDPR), é descrito como "dados pessoais relacionados à saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelam informações sobre seu estado de saúde".

Esse conceito abrange não apenas dados diretamente relacionados à saúde, mas também informações que, em determinados contextos, podem permitir inferências sobre a saúde do indivíduo, como agendamentos de consultas, frequência de atividades físicas, hábitos alimentares, entre outros. Esses dados pessoais podem ser coletados por profissionais de saúde, como no caso dos prontuários eletrônicos, tornando-se uma fonte rica de informações detalhadas sobre o estado de saúde do paciente.

Com o avanço das tecnologias, esses dados pessoais sensíveis de saúde também se integram com sistemas de inteligência artificial para auxiliar na realização de diagnósticos e predições. Nesse cenário, a saúde se transformou em um produto, com estratégias cada vez mais agressivas para a coleta e utilização de dados sensíveis dessa natureza.

Com isso, há uma crescente preocupação com os riscos associados ao uso indevido dos dados de saúde, especialmente no contexto da inteligência artificial. Nesse sentido, foram identificados sete riscos principais relacionados à utilização da IA na área da saúde: danos ao paciente devido a erros de IA; uso inadequado de ferramentas médicas baseadas em IA; vieses na implementação dessas ferramentas, que podem perpetuar desigualdades; falta de transparência; questões de privacidade e segurança; lacunas na prestação de contas; e obstáculos para uma implementação eficaz, conforme defendido por Vieira, Santana, Mello e Miranda.

Esse cenário de uso e coleta, processamento e armazenamento de dados pessoais sensíveis de saúde não se limita apenas às instituições de saúde no setor privado; na esfera pública, percebe-se a ocorrência desta prática. Um exemplo relevante citado por Teffé é o DATASUS, sistema que reúne informações sobre todos os indivíduos que utilizam o Sistema Único de Saúde (SUS), no Brasil.

O DATASUS, portanto, se configura como uma importante fonte de dados para Secretarias de Saúde em estados e municípios brasileiros, além de desempenhar um papel crucial no planejamento e execução de políticas públicas. Um exemplo claro disso foi durante a pandemia de COVID-19, quando os dados pessoais sensíveis de saúde foram fundamentais para o acompanhamento da evolução da doença e a alocação de recursos em benefício da população.

No entanto, esse cenário também expôs vulnerabilidades. Durante a pandemia, houve um aumento significativo nos ataques cibernéticos e vazamentos de dados, afetando instituições públicas, incluindo o DATASUS. Isso evidencia a urgente necessidade de adequações nas políticas de segurança e regulamentações de proteção de dados pessoais, a fim de garantir que, ao se buscar soluções eficazes para políticas públicas, os direitos e as garantias individuais não sejam violados.

3 OS RISCOS DE INTELIGÊNCIA ARTIFICIAL SOBRE DADOS PESSOAIS SENSÍVEIS DE SAÚDE

De acordo com Santos, citado por Nunes, Guimarães e Dadalto (2022), a inteligência artificial é um campo da ciência da computação que visa, por meio de símbolos computacionais, desenvolver mecanismos e dispositivos capazes de simular a habilidade humana de pensar, resolver problemas e, em última instância, exibir comportamentos inteligentes.

Segundo traz Gualtieri e López (2024), no artigo 3, item 1 do AI Act, IA é:

> um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais.

Russell e Norvig citados por Gualtieri e López (2024) definem a IA como: "*O campo dedicado à construção de agentes inteligentes, que são funções que tomam*

inputs de percepção do ambiente externo e produzem comportamentos (ações) com base nessas percepções."

É importante observar que, nesse contexto, o uso da Inteligência Artificial geralmente requer dados pessoais e sensíveis, especialmente na área da saúde. Para essa análise, é interessante ter em mente que, embora haja uma relação, há diferenças fundamentais entre Privacidade e Proteção de Dados Pessoais. Quanto a Privacidade garante que as pessoas possam se desenvolver sem a interferência do Estado, assegurando sua intimidade e autonomia. Já a Proteção de Dados Pessoais está relacionada ao surgimento da sociedade da informação e à preocupação com a manipulação desses dados para fins de controle social, conforme defendem Godinho e Rodrigues (2024).

Através do chamado *machine learning* (aprendizado de máquina), os computadores são programados para aprender de maneira semelhante ao ser humano. Quase todo aprendizado de máquina é baseado em redes neurais, que são sistemas computacionais compostos por nós interconectados, funcionando de maneira análoga aos neurônios do cérebro humano. Utilizando algoritmos, essas redes são capazes de identificar padrões ocultos e correlações em dados brutos, agrupá-los e classificá-los, além de aprender e melhorar continuamente com o tempo.

