

**A COLETA DAS  
INFORMAÇÕES PESSOAIS  
PELA INTELIGÊNCIA  
ARTIFICIAL E A  
COMERCIALIZAÇÃO DA ÍRIS  
COMO DESAFIO À  
PROTEÇÃO DE  
PRIVACIDADE**

**THE COLLECTION OF PERSONAL INFORMATION BY ARTIFICIAL  
INTELLIGENCE AND THE COMMERCIALIZATION OF THE IRIS AS A  
CHALLENGE TO PRIVACY PROTECTION**

Ciências Sociais Aplicadas • 16/09/2026

REGISTRO DOI: [10.70773/revistatopicos/789523572](https://doi.org/10.70773/revistatopicos/789523572)

---

Carla Cristina Alves Moura<sup>1</sup>

João Marcos Silva Pessoa<sup>2</sup>

Rosália Maria Carvalho Mourão<sup>3</sup>

---

## RESUMO

O presente artigo aborda os desafios jurídicos e sociais decorrentes da coleta de dados pessoais por sistemas de inteligência artificial e da comercialização de dados biométricos, especialmente da íris, diante da necessidade de proteção da privacidade e dos direitos fundamentais. O estudo tem como objetivo analisar os impactos dessas práticas sobre os titulares dos dados e verificar a adequação dos instrumentos jurídicos brasileiros diante das novas formas de coleta, tratamento e utilização de informações pessoais. Para tanto, utiliza abordagem qualitativa, método dedutivo e pesquisa bibliográfica e documental, com análise de legislação, doutrina, produções acadêmicas, manifestações de órgãos reguladores e estudos de caso relacionados à temática. Os resultados indicam que a natureza única e imutável dos dados biométricos amplia os riscos decorrentes de sua utilização, especialmente quando o fornecimento ocorre mediante compensação econômica e sem plena compreensão de suas consequências. A análise também evidencia que a legislação brasileira oferece mecanismos relevantes de proteção, mas demanda constante aprimoramento, fiscalização e medidas preventivas para acompanhar a evolução tecnológica. Conclui-se que a proteção efetiva dos dados pessoais depende da adequação normativa, da atuação dos agentes responsáveis pelo tratamento e do fortalecimento da educação digital dos titulares.

**Palavras-chave:** Inteligência artificial; Dados biométricos; Proteção de dados pessoais; Privacidade; Direitos fundamentais.

## ABSTRACT

This article addresses the legal and social challenges arising from the collection of personal data by artificial intelligence systems and the commercialization of biometric data, particularly iris data, in view of the need to protect privacy and fundamental rights. The

study aims to analyze the impacts of these practices on data subjects and assess the adequacy of Brazilian legal instruments in light of new forms of collecting, processing, and using personal information. To this end, it adopts a qualitative approach, a deductive method, and bibliographic and documentary research, analyzing legislation, legal scholarship, academic publications, statements from regulatory bodies, and case studies related to the topic. The results indicate that the unique and immutable nature of biometric data increases the risks arising from its use, especially when data provision occurs in exchange for financial compensation and without a full understanding of its consequences. The analysis also demonstrates that Brazilian legislation provides relevant protection mechanisms but requires continuous improvement, oversight, and preventive measures to keep pace with technological developments. It is concluded that effective protection of personal data depends on regulatory adequacy, the actions of data processing agents, and the strengthening of data subjects' digital literacy.

**Keywords:** Artificial intelligence; Biometric data; Personal data protection; Privacy; Fundamental rights.

## 1. INTRODUÇÃO

Com a evolução tecnológica e o crescente volume de dados disponíveis em rede, os sistemas de inteligência artificial têm se expandido significativamente, em razão disso, há um crescimento exponencial da dependência do ser humano às plataformas de IA.

A funcionalidade dessa rede tem sido disseminada, diversas pessoas todos os dias fazem uso desse meio, as plataformas vêm sendo treinadas diariamente para realizar tarefas com maior facilidade,

substituindo parte da mão de obra humana, dessa maneira, assumindo cada vez mais um papel significativo na vida das pessoas e empresas.

Os sistemas das inteligências artificiais são estruturados por coleta de informações, entende-se que quanto maior for a base de dados disponíveis, mais precisos e completos serão os resultados apresentados. Nesse contexto, observa-se que a coleta de dados é feita de forma gradual e inicialmente branda, com a disponibilização de informações pessoais fornecidas pelo próprio usuário durante sua pesquisa, podendo evoluir para um tratamento de dados mais específicos e sensíveis, com o objetivo de compreender as preferências do indivíduo e personalizar os serviços ofertados.

Ademais, é válido ressaltar que um dado biométrico é uma espécie de dado pessoal sensível, sendo assim, ele diz respeito sobre características físicas e genéticas utilizadas para identificar ou confirmar a identidade de uma pessoa de maneira mais segura, sendo essas características peculiares a cada indivíduo, necessitando de tratamento mais rigoroso, visando uma maior proteção jurídica no que concerne à sua coleta, armazenamento e utilização.

A disponibilização dos dados sensíveis está se expandindo e se tornando mais comum, nesse contexto, existem pessoas que vendem dados biométricos como a íris ocular por valores irrisórios, sem possuir plena compreensão acerca do objetivo dessa coleta. Conforme o Instituto Brasileiro de Defesa do Consumidor – IDEC (2025), verificou-se que no final do ano de 2024 e início do ano de 2025, indivíduos brasileiros aceitaram fornecer o escaneamento da sua íris em troca de compensações financeiras. Essa realidade

evidencia a vulnerabilidade dos titulares dos dados e suscita relevantes preocupações quanto a proteção da privacidade.

