

150. A VENDA DA ÍRIS NO BRASIL: DIREITOS, RISCOS E IMPLICAÇÕES JURÍDICAS

Mayume Caires Moreira

Mestra, Unicesumar.
Maringá – Paraná – Brasil
mayume.caires@unicesumar.edu.br
<https://orcid.org/0000-0002-1333-1891>
<http://lattes.cnpq.br/7810923422029283>

Amanda Brasil da Silva

Graduanda, Unicesumar.
Maringá – Paraná - Brasil
ra-24001328-2@alunos.unicesumar.edu.br
<https://orcid.org/0009-0000-8343-1591>
<https://lattes.cnpq.br/4335562962560110>

Julia Freitas Volpato

Graduanda, Unicesumar.
Maringá – Paraná - Brasil
ra-24000236-2@alunos.unicesumar.edu.br
<https://orcid.org/0009-0009-0968-2232>
<https://lattes.cnpq.br/1828882081073334>

Maysa Piasentin

Graduanda, Unicesumar.
Maringá – Paraná - Brasil
ra-24183081-2@alunos.unicesumar.edu.br
<https://orcid.org/0009-0009-7764-2275>

RESUMO

Com o avanço da tecnologia, surgem também preocupações cada vez maiores como a invasão da privacidade. Em 2025, vivenciamos um cenário que antes parecia futurista: além do reconhecimento facial (Face ID), passou-se a adotar o cadastro da íris como forma de identificação. No entanto, essa prática não pode passar despercebida e deve ser minuciosamente analisada antes de se converter em resultados práticos. Esta pesquisa foi motivada pelo pouco destaque que foi dado a uma prática tão perigosa e até então desconhecida, como a venda da íris do olho. Dessa forma, este artigo tem como objetivo analisar os diversos aspectos envolvidos nessa nova fronteira entre tecnologia, identidade e economia, refletindo sobre as implicações do projeto Worldcoin e os desafios éticos e sociais que emergem em uma realidade onde até mesmo a íris pode se tornar um ativo negociável. A pesquisa foi desenvolvida a partir da análise de um caso prático, complementada por estudos e referências bibliográficas relevantes ao tema. Espera-se, com este trabalho, alertar a população sobre os riscos associados às novas tecnologias, a comercialização de dados pessoais e conscientizá-las sobre seus direitos.

PALAVRAS-CHAVE: Proteção de Dados. LGPD. Aspectos jurídicos.

ABSTRACT

With technological advancement, increasing concerns have emerged, such as the invasion of privacy. In 2025, we are experiencing a scenario that once seemed futuristic: in addition to facial recognition (Face ID), iris registration has begun to be used as a form of identification. However, this practice cannot go unnoticed and must be thoroughly analyzed before being implemented in practice. This research was motivated by the limited attention given to such a dangerous and previously unknown practice, namely the sale of the human iris. Thus, this article aims to analyze the various aspects involved in this new frontier between technology, identity, and economy, reflecting on the implications of the Worldcoin project and the ethical and social challenges that arise in a reality where even the iris can become a tradable asset. The research was developed through the analysis of a practical case, complemented by studies and bibliographic references relevant to the topic. This work seeks to raise public awareness about the risks associated with new technologies, the commercialization of personal data, and to inform individuals about their rights.

KEYWORDS: Data Protection. LGPD. Legal Aspects.