Para que as redes neurais funcionem de maneira eficaz, é necessário alimentá-las com grandes volumes de dados, o que exige a utilização de *big data* nos sistemas. Esses dados permitem o treinamento das redes para resolver problemas. Na área da saúde, isso se traduz em aplicações que vão desde o diagnóstico precoce até a administração de medicamentos. Em outras palavras, o aprendizado de máquina baseia-se na capacidade de prever o futuro com base em dados do passado, conforme explica o professor Hal Daumé III, citado por Nunes, Guimarães e Dadalto (2022).

Vale ressaltar que, conforme Azevedo e Silva (2024), a Inteligência Artificial é um dos fenômenos mais transformadores da era contemporânea, influenciando todos os setores da sociedade, o meio ambiente e as formas de interação humana. Os autores destacam que essa tecnologia é paradoxal, pois, por um lado, tem o potencial de otimizar processos, melhorar a acessibilidade a serviços e impulsionar inovações antes inimagináveis; por outro, levanta preocupações significativas sobre vieses discriminatórios e opacidade, problemas que se intensificam à medida que a

tecnologia, sem regulação adequada, se infiltra cada vez mais nas decisões que afetam diretamente a vida das pessoas.

Na área da saúde, a inteligência artificial tem sido cada vez mais utilizada como um "segundo cérebro", auxiliando no diagnóstico de doenças e no atendimento aos pacientes. No entanto, é fundamental que o uso dessa tecnologia seja acompanhado pela supervisão humana, para evitar danos tanto aos pacientes quanto aos profissionais de saúde.

Ou seja, à medida que a Inteligência Artificial se torna mais integrada à nossa vida cotidiana, aumenta o risco de perpetuar desigualdades existentes e de criar novas formas de exclusão e discriminação. Além disso, vive-se em um cenário em que essa tecnologia é implementada sem a devida transparência ou explicação sobre os processos que levam aos seus resultados. Isso representa desafios significativos para reguladores e formuladores de políticas públicas, conforme apontam Azevedo e Silva (2024).

Portanto, há uma preocupação em relação aos vieses discriminatórios que podem surgir com o uso da Inteligência Artificial, especialmente na ausência de transparência e regulamentação adequadas. Esses vieses podem ocorrer devido ao uso de dados de treinamento tendenciosos, à falta de representatividade nesses dados e à ausência de diversidade nas equipes de desenvolvimento, além das correlações indiretas entre os dados que acabam gerando enviesamento. Também existe a possibilidade de discriminação algorítmica por design, o que pode resultar na reprodução de desigualdades raciais, conforme ressaltam Azevedo e Silva (2024).

Essa precaução, em relação ao uso dos dados pessoais e sensíveis, está prevista na Lei Geral de Proteção de Dados (LGPD), especificamente no artigo 20, que exige que o controlador forneça informações sobre os critérios e procedimentos utilizados em decisões automatizadas, por exemplo. Ou seja, em processos nos quais a tecnologia assume certa autonomia e envolve dados pessoais e sensíveis, é necessário que haja o acompanhamento e revisão por um ser humano, com o objetivo de prevenir danos, especialmente ao titular dos dados – no caso da saúde, ao paciente.

Exemplos preocupantes do uso de dados sensíveis com a Inteligência Artificial incluem, por exemplo, o reconhecimento facial, que apresenta uma alta taxa de falsos positivos, especialmente em mulheres negras e pessoas não binárias, sendo mais preciso para homens brancos. Em um contexto de segurança pública, isso pode

reforçar a seletividade penal e perpetuar o racismo estrutural, segundo Azevedo e Silva (2024). Da mesma forma, o uso de dados de saúde, como imagens médicas, está sujeito a erros de interpretação, o que pode levar a diagnósticos incorretos e, consequentemente, a condutas médicas inadequadas.

A área da saúde tem passado por transformações significativas ao longo do tempo. Chen, citado por Nunes, Guimarães e Dadalto (2022), apresenta uma linha do tempo dessa evolução, destacando o uso crescente da tecnologia. Ele dividiu essa trajetória em diferentes "eras".

A Era 1.0, no século XIX, foi marcada pela adoção de abordagens mais inteligentes para a saúde pública, com a implementação de medidas de saneamento básico e o início das pesquisas sobre vacinação. A Era 2.0, no século XX, correspondeu ao crescimento das grandes indústrias farmacêuticas, o que possibilitou a produção em massa de antibióticos.