Além disso, a íris configura-se como um dado biométrico imutável e único, razão pela qual a sua comercialização pode ser vista como uma coisificação do corpo humano, assim, muitas vezes pessoas em situação de vulnerabilidade podem ser seduzidas por quaisquer valores que lhe sejam apresentados. De modo, a comprometer o direito à privacidade e à proteção dos dados pessoais, assegurados constitucionalmente pelo art. 5º, incisos X e LXXIX, bem como a dignidade da pessoa humana, princípio norteador da Constituição Federal.

Diante desse cenário, percebe-se que a crescente utilização de sistemas de inteligência artificial e a ampliação da coleta e do tratamento de informações pessoais constituem desafios relevantes para a proteção dos direitos dos titulares, a problemática torna-se ainda mais relevante quando se considera que muitos usuários fornecem informações sem plena clareza acerca da finalidade, da extensão do tratamento e das possíveis utilizações futuras desses dados.

Entende-se, portanto, que os dados estão se tornando mercadorias, apesar de sua natureza personalíssima, demonstrando a importância de um debate jurídico sobre os limites do fornecimento de informações para sistemas de inteligência artificial e sobre os impactos futuros que podem surgir em consequência da disponibilização dessas plataformas em livre acesso.

Desse modo, a presente pesquisa parte da necessidade de compreender em que medida a coleta de dados pessoais por

sistemas de inteligência artificial, aliada à comercialização de dados biométricos, configura um desafio à efetiva proteção da privacidade e à garantia dos direitos fundamentais na era digital.

A questão mostra-se relevante diante da necessidade de compreender se os instrumentos jurídicos atualmente existentes são suficientes para acompanhar as novas formas de coleta, tratamento e utilização de dados biométricos, bem como para identificar possíveis lacunas na proteção dos titulares, diante disso, questiona-se: em que medida os instrumentos jurídicos atualmente existentes no ordenamento jurídico brasileiro são suficientes para garantir a efetiva proteção da privacidade e dos direitos fundamentais dos titulares diante da coleta de informações pessoais por sistemas de inteligência artificial e da comercialização de dados biométricos?

Nesse contexto, torna-se necessário compreender o cenário em que ocorre a comercialização da íris e a coleta de informações pelas plataformas de inteligência artificial, considerando seus impactos jurídicos e sociais sobre os direitos fundamentais dos titulares, especialmente a privacidade e a autodeterminação informativa. A análise também envolve a legislação brasileira vigente, especialmente no tocante à proteção de dados pessoais, buscando verificar sua adequação diante das novas formas de utilização de dados biométricos e, a partir disso, contribuir para a identificação de eventuais lacunas normativas e para o desenvolvimento de medidas jurídicas capazes de mitigar os riscos decorrentes dessa utilização.

## **2. FUNDAMENTAÇÃO TEÓRICA**

## **2.1. Comercialização da Íris e Coleta de Dados Pela Inteligência Artificial**

Inicialmente, a venda da íris surgiu no Brasil a partir da atuação da empresa Tools for Humanity, responsável pelo projeto World, que já se encontrava presente na realidade de vários países, desenvolvendo essa mesma atividade, no entanto, a Autoridade Nacional de Proteção de Dados (ANPD), alegou que esse tipo de prática interfere na livre manifestação de vontade do indivíduo. De modo, que pessoas em situações de vulnerabilidade econômica podem enxergar essa oferta como uma alternativa viável, além de tal prática conflitar diretamente com o fundamento da dignidade da pessoa humana, previsto no Art. 1º, inciso III, da Constituição Federal.

Assim, se trata de uma informação personalíssima, ligada diretamente a dignidade da pessoa humana, mesmo que no âmbito digital, em virtude desses dados são exclusivos de cada pessoa, e ao momento que se disponibiliza como um produto para a venda, avilta a própria condição humana, como, por exemplo, a proibição da venda de órgãos, pois, caso tais práticas fossem permitidas no Brasil, na atual situação em que vivemos, isso poderia repercutir em diversos outros embates jurídicos.

Além disso, é importante observar que a comercialização da íris tem gerado repercussão no cenário internacional, especialmente diante de questionamentos quanto à conformidade dessa prática com normas de proteção de dados. Nesse sentido, de acordo com Jornal G1 (2024) autoridades europeias passaram a adotar medidas mais rigorosas, a exemplo da Espanha, onde foi determinado que a empresa responsável pelo escaneamento de íris excluísse todos os

dados biométricos coletados, em razão de possíveis violações as regras de proteção de dados.

Dessa maneira, fica evidente a crescente preocupação com o tratamento inadequado de dados sensíveis e reforça a necessidade de um controle mais efetivo sobre essa atividade, assim, há a demonstração de que a comercialização desses dados, além de suscitar debates éticos, também enfrenta barreiras jurídicas relevantes, especialmente quando não observado o princípio da transparência e proteção dos direitos dos titulares.

Paralelamente a esse cenário, a coleta de dados pelas plataformas de inteligência artificial tem se intensificado, tornando-se essencial para o funcionamento dessas tecnologias, segundo Doneda (2020), o tratamento de dados pessoais ocorre de forma cada vez mais integrada às atividades digitais cotidianas, muitas vezes sem plena consciência do titular quanto à extensão dessa coleta, de modo que fica evidente que esse processo ocorre de forma contínua, permitindo o aprimoramento dos serviços e contribuindo para a naturalização da coleta de dados no ambiente virtual.