1 INTRODUÇÃO

No início deste ano, vídeos de filas extensas em São Paulo chamaram a atenção de milhões de usuários nas redes sociais. Nessas imagens, pessoas aguardam para realizar um procedimento até então inusitado: a coleta da íris ocular, e como pagamento, criptomoedas. A cena, que à primeira vista remete a um futurismo, faz parte de um projeto da Worldcoin, conduzido pela empresa Tools for Humanity. Utilizando um dispositivo chamado Orb, a proposta do projeto é criar um novo tipo de identidade digital baseado em biometria ocular, o que a empresa chamou de “prova de humanidade”. Segundo a Tools for Humanity (2025), o objetivo não é apenas verificar identidades, mas estabelecer um novo padrão de reconhecimento individual em um mundo cada vez mais dominado por inteligências artificiais e interações digitais automatizadas. A promessa é que a verificação biométrica, uma vez criptografada e fragmentada, será de posse exclusiva do usuário, garantindo anonimato e segurança, devido ao fato de que esse processo não pode ser replicado por robôs. Ainda assim, o projeto levanta questões éticas, sociais e jurídicas profundas: até que ponto é seguro e ético trocar dados biométricos por moedas digitais? Como garantir que essas informações não sejam utilizadas de forma indevida no futuro? E, principalmente, o que motiva tantas pessoas a cederem dados tão sensíveis em troca de R\$500? O avanço de iniciativas como essa expõe lacunas na legislação sobre proteção de dados e revela o quanto a população está disposta a negociar sua privacidade e seus direitos diante de promessas de benefícios financeiros imediatos. Esta discussão está inserida em um contexto maior de debates sobre privacidade de dados, vigilância digital, inclusão financeira e desigualdade social. Em países com altos índices de pobreza e exclusão digital, o apelo de recompensas monetárias pode ser mais forte do que as preocupações com a segurança de dados pessoais. Além disso, pode surgir o risco de naturalizar a troca de dados sensíveis por vantagens econômicas, sem que haja a devida compreensão sobre os impactos de longo prazo. O valor simbólico e prático atribuído aos dados biométricos passa a ser reconfigurado, fazendo com que o próprio conceito de identidade seja transformado. A Worldcoin pode representar o início de uma nova era digital, marcada pela interseção entre tecnologia, economia e identidade. No entanto, também serve como alerta para os limites da ética em tempos de inovação acelerada. É fundamental que o debate sobre o uso de dados biométricos seja acompanhado por políticas públicas eficazes, regulamentações claras e um esforço conjunto para garantir que os direitos fundamentais dos cidadãos sejam preservados. A tecnologia, por si só, não é

nem boa nem má — seu impacto depende de como é utilizada e de quem detém o controle sobre ela.

2 REFERENCIAL TEÓRICO

Primeiramente, Flávia Martins Bahia (2020), comenta a respeito do Princípio da Dignidade Humana como mola propulsora do respeito e da observância aos direitos fundamentais. Nessa perspectiva, a autora advoga que o Estado Democrático de Direito está afinado à ideia de que a essência mínima do ser humano precisa ser protegida contra agressões e arbitrariedades. Ao poder público, cabe a relevante missão de tentar conter as possibilidades de ofensa e, principalmente, as nocivas consequências decorrentes de violências à dignidade humana e à proteção aos direitos fundamentais bem como humanos (Bahia, 2020). Dentro do rol não taxativo dos direitos fundamentais, dois são pertinentes, quanto ao assunto proposto, o direito à privacidade e o direito à personalidade. O direito à privacidade, segundo Cleber Masson (2019), faz com que o titular tenha a prerrogativa de não expor suas particularidades, sem que haja critério e fundamento cuidadosamente estabelecidos para tanto. Posto isso, a privacidade, assim como qualquer outro direito fundamental, não escapa da participação do ente público, especialmente no que diz respeito à formulação de políticas públicas voltadas à proteção social e à prestação de serviços.

No que diz respeito à personalidade, embora não expressa explicitamente no Texto Constitucional, está contida em direitos como imagem e a honra, esses guardados pelo artigo 5^a da Constituição de 1988. Além disso, sem comprometer a interpretação jurídica, a personalidade também pode se conectar à privacidade. De forma clara e objetiva, destaca-se que a personalidade e a privacidade são temáticas centrais no que concerne aos debates e polêmicas envolvendo a íris ocular. Mesmo com a sensação de segurança trazida pelo avanço de tecnologias importantes, nascem, paralelamente, desafios relacionados à gestão desses dados a fim de que eles sejam utilizados para finalidades agregadoras, e não para a exposição desnecessária e criminosa daquele que confiou a sua particularidade e que não assistiu o cumprimento de uma eficaz tutela a respeito (Machado; Lima, 2021).