A Era 3.0, a partir de 1980, ficou marcada pelos avanços da tecnologia computacional, que permitiram o uso de imagens no cuidado de saúde, facilitando diagnósticos mais rápidos e proporcionando amplo acesso à literatura médica, além de consolidar a medicina baseada em evidências.

Atualmente, vivemos a Era 4.0, caracterizada pela medicina inteligente, com o uso de medicina de precisão, telemedicina, automação, *big data* e inteligência artificial.

É fundamental discutir as questões éticas e regulatórias relacionadas ao uso de tecnologias, como a Inteligência Artificial (IA), especialmente quando se trata de dados sensíveis. Embora seja um desafio complexo, essa discussão é imprescindível, pois, frequentemente, a atenção recai sobre os benefícios da tecnologia na área da saúde, como o aumento da expectativa e da qualidade de vida.

No entanto, é crucial lembrar de eventos históricos que marcaram profundamente a humanidade. As atrocidades cometidas durante a Segunda Guerra Mundial, especialmente os experimentos médicos nazistas, caracterizados por extrema crueldade e realizados em cobaias humanas, eram, de fato, permitidos pelas leis alemãs da época. Em resposta a essas barbaridades, surgiu o Código de Ética Médica de Nuremberg, com o objetivo de estabelecer normas para proteger os direitos dos seres humanos em pesquisas científicas. Esse código foi criado a partir da reflexão sobre as crueldades cometidas, conforme apontado por Motta, Vidal e Siqueira-Batista, citados por Nunes, Guimarães e Dadalto (2022).

Segundo Gomes, citado por Nunes, Guimarães e Dadalto (2022), é fundamental questionar a Inteligência Artificial (IA) e seus propósitos, especialmente no contexto da saúde, em vez de simplesmente aceitá-la como inevitável ou uma fatalidade. A IA deve ser empregada em benefício da humanidade, e, para isso, é necessário um controle social adequado, com a definição de regras e limites.

Isso é particularmente importante no contexto brasileiro, onde a população é extremamente vulnerável, levando em consideração o histórico de formação do povo, que envolve fatores como o nível educacional e a compreensão das novas tecnologias. Além disso, é essencial garantir que a autodeterminação informada dos cidadãos seja respeitada, o que exige a intervenção do Estado para cumprir seu papel de proteção.

Nesse contexto, é crucial discutir a regulação da Inteligência Artificial (IA). A regulamentação pode ser uma forma de garantir um mínimo de padronização e proporcionar maior segurança jurídica. No entanto, se for excessiva, pode limitar os avanços tecnológicos. Por isso, é importante estabelecer limites claros para o uso da IA. Alguns países optam por definir apenas princípios gerais, enquanto outros buscam regulamentar cada aplicação da tecnologia.

A *Artificial Intelligence Act* (*AI Act*) propõe estabelecer marcos gerais para a IA levando em consideração os riscos associados ao seu uso, e define obrigações específicas de governança para mitigar esses riscos.

Segundo Vainzof (2024), a *AI Act* é uma norma robusta e prescritiva, concebida para impulsionar o desenvolvimento e a adoção segura da Inteligência Artificial, ao mesmo tempo em que assegura a proteção dos direitos fundamentais e classifica os riscos associados ao seu uso. Vale ressaltar que a *AI Act* possui efeitos extraterritoriais, aplicando-se a entidades que operam tanto dentro quanto fora da União Europeia (UE). Da mesma forma que o GDPR serviu de modelo para a LGPD no Brasil, há uma tendência de que o texto da *AI Act* também inspire outras legislações ao redor do mundo.

Vainzof (2024) apresenta o contexto histórico da *AI Act* como parte de um esforço da União Europeia para democratizar a "Década Digital", promovendo a educação digital entre seus cidadãos e regulamentando as empresas para enfrentar os desafios da evolução social e tecnológica. Os objetivos da UE são: (i) garantir uma população com competências digitais e profissionais altamente qualificados; (ii) estabelecer infraestruturas digitais seguras e sustentáveis; (iii) impulsionar a

transformação digital dos negócios; e (iv) promover a digitalização dos serviços públicos. Assim, em 2024, o Conselho Europeu aprovou a *AI Act,* a primeira legislação no mundo a estabelecer um padrão global para a regulamentação da Inteligência Artificial.

Não se pode negar que o uso da Inteligência Artificial apresenta riscos à segurança e à proteção dos dados pessoais e sensíveis dos cidadãos. É essencial garantir transparência e previsibilidade no comportamento desses sistemas, pois eles podem resultar em falhas ou ações maliciosas.