Nesse contexto, a coleta de dados não se limita a informação básica, evoluindo para a análise detalhada do comportamento do usuário, a partir das interações realizadas, os sistemas de inteligência artificial, conseguem identificar padrões e construir perfis digitais cada vez mais precisos, como afirmar Bioni (2021, p. 358) que “os nossos dados pessoais redimensionam, portanto, a autonomia e o livre desenvolvimento da personalidade de cada um de nós”, assim, os dados passam a ser utilizados de forma estratégica, ampliando o poder das plataformas sobre a experiência do usuário.

Dessa forma, verifica-se que a evolução da coleta de dados alcança informações sensíveis, como a íris, que, por serem únicas e imutáveis, apresentam elevado valor econômico e maiores riscos em caso de uso indevido, intensificando as preocupações com a proteção de privacidade.

## **2.2. Impactos aos Direitos Fundamentais**

Cumpramos observar que, por se tratar de algo totalmente novo, não há previsão acerca do que pode ocorrer caso seja permitida a venda desses dados, uma vez que se desconhece o destino que lhes será dado. Isso pode resultar no uso indevido da identidade por terceiros, no vazamento de informações, no acesso não autorizado a contas, entre diversas outras possíveis implicações. Assim, ao renunciar aos próprios dados, o indivíduo se submete a toda sorte de riscos.

Ademais, a comercialização da íris como de outros dados biométricos intensifica ainda mais as preocupações que pode vir a surgir no âmbito jurídico e ético, sobretudo por se tratar de um identificador único diretamente vinculado à identidade do indivíduo.

Nesse cenário, a utilização dessa tecnologia amplia de forma significativa os riscos à privacidade, na medida em que possibilita a identificação precisa e contínua do usuário, conforme leciona Lima (2020, p. 32):

*[...] a tecnologia funciona como um código de barras, o que torna possível a identificação do usuário na Internet, assim como de um produto na prateleira de um supermercado. Mas, com a possibilidade de o localizar por radiofrequência, compromete-se a proteção da vida privada e dos dados pessoais dos usuários.*

Desse modo, a eventual permissão para a venda desses dados não apenas reforça a lógica de mercantilização do corpo humano, mas também expõe o titular a riscos contínuos e irreversíveis, considerando que, diferente de outros dados, a íris não pode ser alterada em caso de vazamento ou uso indevido.

Destaca-se a grande vulnerabilidade do titular dos dados, sobretudo da população economicamente desfavorecida, diante da possibilidade de comercialização de dados biométricos. Em muitos casos, a necessidade financeira pode levar esses indivíduos a consentirem com a cessão de seus dados sem a plena compreensão dos riscos envolvidos.

Nesse sentido, Zuliani (2012) entende ser necessária uma regulamentação mais específica, baseado no crescimento do setor digital e na vulnerabilidade dos usuários. Assim, cria-se um cenário de exploração indireta, em que a desigualdade social funciona como fator determinante para disposição de dados sensíveis, transformando a privacidade em um bem negociável.

Diante disso, a aparente autonomia do titular é relativizada, uma vez que sua escolha pode estar condicionada por necessidades imediatas, deixando claro a fragilidade que demanda maior atenção

do ordenamento jurídico para evitar abuso e assegurar a efetividade da proteção dos direitos fundamentais, como previsto na Constituição Federal no seu Art. 5º, inciso X que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas”. Dessa maneira, a proteção constitucional reforça a necessidade de limites claros à utilização e à comercialização desses dados, evitando que a condição de vulnerabilidade econômica seja explorada.

Outrossim, é possível evidenciar de forma clara a vulnerabilidade informal e econômica dos indivíduos diante a crescente monetização de dados biométricos, conforme o relatado em uma reportagem da CNN Brasil (2025).

**Figura 1.** Manchete CNN Brasil riscos de escanear a íris

**Conheça o que está por trás e os riscos de escanear a íris por dinheiro**

Tools for Humanity desenvolve o projeto World ID, um sistema que se vale dos padrões da íris para criar um código de validação, impossível de ser reproduzido por inteligência artificial

**Da CNN Brasil\***

20/01/25 às 15:25 | Atualizado 29/01/25 às 17:42

**Fonte:** Jornal CNN Brasil

Conforme destacado na mesma reportagem, o motoboy Bruno Barbosa Souza, afirmou ter aderido ao escaneamento da íris após indicação de uma colega, sendo atraído principalmente pela promessa de ganho financeiro rápido, sem compreender a finalidade da coleta de seu dado biométrico.

De igual modo, ao descrever o procedimento como simples, apenas realizando um cadastro em aplicativo e com o fornecimento de dados pessoais e consequente agendamento para o escaneamento, deixa claro a facilidade de acesso a esse tipo de serviço, dessa

maneira, a possibilidade de recebimento quase imediato do valor aproximado de R\$450,00 demonstra que fatores econômicos podem influenciar diretamente a decisão do titular. Assim o caso concreto ilustra a fragilidade do consentimento prestado, uma vez que ocorre sem devido esclarecimento, comprometendo sua validade e colocando em risco direitos fundamentais relacionados a proteção e privacidade de dados pessoais.

Nessa perspectiva, a coleta de dados pelas plataformas de inteligência artificial também merece destaque na discussão, pois apresente um fator relevante de impacto aos direitos fundamentais, na medida em que ocorre de forma contínua e, muitas vezes, sem plena percepção do titular.

A partir do uso cotidiano de aplicativos e sistemas digitais, informações relacionadas a hábitos, preferências e comportamentos passam a ser constantemente registradas e analisadas, ampliando de forma significativa o nível de exposição do indivíduo no ambiente digital, sendo que, conforme Mendes (2019), a proteção de dados pessoais constitui instrumento essencial para a tutela dos direitos da personalidade no ambiente digital, assim, os riscos anteriormente associados à comercialização de dados se estendem à própria dinâmica de coleta, que por sua natureza silenciosa intensifica as violações à privacidade.