Na qualidade de dados sensíveis, é essencial analisar cuidadosamente o uso de informações biométricas, como a íris, tendo em vista os preceitos e regras dispostos na LGPD. Essa legislação visa dar um seguro regramento que reflita, portanto, estabilidade e pacificação social para que problemas causados pela falta de cuidado cibernético não

gerem indenizações civis altíssimas para o Estado ou, até mesmo, para empresas privadas. Ademais, em termos de fiscalização em novembro de 2024, a ANPD instaurou o processo de fiscalização n.º 00261.006742/2024-53 para apurar possíveis irregularidades no tratamento de dados biométricos sensíveis, especialmente diante do potencial impacto sobre os direitos fundamentais dos titulares. A legislação brasileira, por meio da Lei Geral de Proteção de Dados Pessoais (LGPD), classifica os dados biométricos – como íris, digitais, voz e padrões faciais – como dados pessoais sensíveis, exigindo um regime jurídico mais rigoroso e restritivo para o seu tratamento.

A Coordenação-Geral de Fiscalização da ANPD, Autoridade Nacional de Proteção de Dados, solicitou à empresa uma série de informações e documentos, como o registro das operações de tratamento de dados, o relatório de impacto à proteção de dados pessoais, além de esclarecimentos sobre: Embora a Tools For Humanity tenha enviado os documentos solicitados, o processo ainda está em análise. A investigação reforça o posicionamento da ANPD quanto à necessidade de que o uso de tecnologias biométricas no Brasil esteja sempre em consonância com os princípios da LGPD, especialmente os de necessidade, finalidade, adequação, segurança e responsabilização. Não se pretende, com esta fiscalização, impor que a íris não possa ser usada, mas sim, que esse ato deva ser cuidadosamente realizado e, para isto, a visualização e prática sobre o que diz a Lei n 13.709/2018, que é responsável, justamente, por regulamentar a proteção de dados, é essencial. O artigo 11 da LGPD, traz alguns pontos importantes:

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

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

- a) cumprimento de obrigação legal ou regulatória pelo controlador;
- b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis (...) (Brasil, 2018, grifo).

Observa-se portanto que, ao se equilibrar os interesses envolvidos, não há impedimento quanto ao uso de dados sensíveis, como é o caso da íris ocular. Entretanto, se isso ocorrer às avessas do esperado pela Lei, nasce um cenário de hipervulnerabilidade. Thiago Adriano Coleti (2022) declara que é essencial dar ao titular do dado total transparência e clareza sobre como as suas informações estão sendo administradas. Na

ausência ou fraqueza dessa “cultura”, o indivíduo vê-se diante de uma estrutura que ainda não pode ser apta a transmitir a responsabilidade e o fortalecimento almejados. Salienta-se que, em caso de vazamento de dados sensíveis, a responsabilidade civil é um modo de fazer com que o autor do dano experimentado pela vítima possa recompensá-la pela exposição indevida e por todas as consequências potencialmente esperadas.

Cumprе destacar que o Projeto de Lei 36/2025, caso seja aprovado, promete tornar Lei este conteúdo: “Altera Lei n 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados- LGPD), para proibir a oferta mediante pagamento de disponibilidade de dados biométricos sensíveis e estabelecer medidas mais rigorosas de proteção a esses dados” (Brasil, 2025). Embora a venda desses dados biométricos, mesmo com o início de uma fiscalização pareça uma prática inofensiva a priori, a verdade é que pode trazer consequências graves e irreversíveis.

Um dos principais riscos é a perda de controle de dados pessoais, podendo gerar, furto de identidade, uso indevido de dados, vazamento de informações pessoais, perda de privacidade e o acesso indesejado a contas e sistemas. Desse modo, ao fazer essa prática, pode estar se sujeitando a fatos imprevisíveis e prejudiciais. Incluindo a criação de perfis e logins específicos sobre você, operando suas escolhas e deliberações. Além disso, não saber como essas informações serão usadas e sem o seu controle, pode gerar angústia e incerteza sobre o futuro.