Vainzof (2024) destaca a dificuldade de monitorar e assegurar a segurança, citando, por exemplo, os sistemas de IA utilizados em dispositivos médicos, que podem interpretar erroneamente os dados, levando a diagnósticos incorretos. Por isso, é fundamental estabelecer requisitos específicos de segurança e garantir uma cobertura adequada para os sistemas de IA, por meio de uma regulamentação robusta e adaptada, que proteja efetivamente os cidadãos.

É fundamental reconhecer que, embora a tecnologia continue a avançar, ela deve ser empregada com um propósito claro e em benefício das pessoas. O uso da inteligência artificial, por exemplo, pode aumentar o risco de violação dos direitos fundamentais dos cidadãos, especialmente no que diz respeito à privacidade, à não discriminação e à liberdade de expressão. Nesse contexto, é crucial assegurar o direito de controlar como as informações pessoais são utilizadas por terceiros, conforme defende Westin, citado por Rodotá (2008).

Isso se torna particularmente relevante, pois, como destaca Vainzof (2024), a maneira como os dados são coletados, processados e usados para tomar decisões automatizadas pode resultar em discriminação, como no caso do reconhecimento facial, que pode prejudicar minorias étnicas caso os dados de treinamento sejam enviesados. O risco de violação de direitos está diretamente relacionado às características próprias da inteligência artificial, como sua opacidade, complexidade, comportamento autônomo e dependência de grandes volumes de dados.

Nesse contexto, surge o *AI Act,* que estabelece exigências relacionadas à segurança e à proteção dos direitos fundamentais, aplicáveis às novas tecnologias, incluindo a inteligência artificial. Para sua efetiva implementação, é essencial haver clareza jurídica e padrões consistentes. A incerteza legal e a complexidade das regras podem, no entanto, desmotivar as empresas a desenvolver e adotar sistemas de IA.

É fundamental compreender que a inteligência artificial desempenha um papel crucial no desenvolvimento econômico, social e na competitividade das organizações, o que torna necessária à sua regulação.

Segundo Vainzof (2024), essa regulação pode adotar duas abordagens: a permissiva, que propõe normas com caráter principiológico e delega a implementação para órgãos setoriais competentes, com base nas legislações existentes, como ocorre no Reino Unido e nos EUA; e a precavida, que envolve a definição detalhada de medidas de controle e governança, com foco na precaução devido ao potencial de danos que a IA pode causar.

Um exemplo disso é a resistência ao uso da tecnologia de reconhecimento facial, como a proibição adotada em São Francisco em 2019. Preocupações com a privacidade e o uso de deepfakes no contexto eleitoral têm impulsionado diversas iniciativas regulatórias, como destaca Vainzof (2024).

Assim, diversas regulamentações estão surgindo em vários países, como: o Reino Unido, que se baseia em cinco princípios fundamentais; o Canadá, que propõe uma abordagem focada no risco para regular o comércio internacional e interprovincial; a China, cujo objetivo é garantir que o conteúdo da IA esteja alinhado aos valores sociais e morais; Singapura, com uma abordagem regulatória rigorosa, ainda segundo Vainzof (2024).

E o Brasil, que propôs o Projeto de Lei 2338 de 2023, com o intuito de proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico.

Essa discussão levanta uma questão importante: em um universo de tecnologia, uso de inteligência artificial, big data e grande coleta de dados, que envolvem altos riscos de impacto para as pessoas, quem é responsável por responder por isso?

É interessante observar que a atividade em si de uso de IA precisa, fundamentalmente, de dados, muitos dados. Dados este, que são coletados, cruzados, perfilizados, e que precisam ser respeitados, pois eles possuem donos, os quais tem o direito de decisão sobre eles. Segundo Rodotá (2008) “. A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio”.

O fator risco torna-se elemento importante na definição quanto a responsabilidade, cuja percepção de Rodotá (2008) expressa “A presença de riscos conexos ao uso das informações coletadas, e não um natural vocação ao sigilo de certos dados pessoais, foi o que levou ao reconhecimento de um “direito à autodeterminação informativa” como direito fundamental do cidadão.”

4 A EVOLUÇÃO E OS PRINCIPIOS DA RESPOSNABILIDADE CIVIL: DA REDISTRIBUIÇÃO À PROTEÇÃO DOS DIREITOS FUNDAMENTAIS

A responsabilidade civil é um dos pilares do Direito, incumbindo a obrigação de indenizar o dano sofrido por outrem, quando este for resultado de um ato ilícito. O conceito básico de responsabilidade civil surge da necessidade de corrigir e reparar o prejuízo causado, assegurando que ninguém possa causar danos injustificados a outrem sem sofrer as consequências. Nesse contexto, surge o dever legal de responsabilizar o agente que, por meio de sua ação ou omissão, causou o dano. A ideia de que a ninguém é dado o direito de causar prejuízos à sociedade ou aos indivíduos é fundamental para a construção do arcabouço jurídico que regula a responsabilidade civil.