Nesse contexto, tal prática compromete diretamente à autodeterminação informativa, uma vez que o titular nem sempre possui controle efetivo sobre quais dados estão sendo coletado e de que forma serão utilizados. A complexidade dos sistemas de inteligência artificial, aliada à ausência de transferência em muitos casos, dificulta a compreensão e a tomada de decisões conscientes

por parte do indivíduo, o que contraria diretamente a proteção assegurada pela Constituição Federal de 1988, que dispõe:

*Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*

*[...]*

*X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;*

Dessa forma, ainda que exista um consentimento formal, este pode se mostrar fragilizado, evidenciando a necessidade de maior proteção jurídica para assegurar a efetividade dos direitos fundamentais no ambiente digital.

### **2.2.1. Vigilância Digital e Riscos de Monitoramento Constante**

A crescente utilização de dados biométricos, como a íris, insere o indivíduo em um contexto de potencial vigilância digital contínua, na medida em que as informações proporcionam sua identificação de forma precisa em diferentes ambientes e plataformas, esse cenário já se mostra concreto na realidade, conforme demonstrado na Figura 2, que evidencia a adesão ao escaneamento de íris em escala global, com ênfase para a América Latina, onde, dos mais de 10 milhões de registros realizados, aproximadamente 6,7 milhões concentram-se nessa região.

**Figura 2.** Expansão global do escaneamento de íris e distribuição de usuários da plataforma



**Fonte:** Worldcoin.

Esse cenário contribui para a formação de uma verdadeira sociedade de vigilância, que a coleta massiva de dados se torna prática comum e naturalizadas, nesse raciocínio, o indivíduo, deixa de ser apenas usuário de serviços digitais e passa a ser observado e categorizado, gerando impactos na forma como os direitos fundamentais são exercidos no ambiente digital.

Além disso, a possibilidade de monitoramento constante tende a influenciar diretamente o comportamento dos indivíduos, que passam a agir de forma mais esquematizada diante da vigilância, esse fenômeno compromete a privacidade, liberdade de expressão e autonomia pessoal, que são pilares do Estado Democrático de Direito. Nesse sentido, existe a lógica do panoptismo desenvolvida por Foucault (1987, p. 224), segundo o qual “a visibilidade é uma armadilha”, na medida que o indivíduo, ao se perceber potencialmente vigiado, passa a internalizar o controle de regular suas condutas.

Cumprir destacar que, esses dados podem ser utilizados tanto por empresas quanto pelo próprio Estado, o que amplia ainda mais os riscos envolvidos, no âmbito privado, há utilização para fins comerciais, enquanto, na esfera pública, pode haver o emprego para controle social e segurança, levantando questionamentos quanto aos limites dessa atuação e à necessidade de mecanismos eficazes de proteção dos direitos fundamentais frente ao avanço tecnológico.

### **2.3. Proteção de Dados na Legislação Brasileira**

No direito digital, a definição de dados pessoais e dados sensíveis constitui um elemento fundamental para a compreensão da insegurança jurídica existente na coleta e comercialização das informações e dados, nesse sentido, a Lei Geral de Proteção de Dados estabelece que:

*Art. 5º Para os fins desta Lei, considera-se:*

*I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;*

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

A partir da distinta normativa, observa-se que os dados biométricos, como a íris, estão classificados como dados pessoais sensíveis, demandando, portanto, uma fiscalização e proteção jurídica mais rigorosa, especialmente diante os avanços das tecnologias da

inteligência artificial, como a previsão do Art. 11, §3º da Lei Geral de Proteção de Dados:

*Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:*

*(...)*

*§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências (Brasil, 2018).*

Diante do texto legal apresentado, é nítida a ligação com o comércio da íris, em que o poder público tem respaldo legal para barrar esse tipo de negócio, não para ocasionar problemas a população, mas para evitar futuros embates, além de que esse conteúdo está ligado diretamente a preceitos fundamentais, bem como, a empresa oferecia vantagens econômicas em troca do fornecimento desse dado.

Ademais, a inteligência artificial vem ganhando cada vez mais espaço em meio a sociedade e estabelecendo uma certa relação de dependência, na qual as pessoas usam indiscriminadamente sem restringir as informações que se é solicitado, pois quando fazem o seu uso, fornecem vários dados pessoais de identificação, inclusive fatos e acontecimentos de suas vidas, no entanto, sempre ao acessarem uma dessas plataformas e antes de começarem propriamente dito a sua aplicação, lhes é solicitado várias autorizações, sendo que sequer fazem a leitura do que estão

consentido, e simplesmente começam um fornecimento, como se visualiza por meio do Art. 7, I da LGPD, “o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular.”

Assim, essa coleta desmedida ocorre em razão da ausência de uma limitação mais rigorosa à liberdade das empresas na captação de dados que não são necessários aos objetivos para os quais foram obtidos, o que acaba por abranger informações pessoais relevantes, mas dispensáveis naquele contexto.

No que se refere aos direitos do titular, o Art. 18 da LGPD, estabelece um conjunto de garantias que visam assegurar maior controle do indivíduo sobre suas informações pessoais. Dentre esses direitos, destacam-se o acesso aos dados tratados, a possibilidade de correção de informações incompletas ou desatualizadas, bem como a eliminação de dados desnecessários ou tratados em desconformidade com a lei.