Outrossim, é como se o indivíduo estivesse vendendo uma parte essencial de sua identidade, sem saber o que pode acontecer ao fazer isto, e como pode ser usada. Ao vender dados biométricos como a íris do olho, você pode se submeter a falta de privacidade, afinal outras pessoas terão acesso a suas informações pessoais, podendo acessar contas ou não, sistemas, bancos e aplicativos, comprometendo sua segurança digital. Portanto, é essencial que as pessoas tenham consciência ao vender a íris do olho e o que esse fato pode causar, ao invés de fazer a venda, tomar medidas preventivas para proteção desses dados. Isso engloba, compreender os riscos associados ao vender a íris do olho é necessário que as pessoas sejam cuidadosas ao fornecer seus dados. Além disso, a ANPD alertou para diversos riscos identificados no uso de tecnologias biométricas, entre eles: Finalidades ocultas ou não informadas no momento da coleta dos dados; Consentimentos genéricos, sem destaque ou clareza quanto à finalidade; riscos discriminatórios derivados de vieses tecnológicos, que podem afetar grupos vulneráveis e vazamentos de dados, caso não haja proteção adequada dos sistemas.

3 METODOLOGIA

Utilizou-se o método de pesquisa hipotético-dedutivo que parte do problema que versa sobre a análise da temática acerca do exercício da venda da Íris de olho em troca de pagamento, seus excessos e os riscos oferecidos. Sendo que o método passou pela formulação de hipótese e por um processo de inferência dedutiva, o qual testa a predição da ocorrência de fenômenos abrangidos pela referida hipótese, mediante aplicação da técnica de pesquisa bibliográfica e documental, consistente na análise e na própria legislação pátria. Empregou-se a técnica de pesquisa bibliográfica. A hipótese foi explorada e testada por meio da análise crítica de documentos legais e doutrinários, bem como da observação de situações práticas relatadas em veículos de imprensa e estudos acadêmicos. Assim, foi possível identificar padrões de comportamento, lacunas legislativas e possíveis interpretações jurídicas acerca da questão.

O processo dedutivo permitiu avaliar se as inferências extraídas a partir do conteúdo normativo e doutrinário confirmar ou refutar a hipótese inicialmente formulada. A pesquisa utilizou técnicas de investigação bibliográfica e documental. A bibliografia consultada abrange obras de autores nacionais e estrangeiros que discutem a proteção de dados, a ética na biotecnologia, os limites da autonomia privada e o impacto da tecnologia sobre os direitos fundamentais. Além disso, a pesquisa documental englobou a análise de legislações vigentes, como a Constituição Federal de 1988, o Código Civil Brasileiro e, especialmente, a Lei nº 13.709/2018 — a Lei Geral de Proteção de Dados Pessoais (LGPD), que trata diretamente do tratamento e proteção de dados sensíveis, entre os quais se incluem os biométricos, como a íris.

A abordagem qualitativa da pesquisa permite a interpretação dos dados com base em critérios descritivos e analíticos, priorizando a compreensão do contexto em que o fenômeno ocorre, em detrimento de sua quantificação. Isso possibilitou uma análise crítica e aprofundada sobre as implicações jurídicas da comercialização voluntária da íris, atentando-se para os efeitos sobre o exercício da liberdade individual e a possível vulnerabilização de grupos sociais em situação de desigualdade.

A interdisciplinaridade também se faz presente na metodologia, tendo em vista que o fenômeno em análise não pode ser compreendido unicamente sob a ótica do Direito. Desse modo, a metodologia adotada oferece uma base sólida para o exame crítico e também reflexivo sobre os limites legais e morais da venda da íris no Brasil, contribuindo

para a construção de uma visão jurídica mais clara, humana e atualizada sobre o tema em questão.

4 RESULTADOS ALCANÇADOS OU ESPERADOS

A expectativa é que os resultados da pesquisa revelem preocupações relevantes no âmbito jurídico, ético e social. Do ponto de vista legal, a prática confronta-se com as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD), que classifica os dados biométricos como sensíveis, exigindo, portanto, consentimento livre, informado e inequívoco para o seu tratamento. No entanto, quando a coleta desses dados é condicionada a algum tipo de recompensa financeira, especialmente em contextos de desigualdade econômica, questiona-se a real liberdade desse consentimento. Em muitos casos, o consentimento fornecido pode ser mais fruto da necessidade imediata do indivíduo do que de uma escolha consciente e clara.