Inicialmente, a responsabilidade civil tinha raízes no conceito de vingança, presente em diversas culturas antigas, onde o dano causado por um indivíduo justificava uma reação proporcional, muitas vezes com caráter punitivo. Contudo, ao longo dos séculos, a função da responsabilidade civil passou por uma significativa transformação. Segundo Flaviana Soares (2009), a evolução desse conceito se deu de um modelo retributivo, caracterizado pela regra do "olho por olho, dente por dente", para um modelo mais moderno que passou a considerar a culpa e o risco como elementos centrais na atribuição de responsabilidades.

Esse processo evolutivo se insere em um contexto mais amplo, que vai além das esferas individuais, englobando também a coletividade. O objetivo fundamental da responsabilidade civil é proteger o que é lícito e reprimir o que é ilícito, impondo a obrigação de reparar os danos causados pela violação de um dever jurídico. Em termos legais, conforme o artigo 187 do Código Civil Brasileiro, o ato ilícito ocorre quando um direito é exercido de maneira excessiva, ultrapassando os limites impostos pela boa-fé, pelos bons costumes ou pela finalidade social ou econômica do direito.

O dano, portanto, refere-se à lesão de um bem jurídico protegido, podendo ser de natureza moral ou patrimonial, sendo esse o elemento central para a configuração da responsabilidade civil e, por conseguinte, seu fundamento. Assim, quando ocorre a inutilização ou deterioração de um bem devido a um ato prejudicial, a responsabilidade deve ser atribuída de forma objetiva ou subjetiva.

De acordo com Nelson Rosenvald, a responsabilidade civil é a obrigação de reparar os danos causados por culpa ou determinados por lei, refletindo uma dimensão que também encontra paralelo no Direito Penal, onde a responsabilidade se traduz na obrigação de suportar uma pena. Para os autores Cristiano de Farias e Felipe Neto, a responsabilidade civil, em sua definição clássica, é compreendida como a obrigação de reparar danos causados por culpa do agente, ou, em casos excepcionais, de acordo com a legislação vigente, mesmo na ausência de culpa.

Jean Paul Ricoeur, citado por Rosenvald, define a responsabilidade civil como o ato de imputar uma ação a alguém, atribuindo-lhe a autoria do dano, tornando-o responsável pela sua reparação. Já Immanuel Kant vê a responsabilidade como um juízo moral que atribui a alguém a autoria de uma ação que pode ser censurável, conferindo ao agente a responsabilidade de reparar os danos resultantes dessa ação.

A responsabilidade civil, ao longo de sua evolução, gerou uma importante discussão entre as teorias subjetiva e objetiva da responsabilidade. Tradicionalmente, a responsabilidade subjetiva exige que se prove a culpa do agente — seja por dolo, negligência, imprudência ou imperícia — para que ele seja responsabilizado pelos danos causados. Neste modelo, o agente deve ser culpado pelo dano para que haja a obrigação de indenizar.

Por outro lado, a responsabilidade objetiva se baseia na ideia de risco. Nesse modelo, o agente é responsável pelos danos independentemente de culpa, bastando que o dano seja decorrente de uma atividade de risco ou de um fato que envolva perigo para os outros. Esse modelo busca uma abordagem mais justa, onde a responsabilidade recai sobre quem assume um risco, sem a necessidade de provar a culpa.

Raymonda Saleilles e Loius Josserand, citados por Rosenvald, Farias e Neto, afirmam que a evolução tecnológica e as transformações sociais dificultam a identificação da culpa em muitos casos, como em acidentes de trabalho ou desastres industriais. O exemplo da "Lei de Responsabilidade por Acidente de Trabalho" na França, de 1898, ilustra a mudança histórica na maneira de tratar a responsabilidade

civil, com foco na reparação dos danos de maneira objetiva, sem a exigência de culpa do agente.

A função principal da responsabilidade civil é restaurar o equilíbrio patrimonial da vítima, transferindo o prejuízo ao agente responsável pelo ato ilícito. Isso se alinha aos conceitos de ato ilícito, culpa, abuso do direito, dano e nexo causal. O ato ilícito é entendido como qualquer fato que viole a ordem jurídica, seja por ação ou omissão, e que gere consequências jurídicas. Para Pontes de Miranda, o ato ilícito é um evento jurídico que, por sua natureza, gera efeitos no ordenamento.