Além disso, a legislação também prevê o direito à portabilidade dos dados a outro fornecedor de serviço ou produto, ampliando a autonomia do titular sobre suas informações. Tais prerrogativas reforçam a ideia de que o indivíduo não deve ocupar uma posição passiva no tratamento de seus dados, mas sim atuar como sujeito de direitos, podendo intervir sempre que necessário para resguardar sua privacidade e garantir a adequada utilização de suas informações.

Com relação a proteção de dados no ordenamento jurídico, o Art. 5º, LXXIX da CF, assegura o direito fundamental à proteção de dados pessoais, garantindo ao titular uma proteção jurídica sobre suas

informações, mas na prática essa segurança nem sempre se concretiza de forma efetiva. Isso porque, de acordo com o Art. 5º, VI, da LGPD, as empresas que atuam como controladoras são responsáveis pelas decisões sobre o tratamento desses dados, o que lhes confere uma posição de destaque dentro dessa relação.

Na realidade, essas empresas, especialmente as de grande porte e ligadas à inteligência artificial, possuem maior poder econômico, tecnológico e organizacional, o que acaba gerando um desequilíbrio em relação ao titular dos dados. Assim, mesmo existindo uma garantia constitucional, ela muitas vezes permanece mais no plano teórico, já que os controladores detêm uma liberdade maior na forma como coletam e utilizam as informações, nem sempre observando, com o rigor necessário, os limites impostos pela legislação. Dessa forma, percebe-se que a proteção assegurada ao indivíduo pode se mostrar fragilizada diante desse cenário, o que evidencia a necessidade de uma aplicação mais efetiva das normas de proteção de dados.

Diante desse cenário, embora já exista um embasamento jurídico relevante voltado à proteção de dados pessoais, tanto em nível constitucional quanto infraconstitucional, percebe-se que a simples previsão normativa não é suficiente para assegurar, por si só, a efetividade dessas garantias. Torna-se necessário, portanto, não apenas o aprimoramento contínuo dessas normas, mas também a atuação mais firme do poder público, especialmente por meio de mecanismos de fiscalização e controle, a fim de reduzir o desequilíbrio existente entre os titulares e os agentes de tratamento e garantir que a proteção de dados se concretize de forma real no cotidiano.

No âmbito das punições normativas da Lei Geral de Proteção de Dados, destaca-se a previsão de sanções administrativas como meio para assegurar o cumprimento de suas diretrizes, nos termos do Art. 52 da LGPD, a legislação estabelece a possibilidade de aplicação de medidas como advertências e multas, que podem alcançar valores expressivos, além do bloqueio e da eliminação dos dados pessoais relacionados à infração, em vista disso, evidenciam - se as preocupações do legislador em conferir coercitividade às normas de proteção de dados, indo além de uma previsão meramente declaratória.

Nesse sentido, as sanções administrativas assumem papel relevante ao atuar como forma de desestimular práticas irregulares por parte dos agentes de tratamento, especialmente em contextos que envolvem o uso de tecnologias como a inteligência artificial, Ao prever consequências concretas para o descumprimento da legislação, a LGPD busca equilibrar a relação entre titulares e controladores, reforçando a necessidade de observância dos limites legais e contribuindo para a efetiva proteção dos dados pessoais no ambiente digital.

## **2.4. Lacunas e Diretrizes Regulatórias para a Proteção de Dados**

Faz-se necessário suscitar que existem limitações legais para o comércio da íris, assim como de qualquer outro dado biométrico, no entanto, na visão de Eugen Ehrlich (1913), o direito não se desenvolve por conta própria, mas ele surge da necessidade da população, assim, o direito sempre é posterior ao fato, pois ele depende que de uma carência da sociedade, se originando uma morosidade processual.

Ademais, o que se refere ao tratamento de dados, o Brasil ainda é iniciante nessa área, de modo que as previsões legais são, muitas vezes, limitadas, pouco rigorosas ou, em determinados casos, até inexistentes.

Em consequência, é imprescindível uma maior adequação e um acompanhamento mais célere as necessidades legais, assim, é válido citar o Projeto de Lei nº 36/2025, que traz em seu texto a especificação dos dados biométricos, além de uma previsão clara sobre a sua comercialização, e prevê expressamente a proibição quanto a sua venda, e mais importante ainda, detalha as infrações para quem infringir a disposição legal, a Lei Geral de Proteção de Dados estabelece diretrizes para essas questões, mas por falta de uma clareza sobre o tema, acaba por gerar lacunas que podem ser exploradas por empresas.

Além disso, a própria lógica de monetização de dados biométricos, tende a transformar atributos corporais em ativos econômicos, o que levanta discussões éticas e jurídicas relevantes acerca da indisponibilidade de alguns direitos da personalidade, ainda que a legislação brasileira, em especial a Lei Geral de Proteção de Dados, estabeleça princípios como finalidade, necessidade e transparência, sua aplicação prática enfrenta desafios.

Nesse sentido, a lacuna regulatória não apenas fragiliza a proteção do titular, mas também reforça a necessidade de interpretação mais rigorosas e de complementação normativa capaz de acompanhar a complexidade das novas formas de exploração de dados sensíveis.

No que se refere à proteção, a Lei Geral de Proteção de Dados adota uma forma que vai além, trazendo o princípio da prevenção, previsto

no Art. 6º. Esse princípio determina aos agentes de tratamento, o controlador e o operador, o dever de adotar medidas capazes de evitar a ocorrência de prejuízos antes mesmo da sua ocorrência, o que se mostra relevante no contexto da inteligência artificial.

Dessa maneira, o Art. 38 da LGPD prevê a elaboração do relatório de impacto à proteção de dados pessoais, dispositivo que tem como finalidade antecipar riscos e avaliar as consequências do tratamento, funcionando como mecanismo de controle prévio.