Sob a perspectiva ética, caminha para que se levante o debate sobre a exploração de populações vulneráveis em nome da inovação tecnológica. A promessa de ganho financeiro imediato pode mascarar os riscos a longo prazo relacionados à privacidade e à segurança dos dados coletados. Além disso, muitas vezes os participantes não têm total compreensão das implicações do uso de suas informações biométricas por terceiros, o que amplia ainda mais a assimetria na relação entre os titulares dos dados e as empresas coletoras. Essa assimetria é agravada pela falta de transparência nas práticas empresariais e pela linguagem técnica ou ambígua frequentemente utilizada nos termos de uso e políticas de privacidade.

Assim, o indivíduo, embora formalmente tenha aceitado os termos, muitas vezes não possui os meios adequados para entender o real alcance daquela autorização. Espera-se, portanto, que a pesquisa evidencie a urgência da implementação de regulamentações mais específicas e rigorosas que delimitam os limites do uso de dados biométricos, especialmente quando há contrapartida financeira envolvida. Tais regulamentações devem também prever mecanismos eficazes de fiscalização e sanção para coibir abusos, bem como medidas educativas que capacitem a população a fazer escolhas informadas.

Do mesmo modo, pretende-se destacar a importância de ampliar a conscientização pública sobre os riscos associados à comercialização de informações sensíveis, promovendo um debate mais informado e responsável. É fundamental envolver diferentes setores da sociedade nesse diálogo, incluindo instituições acadêmicas, órgãos reguladores,

empresas de tecnologia e organizações da sociedade civil. Conclui-se que a proteção da privacidade e dos direitos individuais deve ser uma prioridade inegociável diante dos avanços tecnológicos. A coleta e o tratamento de dados sensíveis não podem ocorrer à revelia dos princípios fundamentais que regem o Estado Democrático de Direito, sob pena de comprometer a dignidade da pessoa humana.

Assim, espera-se que os resultados desta pesquisa sirvam como subsídio para a formulação de políticas públicas e normativas que assegurem um equilíbrio entre inovação tecnológica e respeito aos direitos fundamentais, reafirmando o compromisso com uma sociedade mais justa, ética e informada.

REFERÊNCIAS

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 7 abr. 2025.

BRASIL. Lei Geral de Proteção de Dados (LGPD), de 14 de agosto de 2018, disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. Lei nº 12.965, Marco Civil da Internet, de 23 de abril de 2014, disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

SIL. (1990). Lei nº 8.069, Estatuto da Criança e do Adolescente, de 13 de julho de 1990, disponível em: https://www.planalto.gov.br/ccivil_03/leis/L8069.htm.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. Revista Brasileira de Direito Civil– RBDCivil, Belo Horizonte, v. 25, p.93, jul./set. 2020. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/521> . Acesso em: 20 abr.2025.

UNICEF (Fundo das Nações Unidas para a Infância). Estado Mundial da Infância 2017: Crianças em um mundo digital. Nova Iorque: UNICEF, 2017. Disponível em: <https://www.unicef.org/brazil/relatorios/estado-mundial-da-infancia-2017>. Acesso em: 21 abr. 2025.

HAUGEN, Frances. Audiência no Senado dos EUA: Testemunho sobre práticas do Facebook, 2021. Disponível em: <https://www.commerce.senate.gov>. Acesso em: 21 abr. 2025.

SAFERNET BRASIL. Relatório anual 2023: denúncias anônimas recebidas e encaminhadas. SaferNet, 2024. Disponível em: <https://new.safernet.org.br/content/relatorio-2023>. Acesso em: 21 abr. 2025.

MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS (MMFDH). Relatório de denúncias de pornografia infantil na internet. Brasília: MMFDH, 2022. Disponível em: <https://www.gov.br/mdh>. Acesso em: 21 abr. 2025.

MINISTÉRIO PÚBLICO FEDERAL (MPF). Relatório sobre grupos de exploração sexual infantil no Telegram: denúncia da SaferNet Brasil. Brasília: MPF, 2023. Disponível em: <https://www.mpf.mp.br>. Acesso em: 21 abr. 2025.