Perlingieri, citado por Rosenvald, define o fato jurídico como "qualquer evento idôneo, segundo o ordenamento, a ter relevância", podendo produzir efeitos jurídicos relevantes, como a reparação de danos. Por sua vez, Rosenvald e outros autores esclarecem que o fato ilícito é um ato antijurídico cujos efeitos são contrários à ordem jurídica, ou seja, uma violação de uma obrigação jurídica preexistente.

A caracterização do ato ilícito envolve a análise de dois aspectos: a antijuricidade e a imputabilidade. A antijuricidade é a violação objetiva de direitos alheios, enquanto a imputabilidade diz respeito à capacidade do agente de ser responsabilizado pela conduta. O nexo de causalidade é o vínculo lógico entre a conduta do agente e o dano experimentado pela vítima, sendo essencial para se atribuir a responsabilidade civil. A culpabilidade, por sua vez, é o juízo de censura à conduta do agente, que deve ser analisado à luz da intenção (dolo) ou da negligência (culpa).

Com o advento da modernidade e o avanço das tecnologias, especialmente a partir da revolução industrial e, mais recentemente, com a chamada "quarta revolução industrial", o conceito de responsabilidade civil foi desafiado. O filósofo Ulrich Beck propôs o conceito de "sociedade de risco", onde os avanços tecnológicos e científicos, embora tragam benefícios, também criam novos tipos de risco que podem ameaçar a segurança e a qualidade de vida. Esses riscos são frequentemente invisíveis e incertos, o que exige uma transformação na maneira como as responsabilidades são atribuídas.

A responsabilidade objetiva, especialmente no contexto de atividades que envolvem risco, reflete uma nova abordagem, em que o agente deve se responsabilizar pelos danos decorrentes de sua atividade, independentemente de culpa. Nesse sentido, Clovis do Couto e Silva, citado por Rosenvald, argumenta que

a justiça distributiva deve prevalecer, com a responsabilidade recair sobre quem assumiu o risco.

A evolução da responsabilidade civil também se reflete na construção do conceito de autonomia da vontade, amplamente defendido no Iluminismo e consagrado no Código Civil francês de 1804. No modelo clássico de responsabilidade, o agente que causasse danos precisava demonstrar que não houve culpa em sua conduta. No entanto, o desafio atual é conciliar a liberdade individual, garantida pela autonomia da vontade, com a necessidade de responsabilizar aqueles que, ao exercer essa liberdade, causam danos a outrem.

Como observam Rosenvald, Farias e Neto, os danos causados no exercício da liberdade de ação devem ser reparados, a menos que o agente prove que não há nexo entre sua vontade e o dano. O Direito, portanto, deve equilibrar a liberdade com a necessidade de proteção dos direitos alheios.

É importante destacar que a LGPD, não foi clara quanto à natureza do regime de responsabilidade civil aplicável aos agentes de tratamento. No entanto, a referida lei deixa explícito que o tratamento inadequado de dados acarretará, conforme os termos legais, a responsabilidade dos agentes de tratamento, conforme argumentam Santo, Silva e Padrão (2021). Por ser uma legislação de caráter principiológico, cujo principal objetivo é a proteção plena dos titulares dos dados, a LGPD fundamenta-se na responsabilidade civil objetiva. Assim, os titulares têm o direito de serem indenizados com base na teoria do risco, conforme os autores mencionados.

Santos, Silva e Padrão também destacam que a interpretação principiológica da LGPD não se baseia apenas na análise dos princípios e na interpretação sistemática da lei, mas que esses elementos, por si só, são suficientes para definir a abordagem do tratamento de dados e a correspondente responsabilização em caso de danos. Nesse sentido, os autores citam Caitin Mulholland, que afirma que o legislador buscou identificar as situações danosas originadas especificamente de incidentes de segurança. Estes, por sua vez, estão relacionados ao risco inerente ao processo de tratamento de dados, como vazamentos não intencionais e invasões de sistemas e bases de dados por terceiros não autorizados. Este pensamento é compartilhado por Danilo Doneda e Laura Mendes, citados por Santos, Silva e Padrão, no que diz respeito a *“encerra um risco intrínseco, na medida em que há uma potencialidade danosa considerável em caso de violação desses direitos, que se caracterizam por sua natureza de direito personalíssimo e de direito fundamental”.*

À medida que a sociedade se transforma, a responsabilidade civil deve se adaptar, enfrentando os desafios impostos pela inovação tecnológica, pelo capitalismo de vigilância e pela crescente complexidade das relações sociais. A responsabilidade objetiva se apresenta como uma resposta necessária aos riscos modernos, enquanto os princípios fundamentais, como a dignidade humana e a autonomia da vontade, continuam a orientar a evolução do Direito.