Sob essa perspectiva, esse trabalho preventivo busca evitar que o dano ocorra, ao invés de apenas reagir, o que se demonstra mais eficaz diante da atividade complexa do tratamento de dados. Assim, a proteção de dados pessoais não pode se limitar a medidas reparatórias, sendo essencial a implementação de mecanismos preventivos que assegurem, desde o início, o respeito aos direitos dos titulares.

No que diz respeito à responsabilidade, no Art. 42 da Lei Geral de Proteção de Dados, dispõe que o agente de tratamento que causar dano patrimonial, moral, individual ou coletivo em decorrência do tratamento de dados pessoais é obrigado a repará-lo. Essa previsão se relaciona diretamente com a teoria do risco, segundo a qual aquele que desenvolve atividade que possa gerar danos a terceiros deve assumir as consequências de sua atuação. No contexto da inteligência artificial, em que o tratamento de dados ocorre de forma automatizada e em larga escala, essa responsabilidade ganha ainda mais relevância.

Sob esse ponto de vista, se aproxima da responsabilidade objetiva aplicada às atividades de risco, sem a necessidade de comprovação

da culpa, especialmente diante da complexidade dos sistemas utilizados. Assim, as empresas que utilizam inteligência artificial devem responder pelos danos causados em razão do tratamento de dados, garantindo maior proteção aos titulares e equilíbrio nas relações jurídicas.

No que se refere à efetividade da proteção de dados pessoais, a educação digital revela-se como elemento essencial para o fortalecimento da autonomia do titular em relação ao tratamento de suas informações. Isso porque, conforme aponta Bruno Bioni:

*Trata-se, portanto, de promover o encontro entre o arranjo jurídico-normativo da privacidade informacional com a realidade que lhe é subjacente, buscando-se novas formas para o venerado consentimento do titular dos dados pessoais, nutrindo-se, em última análise, a sua capacidade (autonomia) em controlá-los (2019, p. 256).*

Nesse sentido, percebe-se que a simples previsão normativa não é suficiente, sendo necessário que o titular possua conhecimento e compreensão acerca do tratamento de seus dados para que possa exercer, de forma efetiva, esse controle.

Dessa forma, a educação digital surge como instrumento indispensável para concretizar essa autonomia, permitindo que o indivíduo entenda as consequências do uso da inteligência artificial e até onde as informações que fornece podem chegar, assim, mais do que normas, torna-se necessária a promoção de meios para capacitar o titular, possibilitando o exercício real dos direitos no ambiente digital.

### **3. METODOLOGIA**

#### **3.1. Método de Abordagem**

O presente estudo adota uma abordagem qualitativa, uma vez que busca analisar e interpretar os impactos jurídicos e sociais da comercialização de dados biométricos, especialmente a íris, bem como a coleta de dados pessoais por sistemas de inteligência artificial, à luz da proteção dos direitos fundamentais. Dessa maneira, não há a intenção de quantificar dados, mas sim de compreender o fenômeno em sua complexidade, a partir de uma perspectiva crítica e interpretativa.

No que se refere ao método de abordagem, utiliza-se o método dedutivo, partindo de premissas gerais relacionadas à proteção dos direitos fundamentais e à tutela de dados pessoais, para analisar situações específicas, como a coleta de dados por sistemas de inteligência artificial e a comercialização da íris.

#### **3.2. Técnicas de Pesquisa**

A pesquisa caracteriza-se como bibliográfica e documental; bibliográfica, pois se fundamenta em livros, artigos científicos e produções acadêmicas que abordam o Direito Digital, a proteção de dados pessoais e os direitos fundamentais; e documental, na medida em que analisa legislações pertinentes, como a Constituição Federal de 1988 e a Lei Geral de Proteção de Dados Pessoais (LGPD), além de materiais informativos relacionados à temática.

O estudo compreende, ainda, doutrina especializada, legislação vigente e manifestações de órgãos reguladores, como a Autoridade Nacional de Proteção de Dados (ANPD), bem como reportagens e

estudos de caso que evidenciam, na prática, a coleta e comercialização de dados biométricos.

Ressalta-se, ainda, a utilização de referenciais teóricos clássicos, como as contribuições de Eugen Ehrlich e Michel Foucault, cujas obras, embora não contemporâneas, apresentam conceitos fundamentais que permanecem atuais e aplicáveis ao debate proposto. A inserção desses autores justifica-se pela relevância de suas reflexões acerca da construção social do direito, respectivamente, demonstrando que, apesar da modernidade do tema, suas bases teóricas já eram discutidas há décadas.

Quanto aos procedimentos, a coleta de dados foi realizada por meio de levantamento bibliográfico e documental, seguida de análise qualitativa e interpretativa do conteúdo, com o objetivo de identificar lacunas normativas, avaliar os impactos jurídicos e sociais e propor possíveis diretrizes para o aprimoramento da proteção de dados pessoais no contexto da inteligência artificial.

## **4. RESULTADOS E DISCUSSÕES**

### **4.1. A Comercialização da Íris e a Vulnerabilidade do Titular**

A análise realizada demonstra que a comercialização da íris apresenta riscos em razão da natureza do dado biométrico, que é único e está diretamente relacionado à identificação do indivíduo. Diferentemente de informações que podem ser alteradas após um eventual vazamento, a íris não pode ser simplesmente substituída, o que aumenta os possíveis impactos decorrentes de sua utilização inadequada.