A reflexão sobre a responsabilidade civil, portanto, não se limita apenas ao campo da reparação dos danos, mas envolve também questões éticas, sociais e filosóficas que exigem uma visão abrangente da função do Direito na proteção dos direitos fundamentais e na construção de uma sociedade mais justa e equilibrada.

Com a crescente expansão das tecnologias de informação e comunicação (TICs), especialmente no campo da Inteligência Artificial, surgem questões fundamentais que impactam a vida dos cidadãos, sendo crucial explorar temas como o direito à privacidade e a proteção de dados pessoais sensíveis.

Embora a IA traga benefícios significativos, dependendo de sua aplicação, é impossível negar que, sem a imposição de limites e regras claras — nas quais princípios como não discriminação e transparência sejam primordiais — os direitos fundamentais estarão em risco de serem violados.

Além disso, é importante destacar os potenciais riscos que surgem na ausência de regulamentação sobre o uso da IA, situação que pode levar ao ultrapassamento de limites constitucionais, afetando diretamente a privacidade e a intimidade dos indivíduos.

Quando se aborda o risco e o impacto para os titulares dos dados, fica claro que esses riscos estão intimamente relacionados às atividades que envolvem dados pessoais. No caso específico deste estudo, que foca em dados pessoais sensíveis, como os dados de saúde, é impossível dissociar a atividade de assistência à saúde da coleta, transformação, compartilhamento e armazenamento desses dados.

De maneira similar, dado que o risco é intrínseco à atividade de assistência à saúde, é claro que se trata de uma responsabilidade objetiva. Isso significa que a lesão ao paciente — titular dos dados — configura uma obrigação de reparação, independentemente de culpa. O impacto da utilização indevida desses dados pessoais sensíveis pode ser devastador, a ponto de permitir que a inteligência artificial construa perfis dos titulares, resultando, por exemplo, na negativa de adesão a planos de saúde devido a condições genéticas que indicam doenças caras de serem tratadas.

Isso configura a violação de um dos princípios fundamentais da LGPD, como a não discriminação e a autodeterminação informada.

Ou seja, conforme Azevedo e Silva (2024), à medida que a IA se integra cada vez mais às nossas vidas, aumenta o risco de perpetuar desigualdades já existentes ou criar formas de exclusão e discriminação. Esse problema se agrava ainda mais em um contexto em que a implementação da tecnologia não é acompanhada de maior transparência e clareza sobre os métodos utilizados para alcançar seus resultados. O desafio, portanto, é assegurar que, nesse processo de evolução, as tecnologias sejam utilizadas de forma responsável, ética e sustentável.

É relevante notar, conforme Azevedo e Silva, que a falta de transparência e a incapacidade de explicação não apenas minam a confiança na IA, mas também impõem desafios consideráveis para reguladores e formuladores de políticas públicas.

CONCLUSÃO

Com o avanço contínuo das tecnologias de informação e comunicação (TICs), especialmente no campo da Inteligência Artificial, que exige o uso de grandes volumes de dados pessoais e sensíveis, surgem questões cruciais que impactam diretamente a vida dos cidadãos. Nesse cenário, é fundamental discutir temas como o direito à privacidade, a proteção de dados pessoais sensíveis e a necessidade de regulamentações adequadas para assegurar a proteção dos direitos fundamentais.

Embora a IA ofereça benefícios significativos, dependendo da sua aplicação, não se pode negar que, sem a imposição de limites e regras claras — nas quais princípios como não discriminação e transparência sejam centrais — os direitos fundamentais correm o risco de ser violados.

Além disso, é importante destacar os riscos que surgem na ausência de regulamentação sobre o uso da IA, o que pode levar ao ultrapassamento de limites constitucionais, afetando diretamente a privacidade e a intimidade dos indivíduos.

Ao abordar os riscos e impactos para os titulares de dados pessoais sensíveis, especialmente na área da saúde, fica evidente que esses riscos estão intimamente ligados às atividades que envolvem esses dados. No caso deste estudo, que foca em dados pessoais sensíveis, como os dados de saúde, é impossível dissociar a prática de assistência à saúde da coleta, transformação, compartilhamento e armazenamento desses dados.

De forma semelhante, sendo esse risco inerente à atividade de assistência à saúde, é claro que se trata de uma responsabilidade objetiva. Ou seja, qualquer lesão ao paciente — o titular dos dados — implica uma obrigação de reparação, independentemente de culpa.

Associados à própria natureza de risco da atividade de saúde, os avanços tecnológicos e científicos têm impactado significativamente esse setor. No entanto, esses avanços também trazem grandes riscos, que ameaçam a segurança dos dados pessoais sensíveis, o direito à autodeterminação informada e o direito fundamental à vida privada, inclusive no ambiente digital.

Para garantir a proteção desse direito fundamental, é essencial que exista uma regulamentação que estabeleça regras claras e respeite os limites constitucionais. As atividades na área da saúde devem usar a Inteligência Artificial de forma apropriada, com objetivos, contextos e finalidades bem definidos.

Particularmente em relação aos dados pessoais sensíveis, como os dados de saúde, o uso da IA deve ser conduzido de maneira que não cause danos ao indivíduo. Esse ponto é ainda mais relevante quando se considera a história de violações desses direitos, que resultaram em sofrimento humano significativo. Tais acontecimentos impulsionaram a criação de medidas para assegurar que o desenvolvimento e o crescimento da tecnologia ocorram dentro de limites éticos, respeitando sempre os direitos fundamentais de todos.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988

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: 09 nov. 2024.

BRASIL. Projeto de Lei n.2338/2023. Dispõe sobre o uso da Inteligência Artificial. Disponível em [https://www25.senado.leg.br/web/atividade/materias/-/materia/157233]. Acesso em: 09 nov. 2024.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais [livro eletrônico] / Danilo Doneda. 3. ed. São Paulo: Thomson Reuters Brasil, 2021

GUTIERREZ, Andrei, GODINHO, Gustavo e KRASTINS, Alexandra. Comentários ao EU AI Act: uma abordagem prática e teórica do artificial Intelligence Act da União Europeia / coordenação Rony Vainzof...[et al.]. –São Paulo: Thomson Reuters Brasil, 2024

Nunes H da C, Guimarães RMC, Dadalto L. Desafios bioéticos do uso da inteligência artificial em hospitais. Rev Bioét [Internet]. 2022Jan;30(1):82–93. Available from: https://doi.org/10.1590/1983-80422022301509PT

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Rios RR. Tramas e interconexões no Supremo Tribunal Federal: Antidiscriminação, gênero e sexualidade. Rev Direito Práx [Internet]. 2020Apr;11(2):1332–57. Available from: https://doi.org/10.1590/2179-8966/2020/50276

RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROSENVALD, Nelson. As funções da responsabilidade civil - DIG. 3ª edição. Rio de Janeiro: Saraiva Jur, 2017. E-book. pág.17. ISBN 9788547218249. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788547218249/. Acesso em: 09 nov. 2024.

ROSENVALD, Nelson. As Funções da Responsabilidade Civil. 4ª edição. Rio de Janeiro: Saraiva Jur, 2024. E-book. pág.1. ISBN 9786555598902. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786555598902/. Acesso em: 09 nov. 2024.

ROSENVALD, Nelson; FARIAS, Cristiano Chaves de; NETTO, Felipe Peixoto B. Novo Tratado de Responsabilidade Civil. 4ª edição. Rio de Janeiro: Saraiva Jur, 2019. E-book. pág.616. ISBN 9788553612086. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788553612086/. Acesso em: 09 nov. 2024.

Saldanha, R. de F., Barcellos, C., & Pedroso, M. de M. (2021). Ciência de dados e big data: o que isso significa para estudos populacionais e da saúde? *Cadernos Saúde Coletiva*, *29*(spe), 51–58. https://doi.org/10.1590/1414-462X202199010305

SANTOS, Camila Ferrai, SILVA, Jeniffer Gomes, PADRÃO, Vinicius. Responsabilidade Civil pelo Tratamento de dados pessoais na Lei Geral de Proteção de dados. – Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro – PGE-RJ, Rio de Janeiro, v. 4n. 3, set/dez. 2021. - ISSN 2595-0630 (DOI): 10.46818/v4i3.256

TEFFÉ, Chiara Spadaccini. Dados Pessoais Sensíveis: qualificação, tratamento e boas práticas / Chiara Spadaccini de Teffé. – Indaiatuba, SP: Editora Foco, 2022. ISBN: 978-65-5515-582-2.

VIEIRA, Elba Lúcia de Carvalho, SANTANA, Gustavo Alpoim, MELLO, Ricardo Coutinho. Privacidade na coleta de dados pessoais sensíveis de pacientes: uma análise do uso da inteligência artificial na saúde pública.