Nesse contexto, verificou-se que a oferta de vantagens econômicas em troca do fornecimento de dados biométricos pode comprometer a efetividade do consentimento, especialmente quando direcionada a indivíduos em situação de vulnerabilidade econômica. O caso apresentado na pesquisa, envolvendo o escaneamento da íris mediante compensação financeira, demonstra que a necessidade econômica pode influenciar diretamente a decisão do titular, fazendo com que a escolha seja realizada sem a plena compreensão das consequências do tratamento do dado.

#### **4.2. Coleta de Dados Pela Inteligência Artificial e Impactos aos Direitos Fundamentais**

A pesquisa também permitiu identificar que a coleta de dados realizada por sistemas de inteligência artificial ocorre de maneira contínua e pode alcançar informações relacionadas aos hábitos, preferências e comportamentos dos usuários, esse processo amplia a capacidade de formação de perfis digitais e, conseqüentemente, os riscos relacionados à privacidade e à autodeterminação informativa.

A análise dos materiais estudados demonstra que, embora o consentimento seja previsto pela LGPD como uma das hipóteses para o tratamento de dados pessoais, na prática, os usuários nem sempre possuem conhecimento suficiente sobre quais informações estão fornecendo, para qual finalidade serão utilizadas e quais consequências poderão decorrer desse tratamento.

Verificou-se, portanto, que o problema não está apenas na existência da coleta de dados, mas também na dificuldade de o titular exercer controle efetivo sobre suas próprias informações, além da

complexidade dos sistemas de inteligência artificial e a quantidade de dados envolvidos dificultam a compreensão do tratamento realizado, tornando necessária uma proteção que ultrapasse o simples fornecimento de consentimento.

#### **4.3. Limites da Proteção Jurídica e Lacunas Regulatórias**

A análise da Constituição Federal e da Lei Geral de Proteção de Dados demonstrou que o ordenamento jurídico brasileiro já dispõe de mecanismos relevantes para a proteção dos dados pessoais. A Constituição Federal reconhece a proteção de dados pessoais como direito fundamental, enquanto a LGPD estabelece princípios, direitos dos titulares, hipóteses de tratamento, mecanismos preventivos e sanções aplicáveis aos agentes de tratamento.

Entretanto, os resultados da pesquisa indicam que a existência dessas normas não significa que todos os problemas relacionados às novas tecnologias estejam solucionados. A rápida evolução da inteligência artificial e das formas de coleta e exploração de dados produz situações que exigem constante atualização e interpretação do ordenamento jurídico.

No caso específico da comercialização da íris, verifica-se que a natureza sensível do dado e a possibilidade de obtenção de vantagem econômica a partir de seu tratamento exigem atenção especial. A previsão do art. 11, § 3º, da LGPD demonstra que o legislador já reconhece a necessidade de controle sobre o compartilhamento de dados pessoais sensíveis com finalidade econômica. Entretanto, a pesquisa evidencia a necessidade de maior clareza normativa quanto às novas formas de exploração desses dados.

Nesse sentido, o Projeto de Lei nº 36/2025, analisado no decorrer da pesquisa, demonstra a existência de uma tentativa de acompanhar essas novas situações, especialmente ao estabelecer disposições mais específicas relacionadas aos dados biométricos e à sua comercialização.

Dessa forma, os resultados confirmam a existência de uma distância entre a evolução tecnológica e a capacidade de resposta do ordenamento jurídico. A proteção normativa existente constitui importante instrumento de tutela, mas necessita ser acompanhada por regulamentação, fiscalização e mecanismos capazes de responder às novas formas de coleta, tratamento e exploração dos dados pessoais.

#### **4.4. Medidas Necessárias para o Fortalecimento da Proteção de Dados**

A partir dos resultados obtidos, verifica-se que o fortalecimento da proteção dos dados pessoais depende não apenas da criação de novas normas, mas também da efetiva aplicação dos mecanismos já existentes.

Nesse aspecto, instrumentos como o princípio da prevenção, o relatório de impacto à proteção de dados pessoais e as sanções administrativas previstas na LGPD demonstram-se relevantes para antecipar riscos e responsabilizar os agentes que realizarem tratamento inadequado de dados.

Além disso, a pesquisa demonstra que a educação digital constitui mecanismo importante para o fortalecimento da autonomia dos titulares, a compreensão sobre quais informações são fornecidas, como são utilizadas e quais riscos estão relacionados ao seu

tratamento permite que o indivíduo exerça de maneira mais efetiva seus direitos. Assim, os resultados indicam que a proteção adequada depende da atuação conjunta do poder público, dos agentes de tratamento e dos próprios titulares. A fiscalização e o aprimoramento da regulamentação devem ser acompanhados de medidas destinadas a ampliar a informação e a conscientização dos usuários.

Diante do exposto, a análise realizada demonstra que a comercialização da íris e a coleta de dados pessoais por sistemas de inteligência artificial constituem desafios concretos à proteção da privacidade e dos direitos fundamentais. Embora a legislação brasileira ofereça instrumentos importantes de proteção, sua efetividade depende da constante adequação do ordenamento jurídico, da fiscalização dos agentes de tratamento e da capacidade do titular de compreender e exercer seus direitos.

## **5. CONSIDERAÇÕES FINAIS**

Verifica-se que o ordenamento jurídico brasileiro possui instrumentos importantes para a proteção dos titulares, especialmente a Constituição Federal de 1988 e a Lei Geral de Proteção de Dados Pessoais, entretanto, a existência de proteção normativa não é suficiente para acompanhar, de forma integral, a velocidade das transformações tecnológicas e as novas formas de coleta, tratamento e exploração de dados biométricos, nesse contexto, a pesquisa demonstra que o avanço da inteligência artificial amplia as possibilidades de utilização dessas informações, tornando necessário não apenas observar as normas já existente, mas também avaliar sua efetividade diante as atualizações tecnológicas que se tornam cada vez mais complexas.

Conclui-se que o consentimento do titular pode ser fragilizado quando associado à falta de informação ou à vulnerabilidade econômica. Essa situação torna-se ainda mais relevante no caso da íris, considerando sua natureza única e imutável e os riscos decorrentes de sua utilização inadequada, diferentemente de informações que podem ser modificadas pelo indivíduo, como senhas, os dados biométricos estão diretamente ligados as características do titular, tornando a exposição indevida e preocupante, algo que poderia ser evitado se foi manifestado informações claras acerca da finalidade da coleta, armazenamento e compartilhamento.

Além disso, a análise realizada deixa demonstrado a problemática da exploração econômica das informações, ampliando os riscos de violação à privacidade e autodeterminação informativa, desse modo, a proteção jurídica deve considerar todo o ciclo de utilização dos dados, e não somente o momento em que ocorre a coleta.

Dessa forma, os objetivos propostos são alcançados ao demonstrar que, embora existam mecanismos jurídicos destinados à proteção dos dados pessoais, ainda são necessárias medidas de aprimoramento normativo, fiscalização e prevenção para acompanhar as novas formas de utilização dos dados biométricos e da inteligência artificial.

Mostra-se necessário, portanto, fortalecer mecanismos de fiscalização e de responsabilização dos agentes de tratamento, bem como ampliar a transparência sobre finalidades da coleta e sobre as formas de utilização das informações, a adoção de medidas preventivas também se apresenta relevante, no que tange a

dificuldade de reparar integralmente os efeitos decorrentes de uma eventual utilização indevida de dados biométricos.

Por fim, a pesquisa evidencia que a proteção efetiva dos dados pessoais exige não apenas normas mais adequadas, mas também maior conscientização dos titulares e atuação efetiva dos agentes responsáveis pelo tratamento dessas informações, a preservação não deve depender apenas da capacidade do indivíduo de compreender termos e condições complexos, mas da atuação responsável dos agentes que coletam e tratam esses dados, assim, o desenvolvimento tecnológico deve ser acompanhado de mecanismos capazes de preservar a dignidade da pessoa humana, a privacidade e a autodeterminação informativa, garantindo que os benefícios proporcionados pela inteligência artificial não ocorram em detrimento dos direitos fundamentais dos titulares dos dados.

## REFERÊNCIAS BIBLIOGRÁFICAS

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

CNN BRASIL. **Conheça o que está por trás e os riscos de escanear a íris por dinheiro.** 2025. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/conheca-o-que-esta-por-tras-e-os-riscos-de-escanear-a-iris-por-dinheiro/>. Acesso em: 13 abr. 2026.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados.** 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

EHRLICH, Eugen. **Fundamentos da sociologia do direito.** Brasília: Editora Universidade de Brasília, 1913.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão.** Tradução de Raquel Ramalhete. 20. ed. Petrópolis: Vozes, 1987.

G1. **Espanha determina que World exclua todos os dados de íris escaneadas no país.** Publicado em: 19 dez. 2024. Disponível em: <https://g1.globo.com/tecnologia/noticia/2024/12/19/espanha-determina-que-world-exclua-todos-os-dados-de-iris-escaneadas-no-pais.ghtml>. Acesso em: 16 mar. 2026.

IDEC – Instituto Brasileiro de Defesa do Consumidor. **Venda da íris do olho: conheça os perigos por trás dessa prática.** Disponível em: <https://idec.org.br/dicas-e-direitos/venda-da-iris-do-olho-conheca-os-perigos-por-tras-dessa-pratica>. Acesso em: 14 mar. 2026.

LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e efetividade da Lei Geral de Proteção de Dados.** São Paulo: Almedina Brasil, 2020. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788584936397/>. Acesso em: 12 abr. 2026.

MENDES, Laura Schertel. **Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. Panorama Setorial da Internet, ano XI**, n. 2, jun. 2019. Disponível em: <https://www.cgi.br>. Acesso em: 01 abr. 2026.

RICARDO AYRES. **Projeto de Lei nº 36, de 2025**. Altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), para proibir a comercialização de dados biométricos sensíveis. Brasília, DF: Câmara dos Deputados, 2025.

WORLD COIN. **Expansão global do escaneamento de íris e distribuição de usuários da plataforma**. Disponível em: <https://worldcoin.org>. Acesso em: 20 abr. 2026.

ZULIANI, Ênio Santarelli. **Responsabilidade civil pelos vícios dos bens informáticos e pelo fato do produto**. In: SILVA, Regina Beatriz Tavares da; SANTOS, Manoel J. Pereira dos (Coords.). Responsabilidade civil na internet e nos demais meios de comunicação. São Paulo: Saraiva, 2012.

---

<sup>1</sup> Discente do Curso Superior de Direito do UNIFSA. E-mail: [acesse o artigo original para visualizar o e-mail](#). LATTES: <http://lattes.cnpq.br/1309316441330480>.

<sup>2</sup> Discente do Curso Superior de Direito do UNIFSA. E-mail: [acesse o artigo original para visualizar o e-mail](#). LATTES: <http://lattes.cnpq.br/5821624988050552>.

<sup>3</sup> Doutora em Ciências Criminais pela PUCRS. Mestre em Letras pela UFPI. Especialista em Literatura Brasileira UESPI. Graduada em Letras pela UFPI. Graduada em Direito pelo Instituto Camillo Filho. E-

mail: [acesse o artigo original para visualizar o e-mail](#). LATTES:  
<http://lattes.cnpq.br/8019442960641857>.